UNIVERSITY OF SOUTHAMPTON

Faculty of Engineering and Physical Science
School of Electronics and Computer Science
Next Generation Wireless Communication Research Group

Continuous-Variable Quantum Key Distribution Systems

by

Xin LIU

BEng, MEng

A thesis for the degree of Doctor of Philosophy

Supervisors:

Prof. Lajos Hanzo
FREng, FIEEE, FIET, DSc
Chair of Next Generation Wireless Research Group
and
Prof. Soon Xin Ng
PhD, BEng, CEng, FIET, SMIEEE, FHEA
and
Dr. Chao Xu
SMIEEE

January 2025

Dedicated to my beloved parents.

University of Southampton

Abstract

Faculty of Engineering and Physical Science
School of Electronics and Computer Science

Doctor of Philosophy

Continuous-Variable Quantum Key Distribution Systems

by Xin LIU

Quantum Key Distribution (QKD) is capable of supporting ultimate information security. QKD systems can be categorized into two types, namely Discrete Variable QKD (DV-QKD) and Continuous Variable QKD (CV-QKD) systems, but the detectors of CV-QKD exhibit more convenient compatibility with the operational network infrastructure. As a further benefit, CV-QKD is capable of providing a higher key rate than its DV-QKD counterpart, since the associated homodyne or heterodyne detection offers the prospect of high detection efficiency. Therefore, we mainly focus on studying CV-QKD systems.

We commence by a brief review of the associated classical post-processing, with an emphasis on Forward Error Correction (FEC)-coded reconciliation schemes. A comprehensive parametric study of Low-Density Parity-Check (LDPC)-coded reconciliation schemes is provided and it is demonstrated that as expected, a longer LDPC code has a better Block Error Rate (BLER) performance and higher reconciliation efficiency, thus offering higher Secret Key Rate (SKR) and longer secure transmission distance. Then the state-of-the-art in both Single-Input Single-Output (SISO) and Multiple-Input Multiple-Output (MIMO) Terahertz (THz) CV-QKD systems is reviewed with an emphasis on the associated quantum transmission part, since the THz band is more tolerant to both weather conditions and atmospheric turbulences than Free Space Optical (FSO) CV-QKD. The SKR versus distance performance reveals that both the thermal noise level, the absorption coefficient and the path loss associated with different frequency bands make a significant difference.

In Chapter 3, new near-capacity CV-QKD reconciliation schemes are proposed, where the Authenticated Classical Channel (ClC) and the Quantum Channel (QuC) are protected by separate FEC coding schemes. More explicitly, all of the syndrome-based QKD reconciliation schemes found in literature rely on syndrome-based codes, such as LDPC codes. Hence at the current state-of-the-art the channel codes that cannot use syndrome decoding such as for example the family of Convolutional Codes (CCs) and polar codes cannot be directly applied. Moreover, the ClC used for syndrome

transmission in these schemes is typically assumed to be error-free in the literature. To circumvent this limitation, a new codeword-based - rather than syndrome-based - QKD reconciliation scheme is proposed, where Alice sends an FEC-protected codeword to Bob through a ClC, while Bob sends a separate FEC protected codeword to Alice through a QuC. Upon decoding the codeword received from the other side, the final key is obtained by applying a simple modulo-2 operation to the local codeword and the decoded remote codeword. As a result, *first of all*, the proposed codeword-based QKD reconciliation system ensures protection of both the QuC and of the ClC. *Secondly*, the proposed system has a similar complexity at both sides, where both Alice and Bob have an FEC encoder and an FEC decoder. *Thirdly*, the proposed system makes QKD reconciliation compatible with a wide range of FEC schemes, including polar codes, CCs and Irregular Convolutional Codes (IRCCs), where a near-capacity performance can be achieved for both the QuC and for the ClC. Our simulation results demonstrate that thanks to the proposed regime, the performance improvements of the QuC and of the ClC benefit each other, hence leading to an improved SKR that inches closer to both the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound and to the maximum achievable rate bound.

In Chapter 4, the feasibility of CV-QKD is considered in the THz band, experiencing time-varying and frequency-selective fading. Advanced multi-carrier modulation is required for improving the SKR. However, the hostile quantum channel requires powerful classical channel coding schemes for maintaining an adequate reconciliation performance. Against this background, for the first time in the open literature, we propose a multi-carrier quantum transmission regime that incorporates both Orthogonal Frequency Dividion Multiplexing (OFDM) and Orthogonal Time Frequency Space (OTFS) transmission over doubly-selective fading THz channels. Furthermore, we propose a modified Multi-Dimensional Reconciliation (MDR) algorithm for CV-QKD, facilitating the integration of OFDM/ OTFS quantum transmission with LDPC coded key reconciliation. Moreover, we harness Analog Beamforming (ABF) for mitigating the severe THz path loss. Our SKR analysis results demonstrate that the proposed OTFS-based and LDPC-assisted CV-QKD system is capable of outperforming its OFDM counterpart in mobile wireless scenarios. Moreover, we also characterize how improving the MIMO dimension increases the beamforming gain and hence reduces the transmission power required for achieving the secure transmission distance target.

Finally, in Chapter 5, the ABF-assisted MIMO OFDM/ OTFS CV-QKD system proposed in Chapter 4 is further developed by harnessing Hybrid Beamforming (HBF). This requires that the full Channel State Information (CSI) is available at both the transmitter (CSI-T) and receiver (CSI-R). In order to fulfil this pre-condition in the face of time-varying frequency-selective THz scenarios, a variety of channel estimation methods are conceived for MIMO OFDM/ OTFS systems. SKR analysis results reveal that

the HBF MIMO OTFS-based and LDPC-assisted CV-QKD system designed offers higher SKR and longer secure transmission distance than its OFDM-based counterpart. Furthermore, the HBF MIMO OTFS-based system relying on realistic estimated CSI performs similarly to that having perfect CSI in both stationary and mobile scenarios. By contrast, the HBF MIMO OFDM-based system associated with estimated CSI fails to achieve an adequate SKR and secure distance for CV-QKD in mobile scenarios due to its excessive BLER.

Declaration of Authorship

I declare that this thesis and the work presented in it is my own and has been generated by me as the result of my own original research.

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
3. Where I have consulted the published work of others, this is always clearly attributed;
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
5. I have acknowledged all main sources of help;
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
7. Parts of this work have been published in the provided List of Publications.

Signed:..... Date:.....

Acknowledgements

First of all, I am deeply indebted to my supervisors Professor Lajos Hanzo, Professor Soon Xin Ng (Michael) and Dr. Chao Xu for their outstanding and expert guidances, wise advices, patience and generous support throughout my PhD journey. Their wisdom and aspiration helped me grow both as a researcher and more importantly as a person.

I would also like to thank all the other colleagues and the staff in the Next Generation Wireless Research Group for their help and support. Special thanks to my colleagues Dr. Daryus Chandra, Dr. Dong Pan, Dr. Yifeng Xiong, Dr. Zeynep Kaykac Egilmez, Dr. Jue Chen, Dr. Qingchao Li, Dr. Xinyu Feng, Dr. Qiling Gao and Mr. Dingzhao Wang for their kindly help and valuable encouragement.

I appreciate the financial support provided by the Southampton – China Scholarship Council (CSC) joint scholarship, which offered me the opportunity to embark on an unforgettable journey at the University of Southampton. Additionally, I gratefully acknowledge the use of the IRIDIS High-Performance Computing Facility and the associated support services at the University of Southampton in the completion of this work.

Finally, I would like to express my heartfelt thanks to my parents, Mr. Aiming Liu and Ms. Youqing Zhang, for their endless love and unwavering support.

List of Publications

Journals:

[1] **X. Liu**, C. Xu, Y. Noori, S. X. Ng and L. Hanzo, "The Road to Near-Capacity CV-QKD Reconciliation: An FEC-Agnostic Design", *IEEE Open Journal of the Communications*, vol. 5, pp. 2089-2112, 2024.

[2] **X. Liu**, C. Xu, S. X. Ng and L. Hanzo, "OTFS-Based CV-QKD Systems for Doubly Selective THz Channels", *IEEE Transactions on Communications*, *accepted*, 2025.

[3] **X. Liu**, C. Xu, S. X. Ng and L. Hanzo, "Hybrid Beamforming Assisted OTFS-Based CV-QKD Systems for Doubly Selective THz Channels", *IEEE Transactions on Communications, under review*.

[4] **X. Liu**, C. Xu, S. X. Ng and L. Hanzo, "Channel Estimation for OTFS-Based CV-QKD in the THz Band", *IEEE Transactions on Vehicular Technology, under review*.

[5] D. Wang, **X. Liu**, C. Xu, S. X. Ng and L. Hanzo, "Reverse-Reconciliation Outperforms Direct-Reconciliation in Polar- and LDPC-Coded CV-QKD", *IEEE Open Journal of Vehicular Technology, under review*.

Contents

List of Acronyms

3GPP	Third Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
6G	Sixth Generation
ABF	Analog Beamforming
ACS	Add Compare Select
AES	Adcanced Encryption Standard
AL	Atmospheric Loss
AoA	Angle of Arrival
AoD	Angle of Departure
ARQ	Automatic Repeat Request
AWGN	Additive White Gaussian Noise
B92	Bennett-92
BB84	Bennett-Brassard-1984
BBM92	Bennett-Brassard-Mermin-1992
BCH	Bose-Chaudhuri-Hocquenghem
BER	Bit Error Rate
BF	Bit-Flipping
BI-AWGN	Binary Input Additive White Gaussian Noise
BLER	Block Error Rate
BP	Belief Propagation
BPSK	Binary Phase-Shift Keying
BR	Blind Reconciliation
BS	Base Station
BSC	Binary Symmetry Channel
CC	Convolutional Code

CCB Chase Combining
CIR Channel Impulse Response
CK Classical Key
ClC Authenticated Classical Channel
CM Covariance Matrix
CN Check Node
CP Cyclic Prefix
CSI Channel State Information
CSI-R CSI at Receiver
CSI-T CSI at Transmitter
CV-QKD Continuous Variable QKD

D2D Device-to-Device
DD Delay-Doppler
DES Data Encryption Standard
DFT Discrete Fourier Transform
DH Diffie-Hellman
DR Direct Reconciliation
DV-QKD Discrete Variable QKD

E91 Ekert-91
ECDH Elliptic-Curve Diffie-Hellman
ECDSA Elliptic Curve Digital Signatur Algorithm
EPR Einsten-Podolsky-Rosen
EXIT Extrinsic Information Transfer

FD Frequency Domain
FDE FD Equalization
FEC Forward Error Correction
FSO Free Space Optical
FSPL Free-Space Path Loss

GG02 Grosshans-Grangier-2002

HARQ Hybrid ARQ
HBF Hybrid Beamforming

ICI Inter-Carrier Interference

IDFT Inverse Discrete Fourier Transform
IRCC Irregular Convolutional Code
ISFFT Inverse SFFT
ITSL InTer-SateLlite
ITU International Telecommunication Union

LDPC Low-Density Parity-Check
LG09 Leverrier-Grangier-2009
LLR Log-Likelihood Ratio
LoS Line of Sight

MDR Multi-Dimensional Reconciliation
MI Mutual Information
MIMO Multiple-Input Multiple-Output
MMSE Minimum Mean-Squared Error

NG Next-Generation
NLoS Non-Line of Sight

OFDM Orthogonal Frequency Dividion Multiplexing
OTFS Orthogonal Time Frequency Space
OTP One-Time Pad

PCM Parity-Check Matrix
PLOB Pirandola-Laurenza-Ottaviani-Banchi
PM Phase-Matching

QK Quantum Key
QKD Quantum Key Distribution
QRNG Quantum Random Number Generator
QuC Quantum Channel

RA Receive Antenna
RC Receive Combiner
RIS Reconfigurable Intelligent Surfaces
RR Reverse Reconciliation
RSA Rivest-Shamir-Adleman

SAGINs Space-Air-Ground Integrated Networks
SARG04 Scarani-Acién-Ribordy-Gisin-2004
SCS Subcarrier Spacing
SFFT Symplectic Finite Fourier Transform
SHA Secure Harsh Algorithm
SISO Single-Input Single-Output
SKR Secret Key Rate
SNR Signal-to-Noise Ratio
SNU Shot-Noise Units
SPA Sum-Product Algorithm
SVD Sigular Value Decomposition

TA Transmit Antenna
TD Time Domain
TDL Time Delay Line
TF Time-Frequency
THz Terahertz
TPC Transmit Precoder
TWF Twin-Field

ULA Uniform Linear Array
URC Unitary Rate Code

VN Variable Node

WF Water Filling

List of Symbols

General Conventions

- Bold uppercase $\mathbf{A}$ and lowercase $\mathbf{a}$ represent matrices and vectors, respectively.
- $\mathbf{A}[m,:]$ and $\mathbf{A}[:,n]$ represent the mth row and the nth column of a matrix $\mathbf{A}$, respectively.
- $\mathbf{A}[m,n]$ represents the element at the mth row and nth column of a matrix $\mathbf{A}$.
- $\mathbf{a}[m]$ represents the mth element of a vector $\mathbf{a}$.

Mathematical Operations and Functions

$(\cdot)^*$: The conjugate of a complex scalar/vector/matrix.

$(\cdot)^{-1}$: The inverse of a matrix.

$(\cdot)^T$: The transpose of a matrix.

$(\cdot)^H$: The Hermitian transpose of a matrix.

$\|\cdot\|$: The Euclidean norm of a vector/matrix.

$\mathfrak{Re}(\cdot)$: The real part of a complex value.

$\mathfrak{Im}(\cdot)$: The imaginary part of a complex value.

$\text{diag}(\mathbf{a})$: A square diagonal matrix formed by vector $\mathbf{a}$.

$\text{rem}(a,b)$: The remainder after division of a by b.

$\mathbb{E}(\cdot)$: The expectation of random variables.

$\min(\cdot)$: The minimum value among a number of variables.

$\log(\cdot)$: Logarithm to base 2.

$\ln(\cdot)$: Logarithm to base the mathematical constant e.

$\text{sign}(\cdot)$: Return the value -1, +1 or 0 according to whether the sign of a given real number is positive or negative, or the given number is itself zero.

$\lfloor \cdot \rfloor$: Rounding a numerical value to its nearest lower integer.

$\lceil \cdot \rceil$: Rounding a numerical value to its nearest higher integer.

$\sum$: The summation of all elements.

$\forall$: For all elements within a certain range.

Special Symbols

$\hat{a}_{\text{in},1}, \hat{a}_{\text{in},2}$: The two input modes for a beam splitter.

$\hat{a}_{\text{out},1}, \hat{a}_{\text{out},2}$: The two output modes for a beam splitter.

$\hat{a}_A, \hat{a}_B, \hat{a}_E$: The transmitted mode of Alice, the received mode of Bob, and the injected Gaussian mode of Eve.

$\mathbf{a}_{Tx}(\theta_{Tx,p}), \mathbf{a}_{Rx}(\theta_{Rx,p})$: The antennas response vectors.

$\mathbf{A}_{Tx}$, $\mathbf{A}_{Rx}$: The antenna responses in matrix form.

$\mathbf{b}, \widetilde{\mathbf{b}}$: The random binary key and its channel-contaminated version.

$\hat{\mathbf{b}}, \widehat{\widetilde{\mathbf{b}}}$: The final reconciled keys are relative to $\mathbf{b}$ and $\widetilde{\mathbf{b}}$, respectively.

$\mathbf{c}, \tilde{\mathbf{c}}, \hat{\mathbf{c}}$: The legitimate codeword of FEC codes, and its contaminated version after transmission through channels and its corresponding decoded codeword.

C: Shannon capacity.

$C_v \backslash c$: All the CNs connected to VN v, except for CN c.

C^{DCMC}: Capacity of Discrete-Input Continuous-Output Memoryless Channel

$\mathcal{C}(N_{\text{FEC}}, K_{\text{info}})$: The classical ensemble of Hamming code with K_{info} information bits and N_{FEC} coded bits.

$C_{LDPC}, \overline{C}_{LDPC}$: The overall complexity of LDPC decoding and the complexity of LDPC code per bit per iteration.

$\mathbf{C}, \widetilde{\mathbf{C}}, \widehat{\mathbf{C}}$: The unnecessarily legitimate codeword of FEC, and its channel-contaminated version and its corresponding decoded version.

$\mathbf{C}_A, \mathbf{C}_B$: The unnecessarily legitimate codeword of FEC at Alice and Bob.

d_c, d_v: The degree of CNs and the degree of VNs.

D: The dimensionality used in MDR.

$\mathbf{e}, \mathbf{e}_A, \mathbf{e}_B$: The error pattern, the error pattern of Alice and the error pattern of Bob.

$\hat{E}, \hat{E}'', \hat{E}'$: The modes of EPR states and the mode of EPR states after beam splitter.

f_c: The carrier frequency.

f_D: The Doppler frequency.

$\mathbf{F}_M$, : DFT matrix

G_a, G_T, G_R: The gain of each antenna element, and the transmitter and receiver antenna gains, respectively.

$\mathbf{G}$: The generator matrix.

$\overline{\mathbf{G}}_n^{\varrho}, \widetilde{\mathbf{G}}^{\varrho}$: The MMSE matrix in FD of OFDM and DD domain of OTFS in the ϱth block.

$\hbar$: Planck's constant.

h: The channel's coefficient.

$\widetilde{h}_p$: The fading gain.

$\widehat{\widetilde{h}}_p$: The estimated channel gain.

$h_{n,m,l}, \overline{h}_{n,\overline{m}}, \widetilde{h}_p \omega_{MN}^{k_p(nM+m-l_p)}$: The fading channel coefficients in TD, FD, and DD domain, respectively.

$h_{n,m,l}^{RF}$: The ABFed fading channel.

$h_{l,v,u}, \widetilde{h}_{p,v,u}$: The lth CIR tap in TD, and channel gain for pth path

$\widehat{h}_{l,v,u}, \widehat{\widetilde{h}}_{p,v,u}$: Estimated lth CIR tap in TD, and estimated channel gain for pth path.

$\mathbf{H}^{\text{PCM}}$: The parity-check matrix.

$\mathbf{H}_{n,m,l}$: The MIMO channel matrix of the lth TDL tap for the symbol of the mth subcarrier of the nth OFDM/OTFS.

$\mathbf{H}_{n,m,l}^{RF}$: The ABFed fading channel.

$\mathbf{H}_n^{RF}, \overline{\mathbf{H}}_n^{RF}, \widetilde{\mathbf{H}}^{RF}$: The nth OFDM ABFed channel matrix in TD and FD, and the OTFS beamformed channel matrix in DD domain.

$\mathbf{H}_n, \overline{\mathbf{H}}_n, \widetilde{\mathbf{H}}$: The nth OFDM channel matrix in TD and FD, and the OTFS channel matrix in DD domain.

$\overline{\mathbf{H}}_n^{\varrho}, \widetilde{\mathbf{H}}^{\varrho}$: The channel matrix in FD of OFDM and DD domain of OTFS in the ϱth block.

$\mathbf{H}^{CE_{v,u}}$, $\widetilde{\mathbf{H}}^{CE_{v,u}}$: Channel estimation matrices in FD and DD domain for the uth antenna of transmitter and the vth antenna of the receiver.

I_t, $I_{\max}$: The iterations number, and the maximum number of iteration for LDPC decoding.

$I_{A,B}$: The mutual information between Alice and Bob.

k_B: Boltzmann's constant.

$\widehat{k}_p$: Estimated Doppler index.

$\mathbf{k}$: The vector of information bits of FEC codes.

K: Ricean factor.

K_{info}: The number of information bits for LDPC codes.

K_{idea}: The SKR in ideal case where the post-processing is perfectly conducted.

$K_{\text{practical}}$: The SKR in realistic case where the imperfection reconciliation scheme is considered.

K_{finite}: The SKR in realistic case where both the imperfection reconciliation scheme and finite-size effect are considered.

$\widehat{l}_p$: Estimated Delay index.

L: The maximum TDL tap in OFDM and OTFS systems.

$\mathfrak{L}$: The distance between the two parties.

$L^0_{v\to c}$: The initialized received LLR from all VN-to-CN messages arriving from VN v to CN c.

$L^t_{c\to v}$, $L^t_{v\to c}$: The message arriving from CN to VN in iteration t and the message coming from VN to CN in iteration t.

L^{total}_v: The total LLR for VN v.

M: The number of subcarriers of OFDM and OTFS.

M_{cp}: The length of the CP.

$\mathbf{M}(\mathbf{y}', \mathbf{u})$: The mapping function sent from Bob to Alice.

$\mathbf{M}(\ddot{\mathbf{s}}'_i, \mathbf{u}^B_i)$, $\mathbf{M}(\ddot{\mathbf{z}}'_i, \mathbf{u}^B_i)$: Mapping functions between $\ddot{\mathbf{s}}'_i$ and $\mathbf{u}^B_i$, and between $\ddot{\mathbf{z}}'_i$ and $\mathbf{u}^B_i$.

$\bar{n}$: The average number of photons.

N: The number of symbols of OFDM and OTFS.

N_s: The number of data stream.

N_0: The noise variance of AWGN.

N_0^{Rx}: The equivalent noise variance of AWGN at receivers.

N_{Tx}, N_{Rx}: The number of transmit and receive antennas.

N_{bl}, N_{sb}: The number of block and sub-block of OFDM/OTFS.

N_{FEC}: Code length.

p_A, p_B: Quadrature components of Gaussian variables of Alice and Bob.

P: The number of paths in OFDM and OTFS systems.

P_l: All the paths falling into the lth TDL.

P_B: The BLER in the reconciliation.

q_A, q_B: In-phase component of Gaussian variables of Alice and Bob.

R: Coding rate.

R^{eff}: The effective transmission rate.

$\bar{\mathbf{r}}_n$, $\widetilde{\mathbf{r}}$: Received signals after digital combining.

$s_{n,m}$, $\bar{s}_{n,\overline{m}}$, $\widetilde{s}_{k,l}$: The modulated symbols in TD, FD, and DD domain, respectively.

$s_{En,m}$: The AWGN introduced by Eve in TD.

$s_{0,n,m}$, $\bar{s}_{0,n,m}$,$\widetilde{s}_{0,k,l}$: The preparation noise symbols in TD, FD, and DD domain of OTFS.

S: The variance of the trusted detector's noise.

SNR^C: The SNR for ClC.

SNR^{Rx}: The SNR after channel equalization by the receivers.

$\mathbf{s}, \mathbf{s}_A, \mathbf{s}_B$: The syndrome side information, the syndrome vector of Alice, and the syndrome vector of Bob.

$\mathbf{s}_n$, $\bar{\mathbf{s}}_n$,$\widetilde{\mathbf{s}}$: The nth OFDM symbols in TD and FD, and the OTFS symbols in DD domain in vector form.

$\mathbf{s_0}_n$, $\mathbf{s_E}_n$: The vector form of $s_{0n,m}$ and $s_{En,m}$.

$\ddot{\mathbf{s}}, \ddot{\mathbf{s}}'$: Input variables for the MDR process and their normalized version at Alice's side.

$\bar{\mathbf{s}}_i^{\text{MDR}}, \widetilde{\mathbf{s}}_i^{\text{MDR}}$: The ith MDR segment of the transmitted symbols in FD of OFDM and DD domain of OTFS, respectively.

$\mathbf{s}^{CE_{v,u}}$, $\widetilde{\mathbf{s}}^{CE_{v,u}}$: Pilot symbols in FD and DD domain.

T: The channel transmissivity.

T_e: The environmental temperature in Kelvin.

$T_{\text{FSPL}}, T_{\text{AL}}, T_{\text{ITSL}}$: The FSPL transmissivity, the AL transmissivity, and The ITSL transmissivity.

$\mathbf{u}^A$: The contaminated version of $\mathbf{u}^B$.

$\mathbf{u}^B$: Modulated version of $\mathbf{b}$.

$\mathbf{u}_i^B$: The 8-dimensional unit-radius sphere for the ith segment in the MDR process.

$\overline{\mathbf{U}}_n^{RF}$, $\overline{\mathbf{V}}_n^{RF}$, $\widetilde{\mathbf{U}}^{RF}$, $\widetilde{\mathbf{V}}^{RF}$: Unitary matrices of SVD of $\overline{\mathbf{H}}_n^{RF}$ and of $\widetilde{\mathbf{H}}^{RF}$.

v: Speed.

v_{el}: the electronic noise.

$v_{n,m}$, $\overline{v}_{n,\overline{m}}$, $\widetilde{v}_{k,l}$: The noise symbols in TD, FD, and DD domain, respectively.

Vs: the variance of Gaussian signals transmitted over QuC.

$V_c \backslash v$: the set of VNs connected to CN c, except for VN v.

V_A, V_B, V_0: The variance of the initial Gaussian signal, the variance of Bob's received signal, and the variance of the thermal state.

$\mathbf{v}^{CE_{v,u}}$, $\widetilde{\mathbf{v}}^{CE_{v,u}}$: Noise in FD and DD domain in CE model.

$\mathbf{V}_{AB}$: The CM related to the information between Alice and Bob.

W: The variance of Eve.

$\mathbf{w}^{Tx,RF}, \mathbf{w}^{Rx,RF}$: ABF matrices.

$\mathbf{W}^{Tx,RF}, \mathbf{W}^{Rx,RF}$: HBF matrices.

$\overline{\mathbf{W}}_{\text{WF},n}^{Tx,BB}$, $\widetilde{\mathbf{W}}_{\text{WF}}^{Tx,BB}$: Digital precoding matrices.

$\hat{X}_A, \hat{X}_B, \hat{X}_E$: the quadrature component transmitted by Alice, the quadrature component transmitted by Bob, and the excess noise quadrature component introduced by Eve.

$\mathbf{x}_i, \mathbf{x}_i'$: The ith segment of the rest of raw data of Alice and its normalized version.

$\mathbf{x}, \mathbf{x}'$: The rest of raw data of Alice, and its normalized version.

$\overline{\mathbf{x}}_n$, $\widetilde{\mathbf{x}}$: Data-carrying symbols before digital precoding.

$y_{n,m}$, $\overline{y}_{n,\overline{m}}$, $\widetilde{y}_{k,l}$: The received symbols in TD, FD, and DD domain, respectively.

$\mathbf{y}, \mathbf{y}'$: The rest of raw data of Bob and its normalized version.

$\mathbf{y}_i, \mathbf{y}'_i$: The ith segment of the rest of raw data of Bob, and its normalized version.

$\mathbf{y}^{CE_{v,u}}$, $\widetilde{\mathbf{y}}^{CE_{v,u}}$: Received contaminated pilot symbols in FD and DD domain.

$\overline{z}_{n,\overline{m}}$: The equalized symbols in FD.

$\overline{\mathbf{z}}_n$, $\widetilde{\mathbf{z}}$: Equalized date stream in FD and DD.

$\overline{\mathbf{z}}$, $\widetilde{\mathbf{z}}$: Decision variables after equalization in the FD of OFDM and DD domain of OTFS, respectively.

$\ddot{\mathbf{z}}, \ddot{\mathbf{z}}'$: Input variables for the MDR process and their normalized version at Bob's sides.

$\bar{\mathbf{z}}_i^{\mathrm{MDR}}, \widetilde{\mathbf{z}}_i^{\mathrm{MDR}}$: The ith MDR segment of the equalized symbols in FD of OFDM and DD domain of OTFS, respectively.

α: Atmospheric loss.

α_{fibre}: The attenuation of a single-mode optical fibre.

α_i^d: The coordinate element of the vector $\boldsymbol{\alpha}_i^{\boldsymbol{d}}$.

$\boldsymbol{\alpha}_i^{\boldsymbol{d}}$: The coordinate of the vector $\mathbf{u}_i$ under the orthonormal basis $\left(\mathbf{A}_8^1\mathbf{y}'_i, \mathbf{A}_8^2\mathbf{y}'_i, ..., \mathbf{A}_8^8\mathbf{y}'_i\right)$.

β: the reconciliation efficiency.

χ_{BE}: the Holevo information between Bob and Eve.

Δf: Subcarrier spacing.

η: the homodyne detector efficiency.

λ: The wavelength of the propagation wave.

$|\psi\rangle$: Coherent states.

$\overline{\mathbf{\Sigma}}_n^{RF}$, $\widetilde{\mathbf{\Sigma}}^{RF}$: The singular value matrices of $\overline{\mathbf{H}}_n^{RF}$ and $\widetilde{\mathbf{H}}^{RF}$.

τ_{max}: Maximum delay.

$\theta_{Tx,p}, \theta_{Rx,p}$: The AoD and AoD of the pth path.

$\widehat{\theta}_{Rx,p}$, $\widehat{\theta}_{Tx,p}$: Estimated AoA and AoD.

$\varsigma_{n,r_n^{FD}}$, $\vartheta_{r^{DD}}$: The non-zero singular value of $\overline{\mathbf{H}}_n^{RF}$ and $\widetilde{\mathbf{H}}^{RF}$.

ξ_{ch}: The excess noise from Eve.

ξ_{total}: The total amount of noise between Alice and Bob.

ξ_{det}: The homodyne detector's noise.

ξ_{line} : The channel noise from the sender Alice.

Chapter 1

Introduction

1.1 Motivation

Given the increasing penetration of commercial Fifth Generation (5G) services, since 2020s researchers have embarked on the exploration of Next-Generation (NG) wireless systems [1]. According to the schedule of the Third Generation Partnership Project (3GPP), the standardizing Sixth Generation (6G) technology will start in the second half of 2025 [2], and the technology is expected to be commercialized globally around 2030. In this context, quantum science has the promise of supporting a range of appealing application scenarios [3–6]. More explicitly, on one hand, quantum computing provides revolutionary acceleration in the information processing speed, which is envisioned to substantially improve the computing efficiency of NG applications [7].

However, the commercialization of quantum computing may also impose a threat to the conventional cryptosystems [8–16], shown in Fig. 1.1(a). The classical cryptosystem mainly exploit the computational complexity of certain mathematical problems to ensure its security. Explicitly, the two communication parties, Alice and Bob exchange their message after encryption and decryption of the plaintext with the aid of keys shared between them through the insecure public channel [17]. Generally, the secret keys of Alice and Bob are specifically designed based on some cryptographic algorithms. To elaborate further, the conventional cryptography encompasses three categories, which are symmetric cryptography, asymmetric cryptography, and Secure Harsh Algorithm (SHA). Symmetric cryptography includes the Data Encryption Standard (DES) [9] and the Adcanced Encryption Standard (AES) [10], where a single public key is used for both the encryption and decryption process. By contrast, the asymmetric cryptography algorithms have both a public and a private key, which are used for encryption and decryption respectively. This family includes the Rivest-Shamir-Adleman (RSA) [11], Diffie-Hellman (DH) [12], Elliptic Curve Digital Signatur Algorithm (ECDSA), and the Elliptic-Curve Diffie-Hellman (ECDH) [13, 14]

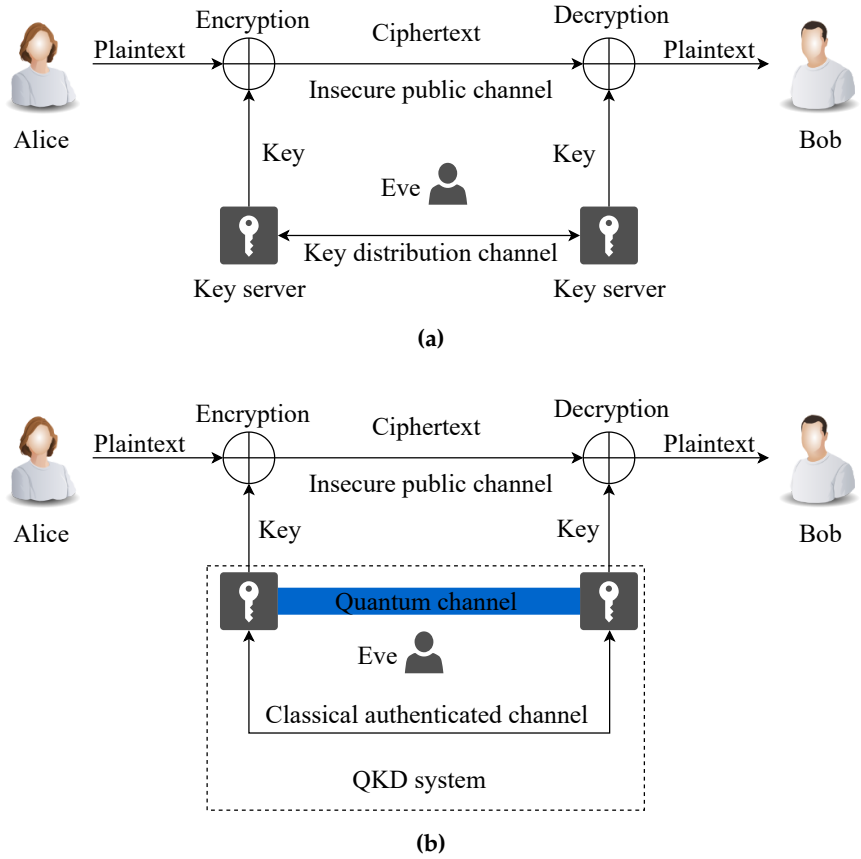


Figure 1.1: Schematics of different secure communication systems [17, 21]: a) **classical cryptosystem**, b) **QKD-based cryptosystem**.

techniques, all of which are based on high-complexity mathematical problems such as the factorization of large prime numbers, discrete logarithm and Elliptic curves, respectively. Finally, the SHA-2 and SHA-3 systems [15] have the advantage of providing a mechanism to ensure the integrity of a file [16]. These classical cryptography algorithms can provide *computational security*, which is practically unbreakable within a relatively short period of time when using state-of-the-art computational sources. However, conventional cryptography may be endangered by the progress in advanced quantum computing techniques. More explicitly, Shor's powerful algorithm is capable of efficiently factorizing large prime numbers and of solving elliptic curve problems. Hence it may impose a serious threat on classic asymmetric cryptography [18]. Similarly, Grover's search algorithm will make symmetric cryptography insecure [19, 20]. Hence, a quantum-safe cryptosystem is needed to tackle this threat.

Against this backdrop, Quantum Key Distribution (QKD) as one of the promising technologies can play an important role in providing sufficiently secure and reliable data transmission for NG communication systems [1, 21–27]. More explicitly, as shown in Fig. 1.1(b), a QKD scheme instructs both the transmitter (Alice) and the receiver (Bob) to encrypt their confidential messages with the aid of a so-called reconciled key agreed by them. A common secret key can be generated over the insecure quantum

channel, with some aid of an additional authenticated public channel for the process of quantum basis comparison, eavesdropping detection and error correction. Once the key is agreed, it is utilised as a One-Time Pad (OTP) to complete the encryption and decryption processes. This so-called OTP system has been proven by Shannon to be *information-theoretically secure* [28]. Furthermore, the QKD-based cryptosystem possesses the capability of eavesdropping detection based on the no-cloning theorem and Heisenberg's uncertainty principle. Hence, QKD is capable of supporting ultimate information security in communication systems [1, 21, 23–27, 29, 30].

1.2 Historical Review

1.2.1 Quantum Key Distribution Protocols

The earliest QKD protocol can be traced back to 1984, which is the Bennett-Brassard-1984 (BB84) protocol [31]. Since then, a variety of QKD protocols have been proposed, which can be divided into two types, i.e. Discrete Variable QKD (DV-QKD) and Continuous Variable QKD (CV-QKD). The state-of-the-art of DV-QKD and CV-QKD schemes is summarized at a glance in Fig. 1.2. More specifically, the landmark BB84 protocol [31] has spawned the family of DV-QKD exemplified by the Ekert-91 (E91) [32], Bennett-Brassard-Mermin-1992 (BBM92) [33], Bennett-92 (B92) [34], six-state [35], decoy-state [36], Scarani-Acién-Ribordy-Gisin-2004 (SARG04) [37], Twin-Field (TWF) [38], and Phase-Matching (PM) [39] protocols. Furthermore, the first CV-QKD protocol was the Gaussian modulation assisted Grosshans-Grangier-2002 (GG02) protocol [40]. This was followed by the no-switching protocol in 2004 [41], in which heterodyne detection is used instead of homodyne detection. Furthermore, the discrete modulation based CV-QKD Leverrier-Grangier-2009 (LG09) protocol was conceived in 2009 [42]. Then a point-to-multipoint CV-QKD protocol was proposed in 2023 [43], aiming for constructing a high-rate downstream network that can facilitate large-scale deployments, enabling multiuser access with the aid of low-cost devices and simplified network structures. A comprehensive overview of QKD protocols can be found in [44–51].

Table 1.1 offers a comparison between the two types of QKD. First of all, for light sources, typically the single photon or the attenuated laser source is utilized in DV-QKD, whilst the coherent state or squeezed state solution is used for CV-QKD. Secondly, the DV-QKD modulates or maps information onto the discrete degrees of freedom of a single photon, such as its polarization or phase. By contrast, the CV-QKD information is modulated or mapped onto the quadrature components of electromagnetic fields[21]. Finally, single-photon detection is required for DV-QKD, which is expensive to implement and yet has a low key rate. By contrast, for CV-QKD either homodyne or heterodyne detection is utilized, which has convenient compatibility with the

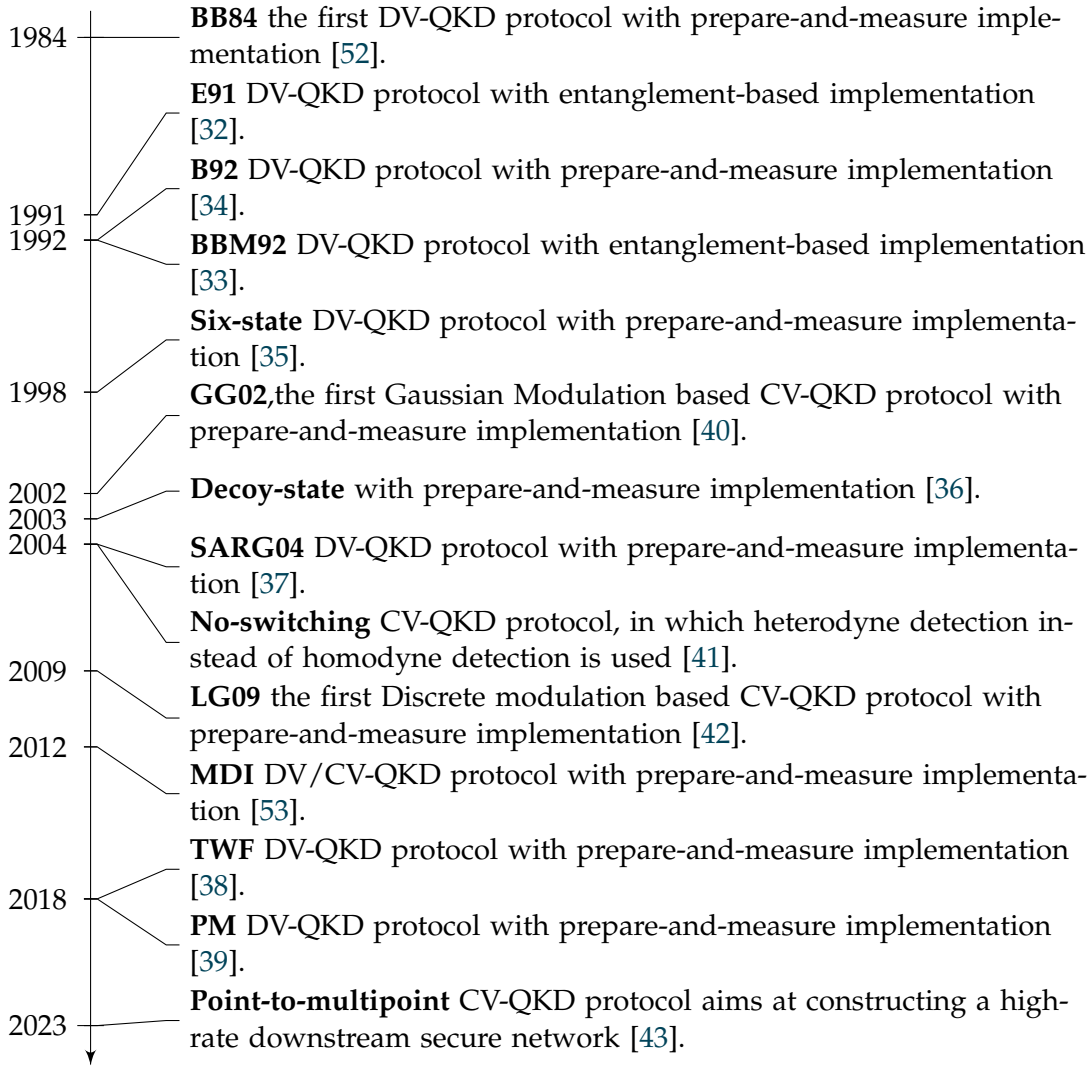


Figure 1.2: Timeline of important milestones in QKD protocols.

operational network infrastructure [21, 54]. As a further benefit, CV-QKD is capable of providing a higher key rate [40, 41, 55, 56] than its DV-QKD counterpart, since both homodyne and heterodyne detections offer the prospect of high detection efficiency. This is beneficial, because a wide range of quantum-safe services such as banking, healthcare and government affairs might be supported not only in the ideal infinite block-length scenario [57], but also in the finite-block-length regime [58]. Therefore, CV-QKD systems have attracted substantial attention from both academia and industry.

As an important step of classical post-processing in QKD, reconciliation plays an pivotal role in ensuring that both the transmitter and the receiver rely on the same bit stream and use it as the reconciled key. More explicitly, the reconciliation process is based on error correction used for mitigating the deleterious effects of noise and interference imposed by Eve [59]. For instance, a simple Hamming code was utilized in the reconciliation step to correct the bit errors in the raw key string shared by the satellite

Table 1.1: Comparisons between two types of QKD.

	DV-QKD	CV-QKD
Light source	Single photon or attenuated laser	Coherent state or squeezed state
Modulation	Polarization or phase	Quadrature components of quantized electromagnetic field
Detection	Single-photon detection	Homodyne or Heterodyne detection

and the ground station for the experimental satellite-to-ground QKD system used in the *Micius* experiment [60]. Inspired by this development, some more advanced Forward Error Correction (FEC) codes have also been investigated, such as Low-Density Parity-Check (LDPC) codes [15, 61–66], polar codes [67–70], rateless codes [71, 72], and their diverse variants. As a further advance, instead of using a fixed FEC code rate, adaptive-rate reconciliation schemes were proposed in [73–75], where the Secret Key Rate (SKR) and the secure transmission distance were optimized for different Signal-to-Noise Ratio (SNR)s. Moreover, a Raptor-like LDPC code was harnessed for QKD in [74], where the rate-compatible nature of the raptor code was exploited for reducing the cost of constructing new matrices for low-rate LDPC codes harnessed at low SNRs. In contrast to the conventional CV-QKD reconciliation, where a so-called single decoding attempt based algorithm was used, a multiple decoding attempt based method was adopted in [66] to improve the SKR performance. Furthermore, a large block length based LDPC coded scheme was analyzed in [76], where a near-capacity performance was achieved for transmission over the Quantum Channel (QuC).

1.2.2 THz CV-QKD Systems

To meet the explosive data-rate demand of NG communication systems, the abundance of bandwidth available in the Terahertz (THz) range has motivated a lot of research efforts [77, 78]. Furthermore, compared to Free Space Optical (FSO) links, THz transmission is more robust to the presence of dust, fog and atmospheric turbulence, but its particle-like behaviour is less pronounced. Nonetheless, the feasibility of CV-QKD for NG wireless communication systems has also been considered in the microwave and THz bands [24, 79–82]. The author of [79] studied the SKR performance in the THz range of 1-50 THz and characterized the asymptotic SKR for both Direct Reconciliation (DR) and Reverse Reconciliation (RR) reconciliation schemes against collective attacks. It was demonstrated in [79] that a Single-Input Single-Output (SISO) CV-QKD system operating at room temperature in the THz regime can achieve distances ranging from a few meters to several hundred meters. Furthermore, the results reveal that below 1 THz, the main limiting factor is the high thermal noise experienced at room temperature, while at higher frequencies, the main limiting factor is the high atmospheric absorption coefficient. A ray-tracing based indoor multipath channel model

was developed for a SISO CV-QKD transmission system operating in the THz band, indicating that multipath propagation degrades the performance of indoor CV-QKD systems [80]. In [81], the feasibility of wireless CV-QKD relying on thermal Gaussian states in the THz band was investigated. Explicitly, the performance of the secret key rate was analysed as a function of the diameter of antenna. The finite block length effects were also taken into account. Furthermore, in [82], the performances of both direct and reverse reconciliation schemes have been investigated and compared for transmission in the optical frequency band, which was followed by the conclusion that the CV-QKD systems operating at infrared or microwave frequencies is, in principle, possible over short distances. Apart from the terrestrial CV-QKD scenario, the THz band has also been studied in [24] for inter-satellite CV-QKD. It is demonstrated that the SKR performance can be improved as a benefit of the reduced preparation noise, since the temperature in space can be significantly lower than in terrestrial scenarios.

Furthermore, in order to improve the secure transmission distance limited by the high path loss of the THz band, Multiple-Input Multiple-Output (MIMO) techniques have been adopted in [83–86]. The MIMO architecture was first proposed for improving the secret key rates of DV-QKD systems in FSO communication systems [87]. Apart from its application in DV-QKD, a MIMO technique also was utilised in quantum backscatter communication and quantum illumination for improving the bit error rate and the target detection rate, respectively, in [88, 89]. Therefore, based on the feasibility of SISO CV-QKD demonstrated in the THz band, the author of [83] proposed a MIMO CV-QKD scheme for improving the secret key rate and the maximum transmission distance of CV-QKD systems operating at THz frequencies, where both the free space path loss and the atmospheric absorption loss were taken into account. Explicitly, the MIMO CV-QKD transmission channel was converted to several parallel SISO channels with the aid of singular value decomposition-based transmit-receive beamforming. It is demonstrated that the achievable SKR may be improved as the carrier frequency is increased. However, there are two opposing factors that affect the SKR: the preparation thermal noise is reduced at higher THz frequencies (which improves the SKR), whereas the channel transmissivity is reduced at higher frequencies (which degrades the SKR). As a further advance, Kundu et al. investigated the effects of channel estimation and the restricted eavesdropping resilience of MIMO CV-QKD systems in [84] and [85], respectively. Explicitly, it is demonstrated in [84] that the practically achievable SKRs are significantly degraded compared to the asymptotic SKRs, particularly at large transmission distances, because the channel estimation error increases due to the reduced channel transmissivity. Furthermore, it is demonstrated in [85] that a coherent state-based CV-QKD protocol may be preferred over a squeezed state based CV-QKD protocol. Finally, it is demonstrated in [86] that a non-negligible SKR can be achieved by both SISO and MIMO-based CV-QKD systems at millimeter frequencies provided that the operating temperature is as low as $T = 4$ K.

Moreover, the classic Orthogonal Frequency Dividion Multiplexing (OFDM) waveform used in Fourth Generation (4G) and 5G, has been harnessed for supporting CV-QKD in the THz band for the sake of mitigating the detrimental multipath effects of wireless channels [69, 90–98]. Briefly, an OFDM-based CV-QKD scheme was proposed for optical fibre transmission in [69, 90–93, 95], where both the security level and the SKR were investigated. Moreover, realistic imperfect modulation was considered in [93], while a singular value decomposition based method was invoked for the reliable simultaneous transmission of multiple data streams in [95]. It was demonstrated in [95] that both the maximum key rate attained at a specific distance and the overall maximum secure transmission distance can be improved with the aid of the OFDM technique. Furthermore, an OFDM-based CV-QKD FSO link was established in [94], which took into account the impact of scintillation intensity, phase noise and the number of subcarriers on the system performance. As a further advance, the authors of [98] analyzed the performance of CV-QKD for transmission over FSO quantum channels with a focus on the theoretical derivation of the SKR. Thirdly, the SKR performance of an OFDM-based CV-QKD scheme operating in the THz band was analyzed both in indoor environments and in inter-satellite links in [96], where the effect of subchannel crosstalk caused by the imperfection of optical devices was considered as well. Thereafter, a realistic imperfect modulation scenario was considered for OFDM-based CV-QKD in [97].A specific modulation noise model was proposed for OFDM-based CV-QKD and the authors investigated the effect of both Gaussian and discrete modulation cases. It was demonstrated in [97] that the asymptotic SKR can be improved by increasing the number of sub-carriers even for realistic discrete modulations.

Furthermore, some recent achievements in THz hardware implementations such as detectors, power-efficient sources and antennas [99–102], can facilitate the practical implementation of CV-QKD in NG communication systems. Therefore, this treatise mainly focuses on the study of CV-QKD-based system design.

1.3 Outline of the Thesis

The rest of this thesis is organized as follows, which is also summarized in Fig. 1.3:

- In **Chapter 2**, a rudimentary introduction will be provided. Firstly, a brief review of the classical syndrome-based decoding technique is introduced in Section 2.2 using example of a $\mathcal{C}(7,4)$ Hamming code and LDPC codes. Afterwards, the classical DV-QKD protocol will be introduced in Section 2.3 with a brief review of the classic BB84 protocol. As a counterpart of DV-QKD, the CV-QKD protocol is reviewed in Section 2.4 including both the quantum transmission and the classical LDPC-coded reconciliation scheme, followed by our SKR analysis. Note that the CV-QKD protocol discussed above with emphasis on the reconciliation

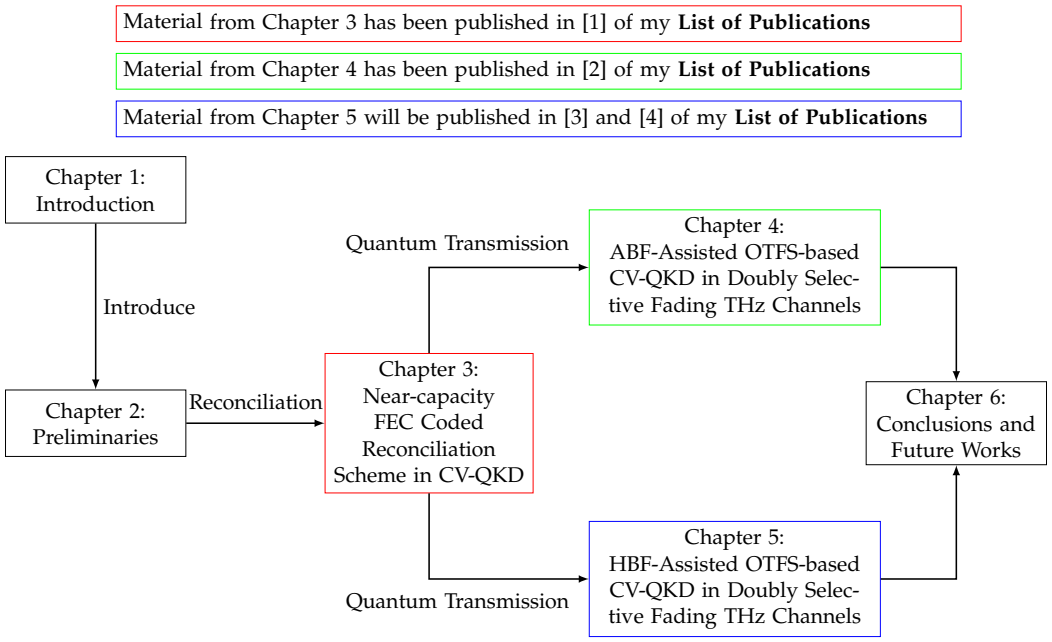


Figure 1.3: The outline of this thesis.

part is based on optical quantum transmission. However, THz based quantum communications has also been studied in the open literature [24, 79–82]. In light of this, both SISO and MIMO THz CV-QKD systems are introduced in Section 2.5 and Section 2.6, respectively, including the system model, channel model, and key rate analysis.

- In **Chapter 3**, we aim for establishing a near-capacity reconciliation scheme for CV-QKD systems. We commence a brief review of the classic CV-QKD protocols [15, 59], relying on a commonly utilized reconciliation scheme in Section 3.2. Following this, different system designs are proposed and compared in Section 3.2 in terms of complexity, compatibility with different FEC codes and near-capacity performance. The corresponding security analysis is conducted in Section 3.3. Then, Section 3.4 presents the BLER and Bit Error Rate (BER) performance of different systems as well as the SKR versus distance, where the performance of the proposed FEC aided CV-QKD is analyzed.

- In **Chapter 4**, we conceive a multi-carrier framework for supporting both OFDM and Orthogonal Time Frequency Space (OTFS) aided LDPC coded CV-QKD reconciliation systems operating in time-varying frequency-selective fading THz channels. An Analog Beamforming (ABF) technique is utilized. Explicitly, our SISO OFDM/OTFS CV-QKD system is conceived in Section 4.2, which introduces the CV-QKD system model, OFDM and OTFS quantum transmission as well as our modified MDR designed for THz fading. Then a MIMO OFDM/OTFS CV-QKD system relying on ABF is proposed in Section 4.3, which is followed by its SKR analysis in Section 4.4. Our simulation results are presented in Section 4.5.

- In **Chapter 5**, the ABF-assisted MIMO OFDM/OTFS CV-QKS system conceived in Chapter 4 is further developed. Explicitly, our MIMO OFDM/OTFS CV-QKD system is conceived in Section 5.2, which introduces our HBF-based MIMO OTFS/OFDM CV-QKD system model as well as our modified Multi-Dimensional Reconciliation (MDR) decoding operating in doubly selective THz channels. Then MIMO OFDM/OTFS channel estimation algorithms are proposed in Section 5.3, which is followed by the associated SKR analysis in Section 5.4. Our simulation results are presented in Section 5.6.
- Finally, in **Chapter 6**, we summarize our findings in Section 6.1, along with a range of promising future research directions in Section 6.2.

1.4 Novel Contributions

- In **Chapter 3**, a near-capacity CV-QKD reconciliation scheme is proposed. The novelties are detailed as follows.
  - Firstly, the Block Error Rate (BLER) performance is analyzed in the context of syndrome-based reconciliation systems, where the Authenticated Classical Channel (ClC) is initially assumed to be error-free, and both the Bit-Flipping (BF) and Belief Propagation (BP) based decoding algorithms are harnessed. More explicitly, we revise Gallager's Sum-Product Algorithm (SPA) for LDPC codes using BP, where both the codeword transmitted through the QuC and the side information conveying the syndrome through the authenticated ClC can be accepted as the input of the modified SPA. Our performance results confirm that the revised BP decoder substantially outperforms the conventional BF decoder in terms of the SKR of the QKD system.
  - Secondly, for the first time in the literature, the effect of a realistic imperfect ClC is characterized for syndrome transmission from Bob to Alice, where RR is considered and the effects of both fading as well as of noise are taken into account. We demonstrate that the QKD system requires error correction for both the quantum and ClC. Consequently, the receiver has to perform FEC decoding of the potentially corrupted encoded syndrome for transmission over the ClC, and FEC decoding of the corrupted reference key sent from Bob over the ClC, making the decoding complexity unbalanced that burdens the receiver side. This calls for clean-slate considerations for a new QKD system design.
  - Thirdly, a new bit-difference based CV-QKD reconciliation scheme is proposed, where Bob transmits the key through the QuC to Alice, and Alice carries out decoding with the aid of the bit-difference side information sent

by Bob through the ClC to Alice. The bit-difference side information is constituted by the vector of bit differences between the key and a legitimate LDPC codeword. This regime allows us to use any arbitrary FEC codes. Our performance results confirm that for a specific FEC this new system has the same performance as the conventional syndrome-based CV-QKD [59], but again, it is compatible with any FEC schemes, including polar codes, Convolutional Code (CC)s and Irregular Convolutional Code (IRCC)s.

- Since the bit-difference vector based CV-QKD system still requires Alice to perform FEC decoding for both the QuC and ClC, a new codeword-based QKD reconciliation system is proposed. In this system, Alice sends a FEC-protected Classical Key (CK) to Bob through the ClC, while Bob sends a separate FEC protected Quantum Key (QK) to Alice through the QuC.Upon a FEC decoding performed at both sides, the final key to be used for the message encryption is the modulo-2 sum of the CK and QK.As a result, for the first time in the open literature, our proposed codeword-based CV-QKD system achieves the following novelties. **Firstly**, the proposed scheme ensures protection of both the QuC and the ClC by FECs. **Secondly**, the system conceived has a symmetric complexity, where both Alice and Bob have an FEC encoder and an FEC decoder. **Thirdly**, the proposed QKD reconciliation scheme is compatible with a wide range of FEC schemes, including polar codes, CCs and IRCCs, where a near-capacity performance can be achieved for both the QuC and for the ClC.
- Our performance results demonstrate that with the aid of IRCCs, near-capacity performance can be achieved for both the quantum and the ClC, which leads to an improved SKR that inches closer to both the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [103] and the maximum achievable rate bound [104]. Therefore, the proposed codeword-based QKD reconciliation system facilitates flexible FEC deployment and it is capable of increasing the secure transmission distance.

- In **Chapter 4**, we conceive a multi-carrier framework for supporting both OFDM and OTFS aided LDPC coded CV-QKD reconciliation systems especially in time-varying frequency-selective fading THz channels, where MIMO ABF technique is utilized. The novel contributions are detailed as follows.
  - Firstly, a multi-carrier OFDM based LDPC assisted CV-QKD reconciliation scheme is established and studied. This is different from the existing literature both in terms of the quantum transmission and reconciliation process, which operate in the face of time-varying and frequency-selective THz propagation.

- Secondly, for the first time in the open literature, an OTFS based quantum transmission scheme is proposed for LDPC coded CV-QKD, which is capable of relying on the same multi-carrier infrastructure as its OFDM counterpart, while providing improved performance in the face of time-varying THz scenarios.
- Thirdly, in order to facilitate LDPC assisted CV-QKD reconciliation for both OFDM and OTFS, a new mapping scheme is devised for our post-processing aided MDR process, where realistic channel fading is taken into account. This is different from the existing MDR schemes found in the open literature, where a Binary Input Additive White Gaussian Noise (BI-AWGN) based quantum channel is assumed [105].
- Fourthly, in order to improve the quantum transmission distance attained in the face of severe THz path loss, MIMO beamforming is conceived based on statistical Channel State Information (CSI), where analog beamformers are conceived based on Line of Sight (LoS) propagation without requiring full knowledge of the multipath CSI at the transmitter.
- Finally, our analysis and simulation results demonstrate that the proposed OTFS-based CV-QKD is capable of outperforming its OFDM counterpart in terms of its SKR, when the user mobility is increased. Moreover, our performance results also demonstrate that the proposed MIMO beamforming scheme is capable of improving secure CV-QKD transmission for both OTFS and OFDM.

- In **Chapter 5**, we conceive a Hybrid Beamforming (HBF)-assisted OTFS-based CV-QKD systems for doubly selective THz channels. The novel contributions are detailed as follows.
  - Firstly, multi-carrier OFDM and OTFS based LDPC assisted CV-QKD reconciliation schemes have been designed and studied in the face of time-varying and frequency-selective THz scenarios, where a HBF technique is conceived for improving the quantum transmission distance attained in the face of severe THz path loss.
  - Secondly, MIMO- OFDM and OTFS channel estimation techniques have been conceived both for the conventional TF domain and for the state-of-the-art DD domain. It is demonstrated that under the idealistic conditions of perfect CSI, the beamforming gain provided by sufficiently large number of antennas makes OFDM and OTFS perform comparably, even in doubly selective fading environments. However, the OFDM-based system relying on realistic channel estimation can only work in stationary scenarios since they suffer from high error-floors in mobile cases.

– Finally, we apply the proposed MIMO OFDM and MIMO OTFS channel estimation methods to both analog and hybrid beamforming aided THz CV-QKD systems. Our analysis and simulation results demonstrate that the proposed OTFS-based CV-QKD is capable of outperforming its OFDM counterpart in terms of SKR, when the user mobility is increased. Moreover, our performance results also demonstrate that the proposed beamforming scheme is capable of improving secure CV-QKD transmission for both OTFS and OFDM in doubly-selective THz fading environments.

Chapter 2

Preliminaries

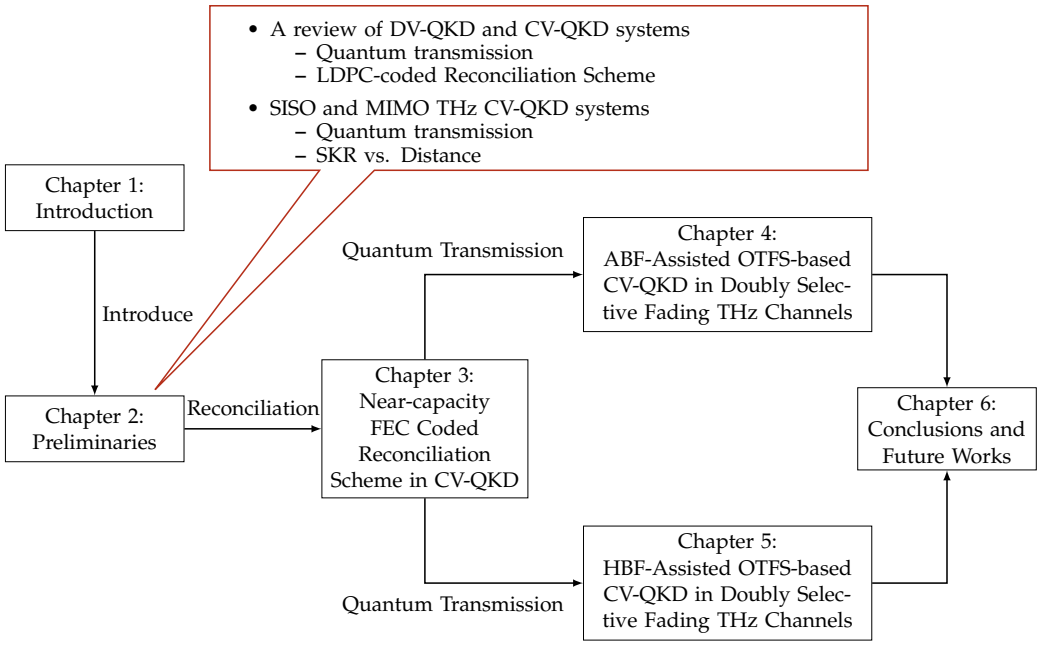


Figure 2.1: The outline of this thesis with the highlight of Chapter 2.

2.1 Introduction

In this chapter, some basic background knowledge will be introduced. The structure of this chapter is described in Fig. 2.1. Firstly, a brief review of the classical syndrome-based decoding technique is introduced in Section 2.2 with examples of the $\mathcal{C}(7,4)$ Hamming and LDPC codes. Afterwards, the classical DV-QKD protocol will be introduced in Section 2.3, which is followed by the introduction of CV-QKD in Section 2.4, including both the quantum domain transmission and classical post-processing relying

on LDPC-coded reconciliation scheme, followed by parametric study and SKR analysis. After that, both SISO and MIMO THz CV-QKD systems found in the literature are introduced in Section 2.5 and Section 2.6, respectively, including their the system model, channel model, and key rate analysis.

2.2 A Brief Review of Classical Syndrome-based Decoding

2.2.1 $\mathcal{C}(7,4)$ Hamming Code

Before introducing the reconciliation scheme using the simple example of the $\mathcal{C}(7,4)$ Hamming code, the basic syndrome decoding algorithm needs to be reviewed, which would be used in the following part. The classical $\mathcal{C}(N_{\text{FEC}}, K_{\text{info}})$ code is designed to map K_{info} information bits onto N_{FEC} coded bits, where the $N_{\text{FEC}} - K_{\text{info}}$ bits are called redundant bits with $N_{\text{FEC}} < K_{\text{info}}$. The purpose of adding the redundant bits after the information bits is to facilitate error detection or error correction. Consider the $\mathcal{C}(7,4)$ Hamming code as an example to illustrate how the syndrome-based decoding algorithm works. The $\mathcal{C}(7,4)$ Hamming code maps 4 information bits onto 7 coded bits and hence becomes capable of correcting a single error. In general, the mapping of K_{info} information bits is performed by multiplying the row vector of information bits by the generator matrix $\mathbf{G}$, which can be formulated as

$$\mathbf{c} = \mathbf{kG}, \tag{2.1}$$

where the row vector $\mathbf{k}$ contains K_{info} elements and the dimension of $\mathbf{G}$ is $K_{\text{info}} \times N_{\text{FEC}}$, and the resultant codeword $\mathbf{c}$ is a row vector having N_{FEC} elements. The matrix multiplication here is based on modulo-2 arithmetic. Given the $\mathcal{C}(7,4)$ Hamming code as an example, its generator matrix $\mathbf{G}$ can be defined by

$$\mathbf{G}_{\text{Hamming}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{2.2}$$

Based on Eq. (2.1) and (2.2), we can generate the code space mapping shown in Table 2.1, where $\mathbf{k}_i$ denotes all the possible combination of information bits and $\mathbf{c}_i$ represents all the associated legitimate codeword bits.

The generator matrix $\mathbf{G}$ can be represented in a systematic form, which is

$$\mathbf{G} = (\mathbf{I}_{K_{\text{info}}} | \mathbf{P}), \tag{2.3}$$

Table 2.1: The code space mapping of the $\mathcal{C}(7,4)$ Hamming code.

i	$\mathbf{k}_i$	$\mathbf{c}_i$
1	0 0 0 0	0 0 0 0 0 0 0
2	0 0 0 1	0 0 0 1 1 1 1
3	0 0 1 0	0 0 1 0 0 1 1
4	0 0 1 1	0 0 1 1 1 0 0
5	0 1 0 0	0 1 0 0 1 0 1
6	0 1 0 1	0 1 0 1 0 1 0
7	0 1 1 0	0 1 1 0 1 1 0
8	0 1 1 1	0 1 1 1 0 0 1
9	1 0 0 0	1 0 0 0 1 1 0
10	1 0 0 1	1 0 0 1 0 0 1
11	1 0 1 0	1 0 1 0 1 0 1
12	1 0 1 1	1 0 1 1 0 1 0
13	1 1 0 0	1 1 0 0 0 1 1
14	1 1 0 1	1 1 0 1 1 0 0
15	1 1 1 0	1 1 1 0 0 0 0
16	1 1 1 1	1 1 1 1 1 1 1

where $\mathbf{I}_{K_{\text{info}}}$ is a $(K_{\text{info}} \times K_{\text{info}})$ identity matrix and $\mathbf{P}$ is a matrix having $K_{\text{info}} \times (N_{\text{FEC}} - K_{\text{info}})$ elements. The codeword $\mathbf{c}$ in Table 2.1 is in its systematic form consisting of K_{info}-bit information word $\mathbf{k}$ followed by $(N_{\text{FEC}} - K_{\text{info}})$ parity bits. A generator matrix $\mathbf{G}$ is associated with an $(N_{\text{FEC}} - K_{\text{info}}) \times N_{\text{FEC}}$-element Parity-Check Matrix (PCM) $\mathbf{H}^{\text{PCM}}$, which is defined as

$$\mathbf{H}^{\text{PCM}} = \left(\mathbf{P}^T | \mathbf{I}_{N_{\text{FEC}} - K_{\text{info}}}\right). \tag{2.4}$$

Hence, the corresponding PCM of the classical $\mathcal{C}(7,4)$ Hamming code, having the generator matrix of Eq. (2.2), can be represented as

$$\mathbf{H}^{\text{PCM}}_{Hamming} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{2.5}$$

By definition, the PCM of $\mathbf{H}^{\text{PCM}}$ is constructed for ensuring that a valid codeword $\mathbf{c}$ has an all-zero syndrome vector, which is

$$\mathbf{s} = \mathbf{c}\mathbf{H}^{\text{PCM}^T} = \mathbf{0}. \tag{2.6}$$

A received word $\bar{\mathbf{c}}$ may be contaminated by an error vector $\mathbf{e} \in \{0,1\}^n$ due to channel impairments. More explicitly, the resultant received words corrupted by the additive noise $\mathcal{E}$ can be formulated as

$$\tilde{\mathbf{c}} = \mathbf{c} + \mathbf{e}. \tag{2.7}$$

The error syndrome $\mathbf{e}$ is a row vector having $(N_{\text{FEC}} - K_{\text{info}})$ elements obtained by the following calculation:

$$\begin{aligned} \mathbf{s} = \tilde{\mathbf{c}}\mathbf{H}^{\text{PCM}^T} &= (\mathbf{c} + \mathbf{e})\mathbf{H}^{\text{PCM}^T} \\ &= \mathbf{c}\mathbf{H}^{\text{PCM}^T} + \mathbf{e}\mathbf{H}^{\text{PCM}^T} \\ &= \mathbf{0} + \mathbf{e}\mathbf{H}^{\text{PCM}^T} \\ &= \mathbf{e}\mathbf{H}^{\text{PCM}^T}. \end{aligned} \tag{2.8}$$

The syndrome vector $\mathbf{s}$ contains the information related to the error pattern imposed by the channel. Generally, there are $2^{K_{\text{info}}}$ legitimate codewords generated by the all possible combination of the K_{info} information bits, and $2^{N_{\text{FEC}}}$ possible received corrupted codewords of $\tilde{\mathbf{c}}$, and $2^{(N_{\text{FEC}}-K_{\text{info}})}$ syndromes $\mathbf{s}$, each of which unambiguously identifies one of the $2^{(N_{\text{FEC}}-K_{\text{info}})}$ error patterns, including the error-free scenario. Therefore, for the classical $\mathcal{C}(7,4)$ Hamming code, the syndrome vector $\mathbf{s}_i$ can detect and correct a single error pattern as specified in Table 2.2. Based on the calculated syndromes, the corresponding error patterns can be used to obtain the predicted codeword $\hat{\mathbf{c}} = \tilde{\mathbf{c}} + \mathbf{e}$, which is one of the legitimate codeword $\bar{\mathbf{c}}$ given the imposed error is within the error correction capability of the classical $\mathcal{C}(7,4)$ Hamming code. Finally, the information bits can be decoded from the predicted codeword by removing the redundant bits.

Table 2.2: Syndromes of the $\mathcal{C}(7,4)$ classical Hamming code.

i	$\mathbf{s}_i$			$\mathbf{e}_i$						
1	0	0	0	0	0	0	0	0	0	0
2	0	0	1	0	0	0	0	0	0	1
3	0	1	0	0	0	0	0	0	1	0
4	0	1	1	0	0	1	0	0	0	0
5	1	0	0	0	0	0	0	1	0	0
6	1	0	1	0	1	0	0	0	0	0
7	1	1	0	1	0	0	0	0	0	0
8	1	1	1	0	0	0	1	0	0	0

To elaborate a bit further, two examples will be given in the following part. Firstly, consider K_{info} information bits of $\mathbf{k} = (0\ 0\ 0\ 1)$. The information bits are encoded using the classical $\mathcal{C}(7,4)$ Hamming code employing the generator matrix of Eq. (2.2), yielding the coded bits of $\mathbf{c} = (0\ 0\ 0\ 1\ 1\ 1\ 1)$. Let us assume that the channel corrupts the legitimate codeword $\mathbf{c}$ by imposing an error pattern of $\mathbf{e} = (0\ 0\ 0\ 0\ 0\ 0\ 1)$ resulting the received word of $\tilde{\mathbf{c}} = (0\ 0\ 0\ 1\ 1\ 1\ 0)$. Based on the received word, its corresponding syndrome can be calculated, that is $\mathbf{s} = (0\ 0\ 1)$, using Eq. (2.8). Now, utilising the look-up Table 2.2, the error pattern of $\mathbf{e} = (0\ 0\ 0\ 0\ 0\ 0\ 1)$, having the corresponding syndrome is $\mathbf{s} = (0\ 0\ 1)$, can be utilised to recover the corrupted codeword, which is $\hat{\mathbf{c}} = \tilde{\mathbf{c}} + \mathbf{e} = (0\ 0\ 0\ 1\ 1\ 1\ 1)$. Lastly, the information bits $\hat{\mathbf{k}} = (0\ 0\ 0\ 1)$ can be recovered by removing the redundant bits based on Table 2.1.

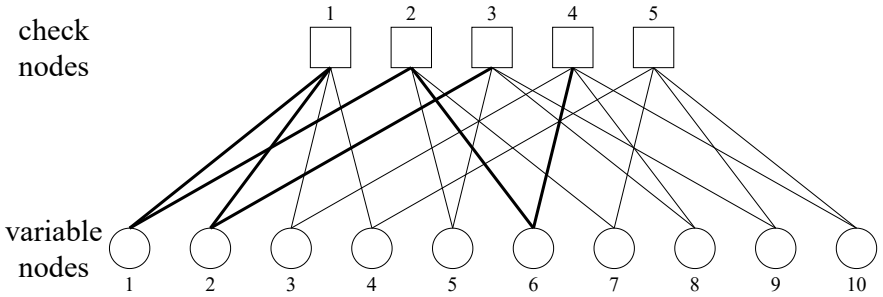


Figure 2.2: The Tanner graph for the code given in Eq. (2.9).

.

Another example we consider is when the channel imposes an error pattern beyond the error correction capability of the classical $\mathcal{C}(7,4)$ Hamming code. More explicitly, we assume that the K_{info} information bits of $\mathbf{k} = (0\ 0\ 0\ 1)$ are encoded into $\mathbf{c} = (0\ 0\ 0\ 1\ 1\ 1\ 1)$ and are sent through the channel that imposes an error pattern of $\mathbf{e} = (0\ 0\ 0\ 0\ 0\ 1\ 1)$. Consequently, the received codeword bit is $\tilde{\mathbf{c}} = (0\ 0\ 0\ 1\ 1\ 0\ 0)$ and the corresponding syndrome is $\mathbf{s} = (0\ 1\ 1)$. Based on the calculated syndrome, the error pattern of $\mathbf{e} = (0\ 0\ 1\ 0\ 0\ 0\ 0)$ is chosen to recover the received codeword. In this case, the recovered codeword is $\hat{\mathbf{c}} = (0\ 0\ 1\ 1\ 1\ 0\ 0)$ instead of the correct codeword of $\mathbf{c} = (0\ 0\ 0\ 1\ 1\ 1\ 1)$. Hence, the decoded information bits are $\mathbf{k} = (0\ 0\ 1\ 1)$, which are different from the original information bits. This example demonstrates that the classical $\mathcal{C}(7,4)$ Hamming code is unable to achieve error-free decoding, when the number of errors is beyond its error correction capability.

2.2.2 LDPC Code

LDPC codes constitute a class of linear block codes defined by a sparse PCM $\mathbf{H}^{\text{PCM}}$ of size $(N_{\text{FEC}} - K_{\text{info}}) \times N_{\text{FEC}}, K_{\text{info}} \leq N_{\text{FEC}}$, where N_{FEC} is the number of columns in $\mathbf{H}^{\text{PCM}}$ and it is also known as the block length, while $(N_{\text{FEC}} - K_{\text{info}})$ is the rank of $\mathbf{H}^{\text{PCM}}$. Hence, the code rate is $R = K_{\text{info}}/N_{\text{FEC}}$. A (d_v, d_c)-regular LDPC code is defined as the null space of a sparse PCM, where each row of $\mathbf{H}^{\text{PCM}}$ contains exactly d_c ones, which is also called the degree d_c of check nodes (CNs) . Each column of $\mathbf{H}^{\text{PCM}}$ contains exactly d_v ones, which is also called the degree d_v of variable nodes (VNs) . Both the degrees of CNs and VNs are small compared to the number of rows in $\mathbf{H}^{\text{PCM}}$. An LDPC code is classified as being irregular if the row weight d_c and column weight d_v are not constant. It is often helpful to use the so-called Tanner graph to represent the PCM $\mathbf{H}^{\text{PCM}}$ [106]. In the Tanner graph representation, there are two types of nodes, which are the VNs (or code-bit nodes) and CNs (or constraint nodes), respectively. If an element of $\mathbf{H}^{\text{PCM}}_{i,j}$ is equal to one, then CN i denoted as c_i is connected by an edge to VN j denoted as v_j in the Tanner graph. Otherwise, there is no connection between them. The notion of degree distribution is used for characterizing the check and variable node

Algorithm 1: The Classic Sum-Product Algorithm of Gallager [108].

1 **Initialization:** Initialize LLR at each VN, $v = 1, 2, ..., n$ for the appropriate channel model. Then, for all i, j for which $h_{i,j} = 1$, set $L^l_{v\to c} = L^0_{v\to c}$.

2 **CN update:** Compute outgoing CN messages $L_{c\to v}$ for each CN using

$$L^t_{c\to v} = 2\tanh^{-1}\left(\prod_{v'\in V_c\setminus v}\tanh\left(\frac{L^{t-1}_{v'\to c}}{2}\right)\right),$$

and then transmit to the VN.

3 **VN update:** Compute outgoing VN messages $L_{v\to c}$ for each VN using

$$L^t_{v\to c} = \begin{cases} L^0_{v\to c} \\ L^0_{v\to c} + \sum_{c'\in C_v\setminus c} L^t_{c'\to v} \quad \text{if } t \geq 1 \end{cases},$$

and then transmit to the CN.

4 **LLR total:** For $v = 1, 2, ..., n$ compute

$$L^{total}_v = L^0_{v\to c} + \sum_{c'\in C_v} L^t_{c'\to v}.$$

5 **Stopping criterion:** Hard decision and early termination check:

$$\hat{c}^{(t)}_v = \begin{cases} 0, & L^{total}_v \geq 0 \\ 1, & \text{otherwise} \end{cases}.$$

If $\hat{\mathbf{c}}\mathbf{H}^{\mathrm{PCM}^T} = \mathbf{0}$ or the number of affordable iterations reaches the maximum limit, stop; else, go to step 2.

degrees [107]. For example, as shown in Fig. 2.2, for the first VN, there are two edge connections seen in bold lines with the first and second CN. In a similar fashion, the second VN is connected with the first and third CN. The corresponding PCM $\mathbf{H}^{\mathrm{PCM}}$ is formulated as

$$\mathbf{H}^{\mathrm{PCM}} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{10\times 5}, \tag{2.9}$$

which is a $[10, 5]$-regular LDPC code having the code length of $N_{\mathrm{FEC}} = 10$ and code rate of $R = 0.5$, the row weight is $d_c = 4$ and the column weight is $d_v = 2$. The notation of "$[N_{\mathrm{FEC}}, K_{\mathrm{info}}]$-regular LDPC code" used from now on to represent regular LDPC codes having a code length of N_{FEC}, and information length of K_{info}.

LDPC decoding is popularly performed using the BP algorithm [108], which is an iterative message-passing algorithm commonly used for inference based on graphical

models such as factor graphs [109]. In the context of LDPC codes, the decoding procedure attempts to find a valid codeword by iteratively exchanging the probabilistic information represented by the Log-Likelihood Ratio (LLR) between the CN and VN along the edges of the Tanner graph until either the parity-check condition is satisfied or the maximum affordable number of iterations is reached.

In Algorithm 1, Step 1 prepares the LLR input values at each VN. All VN-to-CN messages arriving from VN v to CN c are initialized to the received LLR, denoted as $L^0_{v\to c}$ at the output of the channel before the first message-passing iteration. Then, Step 2 to Step 5 illustrate the process of finding the most likely codeword by iterative soft information exchange between CN and VN, until either the syndrome defined by $\hat{\mathbf{C}}\mathbf{H}^T$ becomes zero, or the maximum affordable number of decoding iterations is reached. To elaborate further, in Step 2, $L^t_{c\to v}$ is the message arriving from CN to VN in iteration t, and $C_v\backslash c$ denotes all the CNs connected to VN v, except for CN c. In Step 3, $L^t_{v\to c}$ is the message coming from VN to CN in iteration t, and $V_c\backslash v$ is the set of VNs connected to CN c, except for VN v.

2.3 A Brief Review of DV-QKD

2.3.1 Classic Reconciliation Scheme

In this section, the FEC-coded reconciliation scheme in DV-QKD systems will be introduced in detail, commencing with a toy example, namely a Hamming-coded reconciliation scheme, followed by an LDPC-coded one.

2.3.1.1 Hamming-coded Reconciliation Scheme – A Toy Example

In this section, a simple reconciliation example relying on the $\mathcal{C}(7,4)$ Hamming code will be introduced, as illustrated in Fig. 2.3. Note that the Binary Symmetry Channel (BSC) based equivalent QuC is considered here, which is commonly used in DV-QKD research [110]. Moreover, the ClC used for syndrome transmission is assumed to be error-free. The main steps of the reconciliation scheme shown in Fig. 2.3 are as follows.

(a) Alice randomly generates a bit stream $\mathbf{C}$ using a Quantum Random Number Generator (QRNG)[1], and we view this as the initial raw key $\mathbf{b}$ at her side. The length of this is determined by the codeword length of the predefined PCM $\mathbf{H}$. The PCM is known at both sides. Note that the bit stream $\mathbf{b}$ at Alice's side does not have to be a legitimate codeword. It can be viewed as the combination of a legitimate codeword $\mathbf{c}$ and an error pattern $\mathbf{e}_A$, namely $\mathbf{C}_A = \mathbf{C} + \mathbf{e}_A$, because

[1]Note that, the QRNG generates classical random numbers.

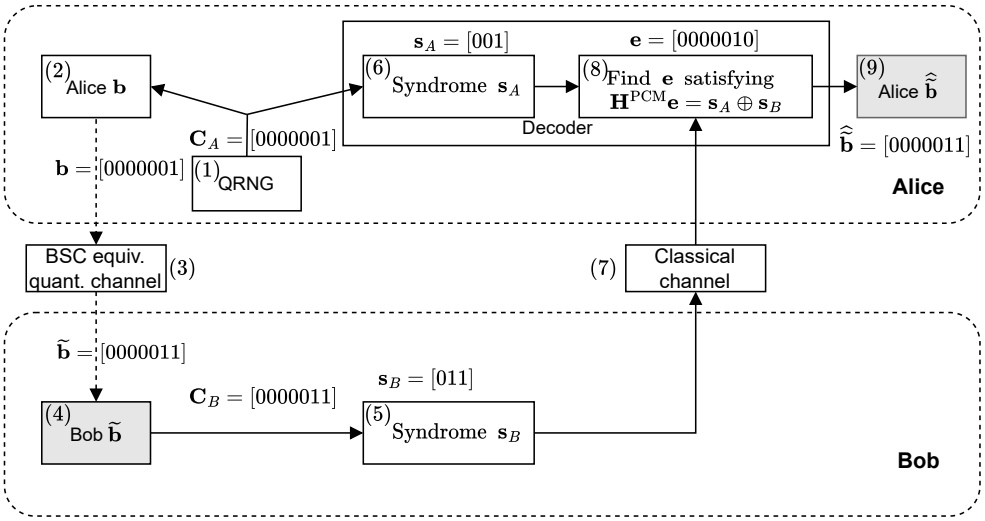


Figure 2.3: Example of an $\mathcal{C}(7,4)$ Hamming-coded reconciliation scheme in the DV-QKD system, where the classic BSC channel is utilised as an equivalent quantum channel. Note that the dash arrow represents the bit stream sent from Bob to Alice through the equivalent QuCs, which is detailed in [21].

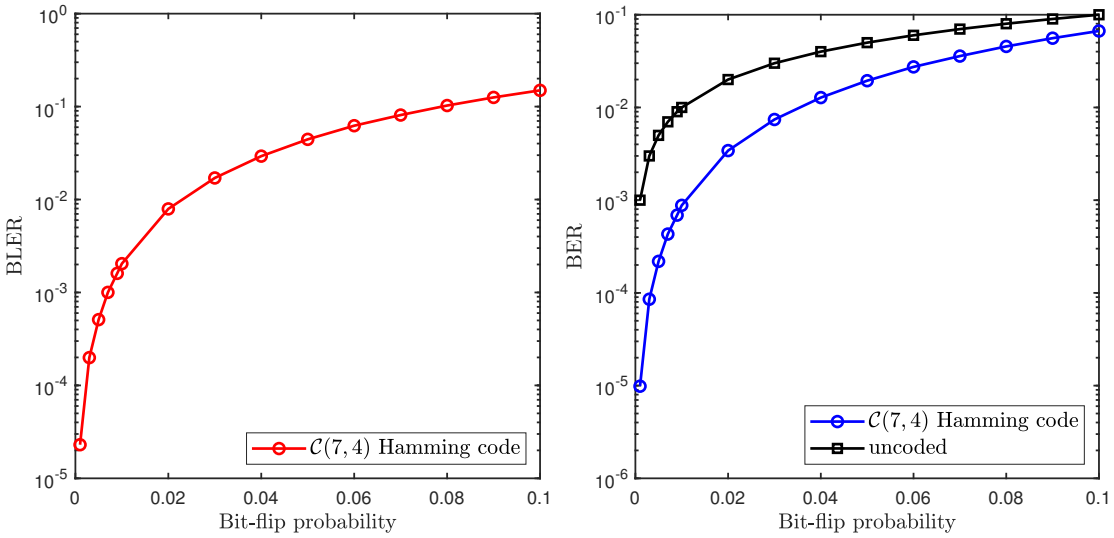
the final objective is to obtain a reconciled key. More specifically, in DV-QKD, the bit stream at Bob's side is the *reference key*, and Alice has to acquire this as the final key [110]. For this $\mathcal{C}(7,4)$ Hamming coded reconciliation scheme aided DV-QKD system, the bit stream generated by the QRNG in block (1) of Fig. 2.3 is $\mathbf{C}_A = [0000001]$. Then Alice treats this random bit stream as the inital key $\mathbf{b} = [0000001]$ in block (2) of Fig. 2.3.

(b) Alice transmits this bit stream $\mathbf{b} = [0000001]$ through a QuC to Bob, which is modelled by the equivalent classical BSC channel and represented by block (3) of Fig. 2.3. The channel-contaminated sequence received by Bob is denoted by $\widetilde{\mathbf{b}} = [0000011]$ in block (4) of Fig. 2.3.

(c) Bob takes the bit stream $\widetilde{\mathbf{b}}$ inferred at the output of the QuC, which may or may not be a legitimate codeword, and forwards it as $\mathbf{C}_B = [0000011] = \mathbf{c} + \mathbf{e}_B$ to the syndrome calculation, which gives $\mathbf{s}_B = \mathbf{C}_B \mathbf{H}^{\mathrm{PCM}^T} = [011]$ in block (5). Then Bob transmits this syndrome as side information to Alice through the authenticated ClC of block (7), which is assumed to be perfectly *noiseless and error-free*.

(d) Meanwhile, Alice calculates the syndrome based on $\mathbf{C}_A$, which gives $\mathbf{s}_A = \mathbf{C}_A \cdot \mathbf{H}^{\mathrm{PCM}^T} = [001]$ in block (6). After that Alice operates syndrome-based decoding to find the most likely error pattern based on the combination of both the syndromes, satisfying $\mathbf{H}^{\mathrm{PCM}}\mathbf{e} = \mathbf{s}_A + \mathbf{s}_B$.

(e) Finally, Alice can obtain a decoded bit stream by adding the error pattern $\mathbf{e}$ to her original bit stream $\mathbf{C}_A$, which is $\widehat{\mathbf{C}}_A = \mathbf{C}_A + \mathbf{e} = \mathbf{c} + \mathbf{e}_A + \mathbf{e} = \mathbf{c} + \mathbf{e}_A + \mathbf{e}_A + \mathbf{e}_B = \mathbf{c} + \mathbf{e}_B = \mathbf{C}_B$, and view $\widehat{\mathbf{C}}_A$ as the final reconciled key. This reconciled key is



(a) BLER **(b)** BER

Figure 2.4: The performance of a Hamming-coded reconciliation aided DV-QKD system, where the QuC is modelled by a classical BSC and the ClC is assumed to be error-free. The bit-flip probability is set to $[0.001, 0.1]$.

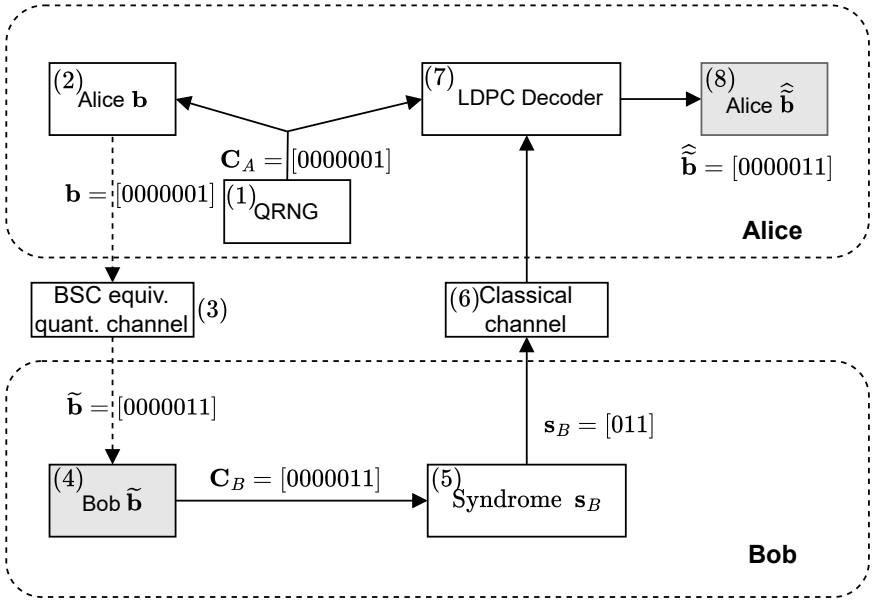


Figure 2.5: An example of LDPC-coded reconciliation scheme in the DV-QKD system where BSC channel is utilised as an equivalent quantum channel. Note that the dash arrow represents the bit stream sent from Bob to Alice through the equivalent QuCs.

Algorithm 2: The Modified Sum-Product Algorithm of Gallager.

1 **Initialization:** Initialize LLR at each VN, $v = 1, 2, ..., n$ for the appropriate channel model. Then, for all i, j for which $h_{i,j} = 1$, set $L^{l}_{v\to c} = L^{0}_{v\to c}$.

2 **CN update:** Compute outgoing CN messages $L_{c\to v}$ for each CN using

$$L^{t}_{c\to v} = (-1)^{\mathbf{s}_B(c)} \cdot 2\tanh^{-1}\left(\prod_{v'\in V_c\setminus v}\tanh\left(\frac{L^{t-1}_{v'\to c}}{2}\right)\right),$$

and then transmit to the VN.

3 **VN update:** Compute outgoing VN messages $L_{v\to c}$ for each VN using

$$L^{t}_{v\to c} = \begin{cases} L^{0}_{v\to c} \\ L^{0}_{v\to c} + \sum_{c'\in C_v\setminus c} L^{t}_{c'\to v} \quad \text{if } t \geq 1 \end{cases},$$

and then transmit to the CN.

4 **LLR total:** For $v = 1, 2, ..., n$ compute

$$L^{total}_{v} = L^{0}_{v\to c} + \sum_{c'\in C_v} L^{t}_{c'\to v}.$$

5 **Stopping criterion:** Hard decision and early termination check:

$$\hat{C}^{(t)}_{v} = \begin{cases} 0, & L^{total}_{v} \geq 0 \\ 1, & \text{otherwise} \end{cases}.$$

If $\hat{\mathbf{c}}\mathbf{H}^{\mathrm{PCM}^T} = \mathbf{s}_B$ or the number of affordable iterations reaches the maximum limit, stop; else, go to step 2.

denoted by $\widehat{\widetilde{\mathbf{b}}}$ in block (9). Observe that this is the same as Bob's bits stream $\widetilde{\mathbf{b}}$, provided that there are no decoding errors.

Fig. 2.4 characterizes both the BLER and BER of the $\mathcal{C}(7, 4)$ Hamming-coded reconciliation aided DV-QKD system. It is shown that both the BLER and BER degrade, i.e. increase with the increase of bit-flip probability, and the bit-flip probability is nearly 0.08 when the BLER is 0.1. This BLER threshold commonly used in the SKR analysis.

2.3.1.2 LDPC-coded Reconciliation Scheme

Fig. 2.5 illustrates the LDPC-coded reconciliation scheme in DV-QKD system. The whole process is mostly similar to that of Hamming-coded reconciliation scheme in Fig. 2.3, except that the blocks of (6) and (8) in Fig. 2.3 are replaced with block (7)-LDPC decoder in Fig. 2.3, which only takes the syndrome from Bob's side $\mathbf{s}_B$.

It is worth mentioning that the LDPC decoding algorithm is a modified SPA of Algorithm 1. In contrast to the conventional SPA decoding algorithm, both the contaminated codeword received from the QuC and the side information received from the ClC are entered into the modified SPA of Algorithm 2. Normally, the side information refers to the syndrome calculated by Bob in the context of LDPC codes. Hence, the SPA decoding algorithm has to be modified. Specifically, we have to change the CN update operation, which is Step 2 in Algorithm 2, based on the syndrome $\mathbf{s}_B$ from Bob received by Alice. The modified CN update operation can be formulated as [15]

$$L_{c\to v}^{t} = (-1)^{\mathbf{s}_B(c)} \cdot 2\tanh^{-1}\left(\prod_{v'\in V_c\setminus v} \tanh\left(\frac{L_{v'\to c}^{t-1}}{2}\right)\right), \tag{2.10}$$

where $\mathbf{s}_B(c) \in \{0,1\}$ represents the parity value at index c. It is plausible that if the syndrome is $\mathbf{s}_B(c) = 0$, the CN update operation remains the same as that of the conventional SPA. Otherwise, for $\mathbf{s}_B(c) = 1$, the CN update operation would flip the sign of the outgoing messages.

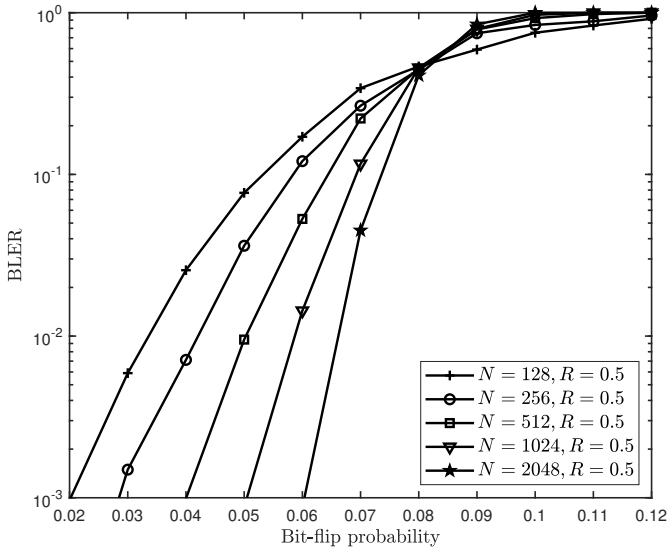
2.3.2 Simulations and Discussions

In this section, the BLER and BER performances of LDPC-coded reconciliation aided DV-QKD system are characterized. The main parameters are listed in Table 2.3.

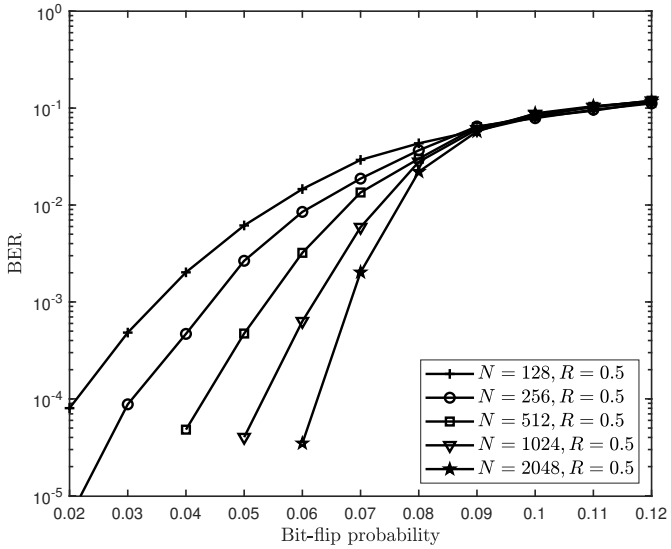
Table 2.3: Simulation parameters.

Parameter	Value
Column weight	3
Coding rate	0.25, 0.4, 0.5, 0.7, 0.8
Code length	128, 256, 512, 1024, 2048
Decoding algorithm	BP
Maximum iteration numbers	50
QuC type	BSC
ClC type	Error-free

Fig. 2.6 shows the BLER and BER performance comparison of $(3,6)$ regular LDPC codes used for DV-QKD reconciliation, where the QuC is modelled as a BSC. Fig. 2.6(a) and Fig. 2.6(b) show the BLER and BER of the LDPC codes, respectively, where the coding rate is $R = 0.5$, but the code lengths N varies from 128 to 2048. It is demonstrated that the BLER and BER performances are gradually improved when the code length increases. Specifically, as shown in Fig. 2.6(a), maximum the bit-flip probability is around 0.02 for the code length $N_{\text{FEC}} = 128$ upon aiming for a target BLER of 10^{-3}, whereas the maximum bit-flip probability is 0.06 for the code length $N_{\text{FEC}} = 2048$ for the same target BLER.



(a) BLER



(b) BER

Figure 2.6: The performance comparison of $(3, 6)$ regular LDPC codes used in DV-QKD reconciliation scheme, where BSC is considered here.

Fig. 2.7 demonstrates the decoding complexity in terms of the average number of iterations. It is illustrated that the average number of iterations required will decrease with the reduction of the bit-flip probability.

2.4 A Brief Review of CV-QKD

In this section, a general CV-QKD scheme[2] is modelled, which contains both the quantum transmission and classical post-processing. Following this, the important post-processing step of multidimensional reconciliation is detailed. Finally, a modified BP

[2]In this treatise, the Gaussian modulated coherent state based CV-QKD protocol is considered.

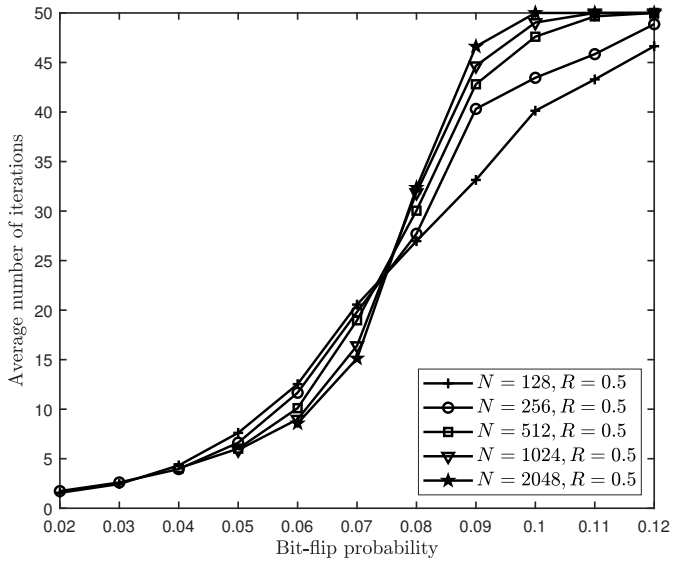


Figure 2.7: The complexity analysis in terms of the average number of iterations of $(3, 6)$ regular LDPC codes used in DV-QKD reconciliation step, where BSC is considered here.

decoding is conceived for the reconciliation scheme.

2.4.1 CV-QKD Protocol

The basic QKD protocol is shown in Fig. 2.8(a), which has a quantum processing part and a classical post-processing part. As for the quantum processing part, Alice prepares Gaussian-modulated coherent states for transmission to Bob. After receiving the signal, Bob makes a measurement relying either on homodyne or on heterodyne detection. This is followed by the classical post-processing part as shown in details in Fig. 2.8(b). Explicitly, the signal $\mathbf{y}$ of Fig. 2.8(a) is a sifted and potentially channel-infested version of $\mathbf{x}$, which suffers from the hostile action of the QuC. Observe in the figure that the post-processing part contains four steps, namely the sifting, parameter estimation, reconciliation, and privacy amplification.

2.4.1.1 Quantum Transmission Part

Fig. 2.9 demonstrates the quantum transmission process of a CV-QKD protocol, which contains the thermal states preparation, eavesdropping attack, and detection measurement. Firstly, Alice generates a pair of independent Gaussian distributed random variables, denoted as $q_A, p_A \sim \mathcal{N}(0, V_s)$, where V_s is the variance of the initial Gaussian signal. Then she uses the random variables q_A, p_A to generate a coherent state $|\psi\rangle$ associated with $\psi = q_A + jp_A$ for transmission. As for Eve, we consider an optimal eavesdropping attack in [112], namely the so-called Gaussian collective attack that can be

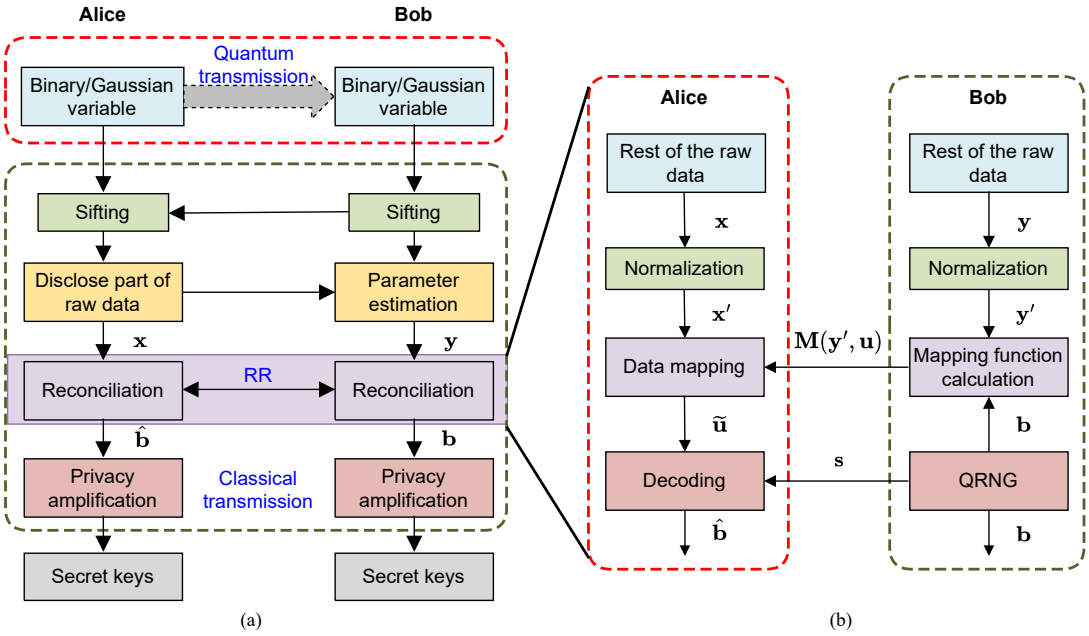


Figure 2.8: (a) Schematic diagram of a QKD protocol. Note that a binary variable is utilized in DV-QKD systems, whilst a Gaussian variable is utilized in CV-QKD systems. Moreover, as for the quantum transmission shown here, it contains the process of converting the binary/Gaussian variable to quantum states and that of converting the quantum states to binary/-Gaussian variable, which is the quantum measurement. (b) Schematic of the multidimensional RR scheme in QKD, where $\mathbf{x}$ and $\mathbf{y}$ are two correlated Gaussian sequences, while $\mathbf{x}'$ and $\mathbf{y}'$ represent their normalized counterparts; $\mathbf{M}(\mathbf{y}', \mathbf{u})$ represents the mapping function sent from Bob to Alice; $\mathbf{b}$ denotes the initial sequence generated by QRNG; $\mathbf{u} = \left(\frac{(-1)^{\mathbf{b}'(1)}}{\sqrt{8}}, \frac{(-1)^{\mathbf{b}'(2)}}{\sqrt{8}}, \ldots, \frac{(-1)^{\mathbf{b}'(8)}}{\sqrt{8}}\right)$ denotes the spherical codes of $\mathbf{b}'$, which is the interleaved bit stream of $\mathbf{b}$; $\tilde{\mathbf{u}}$ is the sequence before decoding and $\hat{\mathbf{b}}$ is the decoding result that is equal to $\mathbf{b}$ when the decoding is successful; $\mathbf{s}$ denotes the additional side information, which is normally the syndrome calculated based on Bob's bit stream. Note that the dimensionality D is set 8.

implemented by the Gaussian entangling cloner attack, where Eve has full control over the channel [113]. Generally, Eve prepares the ancilla modes[3], which are two-mode squeezed states also known as Einsten-Podolsky-Rosen (EPR) states, with variance W. The modes of the EPR states can be described by the operators $\hat{E}$ and $\hat{E}''$, where Eve keeps one of the modes such as $\hat{E}''$ and injects the other mode $\hat{E}$ into the channel. After the interaction with Alice's state Eve gets the output result $\hat{E}'$. Eve then collectively detects both modes of $\hat{E}'$ and $\hat{E}''$, gathered from each run of the protocol, in a final coherent measurement. Furthermore, the input-output relationship of the two-port

[3]Note that a *mode* refers to a specific spatial, temporal, frequency, or polarization configuration of an electromagnetic field [114–116]. Each mode is an independent quantum harmonic oscillator that can be quantized with creation $\hat{a}^\dagger$ and annihilation $\hat{a}$ operators [54, 117]. Furthermore, coherent states considered in our treatise are the eigenstates of the annihilation operator $\hat{a}$, given by $\hat{a}\,|\psi\rangle = \psi\,|\psi\rangle$. Therefore, the annihilation operator $\hat{a}$ is analogous to the complex baseband signal representation used in classical communication systems [118].

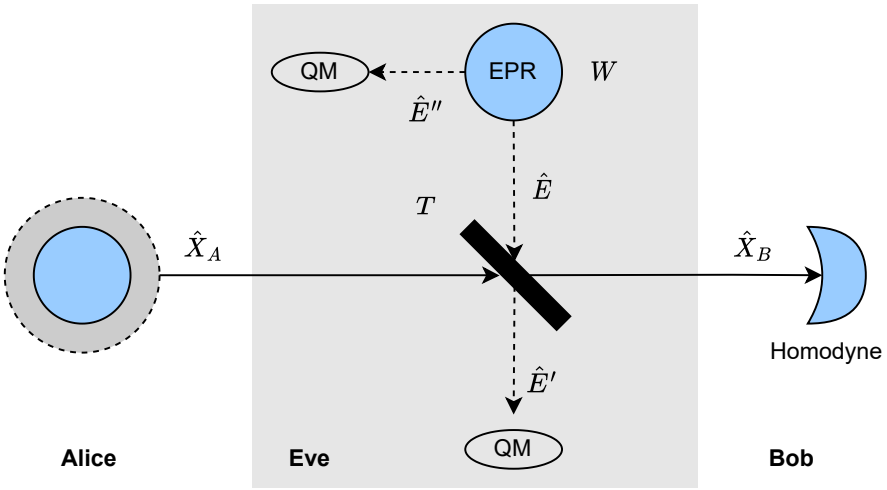


Figure 2.9: Schematic of a CV-QKD protocol using thermal states [79, 111]. The loss in the QuC is modelled by a beam splitter with channel transmissivity T. The eavesdropping attack is a Gaussian collective attack in the form of an entangling cloner attack where the variance of the EPR pair is W with the modes of the EPR beam described by the operator $\hat{E}''$ and $\hat{E}'$. The initial mode sent by Alice $\hat{X}_A$ is a thermal state, and once Bob receives the mode $\hat{X}_B$ he will perform homodyne measurement on it.

(2×2) beam splitter model illustrated in Fig. 2.9 can be presented as [83, 113, 119]

$$\begin{bmatrix} \hat{a}_{\text{out},1} \\ \hat{a}_{\text{out},2} \end{bmatrix} = \begin{bmatrix} \sqrt{T} & \sqrt{1-T} \\ -\sqrt{1-T} & \sqrt{T} \end{bmatrix} \begin{bmatrix} \hat{a}_{\text{in},1} \\ \hat{a}_{\text{in},2} \end{bmatrix}, \tag{2.11}$$

where $\hat{a}_{\text{out},1}$ and $\hat{a}_{\text{out},2}$, and $\hat{a}_{\text{in},1}$ and $\hat{a}_{\text{in},2}$ represent the two input modes and two output modes of the beam splitter, respectively. Based on this, the output mode at Bob's side therefore can be expressed as

$$\hat{a}_B = \sqrt{T}\hat{a}_A + \sqrt{1-T}\hat{a}_E, \tag{2.12}$$

where $\sqrt{T}$ represents the transmission coefficient of the link between Alice and Bob, $\hat{a}_A$ and $\hat{a}_E$ respectively represent the transmitted mode of Alice associated with the coherent state $|\psi\rangle$ and the injected Gaussian mode of Eve, and $\sqrt{1-T}\hat{a}_E$ can be considered as a noise term.

For each of the received modes, Bob applies homodyne measurement to one of the randomly chosen quadratures, i.e. the q or the p quadrature. After the measurement, the input-output relationship between Alice and Bob is given by

$$\hat{X}_B = \sqrt{T}\hat{X}_A + \sqrt{1-T}\hat{X}_E, \tag{2.13}$$

and the input-output relationship of Eve's ancilla mode is

$$\hat{X}_{E'} = -\sqrt{1-T}\hat{X}_A + \sqrt{T}\hat{X}_E, \tag{2.14}$$

where $\hat{X}_B$ is the received quadrature component, which is measured at Bob, $\hat{X}_A$ is the quadrature component transmitted by Alice, $\hat{X}_E$ is the excess noise quadrature component introduced by Eve, and $\hat{X}_{E'}$ is the ancilla quadrature component stored in Eve's quantum memory. Note that the variable $\hat{X}$ corresponds to one of the two quadrature components $\{\hat{q}, \hat{p}\}$, so that we have $\hat{X} \in \{\hat{q}, \hat{p}\}$, which is held for $\hat{X}_A$, $\hat{X}_B$, $\hat{X}_E$ and $\hat{X}_{E'}$. The variance of Alice's transmitted mode is $V_A = V_s + V_0$, where V_s is the variance of the initial Gaussian signal and V_0 is the variance of the vacuum state, and $V_E = W$ is the variance of the excess noise injected by Eve. The variance of the thermal state can be expressed as

$$V_0 = 2\bar{n} + 1, \tag{2.15}$$

where $\bar{n} = \left[\exp\left(\hbar f_c / K_B T_e\right) - 1\right]^{-1}$ while $\hbar$ is Planck's constant, k_B is Boltzmann's constant and T_e is the environmental temperature in Kelvin. It is worthwhile mentioning that the variance of the thermal state in Eq. (2.15) depends on the frequency f_c of operation and the environmental temperature T_e. Normally, for optical frequencies, $\bar{n} \approx 0$, such that $V_0 \approx 1$ Shot-Noise Units (SNU)[4] at room temperature [54, 79, 82]. However, for lower frequencies, we have $V_0 \geq 1$ at room temperature. The relationship described in Eq. (2.15) is portrayed in Fig. 2.10. Observe that with the reduction of the frequency, the variance of the corresponding thermal noise V_0 increases, which will impose a detrimental effect on the CV-QKD system.

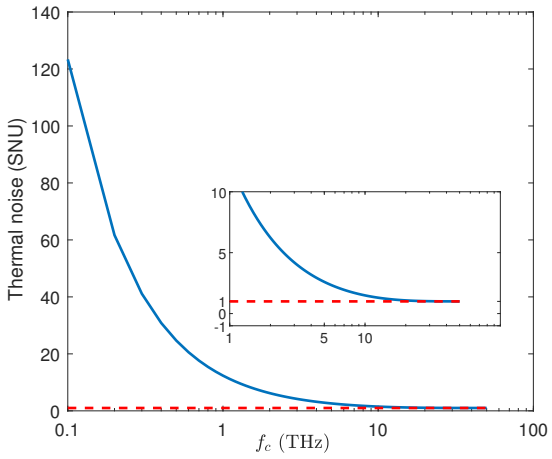


Figure 2.10: The variance of thermal noise versus frequency.

2.4.1.2 Classical Post-processing Part

- *Sifting*: In the sifting step of Fig. 2.8 (a), both Alice and Bob retain the data associated with those specific states, whose preparation and measurement basis happen to be the same, given that both their bases are randomly chosen. More explicitly,

[4]SNU is used to quantify the power of signals relative to the power of the shot noise of a given system [54, 59]. Without special clarification, SNU is used to quantify the power of signals for the whole thesis.

in the BB84 DV-QKD example, Bob randomly chooses one of two legitimate polarization bases to measure his data received from Alice. Then they both publicly communicate with each other to agree about the particular bit-indices, where the measurement basis of Bob is the same as the preparation basis of Alice.

- *Parameters estimation*: In this step of Fig. 2.8(a), Alice and Bob will reveal and compare a random subset of the data, which allows them to estimate some parameters, such as the transmissivity (pathloss coefficient), excess noise, and the SNR of the channel. Then the Mutual Information (MI) between them is calculated to judge whether this channel is secure enough for supporting their communication. If the MI between Alice and Bob is higher than Eve's information concerning the key, the channel is deemed to be secure enough for supporting secret keys transmission, otherwise, the transmission aborts and a new random process is initiated.

- *Reconciliation*: The reconciliation step of Fig. 2.8(a) relies on error correction. There are two styles of reconciliation, namely DR and RR. As for DR, Bob corrects his data according to Alice's data, while Alice's data remains unmodified. By contrast, in RR, Alice corrects her data according to Bob's data and Bob's data remains unmodified. Usually, RR is preferred since it can provide longer secure transmission distance than that of DR. More explicitly, in DR, the channel's transmission coefficient must be above 0.5 to provide a non-zero SKR, which is usually called "3dB limit", while there is no such limitation in the RR case [82, 111][5].

- *Privacy amplification*: Finally, the last step of Fig. 2.8(a) is privacy amplification harnessed for reducing Eve's probability of successfully guessing (a part of) the keys, since Eve has a certain amount of information concerning the key. A hashing function may be used for privacy amplification. For example, a universal hashing function can be used to complete the privacy amplification via turning the reconciled key stream into a shorter-length final key stream. As for the amount by which the reconciled key is shortened, this depends on how much information Eve has gained about the key.

2.4.2 Classic LDPC-coded Reconciliation Scheme

2.4.2.1 Multidimensional Reconciliation

Again, a MDR method is considered, since it exhibits better performance in the lower SNR region, which may translate into a longer secure transmission distance [121]. The multidimensional reverse reconciliation process is shown in Fig. 2.8(b). After the disclosure of the raw data to be used for parameter estimation, as seen in Fig. 2.8(a), the

[5]Despite there is a "3dB limit" for DR, but it is highly tolerant to the preparation noise, while RR is very sensitive to the preparation noise [120].

rest of their raw data $x := \hat{X}'_A$ and $y := \hat{X}'_B$ is constituted by a pair of correlated Gaussian distributed sequences, where $x \sim \mathcal{N}\left(0, \sigma_x^2\right)$, and $y = x + n, n \sim \mathcal{N}\left(0, \sigma_n^2\right)$. Then both Alice and Bob choose D for representing the number of dimensions in the multidimensional reconciliation, which defines how the sequence of transmit data is partitioned into shorter segments. It was shown in [121] that the mapping function used in the multidimensional reconciliation process only exists in $\mathbb{R}, \mathbb{R}^2, \mathbb{R}^4, \mathbb{R}^8$ dimensions, which corresponds to $D = 1, 2, 4, 8$, due to its algebraic structure as proven by Theorem 2 in [121]. Moreover, it was demonstrated in [15, 65, 71, 121] that an eight-dimensional reconciliation scheme ($D = 8$) outperformed the schemes associated with $D = 1, 2, 4$ in terms of the BLER performance attained. Therefore, usually the eight-dimensional ($D = 8$) reconciliation scheme is adopted for practical CV-QKD systems [15, 71, 121]. The main steps of multidimensional RR can be described as follows.

1. Firstly, the rest of the raw data of Alice and Bob, can be viewed as a pair of sequences, denoted as $\mathbf{x}$ and $\mathbf{y}$. The length of the two sequences is set to the FEC codeword length N. Then they are partitioned into $I = N/8$ number of shorter segments, denoted as $\mathbf{x} = [\mathbf{x}_1; \mathbf{x}_2; ...; \mathbf{x}_I]$ and $\mathbf{y} = [\mathbf{y}_1; \mathbf{y}_2; ...; \mathbf{y}_I]$, where $\mathbf{x}_i$, $\mathbf{y}_i, i = 1, 2, ..., I$, are 8×1 column vectors.

2. Both Alice and Bob will normalize each 8-element segment of $\mathbf{x}$ and $\mathbf{y}$ in order to get a uniformly distributed 8-element vector, which is reminiscent of producing equi-probable 2^8-ary symbols. To elaborate on the resultant eight-dimensional reconciliation scheme, the normalized data in the form of the vectors $\mathbf{x}'_i$ and $\mathbf{y}'_i$ can be obtained by $\mathbf{x}'_i = \frac{\mathbf{x}_i}{\|\mathbf{x}_i\|}$ and $\mathbf{y}'_i = \frac{\mathbf{y}_i}{\|\mathbf{y}_i\|}$, where we have $\|\mathbf{x}_i\| = \sqrt{\langle \mathbf{x}_i, \mathbf{x}_i \rangle} = \sqrt{\sum_{d=1}^{8} \mathbf{x}_i \left(d\right)^2}$ and $\|\mathbf{y}_i\| = \sqrt{\langle \mathbf{y}_i, \mathbf{y}_i \rangle} = \sqrt{\sum_{d=1}^{8} \mathbf{y}_i \left(d\right)^2}$. Hence, both the normalized vectors $\mathbf{x}'_i$ and $\mathbf{y}'_i$ are uniformly distributed on the surface of the 8-dimensional unit-radius sphere. Therefore, spherical codes [121], where all codewords lie on a sphere centered on 0 can play the same role for CV-QKD as binary codes for DV-QKD.

3. Bob randomly generates a binary stream $\mathbf{b}$ using a QRNG, whose length is the same as the FEC codeword length N. Then, the random bit sequence $\mathbf{b}$ will be interleaved into $\mathbf{b}'$ and the resultant sequence $\mathbf{b}'$ is partitioned into $\mathbf{b}' = [\mathbf{b}'_1; \mathbf{b}'_2; ...; \mathbf{b}'_I]$, where $\mathbf{b}'_i$ is an 8-element binary column vector. Then each segment $\mathbf{b}'_i, i = 1, 2, ..., I$, will be mapped to the 8-dimensional unit-radius sphere of $\mathbf{u}_i = \left(\frac{(-1)^{\mathbf{b}'_i(1)}}{\sqrt{8}}, \frac{(-1)^{\mathbf{b}'_i(2)}}{\sqrt{8}}, \ldots, \frac{(-1)^{\mathbf{b}'_i(8)}}{\sqrt{8}} \right)$.

4. Bob calculates the mapping function for each segment based on the vectors $\mathbf{u}_i$ and $\mathbf{y}'_i$. This mapping function is used to map $\mathbf{y}'_i$ to $\mathbf{u}_i$ so as to find the relationship between the normalized Gaussian vector $\mathbf{y}'_i$ and the modulated stream $\mathbf{u}_i$, which is represented by a phase rotation between $\mathbf{y}'_i$ and $\mathbf{u}_i$ in the case of $D = 2$, as can seen in Fig. 2.11. More details about how the mapping function works

for our scheme can be seen in our following discourse. On the other hand, Bob also has to calculate the side information represented by the syndrome **s** used for assisting the decoding process. This side-information decoding is slightly different for different reconciliation schemes. To elaborate further, initially we assume that LDPC codes are adopted in the reconciliation scheme considered in this paper. However, it is not necessary to encode **b** using LDPC codes, where the side information **s** could be the syndrome calculated from **b**. But again, the side information is not necessarily constituted by the syndromes in other application scenarios. For example, frozen bits are used as side information in polar code-based reconciliation schemes [69, 75]. Then Bob publicly transmits both the mapping function $\mathbf{M}_i\left(\mathbf{y}_i', \mathbf{u}_i\right)$ and the syndrome **s** to Alice through the classical communication channel. The details of the mapping function calculation can be found in [121] and are also shown as follows

Mapping function calculation: Bob calculates the mapping function $\mathbf{M}_i\left(\mathbf{y}_i', \mathbf{u}_i\right)$ for each 8-element vector, which meets $\mathbf{M}_i\left(\mathbf{y}_i', \mathbf{u}_i\right)\mathbf{y}_i' = \mathbf{u}_i$, using the following formula:

$$\mathbf{M}_i\left(\mathbf{y}_i', \mathbf{u}_i\right) = \sum_{d=1}^{8} \alpha_i^d \mathbf{A}_8^d, \tag{2.16}$$

where α_i^d is the d-th element of $\boldsymbol{\alpha}_i\left(\mathbf{y}_i', \mathbf{u}_i\right) = \left(\alpha_i^1, \alpha_i^2, ..., \alpha_i^8\right)^T$, which is the coordinate of the vector $\mathbf{u}_i$ under the orthonormal basis $\left(\mathbf{A}_8^1\mathbf{y}_i', \mathbf{A}_8^2\mathbf{y}_i', ..., \mathbf{A}_8^8\mathbf{y}_i'\right)$ and it can be expressed as $\boldsymbol{\alpha}_i\left(\mathbf{y}_i', \mathbf{u}_i\right) = \left(\mathbf{A}_8^1\mathbf{y}_i', \mathbf{A}_8^2\mathbf{y}_i', ..., \mathbf{A}_8^8\mathbf{y}_i'\right)^T \mathbf{u}_i$, and $\mathbf{A}_8^d, d = 1, 2, ..., 8$ is the orthogonal matrix of size 8×8 provided in the Appendix of [121]. Note that the 8 orthogonal matrices used in our scheme are listed in Eq. (2.17).

5. Alice then applies the same mapping function to her normalized segment $\mathbf{x}_i'$ in order to map the Gaussian variables to $\widetilde{\mathbf{u}}_i = \mathbf{M}_i\left(\mathbf{y}_i', \mathbf{u}_i\right)\mathbf{x}_i'$, which is actually the noisy version of $\mathbf{u}_i$. Hence, the difference between the variable $\mathbf{u}_i$ and its noisy version $\widetilde{\mathbf{u}}_i$ can reflect the quality of the QuC. Hence it may be exploited for eavesdropping detection.

6. After the mapping operation harnessed for each segment at Alice's side, she then concatenates all the segments into a sequence $\widetilde{\mathbf{u}} = [\widetilde{\mathbf{u}}_1; \widetilde{\mathbf{u}}_2; ...; \widetilde{\mathbf{u}}_I]$ having the length of N. Furthermore, the sequence $\widetilde{\mathbf{u}}$ is turned into $\widetilde{\mathbf{u}}'$ after deinterleaving. She finally carries out the decoding of $\widetilde{\mathbf{u}}'$ with the aid of the syndrome **s** calculated by Bob and obtains the secret key $\hat{\mathbf{b}}$.

In summary, the core idea of multidimensional reconciliation is to convert the noise in the QuC to the ClC via using the specific mapping functions $\mathbf{M}_i\left(\mathbf{y}_i', \mathbf{u}_i\right)$. As a consequence, the noisy version $\widetilde{\mathbf{u}}$ of **b** is obtained, hence the family of commonly used FEC schemes can be applied to CV-QKD. More specifically, Fig. 2.11 demonstrates this conversion process from three different dimensionalities[6], that are D=1, 2, 3, respectively.

[6]As stated that the dimensionality of multidimensional reconciliation can be chosen to be 1, 2, 4 and 8. Here for convenience we exemplify this process via using visible 1, 2 and 3 dimensionalities.

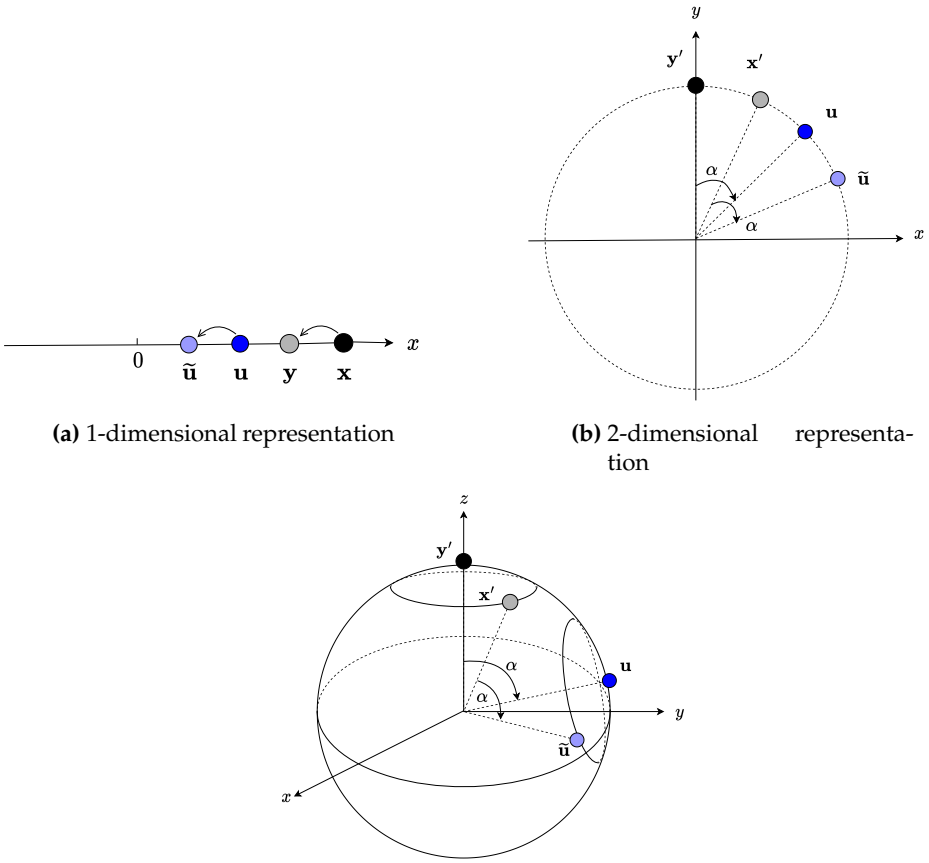
$$\mathbf{A}_8^1 = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1 \end{bmatrix}, \quad \mathbf{A}_8^2 = \begin{bmatrix} 0&-1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&-1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&-1&0&0&0\\ 0&0&0&0&0&0&0&-1\\ 0&0&0&0&0&0&1&0 \end{bmatrix},$$

$$\mathbf{A}_8^3 = \begin{bmatrix} 0&0&-1&0&0&0&0&0\\ 0&0&0&-1&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&-1&0&0&0\\ 0&0&0&0&0&-1&0&0 \end{bmatrix}, \mathbf{A}_8^4 = \begin{bmatrix} 0&0&0&-1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&-1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&-1&0&0&0 \end{bmatrix},$$

$$\mathbf{A}_8^5 = \begin{bmatrix} 0&0&0&0&-1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&0&0&-1\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0 \end{bmatrix}, \mathbf{A}_8^6 = \begin{bmatrix} 0&0&0&0&0&-1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&-1\\ 0&0&0&0&0&0&1&0\\ 0&-1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&-1&0&0&0&0\\ 0&0&1&0&0&0&0&0 \end{bmatrix},$$

$$\mathbf{A}_8^7 = \begin{bmatrix} 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&-1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&-1&0&0&0&0&0&0 \end{bmatrix}, \mathbf{A}_8^8 = \begin{bmatrix} 0&0&0&0&0&0&0&-1\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&-1&0&0&0&0\\ 0&0&-1&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0 \end{bmatrix}. \tag{2.17}$$

In Fig. 2.11(a), the noisy version $\widetilde{\mathbf{u}}$ of $\mathbf{u} = +1$ can be obtained based on the proportion of $\mathbf{y}$ to $\mathbf{x}$ in a 1-dimensional case. Note that the values of $\mathbf{x}$ and $\mathbf{y}$ are not normalized in the 1-dimensional case. As for the 2-dimensional case of Fig. 2.11(b), the normalized vectors $\mathbf{y}'$ and $\mathbf{x}'$ are on the unit-circle, and we have $\mathbf{u} = \left[\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right]^T$. Firstly, Bob calculates the mapping function between $\mathbf{y}'$ and $\mathbf{x}'$, corresponding to α, which physically represents the phase rotation operation. After Alice receives the mapping function, she uses it to get the noisy version $\widetilde{\mathbf{u}}$ of $\mathbf{u}$ by rotating $\mathbf{x}'$ with the same angle α. Similarly, for the 3-dimensional case seen in Fig. 2.11(c), the mapping function can be calculated based on $\mathbf{y}'$ and $\mathbf{u}$ on the surface of the unit-radius sphere. Then the noisy version of $\mathbf{u}$, namely $\widetilde{\mathbf{u}}$ can be obtained by applying the same mapping function to $\mathbf{x}'$. As for



(a) 1-dimensional representation

(b) 2-dimensional representation

(c) 3-dimensional representation

Figure 2.11: The representation of the noise conversion process for $D = 1, 2$ and 3 based on [121].

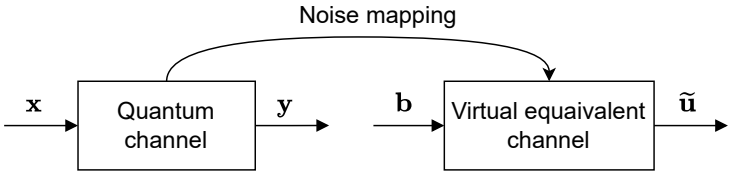
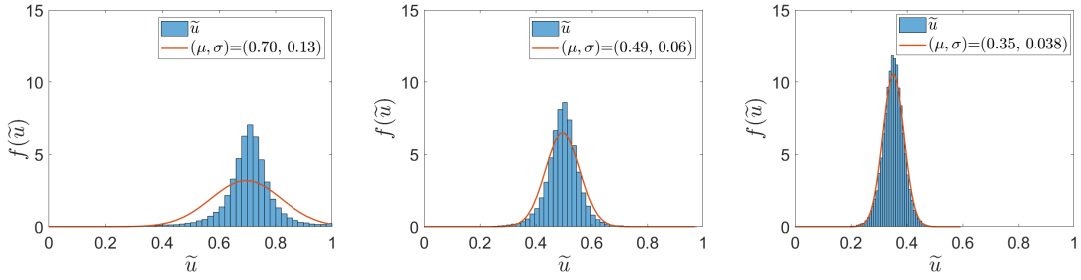


Figure 2.12: The relationship between the QuC and the virtual equivalent channel.

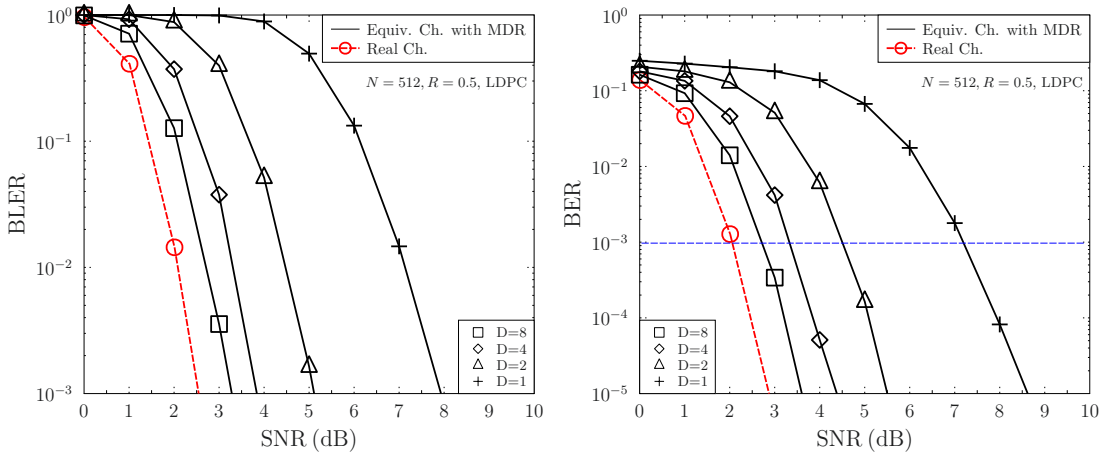
how strong the noise is, it depends on the quality of the QuC, which is modelled by a virtual equivalent BI-AWGN ClC characterized in Fig. 2.12. This is reminiscent of classical modulation and transmission through the AWGN channel [121]. After that, FEC decoding can be applied and finally the reconciled key is generated.

To elaborate a little further, the 2-dimensional reconciliation of a segment is exemplified to illustrate this process. Firstly, after Alice and Bob finish their quantum-domain transmission and detection, sifting and parameter estimation, as well as normalization, they have two sequences, which are $\mathbf{x}'_1 = [0.8865, -0.4626]^T$, $\mathbf{y}'_1 = [0.9748, -0.229]^T$. Let us assume that the random bit stream after interleaving at Bob's side is $\mathbf{b}'_1 = [0, 0]^T$ along with the corresponding $\mathbf{u}_1 = [0.7071, 0.7071]^T$. Then the resultant mapping matrix can



(a) $D = 2$ **(b)** $D = 4$ **(c)** $D = 8$

Figure 2.13: The verification of virtual equivalent Additive White Gaussian Noise (AWGN) channel establishment for multidimensional reconciliation with $D = 2, 4, 8$.



(a) BLER **(b)** BER

Figure 2.14: Comparison between equivalent channel with MDR, where d=1,2,4,8, and real channel, given that the quantum channel is an AWGN channel.

be calculated as $\mathbf{M_1}\left(\mathbf{y}_1', \mathbf{u}_1\right) = \begin{bmatrix} -0.7618 & -0.6479 \\ 0.6479 & -0.7618 \end{bmatrix}$, where $\mathbf{M}_1\left(\mathbf{y}_1', \mathbf{u}_1\right) = \sum_{d=1}^{2} \alpha_1^d \mathbf{A}_2^d$. Note that the pair of orthogonal matrices used in this 2-dimensional scheme are $\mathbf{A}_2^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{A}_2^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Furthermore, α_1^d is the specific element of $\boldsymbol{\alpha}_1\left(\mathbf{y}_1', \mathbf{u}_1\right) = \left(\mathbf{A}_2^1\mathbf{y}_1', \mathbf{A}_2^2\mathbf{y}_1'\right)^T \cdot \mathbf{u}_1$, which is the coordinate of the vector $\mathbf{u}_1$ under the orthonormal basis $\left(\mathbf{A}_2^1\mathbf{y}_1', \mathbf{A}_2^2\mathbf{y}_1'\right)$ [121]. Based on this, the sequence $\widetilde{\mathbf{u}}_1$ at Alice's side after data mapping becomes $\widetilde{\mathbf{u}}_1 = \mathbf{M}\left(\mathbf{y}_1', \mathbf{u}_1\right)\mathbf{x}_1' = [0.8632, 0.5049]^T$, which is a noisy version of $\mathbf{u}_1$. Furthermore, the noise in $\widetilde{\mathbf{u}}_1$ is capable of reflecting the noise level of the quantum transmission between Alice and Bob. Therefore, in our ensuing discourse, the QuC is modelled by an equivalent BI-AWGN ClC.

Note that even though the QuC can be modelled by an equivalent BI-AWGN ClC, there is still a gap between the real quantum channel and the model. Nonetheless, with the increase of the dimensionality from 1 to 2, 4, and 8, the gap between them is reduced, as evidenced by a goodness-of-fit test comparing the variables u and the sequences $\widetilde{\mathbf{u}}$

in Fig. 2.13. It is demonstrated that the fitness of $\widetilde{\mathbf{u}}$ approaches a Gaussian distribution as the dimensionality is increased to 8. Furthermore, Fig. 2.14 shows our comparison between the equivalent channel with MDR and a real AWGN quantum channel, where a (3, 6) regular LDPC code associated with $R = 0.5$ coding rate and $N = 512$ code length is used. It is demonstrated that the dimensionality of $D = 8$ can offer the best performance among all the available dimensionality settings.

2.4.2.2 The Relationship between FEC Codes and Segment Vectors $\widetilde{\mathbf{u}}_i$ after Mapping

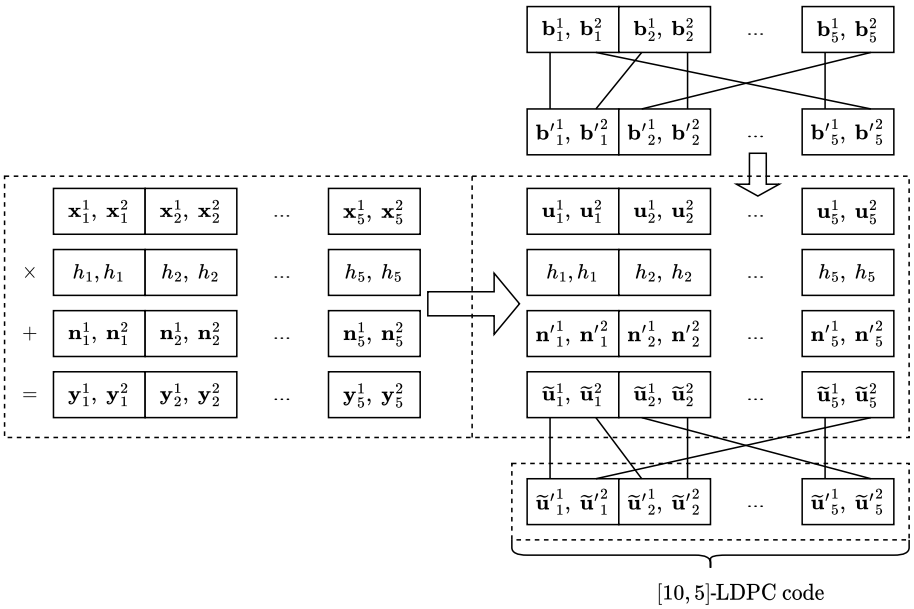


Figure 2.15: The relationship between FEC codes and segmented vectors. Note that a [10,5] LDPC code is applied and 2-dimensional reconciliation is adopted. Correspondingly, $N_{\text{FEC}} = 10$, $D = 2$, and $I = N_{\text{FEC}}/D = 5$.

Once an equivalent ClC has been setup for the QuC, an FEC scheme is needed to proceed. Therefore, in this section, we aim for clarifying how to connect the segment vectors $\widetilde{\mathbf{u}}_i$ after mapping with FEC codes.

In Fig. 2.15, we consider 2-dimensional reconciliation and a [10,5] LDPC code. The PCM of Eq. (2.9), is used for illustrating the relationship between the FEC codes and segmented vectors $\mathbf{u}_i$. In Fig. 2.15, the dashed box at the left represents the relationship between the pair of Gaussian sequences, namely $\mathbf{y}$ and $\mathbf{x}$. Since we consider a [10,5] LDPC code and a 2-dimensional reconciliation scheme ($D = 2$), each of the pair of Gaussian sequences of length $N_{\text{FEC}} = 10$, is divided into $I = N_{\text{FEC}}/D = 5$ segments, yielding $\mathbf{x} = [\mathbf{x}_1; \mathbf{x}_2; \mathbf{x}_3; \mathbf{x}_4; \mathbf{x}_5]$ and $\mathbf{y} = [\mathbf{y}_1; \mathbf{y}_2; \mathbf{y}_3; \mathbf{y}_4; \mathbf{y}_5]$, each of which contains 2 Gaussian elements, i.e. $\mathbf{x}_i = [\mathbf{x}_i^1, \mathbf{x}_i^2]$ for $i = 1, 2, ..., 5$ and $\mathbf{y}_i = [\mathbf{y}_i^1, \mathbf{y}_i^2]$ for $i = 1, 2, ..., 5$. Furthermore, it is assumed that within each segment the channel's fading coefficients

remain constant. For example, we have $\mathbf{h}_1 = [\mathbf{h}_1^1; \mathbf{h}_1^2] = [h_1, h_1]$. On the other hand, the bit stream $\mathbf{b}$ generated by Bob's QRNG seen in Fig. 2.8(b) is correspondingly divided into 5 segments, i.e. $\mathbf{b} = [\mathbf{b}_1; \mathbf{b}_2; \mathbf{b}_3; \mathbf{b}_4; \mathbf{b}_5]$, each of which contains two elements, i.e. $\mathbf{b}_i = [\mathbf{b}_i^1, \mathbf{b}_i^2]$ for $i = 1, 2, ..., 5$. After interleaving, the new bit stream $\mathbf{b}'$ is obtained, which is also partitioned into 5 segments, i.e. $\mathbf{b}' = [\mathbf{b}_1'; \mathbf{b}_2'; \mathbf{b}_3'; \mathbf{b}_4'; \mathbf{b}_5']$, where $\mathbf{b}_i' = [\mathbf{b}_i'^1, \mathbf{b}_i'^2]$ for $i = 1, 2, ..., 5$. In light of this, the affect of the channel's fading coefficient $\mathbf{h} = [\mathbf{h}_1; \mathbf{h}_2; \mathbf{h}_3; \mathbf{h}_4; \mathbf{h}_5]$ and noise $\mathbf{n} = [\mathbf{n}_1; \mathbf{n}_2; \mathbf{n}_3; \mathbf{n}_4; \mathbf{n}_5]$ in the QuC are used for representing the relationship between the modulated sequences $\mathbf{u} = [\mathbf{u}_1; \mathbf{u}_2; \mathbf{u}_3; \mathbf{u}_4; \mathbf{u}_5]$ based on $\mathbf{b}'$ and $\widetilde{\mathbf{u}} = [\widetilde{\mathbf{u}}_1; \widetilde{\mathbf{u}}_2; \widetilde{\mathbf{u}}_3; \widetilde{\mathbf{u}}_4; \widetilde{\mathbf{u}}_5]$. Note that it is assumed that the fading coefficients are known at both sides, and the noise variances of $\mathbf{n} = [\mathbf{n}_1; \mathbf{n}_2; \mathbf{n}_3; \mathbf{n}_4; \mathbf{n}_5]$ and $\mathbf{n}' = [\mathbf{n}_1'; \mathbf{n}_2'; \mathbf{n}_3'; \mathbf{n}_4'; \mathbf{n}_5']$ are the same even thought the exact value of noise $\mathbf{n}'$ is not the same as $\mathbf{n}$ in the QuC. After deinterleaving, a reordered sequence $\widetilde{\mathbf{u}}' = [\widetilde{\mathbf{u}}_1'; \widetilde{\mathbf{u}}_2'; \widetilde{\mathbf{u}}_3'; \widetilde{\mathbf{u}}_4'; \widetilde{\mathbf{u}}_5']$ of $\widetilde{\mathbf{u}}$ is derived, which represents the corrupted sequences of $\mathbf{b}$. Therefore, the sequence $\widetilde{\mathbf{u}}'$ of length 10 will be fed into the [10,5] LDPC decoder.

2.4.2.3 LDPC-coded Reconciliation Scheme

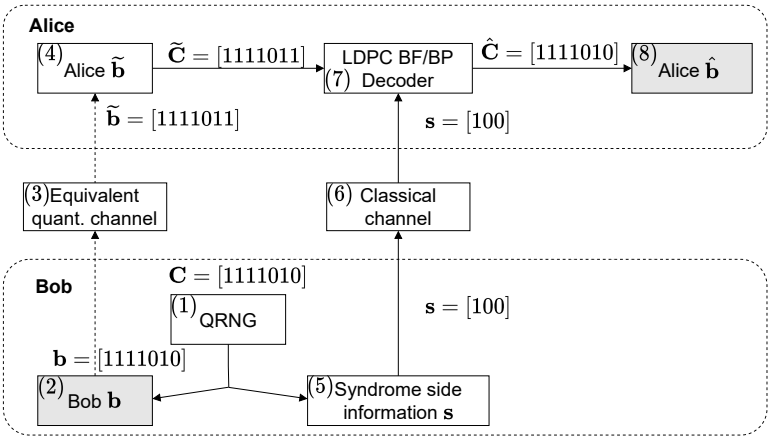


Figure 2.16: *System A* - **the ideal LDPC-coded syndrome-based reconciliation scheme** in the CV-QKD system relying on the BF/BP decoding algorithm. Note that, the dashed arrow represents the bit stream sent from Bob to Alice through the equivalent QuCs as illustrated in Section 2.4.2.

Based on the classic reconciliation scheme introduced above in Section 2.4.2, an LDPC-coded CV-QKD reconciliation scheme is shown in Figure 2.16. Explicitly, a BF/ BP decoding algorithm based LDPC-coded CV-QKD reconciliation scheme is employed, where the ClC used for syndrome transmission is assumed to be error-free. The algorithmic steps are described as follows.

(a) Bob randomly generates a bit stream $\mathbf{C}$ using a QRNG, and we view this as the initial raw key $\mathbf{b}$ at his side. Note that, the QRNG generates classical random

numbers. The length of this is determined by the codeword length of the predefined PCM $\mathbf{H}$. The PCM is known at both sides. Note that, the bit stream $\mathbf{b}$ at Bob's side does not have to be a legitimate codeword, because the final objective is to obtain a reconciled key. More specifically, in the reverse reconciliation scheme, the bit stream generated at Bob's side is the reference key, and Alice has to acquire this as the final key. Let us consider the single-error correcting [7,4,1] Bose-Chaudhuri-Hocquenghem (BCH) code as our rudimentary example, and assume that the bit stream generated by the QRNG in block (1) of Fig. 2.16 is $\mathbf{C} = [1111010]$. Then Bob treats this random bit stream as the initial key $\mathbf{b} = [1111010]$ in block (2) of Fig. 2.16.

(b) Bob transmits this bit stream $\mathbf{b} = [1111010]$ through a QuC to Alice, which is modelled by the equivalent ClC constructed in Fig. 2.12 and represented by block (3) of Fig. 2.16. The channel-contaminated sequence received by Alice is denoted by $\widetilde{\mathbf{b}} = [1111011]$ in block (4), which is corrupted in the last bit position.

(c) Meanwhile, based on the QRNG output Bob calculates the syndrome, say $\mathbf{s} = [100]$ in block (5) and transmits it as side information to Alice through the authenticated ClC of block (6), which is assumed to be perfectly *noiseless and error-free*.

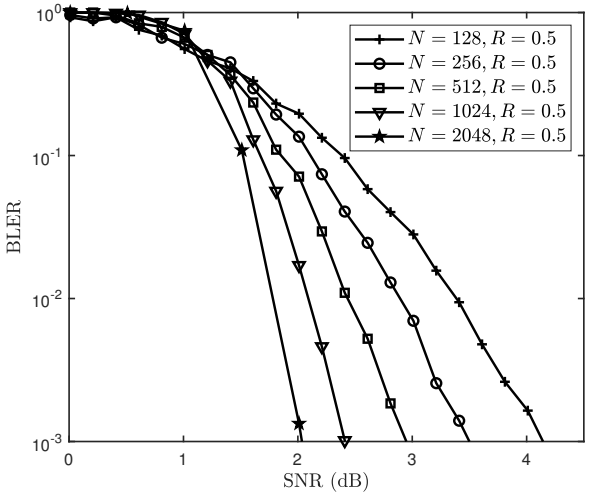
(d) Alice takes the bit stream $\widetilde{\mathbf{b}}$ inferred at the output of the QuC, which may or may not be a legitimate codeword, and forwards it as namely $\widetilde{\mathbf{C}} = [1111011]$ to the decoder. Decoding is carried out by the corresponding FEC decoder with the aid of the syndrome bits she received through the ClC (6) and gets the decoded result of $\hat{\mathbf{C}} = [1111010]$ at the output of block (7). Based on this, Alice gets the decoded codeword as the final reconciled key, which is $\hat{\mathbf{b}} = [1111010]$ shown in block (8). Observe that this is the same as Bob's bit stream $\mathbf{b}$, provided that there are no decoding errors. This is the case, if the QuC inflicts no more than a single error, since the [7,4,1] code can only correct a single error.

2.4.3 Parametric Study and Discussions

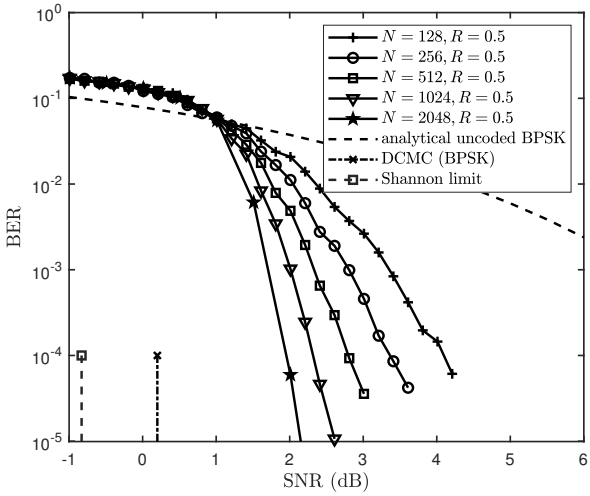
In this section, the same parameters are used in our LDPC-coded reconciliation scheme for CV-QKD as that in DV-QKD seen in Table 2.3 of Section 2.3.2, except that the QuC is modelled as an BI-AWGN channel. In light of this, a parametric study is carried out, which investigates the BLER & BER vs. SNR performances, the coding gain vs. code rate and the complexity analysis.

2.4.3.1 BLER & BER vs. SNR Performance

Fig. 2.17 provides the BLER and BER performance comparison of $(3, 6)$ regular LDPC codes used in the reconciliation of CV-QKD system, where the QuC is modelled by



(a) BLER



(b) BER

Figure 2.17: The performance comparison of $(3, 6)$ regular LDPC codes used in CV-QKD reconciliation scheme, where BI-AWGN is considered here.

a BI-AWGN process. The code rate R of all the LDPC codes is 0.5, but different code lengths N_{FEC} are used, varying from 128 to 2048. It is demonstrated that the BLER and BER performances are gradually improved with the increase of the code length from 128 to 2048. For example, as for the BLER, the SNR required by the code length of $N_{\text{FEC}} = 128$ to achieve a target BLER of 10^{-3} is about 4.2 dB, whereas for the code length of $N_{\text{FEC}} = 2048$, it is about 2.05 dB.

2.4.3.2 Coding Gain vs. Code Rate Performance

Furthermore, the coding gains of LDPC-coded reconciliation schemes having different code rates and code length are tabulated in Table 2.4. In light of this, Fig. 2.18 shows the

Table 2.4: Coding gain of LDPC codes using BP decoding algorithm over BI-AWGN channel.

Code	Code rate R	BER	
		SNR(dB)	Gain (dB)
		10^{-3}	10^{-3}
Uncoded	1.00	6.80	0.00
LDPC$(3,4,128)$	0.25	4.02	2.78
LDPC$(3,4,256)$	0.25	3.22	3.58
LDPC$(3,4,512)$	0.25	2.65	4.15
LDPC$(3,4,1024)$	0.25	2.21	4.59
LDPC$(3,4,2048)$	0.25	1.87	4.93
LDPC$(3,5,100)$	0.4	3.58	3.22
LDPC$(3,5,200)$	0.4	3.00	3.80
LDPC$(3,5,500)$	0.4	2.30	4.50
LDPC$(3,5,1000)$	0.4	1.90	4.90
LDPC$(3,5,2000)$	0.4	1.63	5.17
LDPC$(3,6,128)$	0.5	3.40	3.40
LDPC$(3,6,256)$	0.5	2.81	3.99
LDPC$(3,6,512)$	0.5	2.35	4.45
LDPC$(3,6,1024)$	0.5	2.01	4.79
LDPC$(3,6,2048)$	0.5	1.70	5.10
LDPC$(3,10,100)$	0.7	3.90	2.90
LDPC$(3,10,200)$	0.7	3.40	3.40
LDPC$(3,10,500)$	0.7	3.00	3.80
LDPC$(3,10,1000)$	0.7	2.67	4.13
LDPC$(3,10,2000)$	0.7	2.45	4.35
LDPC$(3,15,100)$	0.8	4.37	2.43
LDPC$(3,15,200)$	0.8	3.95	2.85
LDPC$(3,15,500)$	0.8	3.54	3.26
LDPC$(3,15,1000)$	0.8	3.25	3.55
LDPC$(3,15,2000)$	0.8	3.07	3.73

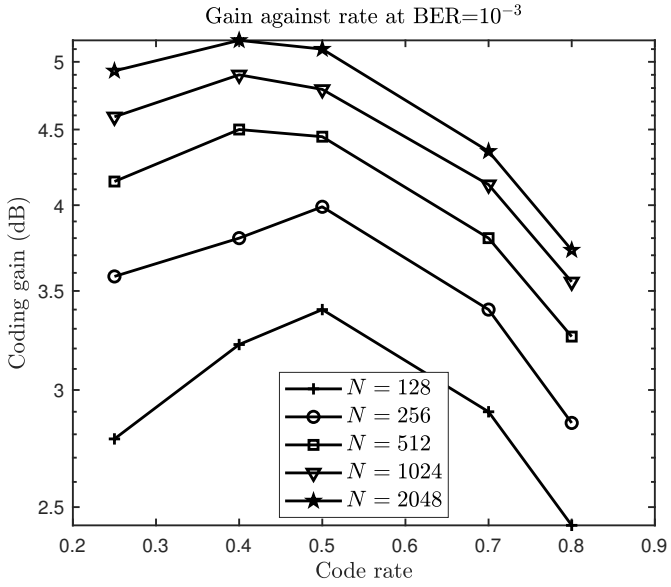


Figure 2.18: Coding gain against code rate for different LDPC codes with column weight 3 at a BER of 10^{-3} over equivalent BI-AWGN channel using the codes summarised in Table 2.4.

coding gain against the code rate for different LDPC codes at a BER of 10^{-3} based on Table 2.4. As the code length N increases, given a fixed code rate, the coding gain will increase, as evidenced in Fig. 2.17. For example, for the code rate of $R = 0.5$, the coding gain of the code length of $N_{\text{FEC}} = 2048$ is 5.10 dB, whilst the corresponding coding gain of code length $N_{\text{FEC}} = 128$ is 3.40 dB. On the other hand, there is a maximum coding gain for each set of LDPC codes that have the same code length N_{FEC}, and it is typically found when the code rate is between 0.4 and 0.5. For example, as shown in Fig. 2.18, the maximum coding gain of the LDPC codes having a codeword length of $N_{\text{FEC}} = 128$ is 3.4 dB when the code rate is 0.5. For LDPC codes having $N_{\text{FEC}} = 256$, the maximum coding gain is 3.99 dB, when the code rate is 0.5.

2.4.3.3 Complexity Analysis

In this section, a simple approximate computational complexity calculation is introduced, which can be used for different LDPC codes.

In the iterative SPA decoding process, the extrinsic LLRs are exchanged between the connected VNs and CNs. More specifically, the extrinsic LLR provided by a VN for each of its connected CNs is obtained as the sum of the LLRs provided by all other connected CN plus the LLR provided by the channel. Meanwhile, the extrinsic LLR furnished by a CN for each of its connected VNs is obtained by the so-called box-plus summation of the LLRs provided by all other connected VNs [122]. To elaborate further, the box-plus sum of two LLRs x and y is given by

$$
\begin{aligned}
f(x,y) =& 2\tanh^{-1}\left(\tanh\left(\frac{x}{2}\right)\tanh\left(\frac{y}{2}\right)\right) && \text{(2.18a)}\\
=& \operatorname{sign}(x)\cdot\operatorname{sign}(y)\cdot\min(|x|,|y|) + \ln\left(1+e^{-|x+y|}\right) - \ln\left(1+e^{-|x-y|}\right) && \text{(2.18b)}\\
\approx& \operatorname{sign}(x)\cdot\operatorname{sign}(y)\cdot\min(|x|,|y|), && \text{(2.18c)}
\end{aligned}
$$

where Eq. (2.18b) is a numerically stable calculation of (2.18a), which may be further simplified to (2.18c) in the so-called min-sum algorithm [122].

In the light of this, the complexity calculation for each CN can be quantified as follows, which characterises the forwards and backwards algorithm [123]:

$$C_v = 3\left(d_v\left(i\right) - 1\right), \tag{2.19}$$

where $d_v\left(i\right)$ is the degree of the ith VN with $v = 1, 2, ..., N$. Likewise, the complexity of each operation of a CN c can be quantified [124, 125] as

$$C_c = 3\left(d_c\left(j\right) - 2\right), \tag{2.20}$$

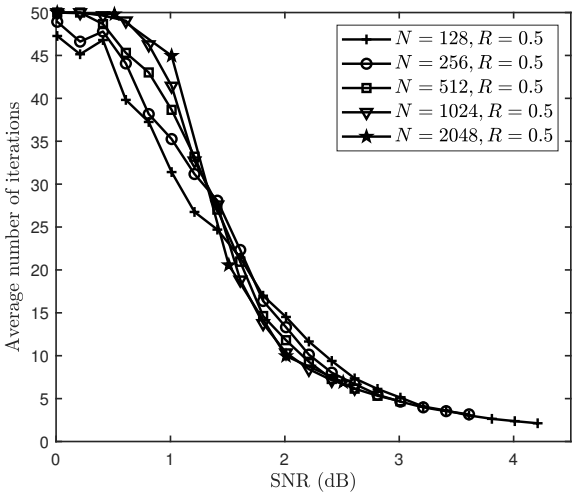


Figure 2.19: The complexity analysis in terms of the average number of iterations of $(3, 6)$ regular LDPC codes used in CV-QKD reconciliation scheme, where BI-AWGN is considered here.

where $d_c\,(j)$ is the degree of the jth CN with $j, c = 1, 2, ..., N\,(1 - R)$. Hence, the overall complexity can be calculated as

$$C_{LDPC} = I_{\max} \times \left(\sum_{i=1}^{N} C_v(i) + \sum_{j=1}^{N(1-R)} C_c(j) \right), \tag{2.21}$$

where $I_{\max}$ represents the maximum number of iterations in the decoding algorithm. Given that the LDPC codes used in our treatise are regular LDPC codes, where the column weight is fixed to 3, the complexity of the LDPC code per bit per iteration can be quantified as

$$\begin{aligned} \overline{C}_{LDPC} &= I_{\max} \times \left(\sum_{i=1}^{N} C_v(i) + \sum_{j=1}^{N(1-R)} C_c(j) \right) \times \frac{1}{N \cdot I_{max}} \\ &= \left(N \cdot 3\,(d_v - 1) + N\,(1 - R) \cdot 3\,(d_c - 2) \right) \times \frac{1}{N} \\ &= 3\,(d_v - 1) + (1 - R) \cdot 3\,(d_c - 2)\,. \end{aligned} \tag{2.22}$$

Hence, the complexity equation of Eq. (2.22) can be reformulated as a function of the VN degree and code rate R, which is

$$\begin{aligned} \overline{C}_{LDPC} &= 3\,(d_v - 1) + (1 - R) \cdot 3\,(d_c - 2) \\ &= 6d_v + 6R - 9. \end{aligned} \tag{2.23}$$

Firstly, similar to Fig. 2.7, Fig. 2.19 quantifies the complexity in terms of the average number of iteration for $(3, 6)$ regular LDPC codes used in our CV-QKD reconciliation

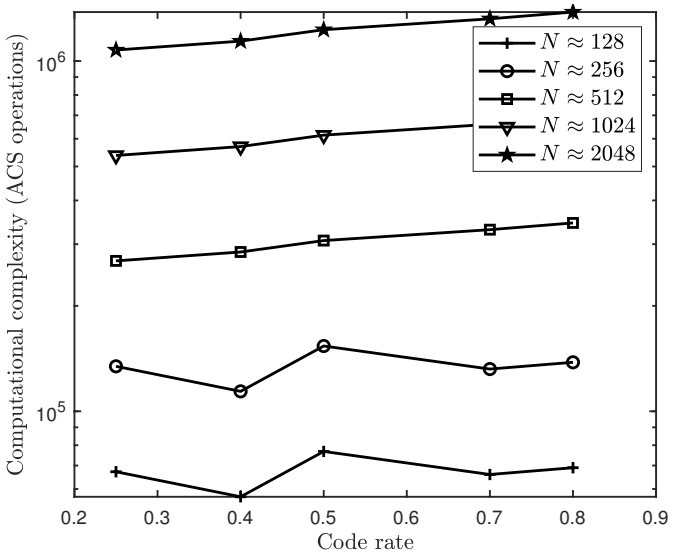


Figure 2.20: The comparison of computational complexity versus coding rate of LDPC codes under different code length setting. The SPA decoding algorithm with $I_{\max} = 50$ is employed.

Table 2.5: Complexity analysis (ACS operations) of LDPC codes with SPA decoding algorithm with $I_{\max} = 50$.

		Complexity	
Code	Code rate R	per bit per iteration	total
LDPC$(3,4,128)$	0.25	10.50	67200
LDPC$(3,4,256)$	0.25	10.50	134400
LDPC$(3,4,512)$	0.25	10.50	268800
LDPC$(3,4,1024)$	0.25	10.50	537600
LDPC$(3,4,2048)$	0.25	10.50	1075200
LDPC$(3,5,100)$	0.40	11.40	57000
LDPC$(3,5,200)$	0.40	11.40	114000
LDPC$(3,5,500)$	0.40	11.40	285000
LDPC$(3,5,1000)$	0.40	11.40	570000
LDPC$(3,5,2000)$	0.40	11.40	1140000
LDPC$(3,6,128)$	0.50	12.00	76800
LDPC$(3,6,256)$	0.50	12.00	153600
LDPC$(3,6,512)$	0.50	12.00	307200
LDPC$(3,6,1024)$	0.50	12.00	614400
LDPC$(3,6,2048)$	0.50	12.00	1228800
LDPC$(3,10,100)$	0.70	13.20	66000
LDPC$(3,10,200)$	0.70	13.20	132000
LDPC$(3,10,500)$	0.70	13.20	330000
LDPC$(3,10,1000)$	0.70	13.20	660000
LDPC$(3,10,2000)$	0.70	13.20	1320000
LDPC$(3,15,100)$	0.80	13.80	69000
LDPC$(3,15,200)$	0.80	13.80	138000
LDPC$(3,15,500)$	0.80	13.80	345000
LDPC$(3,15,1000)$	0.80	13.80	690000
LDPC$(3,15,2000)$	0.80	13.80	1380000

scheme, indicating that the average number of iterations decrease with the improvement of the channel quality. Secondly, based on Eq. (2.23), the computational complexity of the LDPC codes having different parameters is tabulated in Table 2.5. The corresponding computational complexity comparison is portrayed in Fig. 2.20.

2.4.4 Secret Key Rate Analysis

As discussed in Section 2.4.1.2, there are two different reconciliation schemes, namely RR and DR. In light of this, the SKR analysis based on both RR and DR is provided in this section.

2.4.4.1 Secret Key Rate Analysis in RR

The SKR denoted as $R^{\blacktriangleleft}$ for the RR portrayed in Fig. 2.8 using homodyne detection is given by [111]

$$R^{\blacktriangleleft} = I\left(X_A; X_B\right) - \chi\left(X_B; X_E\right), \tag{2.24}$$

where $I\left(X_A; X_B\right)$ is the MI between Alice and Bob, and $\chi\left(X_B; X_E\right)$ is the Holevo information between Bob and Eve.

Firstly, the MI between Alice and Bob can be defined as

$$I\left(X_A; X_B\right) = H\left(X_B\right) - H\left(X_B \mid X_A\right), \tag{2.25}$$

where

$$H\left(X_B\right) = \frac{1}{2}\log_2 V\left(X_B\right) \tag{2.26}$$

is the Shannon entropy and

$$H\left(X_B \mid X_A\right) = \frac{1}{2}\log_2 V\left(X_B \mid X_A\right) \tag{2.27}$$

is known as the conditional Shannon entropy.

Based on the input-output relationship of Eq. (2.13) in Section 2.4.1.1, the variance of X_B in Eq. (2.13) is given by

$$V_B := V\left(X_B\right) = (1-T)W + TV_A. \tag{2.28}$$

Furthermore, the variance of Alice's modes is given by

$$V_A := V\left(X_A\right) = V_S + V_0, \tag{2.29}$$

where V_S is the variance of the initial signal encodings and V_0 is the variance of the vacuum state. Using Eq. (2.25) along with Eq. (2.26) and Eq. (2.27), the MI in Eq. (2.25)

can be formulated as:

$$I\left(X_A : X_B\right) = \frac{1}{2}\log_2\left[\frac{(1-T)W + TV_S + TV_0}{(1-T)W + TV_0}\right] = \frac{1}{2}\log_2\left(1 + \mathrm{SNR}_B\right), \tag{2.30}$$

where SNR_B represents the SNR at Bob's side.

Secondly, the MI between Eve and Bob, which is defined by the Holevo information [126] is expressed as

$$\chi\left(X_B; X_E\right) = S\left(X_E\right) - S\left(X_E \mid X_B\right), \tag{2.31}$$

where $S(\cdot)$ is the von Neumann entropy defined in [59]. The von Neumann entropy of a Gaussian state ρ containing $\mathcal{M}$ modes can be written in terms of its symplectic eigenvalues as follows [127]

$$S\left(\rho\right) = \sum_{m=1}^{\mathcal{M}} G\left(v_m\right), \tag{2.32}$$

where

$$G\left(v\right) = \left(\frac{v+1}{2}\right)\log_2\left(\frac{v+1}{2}\right) - \left(\frac{v-1}{2}\right)\log_2\left(\frac{v-1}{2}\right). \tag{2.33}$$

To elaborate on Eq. (2.33), generally these symplectic eigenvalues can be calculated based on the Covariance Matrix (CM) $\mathbf{V}$ of the Gaussian state using the formula [82]

$$v = \left|i\mathbf{\Omega}\mathbf{V}\right|, \quad v \geq 1, \tag{2.34}$$

where $\mathbf{\Omega}$ defines the symplectic form given by

$$\mathbf{\Omega} := \bigoplus_{m=1}^{M} \boldsymbol{\omega} = \begin{pmatrix} \boldsymbol{\omega} & & \\ & \ddots & \\ & & \boldsymbol{\omega} \end{pmatrix}, \boldsymbol{\omega} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.35}$$

Here $\bigoplus$ is the direct sum indicating the construction of a block-diagonal matrix $\mathbf{\Omega}$ having the same dimensionality as $\mathbf{V}$ by placing $\mathcal{M}$ blocks of $\boldsymbol{\omega}$ diagonally. Eq. (3.9) indicates that first we have to find the eigenvalue of the matrix $i\mathbf{\Omega}\mathbf{V}$ and then take the absolute values. However, in some circumstances, we can simplify the calculation of the eigenvalues. To elaborate further, firstly we consider a generic two-mode CM in the form of

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}. \tag{2.36}$$

Based on [59], the symplectic eigenvalues v_1 and v_2 of $\mathbf{V}$ can be written in the form of [82]

$$v_{1,2} = \sqrt{\frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4\det\mathbf{V}}\right)}, \tag{2.37}$$

where $\det\mathbf{V}$ represents the determinant of the matrix $\mathbf{V}$ and we have

$$\Delta := \det\mathbf{A} + \det\mathbf{B} + 2\det\mathbf{C}. \tag{2.38}$$

In particular, let us consider a CM in the form of

$$\mathbf{V} = \begin{pmatrix} a\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I} \end{pmatrix}, \tag{2.39}$$

where we have

$$\mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.40}$$

which are the two Pauli matrices. Therefore, the symplectic eigenvalues of ρ_{AB} required are given by

$$v_{1,2}^2 = \frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4D^2}\right), \tag{2.41}$$

where we have:

$$\begin{aligned} \Delta &= a^2 + b^2 - 2c^2, \\ D &= ab - c^2. \end{aligned} \tag{2.42}$$

In light of this, back to the Holevo information between Bob and Eve in Eq. (2.31), the von Neumann entropies of $S(X_E) := S(\rho_E)$ and $S(X_E \mid X_B) := S\left(\rho_{E|B}\right)$ can be obtained via calculating the symplectic eigenvalues v of their corresponding CMs, which are $\mathbf{V}_{X_E}$ and $\mathbf{V}_{X_E|X_B}$, respectively. Eve's CM is made up from the two modes $\hat{E}'$ and$\hat{E}''$ and is given by

$$\mathbf{V}_E = \begin{pmatrix} a\mathbf{I}_2 & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I}_2 \end{pmatrix}, \tag{2.43}$$

where $a = (1-T)V + TW$, $b = W$, and $c = \sqrt{T(W^2-1)}$. Then Eve's symplectic spectrum can be determined by using Eq. (3.12) as follows:

$$v_E = \frac{1}{2}\left[\sqrt{(a+W)^2 - 4T(W^2-1)} \pm (a-W)\right]. \tag{2.44}$$

Meanwhile, Eve's conditional CM is defined as [59]

$$\mathbf{V}_{E|B} = \mathbf{V}_E - (V_B)^{-1}\mathbf{C}\Pi\mathbf{C}^T \tag{2.45}$$

where $\mathbf{V}_E$ is defined in Eq. (2.43) and we have

$$\mathbf{\Pi} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{2.46}$$

while $V_B = TV + (1-T)W$ can be obtained via Eq. (2.28). Furthermore, $\mathbf{C}$ in Eq. (2.45) is a 4×2 matrix describing the quantum correlations between Eve's modes $\left\{\hat{E}', \hat{E}''\right\}$ and Bob's output mode X_B and it is defined as

$$\mathbf{C} = \begin{pmatrix} \xi\mathbf{I}_2 \\ \phi\mathbf{Z} \end{pmatrix}, \tag{2.47}$$

where $\xi = -\sqrt{T(1-T)}\,(V-W)$ and $\phi = \sqrt{1-T}\sqrt{W^2-1}$ and we have used $X_B = \sqrt{T}X_A + \sqrt{1-T}E$ and $E' = -\sqrt{1-T}X_A + \sqrt{T}E$. Thereafter, Eve's conditional CM $\mathbf{V}_{E|X_B}$ has the form of

$$\mathbf{V}_{X_E|X_B} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \tag{2.48}$$

where we have:

$$\begin{aligned} \mathbf{A} &= \begin{pmatrix} \frac{VW}{T(V-W)+W} & 0 \\ 0 & (1-T)V+TW \end{pmatrix}, \\ \mathbf{B} &= \begin{pmatrix} \frac{1-T+TWV}{TV+W-TW} & 0 \\ 0 & W \end{pmatrix}, \\ \mathbf{C} &= \begin{pmatrix} \sqrt{T\left(W^2-1\right)}\left[\frac{V}{TV+W-TW}\right] & 0 \\ 0 & -\sqrt{T\left(W^2-1\right)} \end{pmatrix}. \end{aligned} \tag{2.49}$$

Hence, the corresponding symplectic spectra $v_{X_E|X_B}$ of $\mathbf{V}_{X_E|X_B}$ can be calculated via using Eq. (2.37). Upon substituting Eq. (2.30) and Eq. (2.31) into Eq. (2.24), the corresponding $R^{\blacktriangleleft}$ can be obtained.

It may be shown that calculating the Holevo information between Bob and Eve in Eq. (2.31) can be simplified via calculating the Holevo information between Alice and Bob as follows [59]

$$\chi\left(X_B; X_E\right) = S\left(\rho_E\right) - S\left(\rho_{E|B}\right) = S(\rho_{AB}) - S\left(\rho_{A|B}\right). \tag{2.50}$$

Let us assume that the CM related to the information between Alice and Bob has the form of

$$\mathbf{V}_{AB} = \begin{pmatrix} a\mathbf{I}_2 & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I}_2 \end{pmatrix}. \tag{2.51}$$

Therefore, the symplectic eigenvalues of ρ_{AB} required can be obtained via calculating the symplectic eigenvalues $v_{1,2}$ of the CM in Eq. (2.51) with the aid of Eq. (2.41). As for the symplectic eigenvalue of $\rho_{A|B}$, it can be shown that:

$$v_3 = \sqrt{a\left(a - \frac{c^2}{b}\right)}. \tag{2.52}$$

Hence, the Holevo information can be formulated as

$$\chi\left(X_B; X_E\right) = G\left(v_1\right) + G\left(v_2\right) - G\left(v_3\right), \tag{2.53}$$

where v_1, v_2 and v_3 are symplectic eigenvalues. Upon substituting Eq. (2.30) and Eq. (2.53) into Eq. (2.24), the corresponding SKR can be obtained. Note that in this dissertation, the way of calculating the Holevo information in Eq. (2.50) will be adopted to obtain the $R^{\blacktriangleleft}$ in the following Chapters.

2.4.4.2 Secret Key Rate Analysis in DR

The SKR $R^{\blacktriangleright}$ for DR using homodyne detection in Fig. 2.8 is given by [111]

$$R^{\blacktriangleright} = I\left(X_A; X_B\right) - \chi\left(X_A; X_E\right), \tag{2.54}$$

where $I\left(X_A; X_B\right)$ is the same as in Eq. (2.30). As for the Hovelo information between Alice and Eve, it can expressed as

$$\chi\left(X_A; X_E\right) = S\left(X_E\right) - S\left(X_E \mid X_A\right), \tag{2.55}$$

where again the von Neumann entropy of $S\left(X_E\right)$ is the same as in Eq. (2.31), whilst the conditional von Neumann entropy of $S\left(X_E \mid X_A\right)$ can be calculated from its corresponding CM of $\mathbf{V}_{X_E|X_A}$. Specifically, Eve's conditional CM relying on direct reconciliation using homodyne detection can be formulated as

$$\mathbf{V}_{X_E|X_A} = \mathbf{V}_{X_E}\left(V_0, V\right), \tag{2.56}$$

where $\mathbf{V}_{X_E}$ is defined in Eq. (2.43). Using (2.34) the corresponding symplectic spectra $v_{E|X_A}$ is formulated as [111]:

$$v_{X_E|X_A} = \frac{1}{\sqrt{2}}(\sqrt{\mid F \pm \sqrt{G} \mid}), \tag{2.57}$$

where we have:

$$\begin{aligned} F = {} & VV_0 + T\left[2 + (T-2)VV_0\right] - TW(T-1)\left(V + V_0\right) \\ & + W^2(T-1)^2, \end{aligned} \tag{2.58}$$

and

$$\begin{aligned} G = {} & (T-1)^2\left[T^2(V-W)^2\left(V_0-W\right)^2 + \left(-V_0V + W^2\right)^2\right. \\ & \left. +2T(V-W)\left(W-V_0\right)\left(-2 + VV_0 + W^2\right)\right]. \end{aligned} \tag{2.59}$$

Upon substituting Eq. (2.30) and Eq. (2.55) into Eq. (2.54), the corresponding $R^{\blacktriangleright}$ can be obtained.

2.4.4.3 SKR Analysis of LDPC-coded RR

The SKR in the ideal case where the post-processing is perfectly conducted, is defined as [59]

$$K_{\text{ideal}} = I_{A,B} - \chi_{B,E}, \tag{2.60}$$

which is the same as in Eq. (2.24). Specifically, $I_{AB} \triangleq I\left(X_A; X_B\right)$ is the classical MI between Alice and Bob based on their shared correlated data, and $\chi_{BE} \triangleq \chi\left(X_B; X_E\right)$ represents the Holevo information [59] that Eve can extract from the information of

Bob. On the other hand, the SKR considers a realistic imperfect reconciliation process can be defined as

$$K_{\text{practical}} = (1 - P_B)\left(\beta I_{A,B} - \chi_{B,E}\right), \tag{2.61}$$

where P_B represents the BLER in the reconciliation step. As for $\beta \in [0,1]$, it represents the reconciliation efficiency, which is defined as [59, 74]

$$\beta = \frac{R}{C} = \frac{R}{0.5\log_2(1+\text{SNR})}, \tag{2.62}$$

where R represents the transmission rate, and C is referred to as the one-dimensional Shannon capacity [108, 128], which is given by the MI as follows [65]:

$$C = I_{AB} = \frac{1}{2}\log_2(1+\text{SNR}) = \frac{1}{2}\log_2\left(\frac{V+\xi_{\text{total}}}{1+\xi_{\text{total}}}\right), \tag{2.63}$$

where we have $V_A = V_s + 1$ and V_s is Alice's modulation variance[7], while ξ_{total} is the total amount of noise between Alice and Bob, which can be expressed as

$$\xi_{\text{total}} = \xi_{\text{line}} + \frac{\xi_{\text{det}}}{T}, \tag{2.64}$$

where $\xi_{\text{det}} = \frac{1+v_{el}}{\eta} - 1$ is the homodyne detector's noise, and v_{el} stands for the electric noise, while η represents the detection efficiency. Furthermore, $\xi_{\text{line}} = \left(\frac{1}{T} - 1\right) + \xi_{\text{ch}}$ represents the channel noise from the sender Alice, where T represents the path loss and ξ_{ch} is the excess noise [111] (i.e. imperfect modulation noise, Raman noise, phase-recovery noise, etc.). Assuming a single-mode fiber having an attenuation of $\alpha_{\text{fibre}} = 0.2$ dB/km, the distance-dependent path loss of such a channel is $T = 10^{-\alpha_{\text{fibre}}\mathfrak{L}/10}$, where $\mathfrak{L}$ denotes the distance between the two parties.

Therefore, the variance of Bob's received signal is

$$V_B = \eta T\left(V_A + \xi_{\text{total}}\right). \tag{2.65}$$

In light of this, the CM related to the information between Alice and Bob, - namely the mode of ρ_{AB} after transmission through the QuC - can be expressed as

$$\begin{aligned}\mathbf{V}_{AB} &= \begin{pmatrix} V_A\mathbf{I}_2 & \sqrt{\eta T\left(V_A^2-1\right)}\mathbf{Z} \\ \sqrt{\eta T\left(V_A^2-1\right)}\mathbf{Z} & \eta T\left(V_A+\xi_{\text{total}}\right)\mathbf{I}_2 \end{pmatrix} \\ &= \begin{pmatrix} a\mathbf{I}_2 & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I}_2 \end{pmatrix},\end{aligned} \tag{2.66}$$

Hence, the symplectic eigenvalues of ρ_{AB} required can be obtained by Eq. (2.41). As for the symplectic eigenvalue of $\rho_{A|B}$, it can be obtained by Eq. (2.52). Hence, the

[7]The modulation variance here represents the variance of Gaussian signals used in the modulator of CV-QKD.

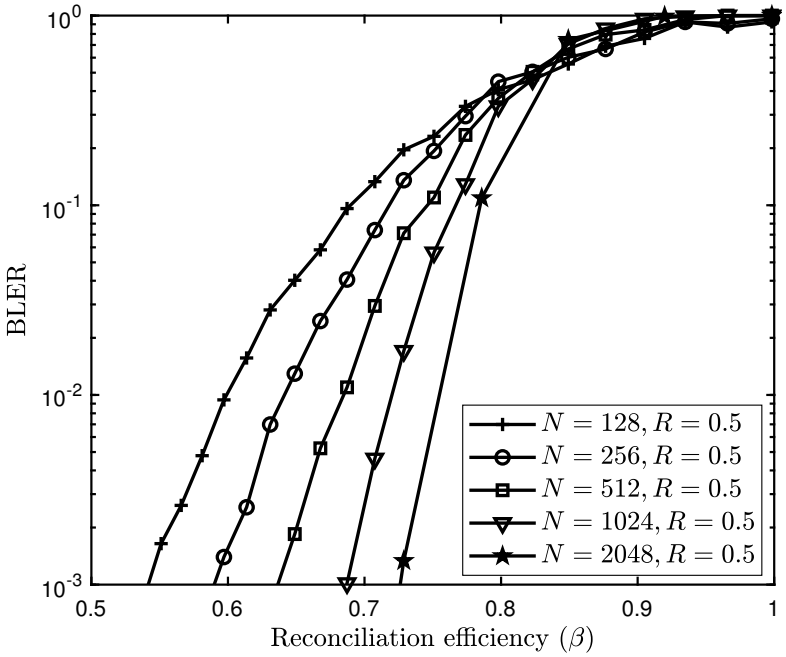


Figure 2.21: BLER versus reconciliation efficiency β of (3,6) regular LDPC codes used in CV-QKD. The corresponding performance of BLER versus SNR is demonstrated in Fig. 2.17(a).

Table 2.6: Reconciliation efficiencies βs of (3,6) regular LDPC-coded reconciliation scheme in CV-QKD at different BLER thresholds, which are β_1 at BLER equals to 0.1 and β_2 at BLER equals to 0.2, followed by the corresponding SNRs.

Code rate	Block length	BLER=0.1		BLER=0.2	
		SNR_1 (dB)	$\beta_1(\%)$	SNR_2 (dB)	$\beta_2(\%)$
0.5	128	2.38	69	2.09	72
0.5	256	2.17	71	1.90	74
0.5	512	1.97	73	1.73	76
0.5	1024	1.73	76	1.55	78
0.5	2048	1.46	79	1.40	80

Holevo information can be calculated by Eq. (2.53). Thereafter, the corresponding SKR in Eq. (2.61) can be obtained.

Fig. 2.21 portrays the BLER versus reconciliation efficiency β based on the BLER versus SNR associated with different LDPC codes in Fig. 2.17, where the corresponding reconciliation efficiencies are calculated based on Eq. (2.62). It is demonstrated that there is a trade-off between the BLER and the reconciliation efficiency. To elaborate further, for the reconciliation scheme associated with a specific LDPC code, BLER increases with the reconciliation efficiency. Furthermore, given the same BLER level, the reconciliation efficiency of a larger block is higher than that of a shorter block. For example, the reconciliation efficiency for $N_{\text{FEC}} = 2048$ is higher than that for $N_{\text{FEC}} = 128$ at BLER of 10^{-1}. Hence, both the BLER and reconciliation efficiency affect the final secret key rate. In the light of this, the reconciliation efficiency β of the family of (3,6)

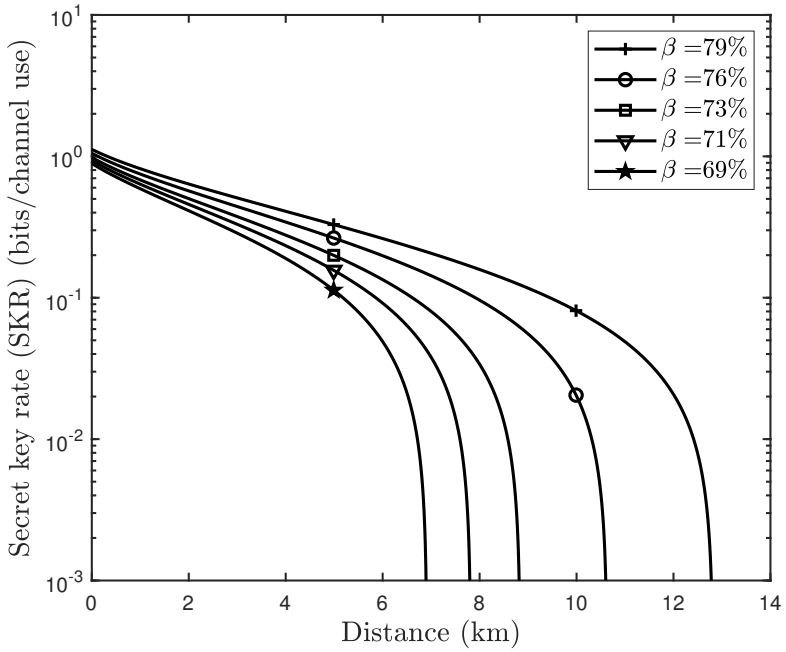


Figure 2.22: The effective secret key rate $K_{\text{practical}}$ analysis that takes the LDPC-coded reconciliation scheme into account versus distance under different reconciliation efficiencies. The values of different reconciliation efficiencies are gleaned from Table 2.6 of β_1 at the threshold of BLER equals to 0.1, which are 69%,71%,73%,76% and 79%. The other parameters are as follows: the modulation variance $V_A = 35$ SNU, excess noise is $T_{ch} = 0.002$ SNU, the efficiency of the homodyne detector is $\eta = 0.98$, the standard loss coefficient of a single-mode optical fiber is $\alpha = 0.2$ dB/km, and the electric noise is $v_{el} = 0.01$ SNU.

regular LDPC codes is tabulated in Table 2.6 at BLER= 0.1 and 0.2, together with the corresponding SNRs.

Fig. 2.22 characterizes the performance of the practical SKR calculated via Eq. (2.61) versus distance, where a practical reconciliation scheme that takes the reconciliation efficiency into account is considered. The reconciliation efficiencies of LDPC codes at different code lengths at BLER $= 0.1$ and 0.2 are gleaned from Table. 2.6. It is demonstrated in Fig. 2.22 that both the SKR and the maximum secure transmission distance will increase with the reconciliation efficiency β. Accordingly, a longer LDPC code provides a higher SKR and/or longer secure transmission distance, since it has a higher reconciliation efficiency. Furthermore, it is observed in Fig. 2.22 that the BLER will also influence the SKR.

2.5 SISO THz CV-QKD

In this section, the application of SISO CV-QKD in THz bands is reviewed based on the recent literature.

2.5.1 System Model

The basic system model of THz CV-QKD is similar to the one described in Section 2.4.1.1, which is commonly used in optical CV-QKD research. However, there are some differences between them. To elaborate further, firstly, the thermal noise in the THz band is higher than that in the optical band, which is seen by comparing Eq. (2.15) and Fig. 2.10. Secondly, the channel model commonly used in optical CV-QKD research is based on the attenuation in fibre channels, namely on $T = 10^{-\alpha_{\text{fibre}}\mathfrak{L}/10}$, where $\mathfrak{L}$ denotes the distance between the two parties and α_{fibre} is the distance-dependent attenuation in fibre channels. By contrast, there are three popular channel models in the THz CV-QKD literature, which are summarized in Section 2.5.2.

2.5.2 Channel Model

2.5.2.1 The Free-Space Path Loss Model

The commonly used Free-Space Path Loss (FSPL) model can be expressed as [129]

$$T_{\text{FSPL}} = \left(\frac{\lambda}{4\pi\mathfrak{L}}\right)^2 G_T G_R, \tag{2.67}$$

where G_T and G_R represent the transmitter and receiver antenna gains, respectively, λ is the wavelength in meter (m) and $\mathfrak{L}$ is the transmission distance from the Base Station (BS) antenna in meter (m). This model is commonly used when considering the path loss in a wide range of frequency bands. However, the effects of FSPL are typically neglected, because power control can be used to compensate it.

2.5.2.2 Atmospheric Loss-based Channel Model

When considering short-distance indoor scenarios, we mainly consider the factors of small miscellaneous loss and atmospheric molecular absorption loss. Therefore, the Atmospheric Loss (AL)-based channel model for the transmissivity T_{AL} can be expressed as [24, 79, 130]

$$T_{\text{AL}} = 10^{-\alpha_f \mathfrak{L}/10}. \tag{2.68}$$

Since different gas molecules have extremely different effects on the electromagnetic waves of different bands, for the THz bands, O2 and H2O(g) are the most important absorption components. The atmospheric absorption coefficient α_f at frequency f is given by

$$\alpha_f = \alpha_f\left(O_2\right) + \alpha_f\left[H_2O(g)\right]. \tag{2.69}$$

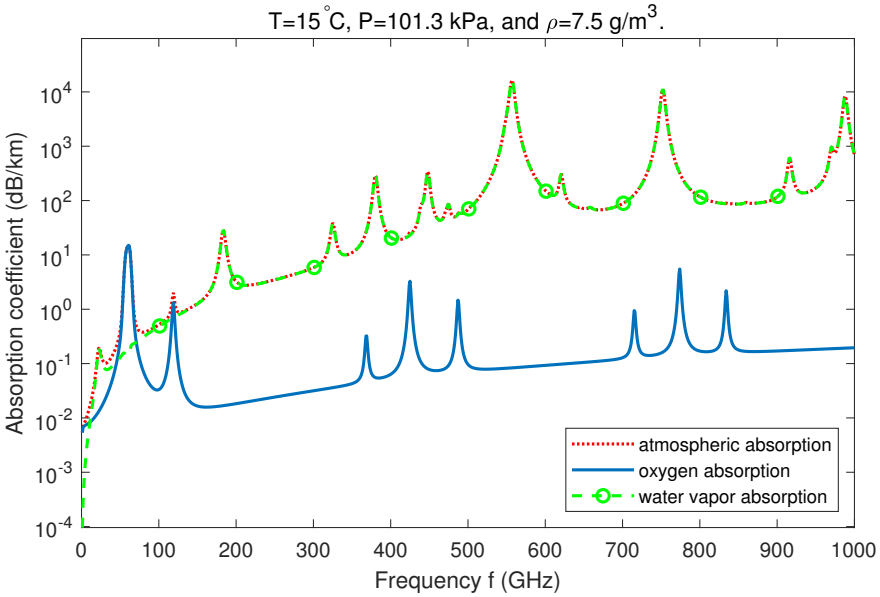


Figure 2.23: Oxygen absorption coefficient, water vapour coefficient, and atmospheric absorption coefficient in the frequency range of 0.1 THz – 1 THz [130, 131].

According to the method described in the International Telecommunication Union (ITU) recommendation P.676-10 [131], we calculate the atmospheric attenuation at frequencies spanning from 0.1 THz to 1 THz. The parameters take the following typical values: the water vapour density is 7.53 g/m^3 and the atmospheric pressure P is 101.3 kPa. The results evaluated from Eq. (2.69) are shown in Fig. 2.23. Observe that the water vapour in the atmosphere plays a major role in the attenuation of THz waves, and that there are some spectral windows associated with low attenuation. The commonly used spectral windows are 300 GHz, 350 GHz, 410 GHz, 670 GHz, and 850 GHz, and the absorption coefficient of these are 3 dB/km, 7 dB/km, 12 dB/km, 38 dB/km, and 51 dB/km, respectively [130], which are shown in Table I of [130].

2.5.2.3 Inter-Satellite-based Channel Model

The atmospheric turbulence potentially causes scintillation, absorption and beam wandering effects, giving rise to severe fading and degradation of quantum applications between ground stations and satellites. However, in the scenario of InTer-SateLlite (ITSL) communication there is negligible absorption, and the beam wandering effect can be ignored, thereby enabling us to approximate the channel as having a fixed attenuation solely due to diffraction effects. The corresponding transmissivity T_{ITSL} is given by [24, 130]

$$T_{\text{ITSL}} = 1 - \exp\left[-2r_a^2/w^2(\mathfrak{L})\right], \tag{2.70}$$

where r_a denotes the radius of the receiving aperture, $\mathfrak{L}$ is the propagation distance of the Gaussian beam, and $w(\mathfrak{L})$ denotes the beam radius at distance $\mathfrak{L}$. Under the

Gaussian approximation, given the minimum of the beam radius (the beam-waist), we can calculate the beam radius at a certain distance as [24, 130]

$$w(\mathfrak{L}) = w_0\sqrt{1+\left(\lambda\mathfrak{L}/\pi w_0^2\right)^2}, \tag{2.71}$$

where w_0 denotes the radius of the beam waist and λ is the wavelength of the beam.

2.5.3 Security Analysis

The security analysis is the same as illustrated in Section 2.4.4.

2.5.4 Performance Analysis

Table 2.7: Absorption coefficient under different frequencies [79, 83, 130].

Frequency	Absorption coefficient α_f (dB/km)
100 GHz	0.6
200 GHz	1.2
300 GHz	3
10 THz	10^3
15-34 THz	50
40-55 THz	1.77×10^3

In this section, the SKR versus distance trends associated with different parameters, such as the frequency, and the type of channel model are investigated. Different frequencies associated with their corresponding absorption coefficients are characterized in Table 2.7. It can be seen from Table 2.7 that with the increase of the frequency considered, the corresponding absorption coefficient tends to increase, but there is a relatively low absorption coefficient of 50 dB/km between 15 THz and 34 THz. Moreover, the absorption coefficients of the frequency bands spanning from 1 GHz to 1000 GHz are seen in Fig. 2.23 [132]. However, the higher frequencies listed in Table 2.7 are not characterized in this figure.

Fig. 2.24 portrays the SKR versus distance associated with different frequencies in the AL-based channel model given in Eq. (2.68). Basically, the performance can be categorized into two sets in terms of the frequency. Specifically, the first set includes the frequencies of 100 GHz, 200 GHz and 300 GHz, while the second set includes the the frequencies of 10 THz, 15 THz, 30 THz and 40 THz. For the first set, it is demonstrated that the system operating at 200 GHz provides the longest secure distance, followed by the system at 100 GHz, while the one at 300 GHz performs the worst. This is unexpected, since the absorption coefficients increase with the increase of frequency from 100 GHz to 200 GHz and 300 GHz. However, the actual trend observed is governed

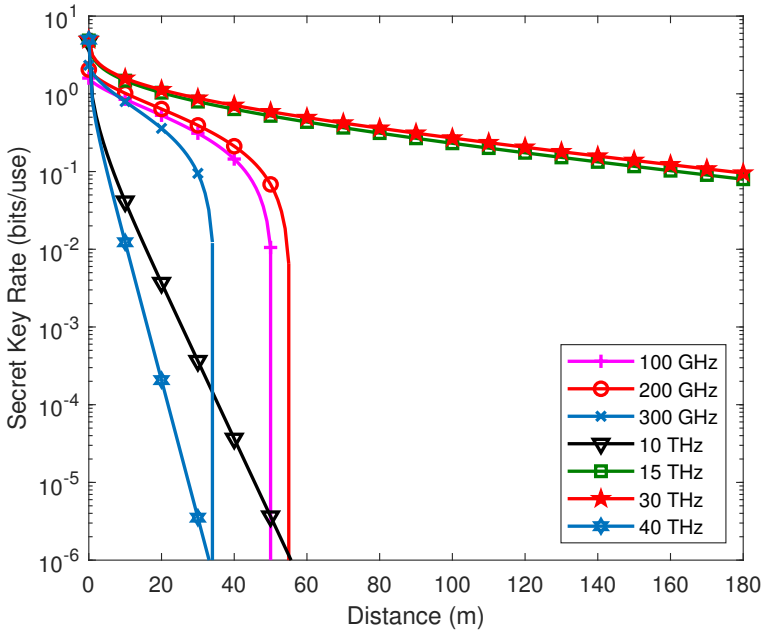


Figure 2.24: Secrete key rate versus distance with the AL channel model under different frequencies. The absorption coefficients in different frequencies are listed in Table 2.7. Other simulation parameters are : $V_s = 10^3$ SNU, $W = 1$ SNU, $T_e = 296$ K.

by the interplay of two main factors, namely due to the effect of the absorption coefficient and of the variance of thermal noise level. To elaborate further, the smaller the absorption coefficient, the longer the secure distance. However, the lower the frequency, the higher the thermal noise variance, as illustrated in Fig. 2.10. Therefore, the SKR versus distance performance needs to take the combined effect of both the absorption coefficient and the thermal noise variance into account. In light of this, the system operating at 15 THz and 30 THz performs the best in the second set, followed by the system at 10 THz. The system operating at 40 THz performs the worst. This is because the absorption coefficient at 15 THz and 30 THz is lower than that at 10 THz and 40 THz. Furthermore, the thermal noise levels of all of them are similar, as shown in Fig. 2.10. Therefore, the SKR versus distance performance is dominated by the effect of the absorption coefficient in the second set of frequencies.

2.6 MIMO THz CV-QKD

Firstly, the MIMO THz CV-QKD system is introduced based on [83–85], which includes the coherent signal model, the original channel model and the detection method. This is followed by the security analysis of MIMO THz CV-QKD systems. Finally, some reproduced and some extension results are discussed.

2.6.1 System Model

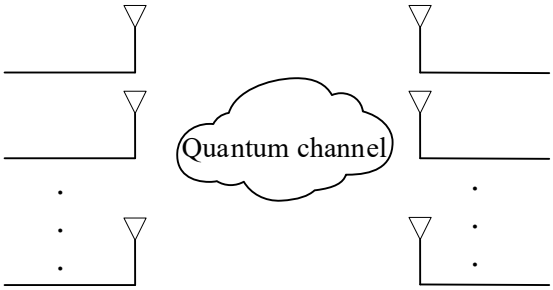


Figure 2.25: System diagram of MIMO-aided QKD [83].

We consider a MIMO THz CV-QKD system, where Alice and Bob aim to establish a secret key sharing process between them. It is assumed Alice's transmitter has N_{Tx} antennas, while Bob's receiver is equipped with N_{Rx} antennas. As seen from Fig. 2.25, the system diagram of MIMO QKD wireless transmission is reminiscent of a classical MIMO system. As for the form of signals, coherent quantum states are utilized to accomplish transmission from each antenna. We consider a Gaussian modulated CV-QKD scheme, where Alice first generates two independent Gaussian distributed random vectors, denoted as $\mathbf{q}_A, \mathbf{p}_A \sim \mathcal{N}(\mathbf{0}_{N_{Tx}\times 1}, V_s\mathbf{I}_{N_{Tx}})$, where V_s is the variance of the initial signal encoding, also referred to as the modulation variance. Then Alice uses the random vectors $\mathbf{q}_A, \mathbf{p}_A$ to generate N_{Tx} coherent states $|\psi_i\rangle$ with $\psi_i = q_{A,i} + jp_{A,i}, \forall i = 1, 2, \ldots, N_{Tx}$ and then transmits them through the QuC to the receiver Bob.

2.6.2 Channel Model

Let $\mathbf{H} \in {}^{N_{Rx}\times N_{Tx}}$ be the channel between Alice and Bob, which is modelled as [83]

$$\mathbf{H} = \sum_{l=0}^{L-1} \sqrt{\gamma_l} e^{j2\pi f_c \tau_l} \mathbf{a}_{Rx}(\theta_{Rx,l})\, \mathbf{a}_{Rx}(\theta_{Rx,l}), \tag{2.72}$$

where fc is the carrier frequency, L is the total number of multipath components, and τ_l, γ_l are the propagation delay and path loss of the lth path, respectively. Furthermore, $\mathbf{a}_{Rx}(\theta_{Rx,l})$ is the Angle of Arrival (AoA) of the lth path at Bob's Uniform Linear Array (ULA) and $\mathbf{a}_{Rx}(\theta_{Rx,l})$ is the Angle of Departure (AoD) of the lth path emerging from Alice's ULA. We note that the component associated with $l = 0$ in Eq. (2.72) corresponds to the LoS path, while the components associated with $L > 0$ model the Non-Line of Sight (NLoS) components. Furthermore, the path loss that combines the

effects of both the FSPL and that of AL, can be modelled as [83]

$$\gamma_l = \begin{cases} \left(\frac{\lambda}{4\pi\mathfrak{L}_l}\right)^2 G_T G_R 10^{-0.1\alpha\mathfrak{L}_l}, & l = 0 \text{ (LoS)} \\ \delta r_l \left(\frac{\lambda}{4\pi\mathfrak{L}_l}\right)^2 G_T G_R 10^{-0.1\alpha\mathfrak{L}_l}, & l = 1, 2, \ldots, L-1 \text{ (NLoS)} \end{cases}, \tag{2.73}$$

where $\mathfrak{L}_l$ is the shortest path length of the lth path between Alice and Bob, α (in dB/Km) is the atmospheric absorption loss, δ is the Rayleigh roughness factor, r_l is the Fresnel reflection coefficient of the lth path, and G_T, G_R are the antenna gains of Alice and Bob's ULA respectively, given by

$$G_T = N_T G_a,\ G_R = N_R G_a, \tag{2.74}$$

where G_a is the gain of each antenna element. Note that since the number of scattered paths at THz frequencies is limited, the number of paths may be limited to $L = 3$ [133]. Moreover, as for the power sharing between the LoS and NLoS paths, it depends on the scenarios considered. Specifically, the power of the NLoS path is lower by about 10 dB to 20 dB than that of the LoS path, provided that there is no LoS blockage [134]. On the other hand, it has also been demonstrated in [135, 136] that both blockage and NLoS propagation substantially affect THz reception. More specifically, the authors of [135] claim that an eavesdropper can intercept LoS signal transmission, even if they are transmitted at high frequencies with the aid of narrow beams. As for [136], the channel characterization of THz signals demonstrated that the Ricean K factor that represents the ratio between LoS and NLoS powers may become as low as -13.6 dB, indicating that the LoS power is about 20 times lower than the NLoS power.

2.6.3 Detection

In this section, the Sigular Value Decomposition (SVD) based transmit-receive beamforming scheme is reviewed, which generalized the SISO beam splitter based channel model for the THz MIMO channel. Then the transmit beamforming and receiver combining techniques are highlighted, followed by the homodyne detection adopted for detection (measurement).

Let $\mathbf{H} = \mathbf{U}\Sigma\mathbf{V}^H$ be the SVD of the channel matrix associated with $\mathbf{U} \in \mathcal{C}^{N_{Rx}\times N_{Rx}}$ and $\mathbf{V} \in \mathcal{C}^{N_{Tx}\times N_{Tx}}$, which are unitary matrices. Furthermore, we have

$$\mathbf{\Sigma} = \begin{bmatrix} \text{diag}\left\{\sqrt{\eta_1}, \ldots, \sqrt{\eta_r}\right\} & \mathbf{0}_{r\times(N_{Tx}-r)} \\ \mathbf{0}_{(N_{Rx}-r)\times r} & \mathbf{0}_{(N_{Rx}-r)\times(N_{Tx}-r)} \end{bmatrix}, \tag{2.75}$$

where r is the rank of the channel matrix and $\sqrt{\eta_1}, \ldots, \sqrt{\eta_r}$ are the r non-zero singular values of $\mathbf{H}$. We consider an optimal eavesdropping attack, where Eve has full control over the channel and introduces an entangled Gaussian attack, which was introduced

in Section 2.4.1.1. The received signal at Bob is therefore given by [83]

$$\hat{\mathbf{a}}_B = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^H\hat{\mathbf{a}}_A + \mathbf{U}\mathbf{S}\hat{\mathbf{a}}_E, \tag{2.76}$$

where $\hat{\mathbf{a}}_B = [\hat{a}_{B,1}, \ldots, \hat{a}_{B,N_{Rx}}]^T$, $\hat{\mathbf{a}}_A = [\hat{a}_{A,1}, \ldots, \hat{a}_{A,N_{Tx}}]^T$ denote the vectors of received mode at Bob and the mode transmitted from Alice, respectively. Furthermore, the vector $\hat{\mathbf{a}}_E = [\hat{a}_{E,1}, \ldots, \hat{a}_{E,N_t}]^{Tx}$ represents the Gaussian mode injected by Eve, and $\mathbf{S}$ is a diagonal matrix given by [83]

$$\mathbf{S} = \begin{bmatrix} \text{diag}\left\{\sqrt{1-\eta_1}, \ldots, \sqrt{1-\eta_r}\right\} & \mathbf{0}_{r\times(N_{Tx}-r)} \\ \mathbf{0}_{(N_{Rx}-r)\times r} & \mathbf{1}_{(N_{Rx}-r)\times(N_{Tx}-r)} \end{bmatrix}. \tag{2.77}$$

Next, it is assumed that Alice and Bob have perfect knowledge of the channel $\mathbf{H}$. Alice thereafter can perform transmit beamforming by multiplying $\hat{\mathbf{a}}_A$ by the matrix $\mathbf{V}$. Meanwhile, Bob performs receiver combining by using $\mathbf{U}^H$ at his end after receiving the signal from the channel. Therefore, the signal received by Bob can be expressed as [83]

$$\hat{\mathbf{a}}_B = \mathbf{U}^H\mathbf{H}\mathbf{V}\hat{\mathbf{a}}_A + \mathbf{U}^H\mathbf{U}\mathbf{S}\hat{\mathbf{a}}_E. \tag{2.78}$$

With the aid of the SVD of $\mathbf{H}$, the effective channel between Alice and Bob is decomposed into r parallel SISO channels with the input and output relationship given by

$$\hat{a}_{B,i} = \sqrt{T_i}\hat{a}_{A,i} + \sqrt{1-T_i}\hat{a}_{E,i}, \quad i = 1, 2, \ldots, r, \tag{2.79}$$

where T_i is the i-th non-zero eigenvalue of $\mathbf{H}^H\mathbf{H}$ corresponding to the non-zero sigular value of $\mathbf{H}$. For each of the r received modes, Bob applies homodyne measurement to one of the randomly chosen quadratures, namely to the $\hat{q}$ or the $\hat{p}$ quadrature. After the measurement, the input-output relationship of the i-th parallel channel between Alice and Bob is given by a generic quantum channel associated with transmittance T_i,

$$\hat{X}_{B,i} = \sqrt{T_i}\hat{X}_{A,i} + \sqrt{1-T_i}\hat{X}_{E,i}, \quad i = 1, 2, \ldots, r. \tag{2.80}$$

By contrast, the input-output relationship of Eve's ancilla mode is

$$\hat{X}_{E',i} = -\sqrt{1-T_i}\hat{X}_{A,i} + \sqrt{T_i}\hat{X}_{E,i}, i = 1, 2, \ldots, r, \tag{2.81}$$

where $\hat{X}_{B,i}$ is the received quadrature, which is measured at Bob, $\hat{X}_{A,i}$ is the quadrature component transmitted by Alice, $\hat{X}_{E,i}$ is the excess noise quadrature component introduced by Eve, and $\hat{X}_{E',i}$ is the ancilla quadrature component stored in Eve's quantum memory for the i-th parallel channel. Note that the variable $\hat{X}$ corresponds to one of the two quadratures $\{\hat{q}, \hat{p}\}$, so that we have$\hat{X} \in \{\hat{q}, \hat{p}\}$, which is held for $\hat{X}_{A,i}$, $\hat{X}_{B,i}$, $\hat{X}_{E,i}$ and $\hat{X}_{E',i}$. The variance of Alice's transmitted mode is $V\left(\hat{X}_{A,i}\right) := V_A = V_s + V_0$, where V_s is the variance of the initial Gaussian signal and V_0 is the variance of the vacuum

state, while $V\left(\hat{X}_{E,i}\right) := V_E = W$ is the variance of the excess noise injected by Eve. The variance of the vacuum state is the same in Eq. (2.15). Finally, the variance of the i-th received mode at Bob is given by

$$V\left(\hat{X}_{B,i}\right) = T_i V_a + (1 - T_i) W. \tag{2.82}$$

2.6.4 Security Analysis

As discussed in Section 2.6.3, the MIMO channel can be decomposed into several parallel SISO channels with the aid of the SVD of the channel. Therefore, it is straightforward to calculate the SKR in MIMO CV-QKD by using the summation of the SKR of each equivalent SISO channel. On the other hand, an approximation of the SKR of MIMO CV-QKD was proposed in [83] based on the condition that the variance V_s of the modulation is much greater than that of the vacuum noise. Hence, the approximation of the RR-based SKR in MIMO CV-QKD is reviewed in this section.

2.6.4.1 Approximation of the SKR in MIMO CV-QKD

The overall SKR of the MIMO CV-QKD system is given by

$$R^{\blacktriangleleft}_{\text{MIMO}} = \sum_{i=1}^{r} R_i^{\blacktriangleleft}, \tag{2.83}$$

where R_i denotes the SKR of each equivalent SISO channel associated with $i = 0, 1, ..., r$. Therefore, the RR based SKR can be expressed as

$$R_i^{\blacktriangleleft} = I\left(X_{A,i}; X_{B,i}\right) - \chi\left(X_{B,i}; X_{E,i}\right), i = 1, \ldots, r, \tag{2.84}$$

where $I\left(X_{A,i}; X_{B,i}\right)$ is the classical MI between Alice and Bob, and $I\left(X_{B,i}; X_{E,i}\right)$ is Eve's accessible information with respect to Bob's measured variables $X_{B,i}$ for the i-th parallel channel. The MI between Alice and Bob for the i-th pair of variables is given by

$$I\left(X_{A,i}; X_{B,i}\right) = \frac{1}{2} \log_2 \left[1 + \frac{T_i V_s}{\Lambda_i\left(V_0, W\right)}\right], \tag{2.85}$$

where we define $\Lambda_i(x, y) \triangleq T_i x + (1 - T_i) y$. Furthermore, the maximum amount of information that Eve can extract from the i-th parallel channel is characterized by the Holevo information as [83]

$$\begin{aligned} \chi\left(X_{B,i}; X_{E,i}\right) &= S\left(X_{E,i}\right) - S\left(X_{E,i} \mid X_{B,i}\right) \\ &= G\left(v_1^i\right) + G\left(v_2^i\right) - \left(G\left(v_3^i\right) + G\left(v_4^i\right)\right), \end{aligned} \tag{2.86}$$

where $S\left(X_{E,i}\right)$ and $S\left(X_{E,i} \mid X_{B,i}\right)$ denote the von Neumann entropy of Eve's state and

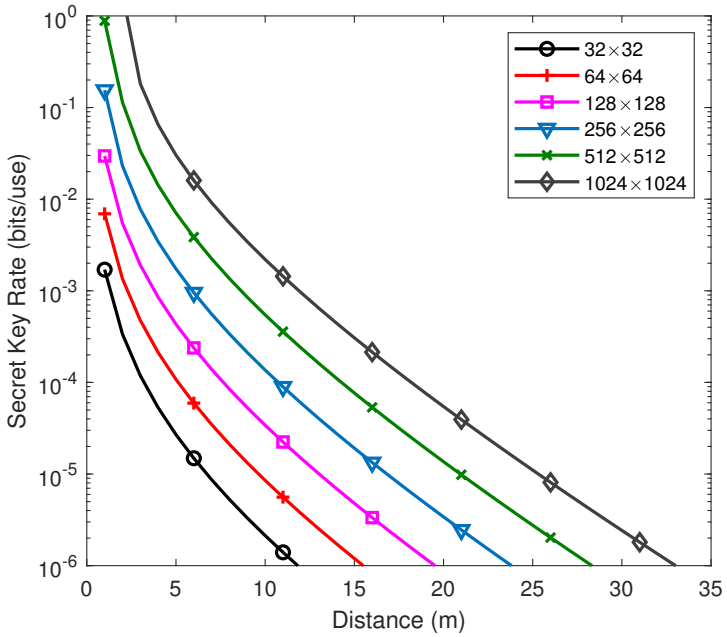


Figure 2.26: Secret key rate versus distance under different MIMO dimensions [83]. The simulation parameters are : $f = 10$ THz with $\alpha = 10^3$ dB/km, $V_s = 10^3$ SNU, $W = 1$ SNU, $T_e = 296$ K, and the antenna gain is $G_a = 30$ dBi. Note that, it is assumed that the reconciliation is perfect, which gives $\beta = 100\%$.

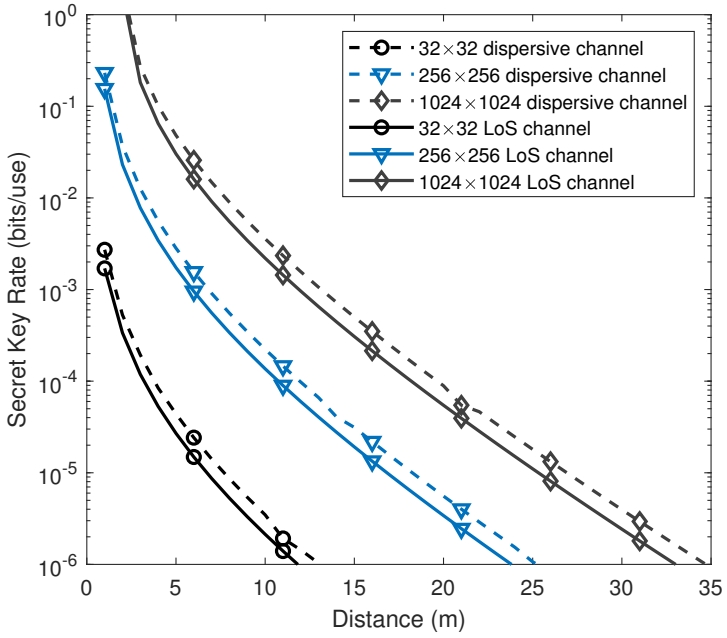


Figure 2.27: Comparison of secret key rate versus distance in LoS and dispersive channel under different MIMO configurations. Here, only two NLoS path is considered due to limited scatterers in terahertz channel. And the power of the NLoS path is 5 dB lower than that of LoS path. Other parameters are the same as that in Fig. 2.26

the conditional von Neumann entropy of Eve's state given $X_{B,i}$, respectively. These can be obtained by calculating the symplectic eigenvalues $v_k^i, k = 1,2,3,4$ of the CM of Eve's state for the i-th parallel channel. Moreover, the function $G(\cdot)$ in Eq. (2.86) is defined in Eq. (2.33). It is assumed in [83] that the variance V_s of the modulation is much higher than that of the vacuum noise. The approximate result therefore can be formulated as [83]

$$R_{\text{MIMO}}^{\blacktriangleleft} \approx \sum_{i=1}^{r} \left\{ \frac{1}{2}\log_2\left[1+\frac{T_i V_s}{\Lambda_i\left(V_0, W\right)}\right] - G\left(\Lambda_i\left(W, V_a\right)\right) - G(W) + G\left(\sqrt{\frac{V_a W \Lambda_i\left(W, V_a\right)}{\Lambda_i\left(V_a, W\right)}}\right) + G\left(\sqrt{\frac{W \Lambda_i\left(W V_a, 1\right)}{\Lambda_i\left(V_a, W\right)}}\right) \right\}. \tag{2.87}$$

Based on Eq. (2.87), it is concluded that the MIMO scheme is capable of providing a multiplexing gain of r, since $R_{\text{MIMO}}^{\blacktriangleleft}$ is a sum of the SKR of r parallel SISO channels.

2.6.5 Performance Analysis

In this section, the performance comparison of the SKR versus distance associated with different MIMO dimensions in [83] is conducted, which is followed by our further comparison that takes the NLoS components into account.

Fig. 2.26 portrays our performance comparison of the SKR versus distance associated with different MIMO dimensions varying from 32×32 to 1024×1024, where only the LoS path is considered. Firstly, it is demonstrated that the SKR will decrease with the increase of distance, because the transmissivity decreases with the increase of distance. Secondly, the SKR of the larger MIMO size of 1024×1024 is notably higher than that of a smaller MIMO size, i.e. 32×32, since a large MIMO provides higher beamforming gain, as detailed in Section 2.6.4.

As a further investigation, Fig. 2.27 characterizes the SKR versus distance performance associated with different MIMO dimensions, where $L = 2$ NLoS paths are considered due to the limited number of scatterers in THz channels. The power of the NLoS is set to be 5 dB lower than that of the LoS path. It is demonstrated in Fig. 2.27 that both the SKR and the maximum secure transmission distance are improved by adding these two NLoS components. Nonetheless, the performance improvement brought about by these two NLoS paths is not pronounced, which is because the power of these NLoS paths is low.

Fig. 2.28 portrays the SKR versus distance associated with 10 THz, 15 THz and 30 THz. Moreover, the corresponding absorption coefficients are $\alpha_f = 10^3$ dB/km at 10 THz, and $\alpha_f = 50$ dB/km at 15 THz and 30 THz. Firstly, it is demonstrated that the maximum secure distance will increase with the decrease of absorption coefficient, as evidenced by comparing the maximum secure distance at 10 THz and that at 15 THz and

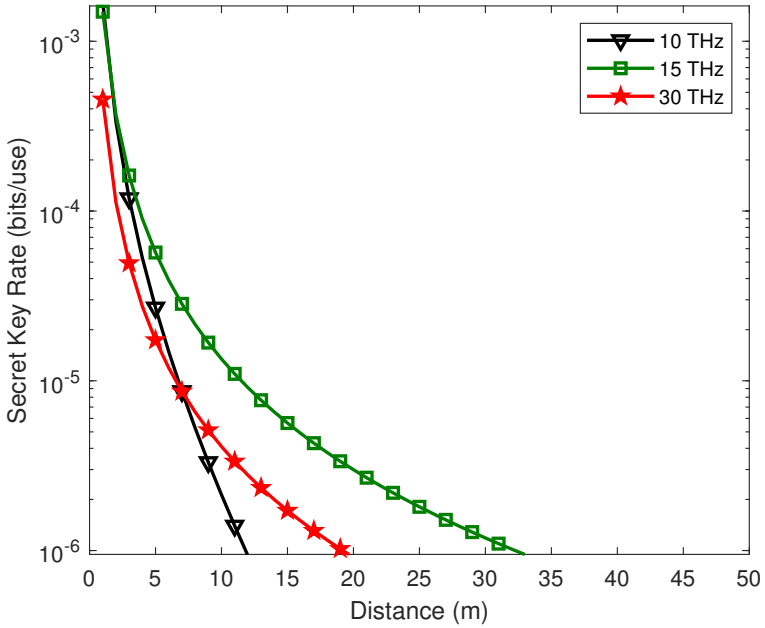


Figure 2.28: Secrete key rate versus distance associated with 10 THz, 15 THz and 30 THz, while the MIMO size is 32×32. The absorption coefficients at different frequencies are listed in Table 2.7. Other simulation parameters are : $V_s = 10^3$ SNU, $W = 1$ SNU, $T_e = 296$ K.

30 THz. Secondly, despite the fact that the absorption coefficient at 15 THz and 30 THz is the same, the maximum secure distance at 15 THz is longer than that at 30 THz. This mainly due to the FSPL difference, as it will increase with the increase of frequency. Note that, the systems operating at 100 GHz, 200 GHz and 300 GHz investigated in Fig. 2.24 fail to attain an acceptable SKR because of the high thermal noise.

2.7 Conclusions

In this Chapter, firstly the syndrome-based decoding process was reviewed by using the examples of a Hamming code and LDPC code. Both the quantum transmission and classic reconciliation schemes have been introduced with an emphasis on the LDPC-coded reconciliation scheme used in CV-QKD. Thereafter, a comprehensive parametric study of an LDPC-coded CV-QKD reconciliation scheme was conducted. This demonstrated the importance of reconciliation efficiency for the SKR versus distance performance. As a further investigation, both the SISO and MIMO THz CV-QKD systems have been introduced with an emphasis on the quantum transmission part. It was demonstrated that both the thermal noise variance level, the absorption coefficient and the path loss associated with the different frequency bands play a significant role in determining the SKR versus distance performance of THz CV-QKD systems.

Chapter 3

The Road to Near-Capacity CV-QKD Reconciliation: An FEC-Agnostic Design

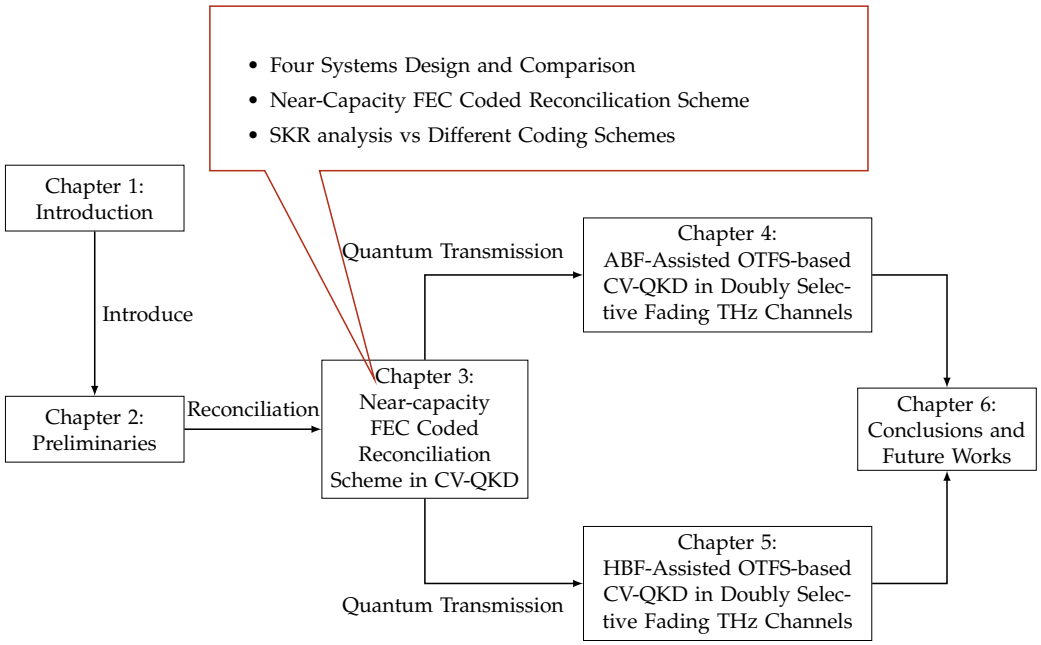


Figure 3.1: The outline of this thesis with the highlight of Chapter 3.

3.1 Introduction

As an important step of classical post-processing in QKD, reconciliation plays an pivotal role in ensuring that both the transmitter and the receiver rely on the same bit stream and use it as the reconciled key. More explicitly, the reconciliation process is

Table 3.1: Novel contributions of this work in comparison to the state-of-the-art schemes.

Contributions	**This work**	[121]	[15, 61–66, 74, 76, 137]	[110]	[138]
DV-QKD(BSC)				✓	
CV-QKD(AWGN)	✓	✓	✓		
Hard-decoding	✓				✓
Soft-decoding incorporates syndromes	✓		✓	✓	
AWGN/Rayleigh for the classical authenticated channel	✓				
Balanced decoding complexity for Alice and Bob	✓				
Compatible application with LDPC, CC, polar codes, IRCC	✓				
Near-capacity for both classical & quantum part	✓				

based on error correction used for mitigating the deleterious effects of noise and interference imposed by Eve [59]. For instance, a simple Hamming code was utilized in the reconciliation step to correct the bit errors in the raw key string shared by the satellite and the ground station for the experimental satellite-to-ground QKD system used in the *Micius* experiment [60]. Inspired by this development, some more advanced FEC codes have also been investigated, such as LDPC codes [15, 61–66], polar codes [67–70], rateless codes [71, 72], and their diverse variants. As a further advance, instead of using a fixed FEC code rate, adaptive-rate reconciliation schemes were proposed in [73–75], where the SKR and the secure transmission distance were optimized for different SNRs. Moreover, a Raptor-like LDPC code was harnessed for QKD in [74], where the rate-compatible nature of the raptor code was exploited for reducing the cost of constructing new matrices for low-rate LDPC codes harnessed at low SNRs. In contrast to the conventional CV-QKD reconciliation, where a so-called single decoding attempt based algorithm was used, a multiple decoding attempt based method was adopted in [66] to improve the SKR performance. Furthermore, a large block length based LDPC coded scheme was analyzed in [76], where a near-capacity performance was achieved for transmission over the QuC.

A list of LDPC coded QKD reconciliation schemes is seen at a glance in Table 3.1. In a nutshell, there are two main types of reconciliation methods, namely the multidimensional [121, 139] and the slice-based reconciliation method [138, 140]. The former achieves better performance in the low-SNR region, which is suitable for longe-range CV-QKD transmission, while the latter in the high-SNR domain, which is suitable for short-distance CV-QKD systems[1]. The soft-decision LDPC decoding adopted for QKD

[1]As for the multidimensional reconciliation, it attains higher reconciliation efficiency than slice based reconciliation due to the fact that there is no quantization process, which can cause performance degradation, and also that the capacity of the virtual established channel gets closer to the capacity of AWGN channel at a low SNR [141]. However, its throughput is limited to 1 bit, hence making it more suitable for long-range CV-QKD transmission system. By contrast, the slice based reconciliation, especially the multilevel coding and multistage decoding aided slice based reconciliation, has the capability of extracting more than 1 bit of information per channel use (bpcu), especially for higher SNRs. This is achieved at the cost of poor quantization performance in the low SNR region, making it more suitable for a short range CV-QKD transmission system.

in [15, 137] outperforms the hard-decision decoding algorithm of [138], but at the cost of a higher complexity. **However**, a major issue is that all the existing studies assume that the ClC used for syndrome transmission is error-free. In practice, the ClC is contaminated both by fading and noise, hence error correction is required for both the QuC and the classical syndrome-feedback channel. Consequently, for the multidimensional reconciliation scheme, the receiver has to perform two separate FEC decoding actions, namely one for the QuC and one for the ClC[2]. This creates an imbalance in terms of the reconciliation complexity, heavily burdening one side. Furthermore, the classic syndrome-based QKD reconciliation system is limited to syndrome-based codes such as LDPC codes, while the family of CCs that are often included in communication standards [142, 143] have not been used in the open literature. Against this background, the novel contributions of this work are as follows:

- Firstly, the BLER performance is analyzed in the context of syndrome-based reconciliation systems, where the ClC is initially assumed to be error-free, and both the BF and BP based decoding algorithms are harnessed. More explicitly, we revise Gallager's SPA for LDPC codes using BP, where both the codeword transmitted through the QuC and the side information conveying the syndrome through the authenticated ClC can be accepted as the input of the modified SPA. Our performance results confirm that the revised BP decoder substantially outperforms the conventional BF decoder in terms of the SKR of the QKD system.

- Secondly, for the first time in the literature, the effect of a realistic imperfect ClC is characterized for syndrome transmission from Bob to Alice, where RR is considered and the effects of both fading as well as of noise are taken into account. We demonstrate that the QKD system requires error correction for both the quantum and ClC. Consequently, the receiver has to perform FEC decoding of the potentially corrupted encoded syndrome for transmission over the ClC, and FEC decoding of the corrupted reference key sent from Bob over the ClC, making the decoding complexity unbalanced that burdens the receiver side. This calls for clean-slate considerations for a new QKD system design.

- Thirdly, a new bit-difference based CV-QKD reconciliation scheme is proposed, where Bob transmits the key through the QuC to Alice, and Alice carries out decoding with the aid of the bit-difference side information sent by Bob through the ClC to Alice. The bit-difference side information is constituted by the vector of bit differences between the key and a legitimate LDPC codeword. This regime allows us to use any arbitrary FEC codes. Our performance results confirm that for a specific FEC this new system has the same performance as the conventional syndrome-based CV-QKD [59], but again, it is compatible with any FEC schemes, including polar codes, CCs and IRCCs.

[2]Note that the QuC and ClC of CV-QKD will be detailed in Section **??-??**.

- Since the bit-difference vector based CV-QKD system still requires Alice to perform FEC decoding for both the QuC and ClC, a new codeword-based QKD reconciliation system is proposed. In this system, Alice sends a FEC-protected CK to Bob through the ClC, while Bob sends a separate FEC protected QK to Alice through the QuC[3]. Upon a FEC decoding performed at both sides, the final key to be used for the message encryption is the modulo-2 sum of the CK and QK[4]. As a result, for the first time in the open literature, our proposed codeword-based CV-QKD system achieves the following novelties. **Firstly**, the proposed scheme ensures protection of both the QuC and the ClC by FECs. **Secondly**, the system conceived has a symmetric complexity, where both Alice and Bob have an FEC encoder and an FEC decoder. **Thirdly**, the proposed QKD reconciliation scheme is compatible with a wide range of FEC schemes, including polar codes, CCs and IRCCs, where a near-capacity performance can be achieved for both the QuC and for the ClC.
- Our performance results demonstrate that with the aid of IRCCs, near-capacity performance can be achieved for both the quantum and the ClC, which leads to an improved SKR that inches closer to both the PLOB bound [103] and the maximum achievable rate bound [104]. Therefore, the proposed codeword-based QKD reconciliation system facilitates flexible FEC deployment and it is capable of increasing the secure transmission distance.

The structure of this chapter is described in Fig. 3.1 and the rest of this chapter is organized as follows. Different system designs are proposed and compared in Section 3.2. The corresponding security analysis in terms of SKR is conducted in Section 3.3. Then, Section 3.4 presents the BLER and BER performance of different systems, where the performance of the proposed FEC aided CV-QKD is analyzed. Finally, Section 3.5 provides our main conclusions and future research ideas.

3.2 System Descriptions and Comparisons

In this section, our new codeword-based reconciliation system will be proposed, following the critical appraisal of the state-of-the-art. More explicitly, four reconciliation systems will be presented in this section. In a nutshell,

[3]Note that in our proposed codeword-based reconciliation system the QK is defined as the specific part of the key that is transmitted through the QuC, while the CK is defined as the remaining part of the key that is transmitted through the ClC. This is different from the terminology of key used in Systems A-C, where the key is only transmitted through the QuC with the aid of some side information.

[4]We note that in the conventional syndrome-based QKD [59], even if Eve infers the syndrome from the ClC, she still cannot extract the QK from the QuC. Similarly, in the proposed system, even if Eve obtains the CK that is suitable for any FEC codes, she still cannot acquire the QK from the QuC. The QKD's Heisenberg's uncertainty principle remains valid for the quantum transmission. As a benefit, the SKR will be improved by using our powerful IRCC FEC schemes for both the ClC and the QuC despite considering realistic imperfect channels.

1. **System A** represents the conventional LDPC-coded reconciliation scheme relying on the idealistic simplifying assumption that the ClC used for syndrome transmission is error-free.

2. **System B** takes into account the fading and noise effects of the ClC, where a separate LDPC code is required for both the QuC and the ClC. Note that System B is a practical version of System A.

3. **System C** is proposed to demonstrate that the bit-difference vector-based side information can play the same role as the syndrome of Systems A and B. Hence System C has the same performance as System A and System B.

4. **System D** represents the proposed codeword-based reconciliation scheme suitable for any arbitrary FEC code. Hence the family of powerful IRCCs can also be applied to achieve a near-capacity performance for both the QuC and ClC.

Note that the following reconciliation systems mainly focus on the details of the reconciliation step within the QKD protocol. More specifically, the BI-AWGN equivalent QuC of Fig. 2.12 is used here for the description of the reconciliation post-processing step.

3.2.1 System A: the Ideal Syndrome-based LDPC-coded Scheme

System A: The first reconciliation system shown in Figure 3.2 is the BF/BP decoding algorithm based LDPC-coded CV-QKD reconciliation scheme, where the ClC used for syndrome transmission is assumed to be error-free. The algorithmic steps are described as follows.

(a) Bob randomly generates a bit stream $\mathbf{C}$ using a QRNG, and we view this as the initial raw key $\mathbf{b}$ at his side. Note that, the QRNG generates classical random numbers. The length of this is determined by the codeword length of the predefined PCM $\mathbf{H}^{\text{PCM}}$. The PCM is known at both sides. Note that, the bit stream $\mathbf{b}$ at Bob's side does not have to be a legitimate codeword, because the final objective is to obtain a reconciled key. More specifically, in the reverse reconciliation scheme, the bit stream generated at Bob's side is the reference key, and Alice has to acquire this as the final key. Let us consider the single-error correcting [7,4,1] BCH code as our rudimentary example, and assume that the bit stream generated by the QRNG in block (1) of Fig. 3.2 is $\mathbf{C} = [1111010]$. Then Bob treats this random bit stream as the initial key $\mathbf{b} = [1111010]$ in block (2) of Fig. 3.2.

(b) Bob transmits this bit stream $\mathbf{b} = [1111010]$ through a QuC to Alice, which is modelled by the equivalent ClC constructed in Fig. 2.12 and represented by block

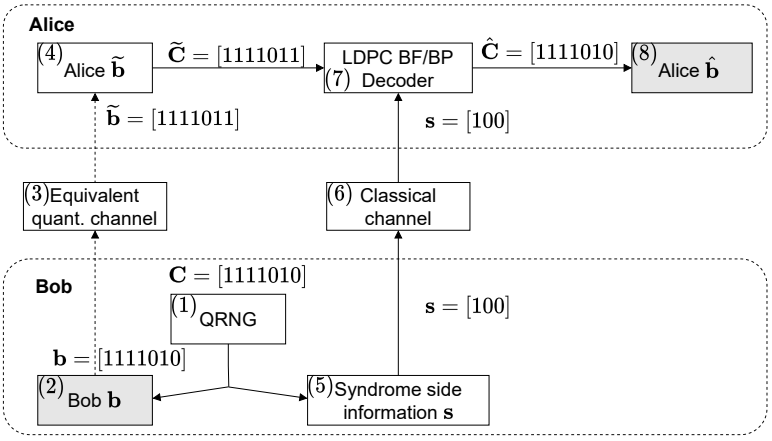


Figure 3.2: *System A* - **the ideal LDPC-coded syndrome-based reconciliation scheme** in the CV-QKD system relying on the BF/BP decoding algorithm. Note that, the dashed arrow represents the bit stream sent from Bob to Alice through the equivalent QuCs as illustrated in Section 2.4.2.

(3) of Fig. 3.2. The channel-contaminated sequence received by Alice is denoted by $\widetilde{\mathbf{b}} = [1111011]$ in block (4), which is corrupted in the last bit position.

(c) Meanwhile, based on the QRNG output Bob calculates the syndrome, say $\mathbf{s} = [100]$ in block (5) and transmits it as side information to Alice through the authenticated ClC of block (6), which is assumed to be perfectly *noiseless and error-free*.

(d) Alice takes the bit stream $\widetilde{\mathbf{b}}$ inferred at the output of the QuC, which may or may not be a legitimate codeword, and forwards it as namely $\widetilde{\mathbf{C}} = [1111011]$ to the decoder. Decoding is carried out by the corresponding FEC decoder with the aid of the syndrome bits she received through the ClC (6) and gets the decoded result of $\hat{\mathbf{C}} = [1111010]$ at the output of block (7). Based on this, Alice gets the decoded codeword as the final reconciled key, which is $\hat{\mathbf{b}} = [1111010]$ shown in block (8). Observe that this is the same as Bob's bit stream $\mathbf{b}$, provided that there are no decoding errors. This is the case, if the QuC inflicts no more than a single error, since the [7,4,1] code can only correct a single error. It is important to mention here that if the classical syndrome-transmission channel inflicts errors, this would results in catastrophic corruption of the QuCs' output. This issue will be addressed by System B.

3.2.2 System B: the Practical Syndrome-based LDPC-coded Scheme

System B: Following the above rudimentary BCH-coded example to introduce how System A works, let us now detail a practical LDPC code based scheme. System B of Fig. 3.3 represents the BP decoding algorithm based CV-QKD reconciliation scheme. In contrast to System A, System B no longer assumes that the ClC is error-free. Hence both

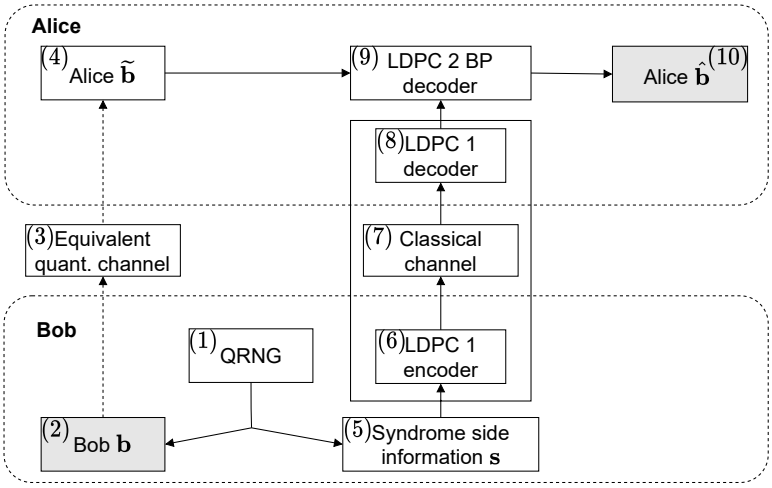


Figure 3.3: *System B* - **the practical LDPC-coded syndrome-based reconciliation scheme** in the CV-QKD system with BP decoding algorithm. Compared to System A, System B no longer assumes that the ClC is error-free, where both ClC and QuC require data protection by error correction.

the classical and the QuC require error correction. Let us consider a [1024,512] LDPC code as our example to introduce System B. More explicitly, the operational steps of System B are

(a) Bob randomly generates a 1024-bit stream using the QRNG of Fig. 3.3, and views this as the initial key $\mathbf{b}$ at his side. Note that, the QRNG generates classical random numbers. Again, the length of this is determined by the codeword length of the predefined LDPC PCM $\mathbf{H}$, which is known to both sides.

(b) Bob transmits this bit stream $\mathbf{b}$ through the equivalent QuC to Alice, who receives the bit stream as $\widetilde{\mathbf{b}}$.

(c) Meanwhile, Bob calculates the syndrome based on the QRNG output - namely $\mathbf{b}$ - as the side information $\mathbf{s}$ and transmits it to Alice through the authenticated ClC protected by the LDPC encoder in block (6) of Fig. 3.3. *Note that*, the rectangular frame shown in Fig. 3.3 that encompasses blocks (6)-(8), constitutes a separate FEC-aided data protection for the ClC, which relies on the LDPC 1 code. The dimensionality of the PCM of such LDPC codes in our example is 512×1024, and hence the syndrome $\mathbf{s} = \mathbf{H}^{\mathrm{PCM}} \cdot \mathbf{b}$ calculated from Bob has the length of 512 bits. After the FEC scheme applied to the syndrome protection, which is protected by another [1024, 512] LDPC code, the encoded syndrome has the length of 1024 bits. Then, after being decoded at Alice's side by the LDPC 1 decoder (8), the syndrome $\mathbf{s}$ having 512 bits is recovered. In the literature [15, 61–65, 74, 76, 110, 121, 137, 138], the ClC is assumed to be *noiseless and error-free*, but a realistic ClC tends to inflict both fading and noise. Hence the ClC's LDPC 1 scheme of Fig. 3.3 may not be able to eliminate all errors imposed on the syndrome. Therefore,

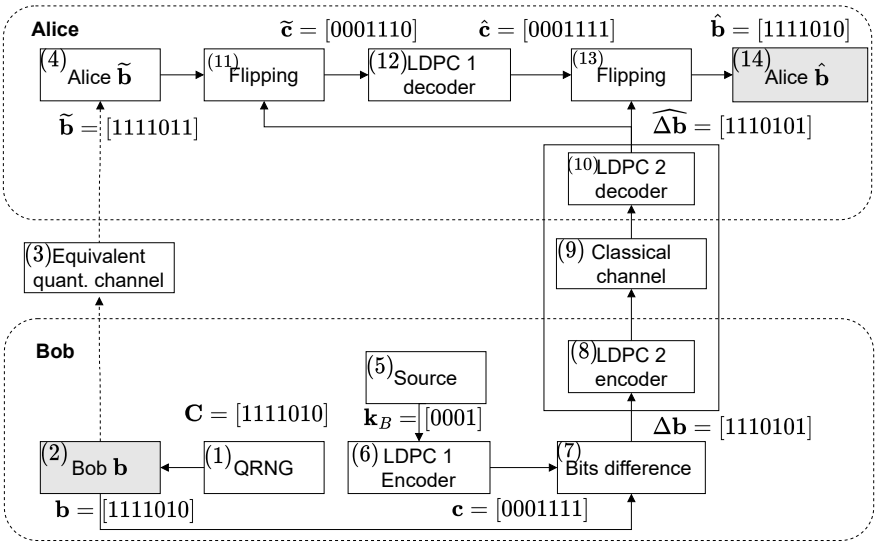


Figure 3.4: *System C* - **the LDPC-coded bit-difference vector-based reconciliation scheme** designed for CV-QKD systems and using the BP decoding algorithm.

the performance of practical FEC schemes in the classical syndrome-transmission channel is taken into account in System B.

(d) Then Alice carries out *BP* decoding of the information received over the QuC with the aid of the syndrome bits to get $\hat{\mathbf{b}}$, as seen in block (9).

Note that, the syndrome-based scheme is limited to FEC codes that rely on syndromes, whereas other codes such as polar codes and CCs cannot be applied. Therefore, the bit-difference vector-based scheme (System C) is proposed to tackle this issue, which is described as follows.

3.2.3 System C: the Proposed Bit-difference Vector-based LDPC-coded Scheme

System C of Fig. 3.4, is our proposed scheme, where the final key generated by the QRNG is transmitted through the QuC and the syndromes of System B are replaced by the bit-difference vector. For convenience, both the QuC and the ClC may adopt the same kind of FEC codes, albeit they may have different length. The corresponding steps are described as follows.

(a) The functions of block (1) to (4) in Fig. 3.4 are the same as described in System A. Here, again a simple [7,4,1] BCH code is used as our rudimentary example. Specifically, the bit stream $\mathbf{b} = [1111010]$ may be obtained from the QRNG, which generates a bit stream C=[1111010], and it is transmitted from Bob to Alice

through the QuC, resulting the corrupted bit stream $\widetilde{\mathbf{b}} = [1111011]$ at Alice's side. This has a single error in the last position.

(b) In contrast to the way of calculating the syndrome in Systems A and B, a legitimate codeword $\mathbf{c} = [0001111]$ is required for deriving the bit-difference vector $\Delta\mathbf{b} = [1110101]$ based on blocks (5) to (7) in Fig. 10, where $\mathbf{k}_B = [0001]$ represents the corresponding random information bits used to obtain $\mathbf{c}$.

(c) Based on the received and protected bit-difference vector $\widehat{\Delta\mathbf{b}} = [1110101]$ at the output of block (10) in Fig. 3.4, Alice flips the bits of $\widetilde{\mathbf{b}}$ in those specific positions, where a logical 1 occurs in $\widehat{\Delta\mathbf{b}}$ at the output of block (3) in Fig. 3.4 to arrive at $\widetilde{\mathbf{c}} = [0001110]$ at the output of (11) before decoding.

(d) Alice then decodes the bit stream $\widetilde{\mathbf{c}} = [0001110]$ to arrive at $\hat{\mathbf{c}} = [0001111]$ after (12) to get the key $\hat{\mathbf{b}} = [1111010]$ at the output of block (13), which is ideally the same as $\mathbf{b}$ at Bob's side.

Observe in Fig. 3.3 (System B) and Fig. 3.4 (System C) that there are two LDPC decoders at Alice's side. By contrast, there is merely a single LDPC encoder and a low-complexity syndrome calculation scheme at Bob's side in System B, while two LDPC encoders are required at Bob's side in System C. Since Alice has to perform computationally demanding LDPC decoding twice in order to infer the final key, this is not a balanced-complexity system[5]. In light of these considerations, the new codeword-based reconciliation System D was proposed for arriving at a solution having a balanced-complexity, where Alice and Bob have a similar complexity, as required in Device-to-Device (D2D) systems for example [146, 147], which is described as follows.

3.2.4 System D: the Proposed Practically Generic Scheme

System D of Figure 3.5, is our proposed scheme that utilizes a pair of FEC codes to protect both the QuC and the classical authenticated channel. For convenience, both the QuC and the ClC may adopt the same kind of FEC codes. The corresponding steps are described as follows.

(a) Both Bob and Alice generate a legitimate codeword based on a pair of predefined PCMs $\mathbf{H}_1^{\text{PCM}}$ and $\mathbf{H}_2^{\text{PCM}}$, which are $\mathbf{b}$ and $\mathbf{c}$. Consider again a simple [7,4,1] BCH code as our rudimentary example, where the pair of legitimate codewords are $\mathbf{b} = [0000000]$ and $\mathbf{c} = [0001111]$, respectively, as indicated in Fig. 3.5. The corresponding uncoded information bits are for example $\mathbf{k}_B = [0000]$ and $\mathbf{k}_A = [0001]$, respectively.

[5]Even though System C is not a balanced-complexity system, there are practical scenarios, where having a balanced complexity is not imperative, such as in ground station to unmanned aerial vehicle (UVA) quantum communication [144, 145], etc.

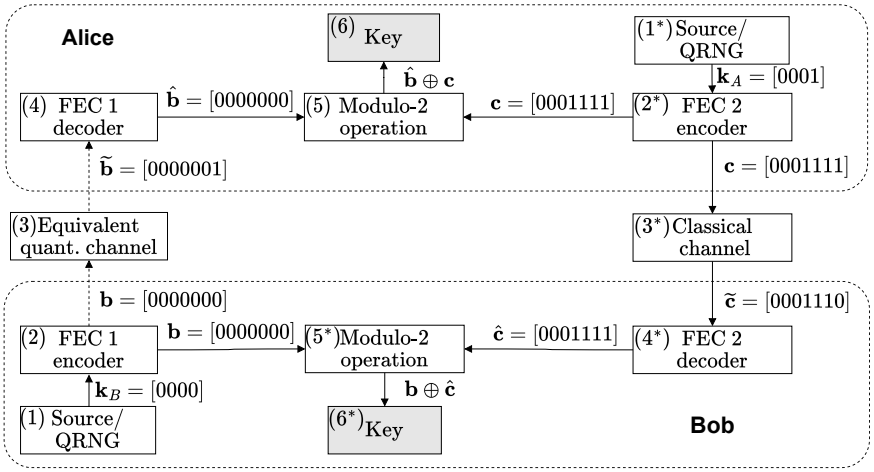


Figure 3.5: *System D* - **the proposed practically generic reconciliation scheme** designed for CV-QKD systems.

(b) Bob transmits his legitimate codeword $\mathbf{b}$ through the QuC, which is modelled again by the equivalent ClC of Fig. 2.12. On the other hand, Alice transmits her legitimate codeword $\mathbf{c}$ through the ClC, which may inflict errors. Note that, the 2 LDPC codes in Fig. 3.5 do not have to be exactly the same code, whose PCMs are the same. However, for convenience, in our study, it is assumed that both QuC and ClC may adopt the same kind of FEC codes, which have exactly the same PCM. The codewords transmission over both the QuC and the ClC is independent. More specifically, the codeword $\mathbf{c}$ is transmitted the same as that in conventional wireless communication, whilst the codeword $\mathbf{b}$ is transmitted with the aid of the equivalent QuC of Fig. 2.12, where the relationship between the Gaussian signals transmitted over the QuC and the random bit stream generated by QRNG is leveraged as can be seen in Fig. 2.8(b).

(c) Both Alice and Bob carry out LDPC BP decoding to get $\hat{\mathbf{b}} = [0000000]$ and $\hat{\mathbf{c}} = [0001111]$, respectively[6].

(d) Furthermore, Modulo-2 operation is carried out at both sides to obtain the final key for both Alice and Bob, which are $\hat{\mathbf{b}} \oplus \mathbf{c}$ and $\mathbf{b} \oplus \hat{\mathbf{c}}$, respectively.

The proposed System D is summarized in Algorithm 3. As a benefit of this design, first of all, the proposed codeword-based - rather than syndrome-based - QKD reconciliation scheme protects both the QuC and ClC. Secondly, the system has a similar complexity for both Alice and Bob, each of whom has a FEC encoder and a FEC decoder. Thirdly, System D makes QKD reconciliation compatible with a wide range of

[6]As for handling decoding failures, it is assumed to be identical to that in the conventional LDPC-based reconciliation scheme of [64], which is based on the classic cyclic redundancy check. Specifically, the system opts for discarding the sifted keys, if decoding failure occurs. Yet, a slight difference is that our codeword-based reconciliation needs two separate steps to check whether decoding is successful or not. We can only proceed to the next step when both parts are correct.

Algorithm 3: Description of *System D*.

1 **Codeword generation:** Both Alice and Bob generate a legitimate codeword, which are $\mathbf{c}$ and $\mathbf{b}$.
2 **Codeword transmission:** Bob transmits his legitimate codeword $\mathbf{b}$ through the equivalent QuC, which is the same process as in the System A, B and C. Meanwhile, Alice transmits her legitimate codeword $\mathbf{c}$ through the ClC.
3 **Decoding:** Both Alice and Bob carry out FEC decoding.
4 **Modulo-2 operation:** Modulo-2 operation is implemented at both sides to obtain the final key for both Alice and Bob, which are $\hat{\mathbf{b}} \oplus \mathbf{c}$ and $\mathbf{b} \oplus \hat{\mathbf{c}}$, respectively.

FEC, including polar codes and the family of CCs. We will demonstrate in Section 3.4 that this design allows us to achieve a near-capacity performance for both the QuC and for the ClC.

3.2.5 Systems Comparison

Table 3.2: Comparisons between four different systems.

	System A	System B	System C	System D
Equivalent QuC	BI-AWGN channel			
ClC	Error-free	Noise and fading		
QK	Bob→Alice	Bob→Alice	Bob→Alice	Bob→Alice
Side information (CK)	Syndromes (Bob→Alice)		Bit-difference (Bob→Alice)	CK (Alice→Bob)
FEC types	Only LDPC	Only LDPC	Any	Any
Improvements over syndrome-based CV-QKD [59]	-	-	Near-capacity, compatible to any FEC	Near-capacity, balanced complexity, compatible to any FEC

In summary, the comparisons between System A (ideal syndrome-based CV-QKD), System B (practical syndrome-based CV-QKD), System C (practical bit-difference vector based CV-QKD) and System D (codeword-based CV-QKD) are summarized in Table 3.2. More specifically, all four systems use the same equivalent QuC, but in System A we assume that the ClC is error-free, while in Systems B, C and D we consider realistic noise and fading in the ClC. Secondly, as for the side information, syndromes are transmitted from Bob to Alice through the ClC in both System A and System B. By contrast, instead of using the syndrome, System C transmits te bit-difference vector from Bob to Alice through the ClC, making the system compatible with any FEC. Furthermore, System D transmits the CK from Alice to Bob through the ClC, making the FEC decoding complexity balanced between both sides. Lastly, only LDPC codes can be applied to both System A and System B, while any kinds of FEC codes can be applied to System C and D. We opted for powerful IRCCs to achieve near-capacity performance.

3.3 Secret Key Rate Analysis

Note that the security level of the proposed System C and D is the same as that of System A and B, since the difference between them only lies in the side information. More specifically, we can only proceed with the reconciliation steps of Fig. 2.8, when the QK is securely received through the QuC, which obeys the Heisenberg's uncertainty principle. Therefore, even if Even steals the side information from the ClC, the final key still cannot be recovered. This is true for Systems A-D. Nonetheless, there are three distinct advantages for the proposed System D. Firstly, it is compatible with any FEC code, rather than being limited to LDPC codes. Secondly, it has a balanced complexity for Alice and Bob, which is particularly favourable in wireless device-to-device scenarios. Lastly, it exhibits near-capacity performance, where the SKR is close to the PLOB. This is achieved by using IRCCs for protecting both the QuC and ClC, making the SNRs required for error-free quantum and classical transmissions near-optimal.

The SKR is defined as [65]

$$K_{\text{finite}} = \gamma \left(1 - P_B\right) \left[\beta I_{AB} - \chi_{BE} - \triangle \left(N_{\text{privacy}}\right)\right], \tag{3.1}$$

where γ denotes the proportion of the key extractions in the total number of data exchanged by Alice and Bob, while P_B represents the BLER in the reconciliation step. Furthermore, I_{AB} is the classical MI between Alice and Bob based on their shared correlated data, and χ_{BE} represents the Holevo information [59] that Eve can extract from the information of Bob. Finally, $\triangle \left(N_{\text{privacy}}\right)$ represents the finite-size offset factor with the finite-size N_{privacy}[7]. It was proven in [58] that when $N_{\text{privacy}} > 10^4$, this factor can be simplified as

$$\Delta \left(N_{\text{privacy}}\right) \approx 7\sqrt{\frac{\log_2(2/\epsilon)}{N_{\text{privacy}}}}, \tag{3.2}$$

where ϵ represents the security parameter[8] for the protocol. As for $\beta \in [0,1]$, it represents the reconciliation efficiency, which is defined as [59, 74]

$$\beta = \frac{R}{C} = \frac{R}{0.5\log_2(1+\text{SNR})}, \tag{3.3}$$

where R represents the transmission rate, and C is referred to as the one-dimensional Shannon capacity [108, 128], which is given by the MI as follows [65]:

$$C = I_{AB} = \frac{1}{2}\log_2(1+\text{SNR}) = \frac{1}{2}\log_2\left(\frac{V+\xi_{\text{total}}}{1+\xi_{\text{total}}}\right), \tag{3.4}$$

[7]Note that the finite-size offset can be viewed as a penalty term imposed by the imperfect parameter estimation step as shown in Fig. 2.8 when using finite length data. The value of N_{privacy} set in our analysis is 10^{12}, which is a value chosen in most of the literature.

[8]This security parameter corresponds to the failure probability of the whole protocol, implying that the protocol is assured to perform as requested except for a probability of at most ϵ. The value of ϵ is chosen to be 10^{-10} in our following analysis, which is widely used in the literature.

where $V_A = V_s + 1$ and V_s is Alice's modulation variance[9], while ξ_{total} is the total amount of noise between Alice and Bob, which can be expressed as

$$\xi_{\text{total}} = \xi_{\text{line}} + \frac{\xi_{\text{hom}}}{T}, \tag{3.5}$$

where $\xi_{\text{hom}} = \frac{1+v_{el}}{\eta} - 1$ is the homodyne detector's noise, and v_{el} stands for the electric noise, while η represents the detection efficiency. Furthermore, $\xi_{\text{line}} = \left(\frac{1}{T} - 1\right) + \xi_{\text{ch}}$ represents the channel noise from the sender Alice, where T represents the path loss and ξ_{ch} is the excess noise [111] (i.e. imperfect modulation noise, Raman noise, phase-recovery noise, etc.). Assuming a single-mode fiber having an attenuation of $\alpha_{\text{fibre}} = 0.2$ dB/km, the distance-dependent path loss of such a channel is $T = 10^{-\alpha \mathfrak{L}/10}$, where $\mathfrak{L}$ denotes the distance between the two parties.

The Holevo information between Bob and Eve can be calculated as follows [59]

$$\chi_{BE} = S\left(\rho_E\right) - S\left(\rho_{E|B}\right) = S(\rho_{AB}) - S\left(\rho_{A|B}\right), \tag{3.6}$$

where $S(\cdot)$ is the von Neumann entropy defined in [59]. The von Neumann entropy of a Gaussian state ρ containing $\mathcal{M}$ modes can be written in terms of its symplectic eigenvalues [127]

$$S\left(\rho\right) = \sum_{m=1}^{\mathcal{M}} G\left(v_m\right), \tag{3.7}$$

where

$$G\left(v\right) = \left(\frac{v+1}{2}\right) \log_2 \left(\frac{v+1}{2}\right) - \left(\frac{v-1}{2}\right) \log_2 \left(\frac{v-1}{2}\right). \tag{3.8}$$

To elaborate on Eq. (3.8), generally these symplectic eigenvalues can be calculated based on the CM $\mathbf{V}$ of the Gaussian state using the formula [82]

$$v = \left|i\mathbf{\Omega}\mathbf{V}\right|, \quad v \geq 1, \tag{3.9}$$

where $\mathbf{\Omega}$ defines the symplectic form given by

$$\mathbf{\Omega} := \bigoplus_{m=1}^{M} \boldsymbol{\omega} = \begin{pmatrix} \boldsymbol{\omega} & & \\ & \ddots & \\ & & \boldsymbol{\omega} \end{pmatrix}, \boldsymbol{\omega} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{3.10}$$

Here $\bigoplus$ is the direct sum indicating the construction of a block-diagonal matrix $\mathbf{\Omega}$ having the same dimensionality as $\mathbf{V}$ by placing $\mathcal{M}$ blocks of $\boldsymbol{\omega}$ diagonally. Eq. (3.9) indicates that first we have to find the eigenvalue of the matrix $i\mathbf{\Omega}\mathbf{V}$ and then take the absolute values. However, in some circumstances, we can simplify the calculation of the eigenvalues. To elaborate further, firstly we consider a generic two-mode CM in

[9]The modulation variance here represents the variance of Gaussian signals used in the modulator of CV-QKD.

the form of

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}. \tag{3.11}$$

Based on [59], the symplectic eigenvalues v_1 and v_2 of $\mathbf{V}$ can be written in the form of [82]

$$v_{1,2} = \sqrt{\frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4\det \mathbf{V}}\right)}, \tag{3.12}$$

where $\det \mathbf{V}$ represents the determinant of the matrix $\mathbf{V}$ and we have

$$\Delta := \det \mathbf{A} + \det \mathbf{B} + 2\det \mathbf{C}. \tag{3.13}$$

In light of this, the CM related to the information between Alice and Bob, - namely the mode of ρ_{AB} after transmission through the QuC - can be expressed as

$$\begin{aligned} \mathbf{V}_{AB} &= \begin{pmatrix} V_A \mathbf{I}_2 & \sqrt{\eta T \left(V_A^2 - 1\right)}\mathbf{Z} \\ \sqrt{\eta T \left(V_A^2 - 1\right)}\mathbf{Z} & \eta T \left(V_A + \xi_{\text{total}}\right)\mathbf{I}_2 \end{pmatrix} \\ &= \begin{pmatrix} a\mathbf{I}_2 & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I}_2 \end{pmatrix}, \end{aligned} \tag{3.14}$$

where we have

$$\mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{3.15}$$

which are the two Pauli matrices. Therefore, the symplectic eigenvalues of ρ_{AB} required are given by

$$v_{1,2}^2 = \frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4D^2}\right), \tag{3.16}$$

where we have:

$$\begin{aligned} \Delta &= a^2 + b^2 - 2c^2, \\ D &= ab - c^2. \end{aligned} \tag{3.17}$$

As for the symplectic eigenvalue of $\rho_{A|B}$, it can be shown that:

$$v_3 = \sqrt{a\left(a - \frac{c^2}{b}\right)}. \tag{3.18}$$

Hence, the Holevo information can be formulated as

$$\chi_{BE} = G\left(v_1\right) + G\left(v_2\right) - G\left(v_3\right), \tag{3.19}$$

where v_1, v_2 and v_3 are symplectic eigenvalues. Upon substituting Eq. (3.4) and Eq. (3.19) into Eq. (3.1), the corresponding SKR can be obtained.

In summary, SKR versus distance L performance metric, used in our following analysis are as follows.

- Once the BLER versus SNR performance is obtained, a fixed BLER corresponds to a fixed SNR.
- The noise term ξ_{total} in Eq. (3.4) is a function of L. Hence, the value of V_A is adjusted for each L to satisfy the fixed SNR based on Eq. (3.4).
- Once V_A is adjusted for each L, χ_{BE} can be obtained, since it is a function of V_A.
- Finally, the target SKR versus distance is derived.

3.4 Performance Analysis

In this section, our BLER performance comparisons will be presented for different reconciliation schemes. Moreover, the SKR versus distance performance indicator will be analyzed. The common simulation parameters[10], which are used in our LDPC based reconciliation scheme are summarized in Table 3.3.

Table 3.3: Simulation parameters.

Parameter	Value
Coding rate (fixed)	0.5
Code length	1024
Decoding algorithm	BF/BP
Maximum number of iterations	50
Quantum equivalent channel type	BI-AWGN
ClC type	AWGN/Rayleigh
QuC quality	SNR
ClC quality	SNR^{C}

3.4.1 Performance Comparison between BF and BP Decoding in System A

Firstly, the performance comparison between the BF and BP decoding in System A is presented by Fig. 3.6, where the classical authenticated channel is assumed to be error-free. Observe from Fig. 3.6 that as expected, BP decoding outperforms BF decoding. Since the BLER performance is a key performance factor in the SKR of Eq. (3.1), the BP decoding algorithm will be adopted in the rest of performance analysis.

3.4.2 Performance Comparison among System B, System C and System D

Let us now compare System B of Fig. 3.3 and System C of Fig. 3.4 as well as System D of Fig. 3.5, given that the authenticated channel is no longer error-free. Instead, an

[10]Note that the code length and code rate used in both the QuC and ClC are the same.

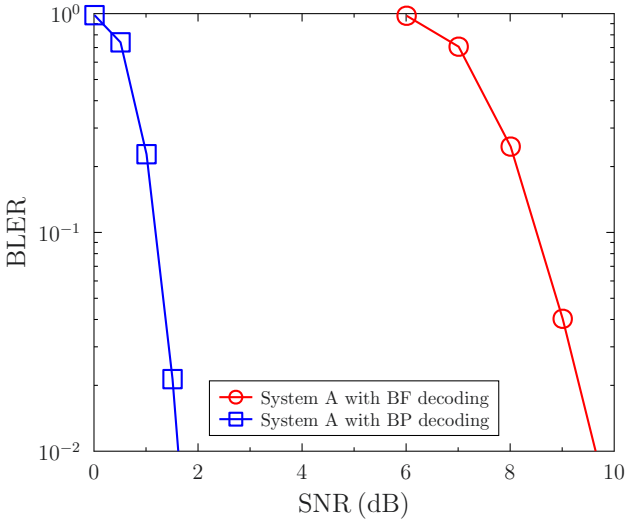


Figure 3.6: Performance comparison between System A of Fig. 3.2 and System B of Fig. 3.3. The code length and code rate of the LDPC code are 1024 and 0.5, respectively. BF decoding is used in System A and BP decoding is utilized in System B. The classical authenticated channel is assumed to be error-free.

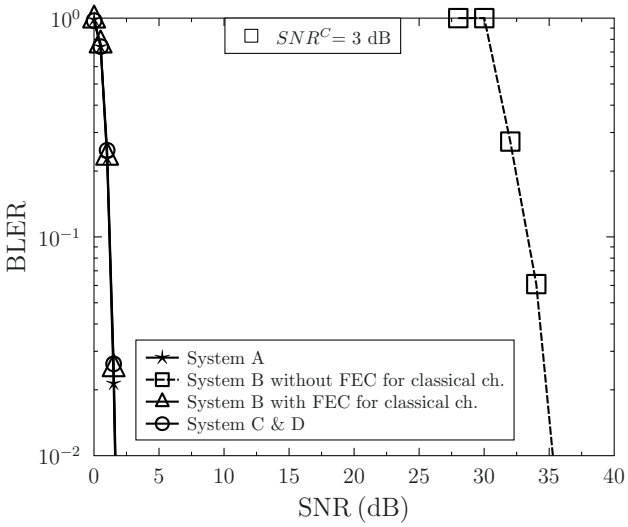


Figure 3.7: Performance comparison among System B, System C and System D. The code length and code rate of the LDPC code are 1024 and 0.5, respectively. BP decoding algorithm is used in System B, System C and System D, as well as System A. The authenticated ClC is assumed to be an **AWGN** channel and the corresponding SNR^C is 3 dB.

AWGN channel and an uncorrelated Rayleigh fading channel as well as perfect channel estimation are assumed for the classical side-information in Fig. 3.7 and Fig. 3.8, respectively.

Fig. 3.7 demonstrates that the performance of the uncoded System B is severely degraded, when the ClC is contaminated by AWGN and hence it is no longer error-free, which confirms that error correction is required for both the ClC and QuC. By contrast,

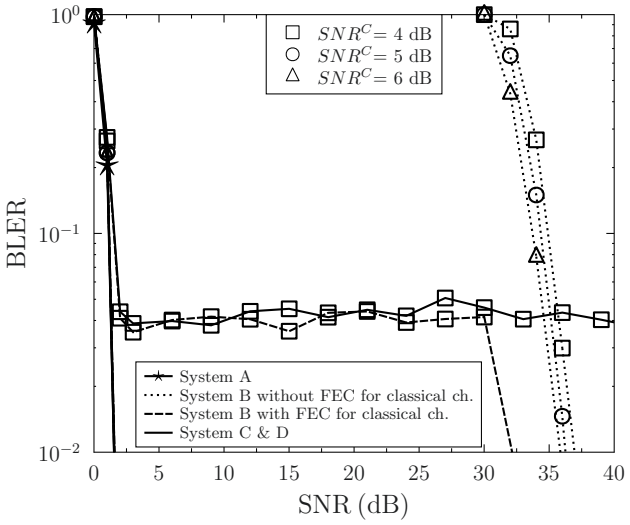


Figure 3.8: Performance comparison among System B, System C and System D. The code length and code rate of the LDPC code are 1024 and 0.5, respectively. BP decoding algorithm is used in System B, System C and System D, as well as System A. The authenticated ClC is assumed to be a **Rayleigh** fading channel.

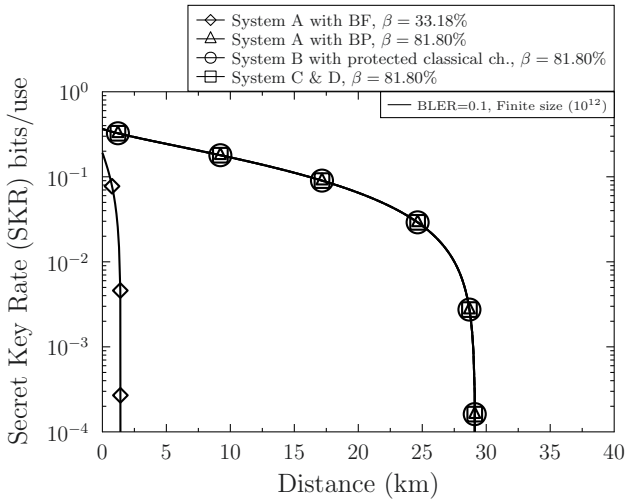


Figure 3.9: The secret key rate analysis versus distance. The values of different reconciliation efficiency are calculated based on the corresponding SNR at the threshold of BLER equals to 0.1.

it can be seen in Fig. 3.7 that when System B, System C and System D employed FEC to protect their ClC, they no longer suffer from performance loss compared to the scenario of the idealistic assumption of having an error-free ClC. The ClC of $SNR^C = 3$dB is sufficient for supporting System B, System C and System D for approaching the performance of the error-free ClC, which is shown by the solid line associated with stars, representing the BP-based performance of System A.

Similarly, Fig. 3.8 provides our performance comparison, when the ClC is modelled by an uncorrelated Rayleigh fading channel having $SNR^C = 4, 5, 6$ dB. It can be seen in Fig.3.8 that System B operating without error protection for the ClC performs worst,

requiring excessive SNR. By contrast, Fig.3.8 shows that when FEC is applied to the ClC, at say $SNR^{C} = 5,6$ dB, System B, System C and System D approach the idealistic scenario of an error-free ClC. By contrast, an error floor is encountered by both System B , System C and System D at $SNR^{C} = 4$ dB, which is too low to mitigate the errors imposed by the Rayleigh faded ClC.

Based on the BLER performances shown above, the corresponding SKR versus distance comparison is portrayed in Fig. 3.9. The parameters are as follows: the modulation variance is adjusted to get a certain target SNR, which is related to the BLER threshold of 0.1 utilized for comparison; the excess noise is $\xi_{\text{ch}} = 0.002$; the efficiency of the homodyne detector is $\eta = 0.98$; the attenuation of a single-mode optical fibre is $\alpha_{\text{fibre}} = 0.2\text{dB/km}$, and the electric noise is $v_{el} = 0.01$. More explicitly, Fig. 3.9 demonstrates that the maximum secure distance of System A using BF decoding is limited at around 1km, while that of System A using BP decoding is about 30 km. A similar performance as that of System A using BP decoding is attained for System B for a protected ClC at $SNR^{C} = 3$ dB, which is a sufficiently high SNR^{C}. System C and System D also achieve a similar SKR performance, as evidenced by Fig. 3.9. Note that the SKR versus distance performance of System B without protecting the ClC is not shown here, because it is extremely low at such low reconciliation efficiency.

3.4.3 Performance Comparison among Different FEC Codes in System D

In this section, comparisons have been made among three different types of FEC codes, which are LDPC codes, CC and IRCC, respectively. The number of LDPC decoding iteration is 50 and that of IRCC decoding is 30. Fig.3.10 and Fig.3.11 characterize the performance of our codeword-based reconciliation scheme using a 1/2-rate CC of constraint-length 7 under AWGN and Rayleigh channels, respectively. The same trend can be observed in Fig. 3.10 and Fig. 3.11, where a higher SNR^{C} of the ClC leads to reduced error floor. We note that as expected, compared to the AWGN scenario of Fig. 3.10, the Rayleigh scenario of Fig. 3.11 requires a higher SNR^{C} for achieving a low BLER.

Let us now consider the most sophisticated FEC scheme of this study, namely the IRCC used, which was discussed in great detail in [148, 149] and shown in Fig. 3.12, where P_{out} and P_{in} represents the number of irregular coding components used. In Fig. 3.12(a), the Extrinsic Information Transfer (EXIT) chart matching process detailed in [150] is briefly illustrated, and the process of IRCC encoding and decoding is shown in Fig. 3.12(b). The EXIT charts [104, 151, 152] and the iterative decoding trajectory of IRCC and Unitary Rate Code (URC) coded Binary Phase-Shift Keying (BPSK) modulation communicating over classical AWGN channel are portrayed in Fig. 3.13. More explicitly, the dotted EXIT curves seen in Fig. 3.13 correspond to 17 component CCs having coding rates ranging from 0.1 to 0.9 with a step size of 0.05. The IRCC design assigns different-length segments to different-rate component codes, so that a narrow

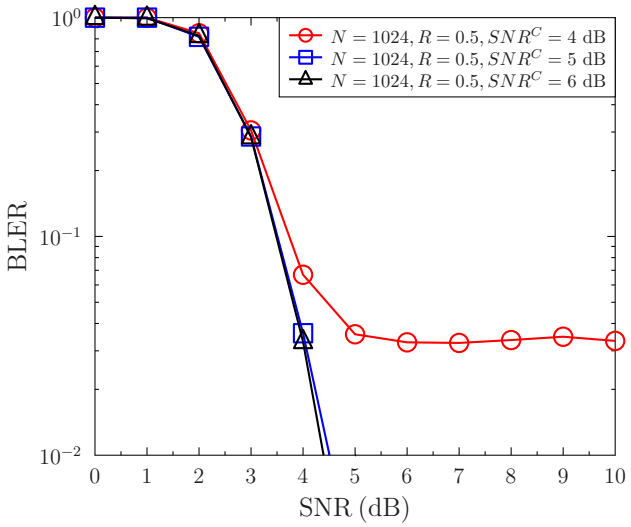


Figure 3.10: Performance comparison in System D with CC. The code length and code rate of the CC code are 1024 and 0.5, respectively. The authenticated ClC is assumed to be a **AWGN** channel.

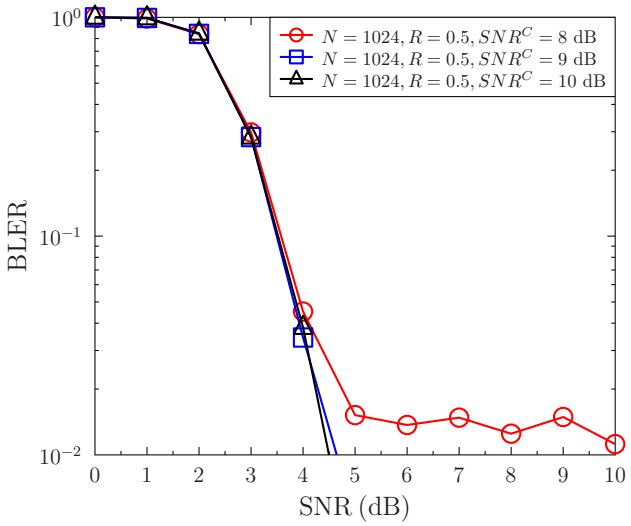
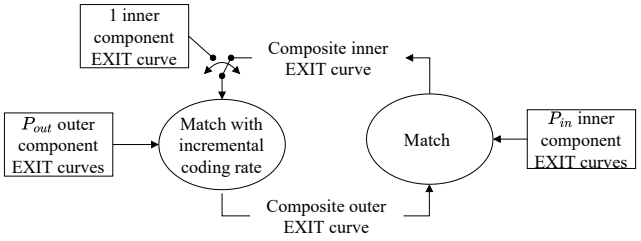
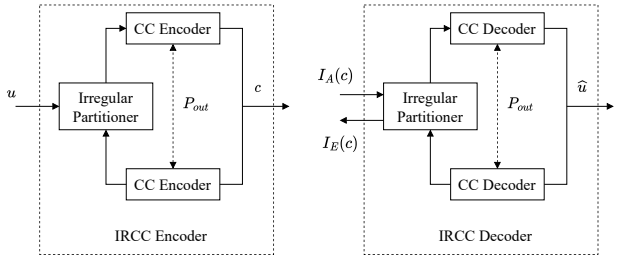


Figure 3.11: Performance comparison in System D with CC. The code length and code rate of the CC code are 1024 and 0.5, respectively. The authenticated ClC is assumed to be a **Rayleigh** fading channel.

tunnel is formed between the inner URC-BPSK coding component's EXIT curve and that of the outer IRCC decoder, as seen in Fig. 3.13. It was shown in [150] that the open tunnel area is proportional to the distance from capacity. More explicitly, as this area tends to zero, the scheme tends to approach the capacity. Hence, the presence of the narrow but open decoding tunnel of Fig. 3.13 indicates decoding convergence at a low SNR that approaches the capacity limit. The IRCC fractions of the component codes are found to be [0.0120603 0 0 0 0 0 0.605992 0.0780007 0 0 0 0.0672488 0.177274 0 0 0 0.0594503] for the 17 subcodes used in Fig. 3.13. To elaborate briefly, for a 1000-bit IRCC the cod-rate of 0.05 is used for 0.0120603·1000≈12 bits. Then the code-rates of 0.1, 0.15, 0.2, 0.25 and 0.3 have 0 weight, so they are unused. The code-rate of 0.35 has a weight



(a) Diagram of interative double EXIT chart matching [148]



(b) Schematic of the IRCC encoding and decoding [149]

Figure 3.12: Schematic of IRCC codes.

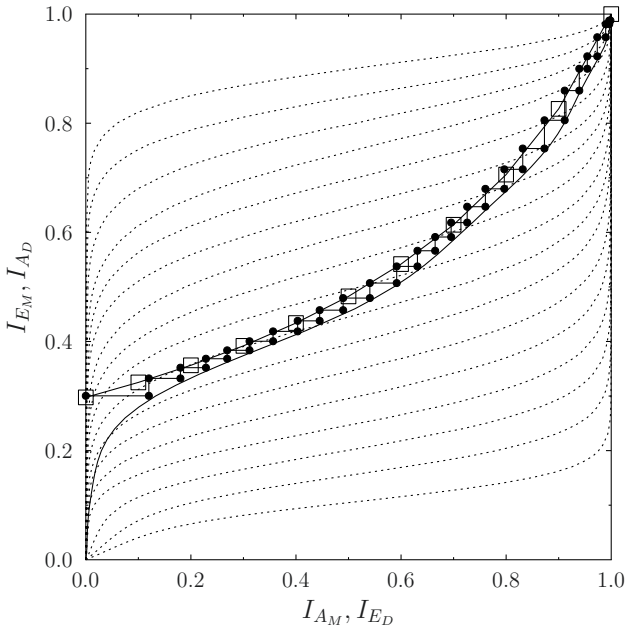


Figure 3.13: EXIT chart and a decoding trajectory of IRCC and URC coded BPSK having a block-length of 10^5, communicating over a classical AWGN channel.

Table 3.4: Reconciliation efficiency of different FEC codes calculated from Eq. (3.3) at the BLER threshold that equals to 0.1, together with the corresponding SNRs. The code length and code rate of them are the same for all of them, which are $N_{\text{FEC}} = 10^4$, $R = 0.5$. The authenticated ClCs are AWGN and uncorrelated Rayleigh channel.

	AWGN		Rayleigh	
Code type	SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$
CC	4.4	52.40	4.4	52.40
LDPC code	1.31	81.04	1.31	81.40
IRCC	0.9	86.41	1.0	85.06
IRCC (10^5)	0.7	89.21	0.7	89.21

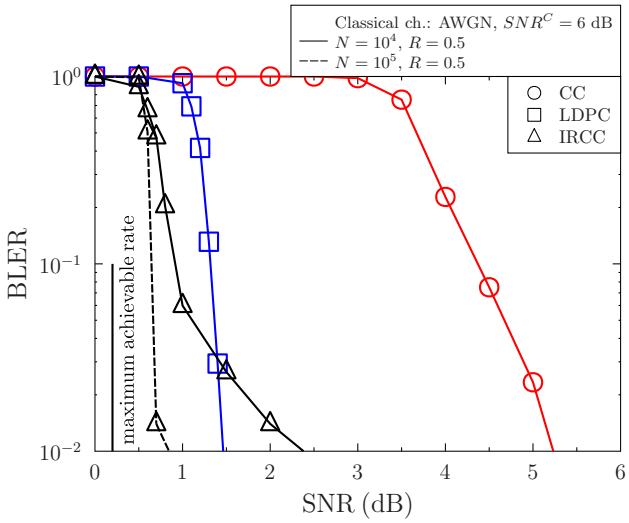


Figure 3.14: Performance comparison of different FEC codes in System D of Fig. 3.5. The code length and code rate of different codes are 10^4 and 0.5, respectively. The authenticated ClC is an **AWGN** channel.

of 0.605992, hence it is used for 0.605992·1000≈606 bits and this process is applied to the remaining code-rates as well.

The BLER of the codeword based reconciliation scheme (System D) of a variety of FEC codes is shown in Fig. 3.14. The corresponding (BLER, β) pair can be obtained as tabulated in Table 3.4. In light of the BLER performance comparison among different FEC codes, the corresponding SKR versus distance performances of different FEC code based reconciliation schemes can be obtained with the aid of the reconciliation efficiencies as shown in Fig. 3.15. For the same BLER, for example BLER=0.1, given the same block length of 10^4 bits, the reconciliation performances associated with IRCC, LDPC and CC exhibit different reconciliation efficiencies, which are 86.41%, 81.04% and 52.40%, respectively. Therefore, the SKR performance of the IRCC scheme is the best. More explicitly, the maximum secure distance associated with the IRCC code (the diamond solid line) is longer than that of LDPC (the square solid line) and of the CC (the square dash line) code. Furthermore, the SKR at each specific secure distance associated with IRCC code is higher than that of the LDPC or CC codes. To elaborate

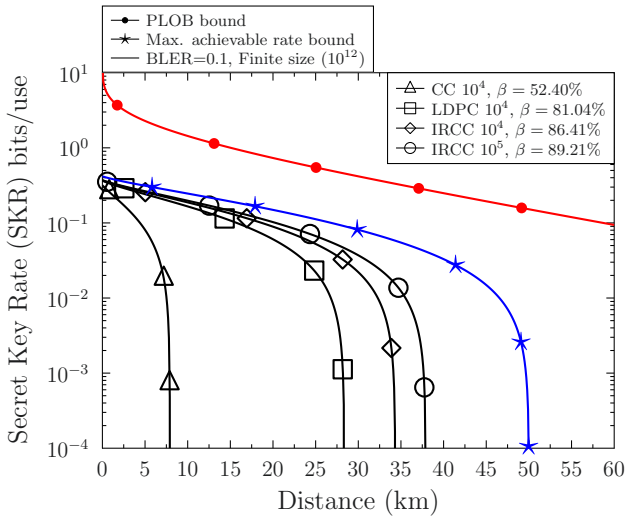


Figure 3.15: The secret key rate versus distance. The values of different reconciliation efficiencies are shown in Table 3.4 at the BLER threshold of 0.1. The other parameters are as follows: the modulation variance is adjusted to get a target SNR, the excess noise is $\xi_{ch} = 0.002$, the efficiency of the homodyne detector is $\eta = 0.98$, the attenuation of a single-mode optical fibre is $\alpha_{\text{fibre}} = 0.2\text{dB/km}$, and the electric noise is $v_{el} = 0.01$. The corresponding PLOB [103] bound and the maximum achievable rate bound are shown as well.

further, the maximum secure distance of the IRCC code with BLER=0.1, $\beta = 86.41\%$ is around 35km, whereas the corresponding maximum secure distance of the LDPC (BLER=0.1, $\beta = 81.04\%$) and CC (BLER=0.1, $\beta = 52.40\%$) codes are around 28km and 8km, respectively. The same conclusion can be drawn for the comparison between LDPC and CC codes at BLER=0.01. Moreover, Fig. 3.15 demonstrates that the SKR performance of a longer block length of $N_{\text{FEC}} = 10^5$ is superior to that of $N_{\text{FEC}} = 10^4$, since a longer block length can offer near-capacity performance, hence leading to a longer secure transmission distance of around 37km. Note that the vertical line shown in Fig. 3.14 represents the minimum SNR required to achieve near-error-free transmission. It is obtained based on [104, 152, 153]

$$C^{DCMC}(SNR) = 1 - \frac{1}{2}\sum_{i=0}^{1}\mathbb{E}\left\{\log_2\left[\sum_{\tilde{i}=0}^{1}\exp\left(\Psi_{i,\tilde{i}}\right)\right]\right\}, \tag{3.20}$$

where we have $\Psi_{i,\tilde{i}} = \frac{-\|s^i - s^{\tilde{i}} + n\|^2 + \|n\|^2}{N_0}$, s^i represents the BPSK symbols, while n is the noise, whose distribution obeys $n \sim \mathcal{CN}(0, N_0)$. The corresponding SNR can be obtained by solving $C^{DCMC}(SNR) = 0.5$, since we consider BPSK and $R = 0.5$, FEC codes. The same capacity line is also drawn in Fig. 3.16.

On the other hand, based on the reconciliation efficiencies seen in Table 3.4 and inferred from Fig. 3.14 as well as Fig. 3.16, the reconciliation efficiencies are similar for

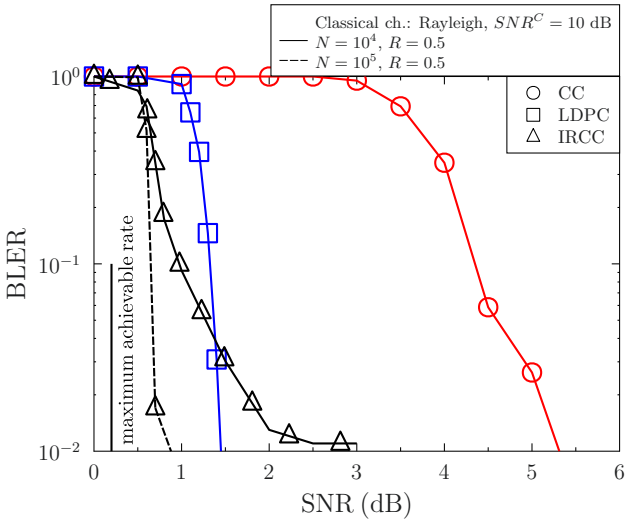


Figure 3.16: Performance comparison of different FEC codes in System D of Fig. 3.5. The code length and code rate of different codes are 10^4 and 0.5, respectively. The authenticated ClC is a **Rayleigh** channel.

the Rayleigh-faded and for the AWGN ClC. This is because the reconciliation efficiencies are mainly determined by the QuC quality characterized by the equivalent channel SNR, provided that the ClC quality is high enough for ensuring that the errors from the classical transmission do not unduly erode the overall system performance, as demonstrated in Fig. 3.16. Intuitively, a higher SNR^C is required in Rayleigh faded ClCs compared to the SNR^C in an AWGN based ClC to achieve nearly the same system performance. Therefore, given that the βs are nearly the same, the SKR of a Rayleigh faded ClC is similar to that in Fig. 3.15.

3.5 Conclusions

The codeword based reconciliation concept was proposed as a general reconciliation scheme that can be applied in conjunction with diverse FEC codes. This is a significant improvement because the popular syndrome-based LDPC-coded reconciliation scheme can only be applied for FEC codes that possess syndromes. Furthermore, in contrast to the general assumption that the classical authenticated channel is error-free and noiseless, a realistic ClC has been considered, which may contain errors. We investigated the performance of our QKD systems when the classical authenticated channel is modelled as an AWGN channel or a Rayleigh channel. We demonstrated that when the ClC quality is sufficiently high, the QKD system will have a relatively low BLER. An error floor is exhibited by the system, when the ClC has errors due to employing a weak channel code or when the ClC quality is too low. More specifically, we have investigated LDPC, CC and IRCC assisted CV-QKD schemes. It was demonstrated that the IRCC aided system performs best among them, followed by the LDPC codes,

Table 3.5: A summary of SKR vs. distance based on Fig. 3.15.

Code type	β(%)	Max. secure distance(km)
CC	52.40	8
LDPC code	81.04	28
IRCC	86.41	35
IRCC (10^5)	89.21	37

whilst the CC code performs the worst. In light of this, the SKR versus distance performance of different FEC codes using optical fibre as the QuC has been compared. It was demonstrated that near-capacity FEC codes such as IRCC can provide higher reconciliation efficiency, hence they can offer a longer secure transmission distance, which is summarized in Table 3.5.

Chapter 4

Analog Beamforming Assisted OTFS-Based CV-QKD Systems for Doubly Selective THz Channels

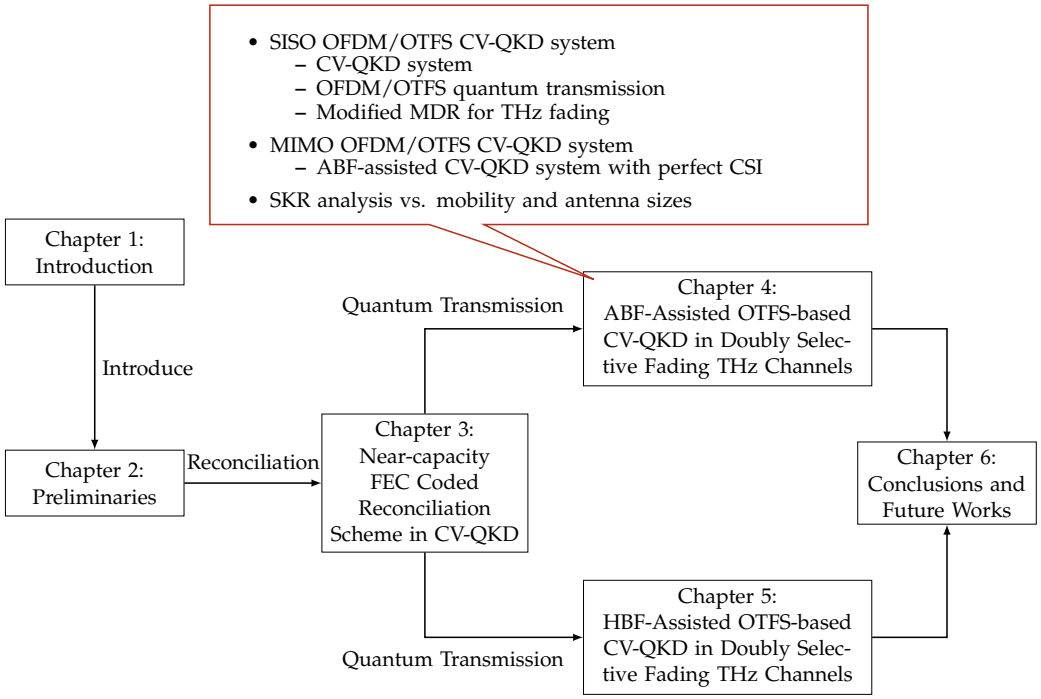


Figure 4.1: The outline of this thesis with the highlight of Chapter 4.

4.1 Introduction

As discussed in Chapter 1, QKD is capable of supporting ultimate information security in communication systems [1, 21, 23–27, 29]. In particular, CV-QKD has attracted

Table 4.1: Novel contributions of this work in comparison to the state-of-the-art THZ CV-QKD schemes.

Contributions	**This work**	[69, 90–93, 95, 97]	[96]	[94, 98]	[79, 81]	[83]	[86]
Optical fibre		✓					
FSO				✓			
Terahertz	✓		✓		✓	✓	✓
SISO	✓	✓	✓	✓	✓		✓
MIMO	✓					✓	✓
Beamforming	✓					✓	✓
Frequency selective	✓	✓	✓	✓			
Time-invariant fading	✓	✓	✓	✓	✓	✓	✓
Time-varying fading	✓						
OFDM	✓	✓	✓	✓			
OTFS	✓						
Channel estimation	✓						

substantial attention from both academia and industry. For CV-QKD either homodyne or heterodyne detection is utilized, which has convenient compatibility with the operational communication network infrastructure [21, 54]. As a further benefit, CV-QKD is capable of providing a higher key rate [40, 41, 55, 56] than its DV-QKD counterpart, since its associated homodyne or heterodyne detection offers the prospect of high detection efficiency. On the other hand, the different reconciliation schemes have been investigated in Chapter 3, where optical fibre is consider as the quantum transmission channel. Furthermore, to meet the explosive data-rate demand of next-generation communication systems, the substantial available bandwidth of the THz range has motivated a lot of research efforts [77, 78]. The feasibility of CV-QKD has also been considered in the THz band [79–82]. Furthermore, in order to improve the secure transmission distance limited by the high path loss of the THz band, MIMO techniques have been adopted in [83–86]. Moreover, the OFDM waveform also used in 4G and 5G, has been introduced to support CV-QKD in the THz band for the sake of mitigating the detrimental multipath effect of wireless channels [69, 90–98].

Table 4.1 summarizes the state-of-the-art CV-QKD schemes, with a focus on using OFDM to improve the SKR in wireless THz channels. Briefly, an OFDM-based CV-QKD scheme was proposed for optical fibre transmission in [69, 90–93, 95], where both the security level and the SKR were investigated. Moreover, realistic imperfect modulation was considered in [93], while a singular value decomposition based method was invoked for the reliable simultaneous transmission of multiple data streams in [95]. It was demonstrated in [95] that both the maximum key rate attained at a specific distance and the overall maximum secure transmission distance can be improved with the aid of the OFDM technique. Secondly, an OFDM-based CV-QKD FSO link was established in [94], which took into account the impact of scintillation intensity, phase noise and the number of subcarriers on the system performance. As a further advance, the authors of [98] analyzed the performance of CV-QKD over FSO quantum channels with a focus on the theoretical derivation of the SKR. Thirdly, the SKR performance of an OFDM-based CV-QKD scheme operating in the THz band was analyzed both in indoor environments and in inter-satellite links in [96], where the effect of sub-channel

crosstalk caused by the imperfection of optical devices was considered as well. Finally, a realistic imperfect modulation scenario was considered for OFDM-based CV-QKD in [97][1]. A specific modulation noise model was proposed for OFDM-based CV-QKD and the authors investigated the effect of both Gaussian and discrete modulation cases. It was demonstrated in [97] that the asymptotic SKR can be improved by increasing the number of sub-carriers even for realistic discrete modulations.

However, all of the OFDM aided CV-QKD schemes investigated operate based on the assumption of time-invariant fading channels in stationary scenarios. In reality, wireless users move freely and their mobility leads to the Doppler effect. The real-world time-varying frequency-selective fading channels destroy OFDM's subcarrier orthogonality and degrade the OFDM performance. Yet these deleterious effects have not been investigated in the context of CV-QKD. As a remedy, a new waveform termed as OTFS modulation has been recently proposed for classical wireless communication in the face of time-varying and frequency selective fading channels [154–159]. More explicitly, the OTFS scheme transforms the time-varying frequency-selective fading experienced in the Time-Frequency (TF) domain into quasi-static flat fading in the Delay-Doppler (DD) domain. As a result, channel estimation in the DD domain requires less frequent updates, while OFDM's Inter-Carrier Interference (ICI) caused by user mobility is also mitigated. At the time of writing, the novel OTFS schemes have not been harnessed in CV-QKD systems.

Against this background, for the first time in the open literature, we propose a multi-carrier framework for supporting both OFDM and OTFS aided LDPC coded CV-QKD reconciliation systems. Time-varying frequency-selective fading, which is a typical high mobility scenario in Space-Air-Ground Integrated Networks (SAGINs) [21, 23, 24, 158], is considered for a THz channel, where both SISO and MIMO beamforming setups are considered. As demonstrated by Table 4.1, the novel contributions of this work are as follows:

- Firstly, a multi-carrier OFDM based LDPC assisted CV-QKD reconciliation scheme is established and studied. This is different from the existing literature both in terms of the quantum transmission and reconciliation process, which operate in the face of time-varying and frequency-selective THz propagation.
- Secondly, for the first time in the open literature, an OTFS based quantum transmission scheme is proposed for LDPC coded CV-QKD, which is capable of relying on the same multi-carrier infrastructure as its OFDM counterpart, while providing improved performance in the face of time-varying THz scenarios.
- Thirdly, in order to facilitate LDPC assisted CV-QKD reconciliation for both OFDM and OTFS, a new mapping scheme is devised for our post-processing aided MDR

[1]The imperfect modulation entails the in-phase and quadrature-phase imbalance and intermodulation distortion in [97].

process, where realistic channel fading is taken into account. This is different from the existing MDR schemes found in the open literature, where a BI-AWGN based quantum channel is assumed [105].

- Fourthly, in order to improve the quantum transmission distance attained in the face of severe THz path loss, MIMO beamforming is conceived based on statistical CSI, where analog beamformers are conceived based on LoS propagation without requiring full knowledge of the multipath CSI at the transmitter.
- Finally, our analysis and simulation results demonstrate that the proposed OTFS-based CV-QKD is capable of outperforming its OFDM counterpart in terms of its SKR, when the user mobility is increased. Moreover, our performance results also demonstrate that the proposed MIMO beamforming scheme is capable of improving secure CV-QKD transmission for both OTFS and OFDM.

The structure of this chapter is described in Fig. 4.1 and the rest of this chapter is organized as follows. Our SISO OFDM/OTFS CV-QKD system is conceived in Section 4.2, which introduces the CV-QKD system model, OFDM and OTFS quantum transmission as well as the modified MDR for THz fading. The MIMO OFDM/OTFS CV-QKD system is proposed in Section 4.3, which is followed by the SKR analysis in Section 4.4. Our simulation results are presented in Section 4.5. Finally, our conclusions are offered in Section 4.6.

4.2 System Model of SISO OFDM/OTFS based CV-QKD

In this section, firstly the CV-QKD system model is reviewed. Then the proposed OFDM/OTFS quantum transmission as well as our modified MDR designed for LDPC assisted CV-QKD are introduced. We note that LDPC codes are used by the syndrome-based reconciliation process and it is assumed that the classical transmission is perfect, which is the common assumption in the open literature [71, 105, 137].

4.2.1 CV-QKD System Model

The classic CV-QKD protocol [105] is summarized in Fig. 4.2, where the RR process using MDR mapping is highlighted.

More explicitly, firstly, Alice maps the Gaussian distributed random variables $\bar{\mathbf{s}}$ to the Frequency Domain (FD) subcarriers of OFDM or $\tilde{\mathbf{s}}$ to the DD of OTFS, which are transmitted with the aid of OFDM/OTFS through wireless THz channels. The random variables received by Bob are firstly equalized in the FD or DD for OFDM and OTFS, respectively, leading to the decision variable of $\bar{\mathbf{z}}$ in the FD or $\tilde{\mathbf{z}}$ in the DD that is equivalent to the noise-contaminated version of the transmitted Gaussian variables. Secondly,

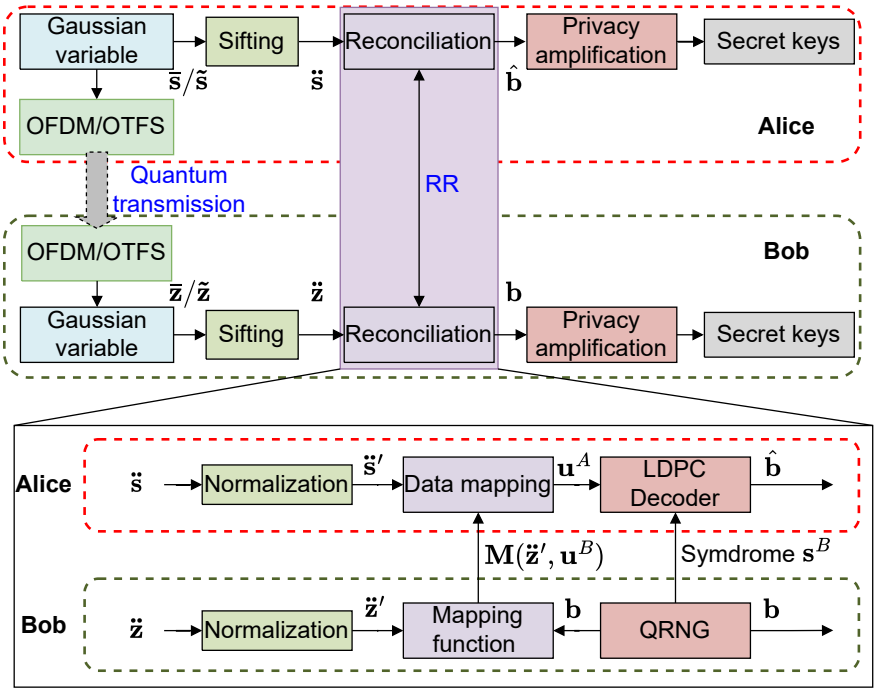


Figure 4.2: CV-QKD protocol diagram of OFDM/OTFS LDPC-aided scheme. Note that the reconciliation part is the same as that in [105].

in the sifting step[2], Alice and Bob synchronize their preparation and measurement basis, providing input variables for the MDR process as $\ddot{\mathbf{s}}$ at Alice's side and $\ddot{\mathbf{z}}$ at Bob's sides. Thirdly, in the RR step, the MDR mechanism is invoked for mapping the modulated version $\mathbf{u}^B$ of the binary data $\mathbf{b}$ to the normalized random variables $\ddot{\mathbf{z}}'$ after either OFDM or OTFS detection at Bob's side. Alice invokes the agreed MDR function $\mathbf{M}(\ddot{\mathbf{z}}', \mathbf{u}^B)$ for mapping the normalized random variable $\ddot{\mathbf{s}}'$ of the OFDM or OTFS transmitted symbols to $\mathbf{u}^A$, which is the contaminated version of $\mathbf{u}^B$. Then the LDPC syndrome $\mathbf{s}^B$ generated based on the key is sent from Bob to Alice, so that Alice's LDPC decoder can apply error correction to $\mathbf{u}^A$ for mitigating the noise-contamination of the raw quantum data. Finally, privacy amplification is applied for reducing Eve's probability of successfully guessing the key. The detailed MDR process will be elaborated on in Sec. 4.2.3.

4.2.2 OFDM/OTFS based Quantum Transmission

In this section, the OFDM scheme of Fig. 4.3 and the OTFS scheme of Fig. 4.4 are introduced for quantum transmission over wireless THz channels. The OFDM and OTFS notations in the Time Domain (TD), FD and DD domain are summarized in Table 4.2.

[2]Note that homodyne detection is used in our proposed scheme, which is different from the heterodyne detection based scheme, since no key sifting process is required. Further related discussions can be found in [21].

Table 4.2: OFDM and OTFS notations.

	TD	FD	DD domain
Transmitter	$s_{n,m}$	$\bar{s}_{n,\bar{m}}$	$\widetilde{s}_{k,l}$
Channel	$h_{n,m,l}$	$\bar{h}_{n,\bar{m}}$	$\widetilde{h}_p \omega_{MN}^{k_p(nM+m-l_p)}$
Receiver	$y_{n,m}$	$\bar{y}_{n,\bar{m}}$	$\widetilde{y}_{k,l}$

4.2.2.1 OFDM based Quantum Transmission

As portrayed by Fig. 4.3, the OFDM transmitter maps the data-carrying symbols to the nth OFDM symbol in FD as $\bar{\mathbf{s}}_n \in \mathcal{C}^{M\times 1}$, and then they are transformed to the TD via the Inverse Discrete Fourier Transform (IDFT), which can be expressed as

$$\mathbf{s}_n = \mathbf{F}_M^H \bar{\mathbf{s}}_n, \tag{4.1}$$

where $\mathbf{F}_M \in \mathcal{C}^{M\times M}$ denotes the Discrete Fourier Transform (DFT) matrix. Meanwhile, the relationship of preparation thermal noise between FD and TD can be represented as $\mathbf{s}_{0n} = \mathbf{F}_M^H \bar{\mathbf{s}}_{0n}$, which is the same as in Eq. (4.1). The received TD signal can be expressed as[3]:

$$\begin{aligned} y_{n,m} =& \sqrt{T} \sum_{l=0}^{L-1} h_{n,m,l} s_{n,<m-l>_M} \\ &+ \sqrt{T} \sum_{l=0}^{L-1} h_{n,m,l} s_{0n,<m-l>_M} + \sqrt{1-T} s_{En,m}, \end{aligned} \tag{4.2}$$

where T represents the channel transmissivity, $h_{n,m,l}$ models the faded Channel Impulse Response (CIR) from the lth Time Delay Line (TDL) tap, with L representing the maximum TDL tap, and s_E represents the AWGN introduced by Eve to extract the key information [83]. Based on (4.2), the TD matrix form is given by

$$\mathbf{y}_n = \sqrt{T}\mathbf{H}_n \mathbf{s}_n + \sqrt{T}\mathbf{H}_n \mathbf{s}_{0n} + \sqrt{1-T}\mathbf{s}_{En} \tag{4.3a}$$

$$= \sqrt{T}\mathbf{H}_n \left(\mathbf{s}_n + \mathbf{s}_{0n}\right) + \sqrt{1-T}\mathbf{s}_{En} \tag{4.3b}$$

$$= \sqrt{T}\mathbf{H}_n \mathbf{s}_n + \mathbf{v}_n, \tag{4.3c}$$

where $\mathbf{H}_n \in \mathcal{C}^{M\times M}$ models the faded CIR matrix. Following this, the received TD signal is transformed into the FD by DFT as follows:

$$\bar{\mathbf{y}}_n = \mathbf{F}_M \mathbf{y}_n = \sqrt{T}\bar{\mathbf{H}}_n \bar{\mathbf{s}}_n + \bar{\mathbf{v}}_n, \tag{4.4}$$

where $\bar{\mathbf{v}}_n = \sqrt{T}\mathbf{H}_n \bar{\mathbf{s}}_{0n} + \sqrt{1-T}\bar{\mathbf{s}}_{En}$.

[3] We note that the input-output relationship of both Eq. (4.2) and Eq. (4.10) are direct extensions of the beam splitter models found in [54, 79, 83–85, 94–96], where doubly selective fading is introduced in our system. Furthermore, we will demonstrate in this treatise that given the same beam splitter channel model, the choice of waveforms between OFDM and OTFS as well as their detector designs have significant impact on the SKR.

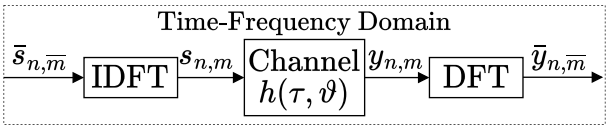


Figure 4.3: System diagram of OFDM transmission scheme.

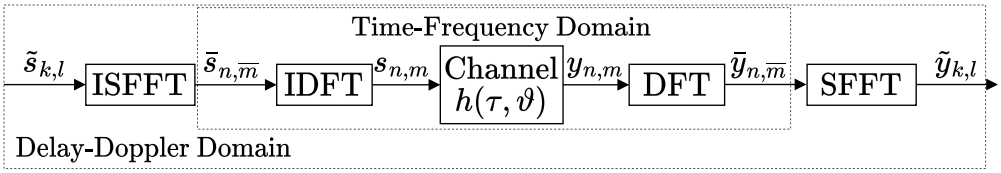


Figure 4.4: System diagram of OTFS transmission scheme.

In time-invariant and frequency-selective fading, the CIR matrix $\mathbf{H}$ of Eq. (4.3) is circulant, i.e. row $m+1$ is a right shift of row m, leading to a diagonal matrix for $\overline{\mathbf{H}}_n = \mathbf{F}_M \mathbf{H}_n \mathbf{F}_M^H$. As a result, the OFDM subcarriers are orthogonal to each other, leading to the following element-wise input-output relationship:

$$\overline{y}_{n,\overline{m}} = \sqrt{T}\overline{h}_{n,\overline{m}}\overline{s}_{n,\overline{m}} + \overline{v}_{n,\overline{m}}, \tag{4.5}$$

where $\overline{h}_{n,\overline{m}} = \sum_{l=0}^{L-1} h_{n,\overline{m},l}\omega_M^{-\overline{m}l}$ is the $\overline{m}$th diagonal element in $\overline{\mathbf{H}}_n$, and $h_{n,\overline{m},l}$ stands for the fading gain in the TD. Therefore, single-tap FD Equalization (FDE) can be invoked as follows:

$$\overline{z}_{n,\overline{m}} = \overline{y}_{n,\overline{m}}/\overline{h}_{n,\overline{m}}, 0 \leq \overline{m} \leq M-1. \tag{4.6}$$

However, when the fading channel becomes time-varying in the face of the Doppler effect, especially when the Doppler frequency f_D becomes comparable to the Subcarrier Spacing (SCS) Δf, the OFDM subcarrier orthogonality no longer holds, which imposes ICI. As a result, the TD fading matrix has to be equalized as a whole, leading to the following FD- Minimum Mean-Squared Error (MMSE) detector:

$$\overline{\mathbf{z}}_n = \left(\overline{\mathbf{H}}_n^H \overline{\mathbf{H}}_n + N_0 \mathbf{I}_M\right)^{-1} \overline{\mathbf{H}}_n^H \overline{\mathbf{y}}_n, \tag{4.7}$$

where N_0 represent the power of the AWGN[4].

4.2.2.2 OTFS based Quantum Transmission

As portrayed by Fig. 4.4, the OTFS transmitter modulates a total number of NM symbols in the DD domain as $\left\{\{\widetilde{s}_{k,l}\}_{k=0}^{N-1}\right\}_{l=0}^{M-1}$, which is transformed into the FD via the

[4]Note that the value of N_0 is to evaluate the noise level as the signal power is normalized to 1 in simulation. But both the realistic signal and noise powers will be elaborated on in Sec. 4.4.

inverse symplectic finite Fourier transform Inverse SFFT (ISFFT):

$$\overline{s}_{n,\overline{m}} = \frac{1}{\sqrt{NM}} \sum_{k=0}^{N-1} \sum_{l=0}^{M-1} \widetilde{s}_{k,l} \omega_N^{nk} \omega_M^{-\overline{m}l}, \tag{4.8}$$

where n, $\overline{m}$, k and l refer to the symbol index, sample index, Doppler index and delay index, respectively. Furthermore, the DD domain symbol $\widetilde{s}_{0,k,l}$ is used to represent the preparation thermal noise and the corresponding signal in FD can be derived into $\overline{s}_{0,n,m}$ using the same operation in Eq. (4.8). Then, an IDFT operation is applied to the FD signal $\overline{s}_{n,\overline{m}}$, hence the TD signal is generated as

$$s_{n,m} = \frac{1}{\sqrt{M}} \sum_{\overline{m}=0}^{M-1} \overline{s}_{n,\overline{m}} \omega_M^{m\overline{m}} = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \widetilde{s}_{k,m} \omega_N^{nk}. \tag{4.9}$$

The same operation from Eq. (4.9) can be applied to the FD signal $\overline{s}_{0,n,m}$ to get $s_{0,n,m}$.

Accordingly, the received TD signal can be expressed as

$$\begin{aligned} y_{n,m} =& \sqrt{T} \sum_{p=0}^{P-1} \widetilde{h}_p \omega_{MN}^{k_p[n(M+M_{cp})+m-l_p]} s_{n,<m-l_p>_M} \\ &+ \sqrt{T} \sum_{p=0}^{P-1} \widetilde{h}_p \omega_{MN}^{k_p[n(M+M_{cp})+m-l_p]} s_{0,n,<m-l_p>_M} \\ &+ \sqrt{1-T} s_{En,m} \\ &= \sqrt{T} \sum_{p=0}^{P-1} \widetilde{h}_p \omega_{MN}^{k_p[n(M+M_{cp})+m-l_p]} s_{n,<m-l_p>_M} + v_{n,m}, \end{aligned} \tag{4.10}$$

where P paths fall into L resolvable TDL, i.e. $P = \sum_{l=0}^{L-1} P_l$, while $\widetilde{h}_p$ and M_{cp} represent the fading gain and the length of the Cyclic Prefix (CP), respectively. Following this, the received FD signal is obtained by the DFT as follows:

$$\begin{aligned} \overline{y}_{n,\overline{m}} &= \sqrt{T} \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} y_{n,m} \omega_M^{-m\overline{m}} \\ &= \sqrt{T} \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} \sum_{p=0}^{P-1} \widetilde{h}_p s_{n,<m-l_p>_M} \cdot \\ &\quad \omega_{MN}^{k_p[n(M+M_{cp})+m-l_p]} \omega_M^{-m\overline{m}} + \overline{v}_{n,\overline{m}}. \end{aligned} \tag{4.11}$$

Finally, the DD domain signal can be obtained by using the Symplectic Finite Fourier Transform (SFFT) operation as

$$\begin{aligned} \widetilde{y}_{k,l} &= \sqrt{T} \frac{1}{\sqrt{MN}} \sum_{n=0}^{N-1} \sum_{\overline{m}=0}^{M-1} \overline{y}_{n,\overline{m}} \omega_N^{-nk} \omega_M^{\overline{m}l} \\ &= \sqrt{T} \sum_{p=0}^{P-1} \widetilde{h}_p \omega_{MN}^{k_p(l-l_p)} \widetilde{s}_{<k-k_p>_N,<l-l_p>_M} + \widetilde{v}_{k,l}. \end{aligned} \tag{4.12}$$

There are two ways of appending CP in OTFS, namely the one using a single CP for the entire OTFS frame and the other one where a CP is inserted in each symbol duration. If a single CP is added to the entire OTFS frame, the TD circular convolution of Eq. (4.10) becomes MN-periodic according to

$$\begin{aligned} y_{n,m} =& \sqrt{T} \sum_{p=0}^{P-1} \widetilde{h}_p \omega_{MN}^{k_p[nM+m-l_p]} s_{<nM+m-l>_{MN}} \\ &+ v_{n,m}, \end{aligned} \tag{4.13}$$

where

$$s_{<nM+m-l>_{MN}} = \begin{cases} s_{n,<m-l>_M}, & m \geq l \\ s_{n-1,<m-l>_M}, & m < l \end{cases}. \tag{4.14}$$

As a result, the input-output relationship of Eq. (4.12) becomes [158]

$$\begin{aligned} \widetilde{y}_{k,l} =& \sqrt{T} \sum_{p=0}^{P-1} \widetilde{h}_p \widetilde{T}(k,l,k_p,l_p) \widetilde{s}_{<k-k_p>_N,<l-l_p>_M} \\ &+ \widetilde{v}_{k,l}, \end{aligned} \tag{4.15}$$

where the DD index-based phase rotations are defined as

$$\widetilde{T}(k,l,k_p,l_p) = \begin{cases} \omega_{MN}^{k_p(<l-l_p>_M)}, & l \geq l_p \\ \omega_N^{-(k-k_p)} \omega_{MN}^{k_p(l-l_p)} = \omega_N^{-k} \omega_{MN}^{k_p(<l-l_p>_M)}, & l < l_p. \end{cases} \tag{4.16}$$

In summary, the OTFS input-output relationship of Eq. (4.12) and Eq. (4.15) can be expressed in the following matrix form:

$$\widetilde{\mathbf{y}} = \sqrt{T} \widetilde{\mathbf{H}} \widetilde{\mathbf{s}} + \widetilde{\mathbf{v}}, \tag{4.17}$$

where $\widetilde{\mathbf{y}} \in \mathcal{C}^{MN \times 1}$ and the κth element of $\widetilde{\mathbf{y}}$ is given by $\widetilde{\mathbf{y}}[\kappa] = \widetilde{y}_{k,l}$, where $k = \lfloor \frac{\kappa}{M} \rfloor$, $l = \kappa - kM$. Similarly, the κth elements of $\widetilde{\mathbf{s}} \in \mathcal{C}^{MN \times 1}$ and of $\widetilde{\mathbf{v}} \in \mathcal{C}^{MN \times 1}$ are given by $\widetilde{\mathbf{s}}[\kappa] = \widetilde{s}_{k,l}$, and $\widetilde{\mathbf{v}}[\kappa] = \widetilde{v}_{k,l}$, respectively, where $\widetilde{\mathbf{v}} = \sqrt{T} \widetilde{\mathbf{H}} \widetilde{\mathbf{s}}_0 + \sqrt{1-T} \widetilde{\mathbf{s}}_E$. Moreover, the DD domain fading matrix $\widetilde{\mathbf{H}} \in \mathcal{C}^{MN \times MN}$is time-invariant and sparse, where the non-zero elements are given by $\widetilde{\mathbf{H}}_{\kappa,\iota} = \widetilde{h}_p \omega_{MN}^{k_p(l-l_p)}$ and $\widetilde{\mathbf{H}}_{\kappa,\iota} = \widetilde{h}_p \widetilde{T}(k,l,k_p,l_p)$ for Eq. (4.12) and Eq. (4.15), respectively. Based on Eq. (4.17), the DD-MMSE detector can be formulated as

$$\widetilde{\mathbf{z}} = \left(\widetilde{\mathbf{H}}^H \widetilde{\mathbf{H}} + N_0 \mathbf{I}_{MN} \right)^{-1} \widetilde{\mathbf{H}}^H \widetilde{\mathbf{y}}. \tag{4.18}$$

4.2.3 Modified MDR for OFDM/OTFS in Doubly Selective THz Channels

As portrayed in Fig. 4.2, the MDR process [105, 121] is employed for enhancing the CV-QKD performance in THz quantum channels, which is summarized as follows:

1. Bob generates the secret key $\mathbf{b}$ using a QRNG. An LDPC syndrome $\mathbf{s}^B$ generated based on the key is transmitted to Alice in a classical channel in preparation for error correction.

2. The Gaussian variables $\ddot{\mathbf{s}}$ are transmitted by Alice either in the FD based on OFDM as $\bar{\mathbf{s}}$ or in the DD domain based on OTFS as $\widetilde{\mathbf{s}}$, as shown in Fig. 4.2.

3. Bob maps the key onto a D-dimansional unit-radius sphere $\mathbf{u}^B$. For this work, we use $D = 8$ as suggested in [105, 121], resulting in the 8-dimensional unit-radius sphere of $\mathbf{u}_i^B = \left[\frac{(-1)^{\mathbf{b}_i(0)}}{\sqrt{D}}, \frac{(-1)^{\mathbf{b}_i(1)}}{\sqrt{D}}, \ldots, \frac{(-1)^{\mathbf{b}_i(D-1)}}{\sqrt{D}}\right]$, where i represents the ith segment in the MDR process. The MDR mapping function ensures that the ideally error-free transmission of Gaussian variables leads to the same unit-radius sphere at the receiver, i.e., $\mathbf{M}(\ddot{\mathbf{s}}_i', \mathbf{u}_i^B)\ddot{\mathbf{s}}_i' = \mathbf{u}_i^B$.

4. On Bob's side, the Gaussian variables are received and equalized either in the FD as $\bar{\mathbf{z}}$ based on the OFDM scheme of Eq. (4.6) and Eq. (4.7) or in the DD domain as $\widetilde{\mathbf{z}}$ based on the OTFS of Eq. (4.18), providing input to the receiver's MDR process as $\ddot{\mathbf{z}}$. The MDR mapping function that ensures $\mathbf{M}(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B)\ddot{\mathbf{z}}_i' = \mathbf{u}_i^B$ is sent from Bob to Alice through a classical channel.

5. Alice demodulates $\ddot{\mathbf{s}}'$ based on the MDR mapping function, producing soft-decision log likelihood ratios (LLRs) for the LDPC decoder to recover the key with the aid of the syndrome-based side information.

However, the conventional MDR found in [75, 160] generally assume a BI-AWGN channel, where the noise variance of LLR computation is uniform across all received Gaussian variables. By contrast, the OFDM FDE decision variables $\bar{z}_{\overline{m}}$ in Eq. (4.6) have a noise variance that remains constant for each subcarrier index in time-invariant fading, but it varies from subcarrier to subcarrier. The OFDM FD-MMSE decision variables $\bar{\mathbf{z}}[\overline{m}]$ in Eq. (4.7) have a noise variance that is consistent for each subcarrier index in doubly selective fading. Moreover, the OTFS DD-MMSE decision variables have a noise variance that is always consistent for each DD index. In light of this, we propose to modify both the OFDM and OTFS transmission arrangement for MDR, which is exemplified by Fig. 4.5, so that the MDR demapper produces reliable LLRs based on consistent noise variance.

More explicitly, the parameters of $M = 16$ and $N = 16$ are used for the $D = 8$ MDR of OFDM/OTFS in Fig. 4.5. Therefore, an LDPC block length of $N_{\text{FEC}} = 2048$ includes $N_{bl} = N_{\text{FEC}}/(M \times N) = 2048/(16 \times 16) = 8$ OFDM/OTFS frames[5]. For the OFDM transmission of Fig. 4.5(a), each $(M \times N) = (16 \times 16)$-element OFDM symbol block is divided into $N_{sb} = N/D = 16/8 = 2$ sub-blocks of $(M \times D) = (16 \times 8)$ elements, so that each MDR segment is formed by $D = 8$ FD symbols on each

[5]Note that BPSK associated with LDPC is considered in our treatise.

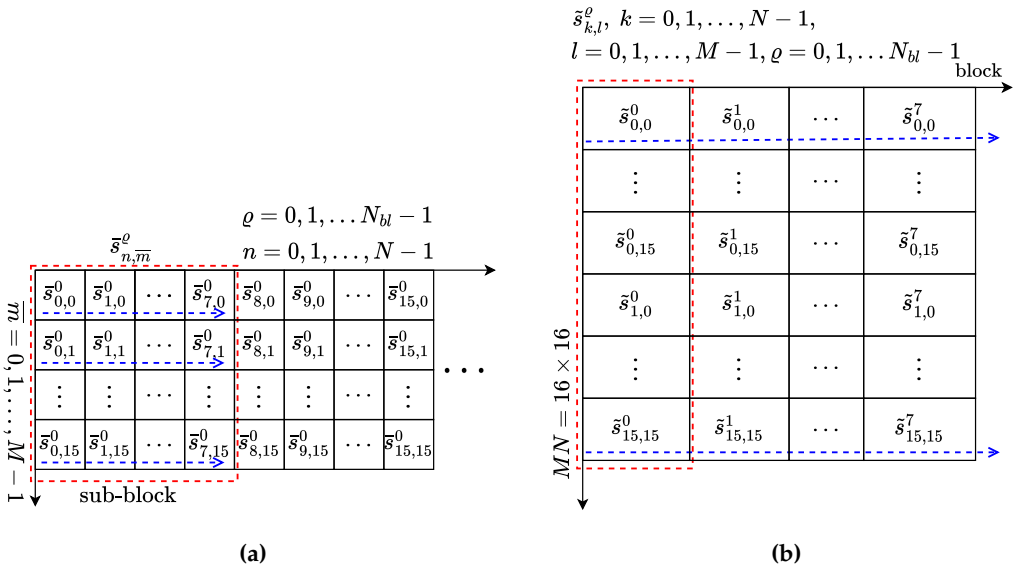


Figure 4.5: An example of transmission arrangements for (a) **OFDM**- and (b) **OTFS**-LDPC assisted CV-QKD, where $N = M = 16$.

subcarrier. This arrangement that represents the ith segment is denoted as $\bar{\mathbf{s}}_i^{\text{MDR}} = \left[\bar{s}_{i,0}^{\text{MDR}}, \cdots, \bar{s}_{i,d}^{\text{MDR}}, \cdots, \bar{s}_{i,D-1}^{\text{MDR}}\right]^T$, where $\bar{s}_{i,d}^{\text{MDR}}$, $d = 0, 1, ..., D-1$ represents the dth element in the ith segment, and the relationship between $\bar{s}_{i,d}^{\text{MDR}}$ and $\bar{s}^{\varrho}_{n,\overline{m}}$ is as follows: $\bar{s}_{i,d}^{\text{MDR}} = \bar{s}^{\varrho}_{n,\overline{m}}$ when $i = \lfloor n/D \rfloor \cdot M + \overline{m} + \varrho\,(N/D \cdot M)$ and $d = \text{rem}(n, D)$, where $n = 0, 1, ..., N-1$, $\overline{m} = 0, 1, ..., M-1$ and $\varrho = 0, 1, ..., N_{bl} - 1$. For the OTFS transmission arrangement of Fig. 4.5(b), a total number of $D = 8$ symbols on each DD index form a MDR segment, the ith of which is denoted as $\widetilde{\mathbf{s}}_i^{\text{MDR}} = [\widetilde{s}_{i,0}^{\text{MDR}}, \cdots, \widetilde{s}_{i,d}^{\text{MDR}}, \cdots, \widetilde{s}_{i,D-1}^{\text{MDR}}]^T$, where $\widetilde{s}_{i,d}^{\text{MDR}}$, $d = 0, 1, ..., D-1$ represents the dth element in the ith segment, and the relationship between $\widetilde{s}_{i,d}^{\text{MDR}}$ and $\widetilde{s}^{\varrho}_{k,l}$ is as follows: $\widetilde{s}_{i,d}^{\text{MDR}} = \widetilde{s}^{\varrho}_{k,l}$ when $i = k \cdot M + l$ and $d = \varrho$, where $k = 0, 1, ..., N-1$ and $l = 0, 1, ..., M-1$ and $\varrho = 0, 1, ..., N_{bl} - 1$. Hence, 8 OTFS symbol blocks are enough to transmit 2048 symbols.

4.2.4 Modified MDR Decoding for OFDM/OTFS in Doubly Selective THz Channels

Based on the modified OFDM/OTFS transmission pattern introduced in Sec. 4.2.3, the revised MDR process tailored for OFDM/OTFS in doubly selective THz channels is summarized in Algorithm 4. Let us introduce the steps of Algorithm 4 based on the OFDM FDE mechanism and then generalize it to OFDM FD-MMSE and OTFS DD-MMSE.

Algorithm 4: The description of MDR scheme conceived for OFDM/OTFS in time-varying and frequency-selective THz fading channels, where the OFDM FDE mechanism is assumed.

1 **Partition:** The sequences $\ddot{\mathbf{s}}$ of Alice's and $\ddot{\mathbf{z}}$ of Bob's data after sifting, whose length is the same as a FEC codeword length N_{FEC}, are partitioned into shorter segments, which can be denoted as $\ddot{\mathbf{s}} = [\ddot{\mathbf{s}}_0; \ddot{\mathbf{s}}_1; ...; \ddot{\mathbf{s}}_{I-1}]$ and $\ddot{\mathbf{z}} = [\ddot{\mathbf{z}}_0; \ddot{\mathbf{z}}_1; ...; \ddot{\mathbf{z}}_{I-1}]$, where $I = N_{\mathrm{FEC}}/D$, and $\ddot{\mathbf{s}}_i, \ddot{\mathbf{z}}_i \in \mathcal{R}^{D\times 1}$. Furthermore, the channel coefficient is also partitioned into $\ddot{\mathbf{h}} = \left[\ddot{\mathbf{h}}_0; \ddot{\mathbf{h}}_1; ...; \ddot{\mathbf{h}}_{I-1}\right]$.

2 **Normalization:** Normalize each segment of $\ddot{\mathbf{s}}_i$ and $\ddot{\mathbf{z}}_i$ by $\ddot{\mathbf{s}}'_i = \frac{\ddot{\mathbf{s}}_i}{\|\ddot{\mathbf{s}}_i\|}$ and $\ddot{\mathbf{z}}'_i = \frac{\ddot{\mathbf{z}}_i}{\|\ddot{\mathbf{z}}_i\|}$, where we have $\|\ddot{\mathbf{s}}_i\| = \sqrt{\langle \ddot{\mathbf{s}}_i, \ddot{\mathbf{s}}_i \rangle} = \sqrt{\sum_{d=0}^{D-1} \ddot{\mathbf{s}}_i(d)^2}$ and $\|\ddot{\mathbf{z}}_i\| = \sqrt{\langle \ddot{\mathbf{z}}_i, \ddot{\mathbf{z}}_i \rangle} = \sqrt{\sum_{d=0}^{D-1} \ddot{\mathbf{z}}_i(d)^2}$

3 **QRNG generation:** At Bob's side, a random bit stream $\mathbf{b}$ is generated via QRNG, the length of which is the same as a FEC codeword length N_{FEC}. Then, the random bit sequence is $\mathbf{b}$ partitioned into $\mathbf{b} = [\mathbf{b}_0; \mathbf{b}_1; ...; \mathbf{b}_{I-1}]$, where $I = N_{\mathrm{FEC}}/D$ and $\mathbf{b}_i$ is a D-dimensional binary column vector. For each segment of $\mathbf{b}_i, i = 0, 1, ..., I-1$, it is mapped to the unit sphere of $\mathbf{u}_i^B = \left(\frac{(-1)^{\mathbf{b}_i(0)}}{\sqrt{D}}, \frac{(-1)^{\mathbf{b}_i(1)}}{\sqrt{D}}, \ldots, \frac{(-1)^{\mathbf{b}_i(D-1)}}{\sqrt{D}}\right)$.

4 **Mapping function calculation:** Bob calculates the mapping function $\mathbf{M}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right)$ for each segment with $\mathbf{M}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right)\ddot{\mathbf{z}}'_i = \mathbf{u}_i^B$ using the following formula:

$$\mathbf{M}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right) = \sum_{d=0}^{D-1} \alpha_i^d \mathbf{A}_d,$$

where α_i^d is the dth element of $\boldsymbol{\alpha}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right) = \left(\alpha_i^0, \alpha_i^1, ..., \alpha_i^{D-1}\right)^T$, which is the coordinate of the vector $\mathbf{u}_i^B$ under orthonormal basis $(\mathbf{A}_0\ddot{\mathbf{z}}'_i, \mathbf{A}_1\ddot{\mathbf{z}}'_i, ..., \mathbf{A}_{D-1}\ddot{\mathbf{z}}'_i)$ and it can be expressed as $\boldsymbol{\alpha}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right) = \left(\mathbf{A}_0\ddot{\mathbf{z}}'_i, \mathbf{A}_1\ddot{\mathbf{z}}'_i, ..., \mathbf{A}_{D-1}\ddot{\mathbf{z}}'_i\right)^T \mathbf{u}_i^B$. Note that $\mathbf{A}_d, d = 0, 1, ..., D-1$ is the orthogonal matrix of size $D \times D$ and has been provided in the Appendix of [105, 121].

5 **Mapping function implement:** Alice operates the same data mapping on $\ddot{\mathbf{s}}'_i$ to map the Gaussian distributed vector to $\mathbf{u}_i^A = \mathbf{M}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right)\ddot{\mathbf{s}}'_i$, which is a noise version of $\mathbf{u}_i^B$.

6 **LLR calculation:** LLR is calculated in the way of

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\|\ddot{\mathbf{s}}_i\|\|\ddot{\mathbf{z}}_i\|\left\|\ddot{\mathbf{h}}_i\right\|^2/D}{\sqrt{D}\sigma^2}\mathbf{u}_i^A[d],$$

with the assumption that in each segment, all of the channel coefficients remain the same, which is $\ddot{\mathbf{h}}_i[d] = \overline{\overline{h}}_i, \forall d \in [0, D-1]$. Then, the LLR for a whole FEC block length $\mathcal{L}\left(\mathbf{u}^A\right)$ can be constructed by those segments of $\mathcal{L}\left(\mathbf{u}_i^A\right)$, which gives

$$\mathcal{L}\left(\mathbf{u}^A\right) = \left[\mathcal{L}\left(\mathbf{u}_1^A\right); \mathcal{L}\left(\mathbf{u}_2^A\right); ...; \mathcal{L}\left(\mathbf{u}_I^A\right)\right].$$

Then, FEC decoding is carried on with the input of $\mathcal{L}\left(\mathbf{u}^A\right)$.

Consider a sequence of ϱ OFDM blocks with $\varrho = 0, 1, ..., N_{bl} - 1$ where $N_{bl} = N_{\text{FEC}}/(MN)$, Eq. (4.6) can be reformulated as

$$\overline{z}_{n,\overline{m}}^{\varrho} = \overline{y}_{n,\overline{m}}^{\varrho} / \overline{h}_{n,\overline{m}}^{\varrho} = \overline{s}_{n,\overline{m}}^{\varrho} + \overline{v}_{n,\overline{m}}^{\varrho} / \overline{h}_{n,\overline{m}}^{\varrho}. \tag{4.19}$$

Therefore, based on the corresponding demapping process of Fig. 4.5, the relationship between the transmitted and segmented signal after sifting - for example taking the real part of all complex values in Eq. (4.19) - can be denoted as $\ddot{\mathbf{s}}_i = \mathfrak{Re}\left[\bar{\mathbf{s}}_i^{\text{MDR}}\right] = \mathfrak{Re}\left[\bar{s}_{i,0}^{\text{MDR}}, \cdots, \bar{s}_{i,d}^{\text{MDR}}, \cdots, \bar{s}_{i,D-1}^{\text{MDR}}\right]^T$, where $\bar{s}_{i,d}^{\text{MDR}} = \bar{s}_{n,\overline{m}}^{\varrho}$ represents the dth element in the ith segment with $i = \lfloor n/D \rfloor \cdot M + \overline{m} + \varrho\,(N/D \cdot M)$ and $d = \text{rem}(n, D)$, while $n = 0, 1, ..., N-1$, $\overline{m} = 0, 1, ..., M-1$ and $\varrho = 0, 1, ..., N_{bl} - 1$. Similarly, the relationship between the received and segmented signal after sifting is $\ddot{\mathbf{z}}_i = \mathfrak{Re}\left[\bar{\mathbf{z}}_i^{\text{MDR}}\right] = \mathfrak{Re}\left[\bar{z}_{i,0}^{\text{MDR}}, \cdots, \bar{z}_{i,d}^{\text{MDR}}, \cdots, \bar{z}_{i,D-1}^{\text{MDR}}\right]^T$ with $\bar{z}_{i,d}^{\text{MDR}} = \bar{z}_{n,\overline{m}}^{\varrho}$. Upon taking the real part of the noise term $\overline{v}_{n,\overline{m}}^{\varrho} / \overline{h}_{n,\overline{m}}^{\varrho}$ in Eq. (4.19) as $\ddot{v}$, the ith segment of the noise term can be denoted as $\ddot{\mathbf{v}}_i = \mathfrak{Re}\left[\left(\text{diag}\left(\ddot{\mathbf{h}}_i\right)\right)^{-1} \ddot{\mathbf{v}}_i'\right]$, where $\ddot{\mathbf{h}}_i = \left[\overline{h}_{i,0}^{\text{MDR}}, \cdots, \overline{h}_{i,d}^{\text{MDR}}, \cdots, \overline{h}_{i,D-1}^{\text{MDR}}\right]^T$ with $\overline{h}_{i,d}^{\text{MDR}} = \overline{h}_{n,\overline{m}}^{\varrho}$, and $\ddot{\mathbf{v}}_i' = \left[\overline{v}_{i,0}^{\text{MDR}}, \cdots, \overline{v}_{i,d}^{\text{MDR}}, \cdots, \overline{v}_{i,D-1}^{\text{MDR}}\right]^T$ with $\overline{v}_{i,d}^{\text{MDR}} = \overline{v}_{n,\overline{m}}^{\varrho}$. In summary, the system model used for our MDR algorithm of the ith segment can be expressed as

$$\ddot{\mathbf{z}}_i = \ddot{\mathbf{s}}_i + \ddot{\mathbf{v}}_i. \tag{4.20}$$

The MDR process therefore spans from step 1-Partition to step 6-LLR calculation as illustrated in Algorithm 4. As for the LLR calculation, the details are as follows. After Alice receives the mapping matrix $\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)$ and $\|\ddot{\mathbf{z}}_i\|$ for each segment, she applies the same mapping to her data $\ddot{\mathbf{s}}_i'$ to obtain $\mathbf{u}_i^A = \mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\ddot{\mathbf{s}}_i'$. By introducing a scaling factor of $\frac{\|\ddot{\mathbf{s}}_i\|}{\|\ddot{\mathbf{z}}_i\|}$, she obtains

$$\begin{aligned} \mathbf{u}_i^{A\prime} &= \frac{\|\ddot{\mathbf{s}}_i\|}{\|\ddot{\mathbf{z}}_i\|}\mathbf{u}_i^A = \frac{\|\ddot{\mathbf{s}}_i\|}{\|\ddot{\mathbf{z}}_i\|}\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\ddot{\mathbf{s}}_i' \\ &= \mathbf{u}_i^B - \frac{1}{\|\ddot{\mathbf{z}}_i\|}\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\mathfrak{Re}\left[\left(\text{diag}\left(\ddot{\mathbf{h}}_i\right)\right)^{-1}\ddot{\mathbf{v}}_i'\right]. \end{aligned} \tag{4.21}$$

Now, we assume that in each segment, all the channel coefficients are the same, which gives $\ddot{\mathbf{h}}_i[d] = \ddot{h}_{i,0} \triangleq \overline{\ddot{h}}_i, \forall d \in [0, D-1]$. Furthermore, $\ddot{h}_{i,d} = \overline{h}_{n,\overline{m}}^{\varrho}$ with $i = \lfloor n/D \rfloor \cdot M + \overline{m} + \varrho\,(N/D \cdot M)$ and $d = \text{rem}(n, D)$, while $n = 0, 1, ..., N-1$, $\overline{m} = 0, 1, ..., M-1$ and $\varrho = 0, 1, ..., N_{bl} - 1$. Hence, $\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\mathfrak{Re}\left[\left(\text{diag}\left(\ddot{\mathbf{h}}_i\right)\right)^{-1}\ddot{\mathbf{v}}_i'\right]$ can be derived as

$$\begin{aligned} &\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\mathfrak{Re}\left[\left(\text{diag}\left(\ddot{\mathbf{h}}_i\right)\right)^{-1}\ddot{\mathbf{v}}_i'\right] = \mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\mathfrak{Re}\left(\frac{\overline{\ddot{h}}_i^*\ddot{\mathbf{v}}_i'}{\left\|\overline{\ddot{h}}_i\right\|^2}\right) \\ &= \frac{1}{\left\|\overline{\ddot{h}}_i\right\|^2}\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\left(\mathfrak{Re}\left(\overline{\ddot{h}}_i\right)\mathfrak{Re}\left(\ddot{\mathbf{v}}_i'\right) + \mathfrak{Im}\left(\overline{\ddot{h}}_i\right)\mathfrak{Im}\left(\ddot{\mathbf{v}}_i'\right)\right) \\ &= \frac{1}{\left\|\overline{\ddot{h}}_i\right\|^2}\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\left(\ddot{\mathbf{v}}_i'^R + \ddot{\mathbf{v}}_i'^I\right) = \frac{1}{\left\|\overline{\ddot{h}}_i\right\|^2}\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\ddot{\mathbf{v}}_i^{\dagger}, \end{aligned} \tag{4.22}$$

where $\ddot{\mathbf{v}}_i'^R \sim \mathcal{N}\left(0, \left[\mathfrak{Re}\left(\overline{\ddot{h}}_i\right)\right]^2 \sigma^2 \mathbb{I}_8\right)$, $\ddot{\mathbf{v}}_i'^I \sim \mathcal{N}\left(0, \left[\mathfrak{Im}\left(\overline{\ddot{h}}_i\right)\right]^2 \sigma^2 \mathbb{I}_8\right)$ with $N_0 = 2\sigma^2$, and hence $\ddot{\mathbf{v}}^\dagger \sim \mathcal{N}\left(0, \left\|\overline{\ddot{h}}_i\right\|^2 \sigma^2 \mathbb{I}_8\right)$. Thereby, Eq. (4.21) can be reformulated as

$$\mathbf{u}_i^{A'} = \mathbf{u}_i^B - \frac{1}{\|\ddot{\mathbf{z}}_i\|} \frac{1}{\left\|\overline{\ddot{h}}_i\right\|^2} \mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right) \ddot{\mathbf{v}}_i^\dagger = \mathbf{u}_i^B - \frac{1}{\|\ddot{\mathbf{z}}_i\|} \frac{1}{\left\|\overline{\ddot{h}}_i\right\|^2} \ddot{\mathbf{v}}_i^\ddagger, \tag{4.23}$$

where $\ddot{\mathbf{v}}_i^\ddagger \sim \mathcal{N}\left(0, \left\|\overline{\ddot{h}}_i\right\|^2 \sigma^2 \mathbb{I}_8\right)$ is the new noise vector after mapping, which has zero mean and a constant variance for the entire segment.

Based on this, the LLR of the sequence in one segment can be calculated by

$$\begin{aligned} \mathcal{L}\left(\mathbf{u}_i^{A'}[d]\right) &= \frac{\mathbb{P}\left(\mathbf{u}_i^{A'}[d]\right) | \mathbf{b}_i[d] = 0)}{\mathbb{P}\left(\mathbf{u}_i^{A'}[d]\right) | \mathbf{b}_i[d] = 1)} \\ &= \ln \frac{\frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{\|\ddot{\mathbf{z}}_i\|^2 \left\|\overline{\ddot{h}}_i\right\|^4 \left(\frac{1}{\sqrt{D}} - \mathbf{u}_i^A[d]\right)^2}{2\pi \left\|\overline{\ddot{h}}_i\right\|^2 \sigma^2}}}{\frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{\|\ddot{\mathbf{z}}_i\|^2 \left\|\overline{\ddot{h}}_i\right\|^4 \left(-\frac{1}{\sqrt{D}} - \mathbf{u}_i^A[d]\right)^2}{2\pi \left\|\overline{\ddot{h}}_i\right\|^2 \sigma^2}}} = \frac{2\|\ddot{\mathbf{z}}_i\| \left\|\overline{\ddot{h}}_i\right\|^2 \mathbf{u}_i^{A'}[d]}{\sqrt{D}\sigma^2} \end{aligned} \tag{4.24}$$

By replacing $\mathbf{u}_i^{A'}$ with $\mathbf{u}_i^A$ using the relationship of $\mathbf{u}_i^{A'} = \frac{\|\ddot{\mathbf{s}}_i\|}{\|\ddot{\mathbf{z}}_i\|} \mathbf{u}_i^A$, Eq. (4.24) can be reformulated as

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\|\ddot{\mathbf{s}}_i\| \|\ddot{\mathbf{z}}_i\| \|\overline{\ddot{h}}_i\|^2}{\sqrt{D} N_0/2} \mathbf{u}_i^A[d]. \tag{4.25}$$

It becomes clear now that Eq. (4.25) incorporates the LLR calculations for MDR as seen in the literature that assume BI-AWGN as a special case [75, 160]. Explicitly, for the special case of a BI-AWGN channel, i.e. where we have $\ddot{\mathbf{h}}_i = \mathbf{1}_{D\times 1}, \forall i \in [0, I-1]$, the LLR for each segment is given by:

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\|\ddot{\mathbf{s}}_i\| \|\ddot{\mathbf{z}}_i\|}{\sqrt{D} N_0/2} \mathbf{u}_i^A[d]. \tag{4.26}$$

In summary, the LLR calculations Eq. (4.25) produce reliable demapping soft-decisions for MDR in fading channels, and the LLRs are passed to the LDPC decoder for further error correction.

Apart from the FDE detection, both the OFDM FD-MMSE of Eq. (4.7) and the OTFS DD-MMSE of Eq. (4.18) can also be appropriately adapted for Algorithm 4. For OFDM FD-MMSE, Eq. (4.7) can be further reformulated as

$$\overline{\mathbf{z}}_n^\varrho = \overline{\mathbf{G}}_n^\varrho \overline{\mathbf{y}}_n^\varrho \quad = \overline{\mathbf{H}}_n^{\varrho\prime} \overline{\mathbf{s}}_n^\varrho + \overline{\mathbf{G}}_n^\varrho \overline{\mathbf{v}}_n^\varrho, \tag{4.27}$$

where $\overline{\mathbf{G}}_n^{\varrho} = \left(\overline{\mathbf{H}}_n^{\varrho\,H}\overline{\mathbf{H}}_n^{\varrho} + N_0\mathbf{I}_M\right)^{-1}\overline{\mathbf{H}}_n^{\varrho\,H}$, and $\overline{\mathbf{H}}_n^{\varrho\prime} = \overline{\mathbf{G}}_n^{\varrho}\cdot\overline{\mathbf{H}}_n^{\varrho} = \left(\overline{\mathbf{H}}_n^{\varrho\,H}\overline{\mathbf{H}}_n^{\varrho} + N_0\mathbf{I}_M\right)^{-1}\cdot \overline{\mathbf{H}}_n^{\varrho\,H}\overline{\mathbf{H}}_n^{\varrho}$. Therefore, the $\overline{m}$th element of $\overline{\mathbf{z}}_n^{\varrho}$ can be approximated as $\overline{z}_{n,\overline{m}}^{\varrho} = \overline{\mathbf{G}}_n^{\varrho}[\overline{m},:]\overline{\mathbf{y}}_n^{\varrho} = \overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m},\overline{m}]\overline{s}_{n,\overline{m}}^{\varrho} + \overline{\mathbf{G}}_n^{\varrho}[\overline{m},:]\overline{\mathbf{v}}_n^{\varrho}$. After compensating the effect of channel fading, the equivalent $\overline{z}_{n,\overline{m}}^{\varrho\prime}$ can be expressed as Eq. (4.28).

$$\begin{aligned}\overline{z}_{n,\overline{m}}^{\varrho\prime} &= \frac{\overline{\mathbf{G}}_n^{\varrho}[\overline{m},:]\overline{\mathbf{y}}_n^{\varrho}\left(\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m},\overline{m}]\right)^*}{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m},\overline{m}]\right\|^2} + \frac{\overline{\mathbf{G}}_n^{\varrho}[\overline{m},:]\overline{\mathbf{v}}_n^{\varrho}\left(\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m},\overline{m}]\right)^*}{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m},\overline{m}]\right\|^2} \\ &= \overline{s}_{n,\overline{m}}^{\varrho} + \overline{v}_{n,\overline{m}}^{\varrho\prime}.\end{aligned} \tag{4.28}$$

The new noise term $\overline{v}_{n,\overline{m}}^{\varrho\prime}$ is still Gaussian distributed with zero mean and a variance of $\frac{\left\|\overline{\mathbf{G}}_n^{\varrho}[\overline{m},:]\right\|^2 N_0}{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m},\overline{m}]\right\|^2}$. Taking for example the real part of $\overline{z}_{n,\overline{m}}^{\varrho\prime}$, we can obtain $\ddot{\mathbf{z}}_i = \ddot{\mathbf{s}}_i + \ddot{\mathbf{v}}_i$ where $\ddot{\mathbf{s}}_i = \mathfrak{Re}\left[\bar{\mathbf{s}}_i^{\mathrm{MDR}}\right] = \mathfrak{Re}\left[\bar{s}_{i,0}^{\mathrm{MDR}},\cdots,\bar{s}_{i,d}^{\mathrm{MDR}},\cdots,\bar{s}_{i,D-1}^{\mathrm{MDR}}\right]^T$ and $\ddot{\mathbf{z}}_i = \mathfrak{Re}\left[\bar{\mathbf{z}}_i^{\mathrm{MDR}}\right] = \mathfrak{Re}\left[\bar{z}_{i,0}^{\mathrm{MDR}},\cdots,\bar{z}_{i,d}^{\mathrm{MDR}},\cdots,\bar{z}_{i,D-1}^{\mathrm{MDR}}\right]^T$ with $i = \lfloor n/D\rfloor\cdot M + \overline{m} + \varrho\,(N/D\cdot M)$ and $d = \mathrm{rem}(n,D)$, while $n = 0,1,...,N-1$, $\overline{m} = 0,1,...,M-1$ and $\varrho = 0,1,...,N_{bl}-1$. Moreover, $\bar{s}_{i,d}^{\mathrm{MDR}} = \bar{s}_{n,\overline{m}}^{\varrho\prime}$ and $\bar{z}_{i,d}^{\mathrm{MDR}} = \bar{z}_{n,\overline{m}}^{\varrho\prime}$ represent the dth element in the ith segment of $\bar{s}_i^{\mathrm{MDR}}$ and $\bar{z}_i^{\mathrm{MDR}}$, respectively. Taking the real part of the noise term in Eq. (4.28), the ith segment of noise term can be denoted as $\ddot{\mathbf{v}}_i = \mathfrak{Re}\left[\bar{v}_{i,0}^{\mathrm{MDR}},\cdots,\bar{v}_{i,d}^{\mathrm{MDR}},\cdots,\bar{v}_{i,D-1}^{\mathrm{MDR}}\right]^T$ with $\bar{v}_{i,d}^{\mathrm{MDR}} = \overline{v}_{n,\overline{m}}^{\varrho\prime}$. Hence, the variance of each element of the noise $\ddot{\mathbf{v}}_i$ becomes $\frac{\left\|\overline{\mathbf{G}}_n^{\varrho}[\overline{m},:]\right\|^2 N_0/2}{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m},\overline{m}]\right\|^2}$. Thereafter, the MDR process is carried out based on Algorithm 4, where $\ddot{\mathbf{v}}_i[d] = \ddot{\mathbf{v}}_i[0]$, i.e. $\bar{v}_{i,d}^{\mathrm{MDR}} = \bar{v}_{i,0}^{\mathrm{MDR}}, \forall d \in [0, D-1]$. By replacing the noise variance in Eq. (4.26), the corresponding LLR calculation associated with FD-MMSE detection in OFDM transmission can be obtained as

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\left\|\ddot{\mathbf{s}}_i\right\|\left\|\ddot{\mathbf{z}}_i\right\|}{\sqrt{D}}\frac{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m},\overline{m}]\right\|^2}{\left\|\overline{\mathbf{G}}_n^{\varrho}[\overline{m},:]\right\|^2 N_0/2}\mathbf{u}_i^A[d]. \tag{4.29}$$

In OTFS transmission, similar to Eq. (4.29), the LLR calculation associated with DD-MMSE detection in OTFS transmission can be obtained as

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\left\|\ddot{\mathbf{s}}_i\right\|\left\|\ddot{\mathbf{z}}_i\right\|}{\sqrt{D}}\frac{\left\|\widetilde{\mathbf{H}}^{\varrho\prime}[\kappa,\kappa]\right\|^2}{\left\|\widetilde{\mathbf{G}}^{\varrho}[\kappa,:]\right\|^2 N_0/2}\mathbf{u}_i^A[d], \tag{4.30}$$

where $\widetilde{\mathbf{G}}^{\varrho} = \left(\widetilde{\mathbf{H}}^{\varrho H}\widetilde{\mathbf{H}}^{\varrho} + N_0\mathbf{I}_{MN}\right)^{-1}\widetilde{\mathbf{H}}^{\varrho}$, and $\widetilde{\mathbf{H}}^{\varrho\prime} = \widetilde{\mathbf{G}}^{\varrho}\cdot\widetilde{\mathbf{H}}^{\varrho} = \left(\widetilde{\mathbf{H}}^{\varrho H}\widetilde{\mathbf{H}}^{\varrho} + N_0\mathbf{I}_{MN}\right)^{-1}\cdot \widetilde{\mathbf{H}}^{\varrho H}\widetilde{\mathbf{H}}^{\varrho}$. More explicitly, the modulated/demodulated symbols for the ith segment can be denoted as $\ddot{\mathbf{s}}_i = \mathfrak{Re}\left[\widetilde{\mathbf{s}}_i^{\mathrm{MDR}}\right] = \mathfrak{Re}\left[\widetilde{s}_{i,0}^{\mathrm{MDR}},\cdots,\widetilde{s}_{i,d}^{\mathrm{MDR}},\cdots,\widetilde{s}_{i,D-1}^{\mathrm{MDR}}\right]^T$, and $\ddot{\mathbf{z}}_i = \mathfrak{Re}\left[\widetilde{\mathbf{z}}_i^{\mathrm{MDR}}\right]$ $= \mathfrak{Re}\left[\widetilde{z}_{i,0}^{\mathrm{MDR}},\cdots,\widetilde{z}_{i,d}^{\mathrm{MDR}},\cdots,\widetilde{z}_{i,D-1}^{\mathrm{MDR}}\right]^T$ with $i = k\cdot M + l + \lfloor\varrho/D\rfloor\cdot MN$ and $d = \mathrm{rem}(\varrho, D)$,

where $k = 0, 1, ..., N-1$, $l = 0, 1, ..., M-1$ and $\varrho = 0, 1, ..., N_{bl}-1$. Moreover, $\widetilde{s}_{i,d}^{\mathrm{MDR}} = \widetilde{s}_{k,l}^{\varrho\prime}$ and $\widetilde{z}_{i,d}^{\mathrm{MDR}} = \widetilde{z}_{k,l}^{\varrho\prime}$ represent the dth element in the ith segment of $\widetilde{s}_i^{\mathrm{MDR}}$ and $\widetilde{z}_i^{\mathrm{MDR}}$, respectively. The ith segment of the noise term can be denoted as $\ddot{\mathbf{v}}_i = \mathfrak{Re}\left[\widetilde{v}_{i,0}^{\mathrm{MDR}}, \cdots, \widetilde{v}_{i,d}^{\mathrm{MDR}}, \cdots, \widetilde{v}_{i,D-1}^{\mathrm{MDR}}\right]^T$ along with $\widetilde{v}_{i,d}^{\mathrm{MDR}} = \widetilde{v}_{n,m}^{\varrho\prime}$. Hence the variance of each element of the noise $\ddot{\mathbf{v}}_i$ becomes $\frac{\left\|\widetilde{\mathbf{G}}^{\varrho}[\kappa,:]\right\|^2 N_0/2}{\left\|\widetilde{\mathbf{H}}^{\varrho\prime}[\kappa,\kappa]\right\|^2}$.

Note that the accuracy of LLRs in Eq. (4.25) and Eq. (4.29) may be affected by the MDR process in mobile scenarios, which will degrade the corresponding SKR performance. To elaborate further, since it is assumed in the generic MDR process that the fading gains of all elements in a segment are identical, the LLR calculation for a segment will assign the same fading value to each element. However, in a time-variant channel, the FD channel $\overline{\mathbf{H}}$ will change with time, therefore the fading values of each element in a segment will differ from each other, which degrades the accuracy of the LLR calculation of Eq. (4.25) and Eq. (4.29). By contrast, the accuracy of LLR calculation in Eq. (4.30) remains unaffected by the MDR process in mobile scenarios, because the DD domain channel $\widetilde{\mathbf{H}}$ does not change with time.

4.2.5 Complexity Analysis for OFDM/OTFS in Doubly Selective THz Channels

Admittedly, the dominant complexity of both the OFDM- and OTFS-based transceivers is that of the detectors. To elaborate further, the complexity of FDE in Eq. (4.6) for a single OFDM symbol is $\mathcal{O}(M)$ since the diagonal elements in $\overline{\mathbf{H}} \in \mathcal{C}^{M\times M}$ are used by the equalizer. Hence the complexity of a block is $\mathcal{O}(MN)$. Since the FD-MMSE equalizer in Eq. (4.7) of each OFDM symbol has the matrix inversion complexity order of $\mathcal{O}(M^3)$, the complexity for a block is $\mathcal{O}(M^3N)$. By contrast, for an OTFS-based system associated with $\widetilde{\mathbf{H}} \in \mathcal{C}^{MN\times MN}$, the complexity of a DD-MMSE equalizer in Eq. (4.18) for a single OTFS block has a matrix inversion complexity order of $\mathcal{O}(M^3N^3)$ [161]. In light of this, it is plausible that the complexity of the FDE of OFDM is the lowest followed by that of the FD-MMSE of OFDM. The complexity of DD-MMSE of OTFS is the highest. Note that these three detectors perform similarly in a stationary scenario. Hence, the FDE of OFDM is the best choice in stationary scenarios.

However, in high-mobility scenarios, the low-complexity single-tap FDE suffers from an error floor, where FD-MMSE based OFDM and DD-based OTFS have to be employed. Hence, it is more meaningful to compare the complexity of the FD-MSME of OFDM-based system and of the DD-MMSE of OTFS-based system in mobile scenarios. Recall that the complexity of the DD-MMSE of OTFS-based system is higher than that of the FD-MMSE of OFDM-based system, which are $\mathcal{O}(M^3N^3)$ and $\mathcal{O}(M^3N)$, respectively. However, the total complexity for a block of N_{bl} OFDM or OTFS symbols

required for completing the MDR process with the aid of LDPC codes is $\mathcal{O}(M^3NN_{bl})$ and $\mathcal{O}(M^3N^3)$ for OFDM and OTFS, respectively. This is because in time-variant channels, the FD matrix $\overline{\mathbf{H}}$ will change with time, which means that the MMSE equalizer of OFDM has to be updated for each OFDM symbol, where the matrix inversion calculations required for updating the MMSE matrix have to be repeated. By contrast, the MMSE equalizer of OTFS does not have to update its MMSE matrix, owing to the fact that the DD-domain fading representation is time-invariant. In light of this, the complexity of OTFS becomes lower than that of OFDM when we have $N_{bl} > N^2$, which is the case when a large number of blocks combined with powerful LDPC codes having long frames length for the sake of achieving a near-capacity performance.

4.3 MIMO OFDM/OTFS CV-QKD system model

In this section, the input-output relationships of the OFDM/OTFS MIMO system model are derived.

4.3.1 OFDM MIMO in Doubly Selective THz Channel

For a MIMO THz scheme using N_{Tx} Transmit Antennas (TAs) and N_{Rx} Receive Antennas (RAs), the TD fading matrix is modelled by [158, 162]:

$$\begin{aligned}\mathbf{H}_{n,m,l} =& \sqrt{N_{Tx}N_{Rx}} \cdot \\ & \sum_{p=0}^{P_l-1} \widetilde{h}_p \omega_{MN}^{k_p(nM+m-l_p)} \mathbf{a}_{Rx}(\theta_{Rx,p}) \mathbf{a}_{Tx}^H(\theta_{Tx,p}),\end{aligned} \tag{4.31}$$

where there are P_l paths falling into the lth TDL. The AoD and AoD $\theta_{Tx,p}$ and $\theta_{Rx,p}$ are Laplacian distributed with means $\overline{\theta}_{Tx}$, $\overline{\theta}_{Rx}$ and variances $\sigma_{\theta_{Tx}}$, $\sigma_{\theta_{Rx}}$, where $\overline{\theta}_{Tx}$ and $\overline{\theta}_{Rx}$ are uniformly distributed over $[0, 2\pi)$. We adopt ULAs at both the transmitter and the receiver, where the antenna response vectors are given by:

$$\begin{aligned}\mathbf{a}_{Tx}(\theta_{Tx,p}) = \frac{1}{\sqrt{N_{Tx}}} \Big[1, e^{j\frac{2\pi d \sin(\theta_{Tx,p})}{\lambda}}, e^{j2\frac{2\pi d \sin(\theta_{Tx,p})}{\lambda}}, \cdots, \\ e^{j\frac{(N_{Tx}-1)2\pi d \sin(\theta_{Tx,p})}{\lambda}}\Big]^T,\end{aligned} \tag{4.32}$$

$$\begin{aligned}\mathbf{a}_{Rx}(\theta_{Rx,p}) = \frac{1}{\sqrt{N_{Rx}}} \Big[1, e^{j\frac{2\pi d \sin(\theta_{Rx,p})}{\lambda}}, e^{j2\frac{2\pi d \sin(\theta_{Rx,p})}{\lambda}}, \cdots, \\ , e^{j\frac{(N_{Rx}-1)2\pi d \sin(\theta_{Rx,p})}{\lambda}}\Big]^T,\end{aligned} \tag{4.33}$$

respectively. In Eq. (4.32) and Eq. (4.33) λ is the wavelength of the signal and $d = \lambda/2$ denotes the aperture domain sample spacing. In the face of user mobility, digital beamforming that requires the time-varying CSI to be available at both the transmitter

and the receiver becomes impractical. Instead, we propose to deploy analog precoding at the transmitter and analog combining at the receiver. Hence the beamformed fading channel is expressed as:

$$h_{n,m,l}^{RF} = \left(\mathbf{w}^{Rx,RF}\right)^{H} \mathbf{H}_{n,m,l} \mathbf{w}^{Tx,RF}, \tag{4.34}$$

where $\mathbf{w}^{Tx,RF} \in \mathcal{C}^{N_{Tx}\times 1}$ and $\mathbf{w}^{Rx,RF} \in \mathcal{C}^{N_{Rx}\times 1}$ are tuned to the LoS antenna response vectors that should satisfy $\left\{\left\|\mathbf{w}^{Tx,RF}[t]\right\| = \frac{1}{\sqrt{N_{Tx}}}\right\}_{t=1}^{N_{Tx}}$ and $\left\{\left\|\mathbf{w}^{Rx,RF}[r]\right\| = \frac{1}{\sqrt{N_{Tx}}}\right\}_{r=1}^{N_{Rx}}$, and $\mathbf{H}_{n,m,l} \in \mathcal{C}^{N_{Rx}\times N_{Tx}}$ is the TD fading matrix in Eq. (4.31).

Therefore, the received signal after analog combining is[6]

$$\begin{aligned} y_{n,m} &= \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{n,<m-l>_M} \\ &+ \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s0_{n,<m-l>_M} + \sqrt{1-T} s_{En,m} \\ &= \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{n,<m-l>_M} + v_{n,m}. \end{aligned} \tag{4.35}$$

The TD matrix form is given by

$$\mathbf{y}_n = \sqrt{T}\mathbf{H}_n^{RF}\mathbf{s}_n + \mathbf{v}_n, \tag{4.36}$$

where $\mathbf{y}_n = [y_{n,0}, y_{n,1}, \cdots, y_{n,M-1}]^T$, $\mathbf{H}_n^{RF}[r,c] = h_{n,r,<r-c>_M}^{RF}$, $\mathbf{s}_n = [s_{n,0}, s_{n,1}, \cdots, s_{n,M-1}]^T$ and $\mathbf{v}_n = [v_{n,0}, v_{n,1}, \cdots, v_{n,M-1}]^T$. Then the FD received signal can be obtained by applying DFT, yielding:

$$\begin{aligned} \overline{y}_{n,\overline{m}} &= \frac{1}{\sqrt{M}}\sum_{m=0}^{M-1} y_{n,m}\omega_M^{-m\overline{m}} \\ &= \frac{\sqrt{T}}{\sqrt{M}}\sum_{m=0}^{M-1}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{n,<m-l>_M}\omega_M^{-m\overline{m}} + \overline{v}_{n,\overline{m}}. \end{aligned} \tag{4.37}$$

The FD matrix form is given by

$$\overline{\mathbf{y}}_n = \mathbf{F}_M\mathbf{y}_n = \sqrt{T}\overline{\mathbf{H}}_n^{RF}\overline{\mathbf{s}}_n + \overline{\mathbf{v}}_n, \tag{4.38}$$

where $\overline{\mathbf{y}}_n \in \mathcal{C}^{M\times 1}$, $\overline{\mathbf{s}}_n = \mathbf{F}_M\mathbf{s}_n \in \mathcal{C}^{M\times 1}$, $\overline{\mathbf{v}}_n = \mathbf{F}_M\mathbf{v}_n \in \mathcal{C}^{M\times 1}$, while $\overline{\mathbf{H}}_n^{RF} = \mathbf{F}_M\mathbf{H}_n^{RF}\mathbf{F}_M^H \in \mathcal{C}^{M\times M}$ is no longer diagonal in time-variant frequency-selective fading.

[6] As in a MIMO scenario, the technique of analog precoding and combining is only used for providing a beamforming gain, but the input-output relationship is consistent with the aforementioned SISO OFDM and OTFS systems. Hence, a similar beam splitter model can be extended to their MIMO counterparts, which is shown in Eq. (4.35) and Eq. (4.41).

The FD-MMSE equalizer operated at the receiver gives

$$\overline{\mathbf{z}}_n = \left[\left(\overline{\mathbf{H}}_n^{RF}\right)^H \overline{\mathbf{H}}_n^{RF} + N_0\mathbf{I}_M\right]^{-1} \left(\overline{\mathbf{H}}_n^{RF}\right)^H \overline{\mathbf{y}}_n. \tag{4.39}$$

We note that when the MIMO fading channel is assumed to be time-invariant that ignores the Doppler effect, $\overline{\mathbf{H}}_n^{RF}$ of Eq. (4.38) becomes diagonal with $\overline{\mathbf{H}}_n^{RF}[\overline{m},\overline{m}] = \overline{h}_{n,\overline{m},\overline{m}}^{RF}$. Based on the OFDM subcarrier orthogonality assume, the FD received signal is given by $\overline{y}_{n,\overline{m}} = \overline{h}_{n,\overline{m},\overline{m}}^{RF}\overline{s}_{n,\overline{m}} + \overline{v}_{n,\overline{m}}$. Therefore, the conventional single-tap FDE operates based on

$$\overline{z}_{n,\overline{m}} = \left[\left(\overline{h}_{n,\overline{m},\overline{m}}^{RF}\right)^* \overline{h}_{n,\overline{m},\overline{m}}^{RF} + N_0\right]^{-1} \left(\overline{h}_{n,\overline{m},\overline{m}}^{RF}\right)^* \overline{y}_{n,\overline{m}}. \tag{4.40}$$

However, the full FD signal representation is $\overline{y}_{n,\overline{m}} = \sum_{\overline{m}'=0}^{M-1} \overline{h}_{n,\overline{m},\overline{m}'}^{RF}\overline{s}_{n,\overline{m}'} + \overline{v}_{n,\overline{m}}$, where the term of $\sum_{\forall\overline{m}'\neq\overline{m}} \overline{h}_{n,\overline{m},\overline{m}'}^{RF}\overline{s}_{n,\overline{m}'}$ would introduce ICI.

4.3.2 OTFS MIMO in Doubly Selective THz Channel

As for the OTFS based on the OFDM Frame CP structure, the received signal after analog combining is as follows:

$$\begin{aligned} y_{n,m} &= \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{<nM+m-l>_{MN}} \\ &+ \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{0<nM+m-l>_{MN}} + \sqrt{1-T}s_{En,m} \\ &= \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{<nM+m-l>_{MN}} + v_{n,m}. \end{aligned} \tag{4.41}$$

After performing DFT and SFFT at the receiver, the DD-domain signal is given by

$$\widetilde{y}_{k,l} = \sqrt{T}\sum_{p=0}^{P-1} \widetilde{h}_p^{RF}\widetilde{T}(k,l,k_p,l_p)\widetilde{s}_{<k-k_p>_N,<l-l_p>_M} + \widetilde{v}_{k,l}, \tag{4.42}$$

where

$$\widetilde{h}_p^{RF} = \sqrt{N_{Tx}N_{Rx}}\widetilde{h}_p \cdot \left[\left(\mathbf{w}^{Rx,RF}\right)^H \mathbf{a}_{Rx}\left(\theta_{Rx},p\right)\mathbf{a}_{Tx}^H\left(\theta_{Tx},p\right)\mathbf{w}^{Tx,RF}\right]. \tag{4.43}$$

The DD-domain input-output relationship cast in matrix form is hence given by

$$\widetilde{\mathbf{y}} = \sqrt{T}\widetilde{\mathbf{H}}^{RF}\widetilde{\mathbf{s}} + \widetilde{\mathbf{v}}, \tag{4.44}$$

where $\widetilde{\mathbf{y}} \in \mathcal{C}^{MN\times 1}$, $\widetilde{\mathbf{y}}[\kappa] = \widetilde{y}_{k,l}$, $\widetilde{\mathbf{s}} \in \mathcal{C}^{MN\times 1}$, $\widetilde{\mathbf{s}}[\kappa] = \widetilde{s}_{k,l}$, $\widetilde{\mathbf{v}} \in \mathcal{C}^{MN\times 1}$, $\widetilde{\mathbf{v}}[\kappa] = \widetilde{v}_{k,l}$, $k = \lfloor\frac{\kappa}{M}\rfloor$, $l = \kappa - kM$, $\widetilde{\mathbf{H}}^{RF} \in \mathcal{C}^{MN\times MN}$, $\widetilde{\mathbf{H}}^{RF}[\kappa,\iota] = \widetilde{h}_p^{RF}\widetilde{T}(k,l,k_p,l_p)$. Therefore, the DD-MMSE

equalizer operates based on

$$\widetilde{\mathbf{z}} = \left[\left(\widetilde{\mathbf{H}}^{RF} \right)^{H} \widetilde{\mathbf{H}}^{RF} + N_0 \mathbf{I}_{MN} \right]^{-1} \left(\widetilde{\mathbf{H}}^{RF} \right)^{H} \widetilde{\mathbf{y}}. \tag{4.45}$$

The MDR process is thereafter carried out based on Eq. (4.39), Eq. (4.40) and Eq. (4.45), which is similar to the SISO cases.

4.4 Secret Key Rate Analysis

The calculation of SKR in the OFDM CV-QKD systems documented in the literature [94, 96, 97], relies on the sum of M independent subchannel SKRs in time-invariant flat fading channels, since the OFDM subcarriers are orthogonal to each other. However, when the fading channel becomes time-variant in the face of the Doppler effect, especially when the Doppler frequency f_D becomes comparable to the subcarrier spacing Δf, the OFDM subcarrier orthogonality no longer holds. It is destroyed by the Doppler-induced ICI. Therefore, the SKR calculation of OFDM CV-QKD systems found in the literature is no longer valid in high-mobility scenarios. More explicitly, when quantum-safe services are provided for next-generation SAGIN [21, 23, 24, 158], more sophisticated solutions are sought. Against this background, we propose to mitigate this problem by using MMSE detection aided OFDM and OTFS schemes, where the effect of small-scale time-varying frequency-selective fading is equalized before SKR calculation. In this way, the classic single stream-based SKR calculation [79, 105, 111] may still be directly applied. Nonetheless, the FD-MMSE aided OFDM and DD-MMSE aided OTFS schemes have different residual noise levels, leading to different SKR performances.

Therefore, the SKR is defined as [65][7]

$$K_{\text{finite}} = \gamma \left(1 - P_B\right) \left[\beta I_{AB} - \chi_{BE} - \triangle \left(N_{\text{privacy}} \right) \right], \tag{4.46}$$

where γ denotes the fraction of key extractions within the total number of data exchanged by Alice and Bob, while P_B represents the BLER in the reconciliation step. Furthermore, I_{AB} is the classical mutual information between Alice and Bob based on their shared correlated data, and χ_{BE} represents the Holevo information that Eve can

[7] Note that Eq. (4.46) is the normalized SKR based on the bandwidth. As for the unnormalized SKR, it can be expressed based on Eq. (4.46) as $K_{\text{finite}}^{\text{UN}} = B \cdot K_{\text{finite}}$, where B represents the bandwith of the multi-carrier systems considered and we have $B = M\Delta f$. In our discussion normalized SKR results are used.

extract from the information of Bob[8]. Finally, $\triangle\left(N_{\text{privacy}}\right)$ represents the finite-size offset factor with the finite-size N_{privacy}. As for $\beta \in [0,1]$, it represents the reconciliation efficiency, which is defined as [59, 74]

$$\begin{aligned}\beta = \frac{R^{\text{eff}}}{C} &= \frac{R^{\text{eff}}}{\mathbb{E}\left[0.5\log_2\left(1+\text{SNR}^{Rx}\right)\right]} \\ &= \frac{R^{\text{eff}}}{\mathbb{E}\left[0.5\log_2\left(1+1/N_0^{Rx}\right)\right]},\end{aligned} \tag{4.47}$$

where R^{eff} represents the transmission rate and $R^{\text{eff}} = \left(1-\frac{M_{cp}}{M}\right)\cdot R$ for OFDM transmission and $R^{\text{eff}} = \left(1-\frac{M_{cp}}{MN}\right)\cdot R$ for OTFS transmission with R representing the coding rate, while C is referred to as the one-dimensional Shannon capacity [108, 128]. Furthermore, SNR^{Rx} represents the SNR after channel equalization by the receivers, which can be expressed as $\text{SNR}^{Rx} = 1/N_0^{Rx} = 1/N_0\text{Y}$. As for the noise variance N_0^{Rx}, it equals to $N_0/\left\|\bar{\bar{h}}_i\right\|^2$, $\frac{\left\|\overline{\mathbf{G}}_n^{\varrho}[\overline{m},:]\right\|^2 N_0}{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m},\overline{m}]\right\|^2}$, and $\frac{\left\|\widetilde{\mathbf{G}}^{\varrho}[\kappa,:]\right\|^2 N_0}{\left\|\widetilde{\mathbf{H}}^{\varrho\prime}[\kappa,\kappa]\right\|^2}$ based on (4.25), (4.29), and (4.30), when the FDE of OFDM, FD-MMSE of OFDM and DD-MMSE of OTFS receivers are used, respectively, while the corresponding coefficient Y equals to $\left\|\bar{\bar{h}}_i\right\|^2$, $\frac{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m},\overline{m}]\right\|^2}{\left\|\overline{\mathbf{G}}_n^{\varrho}[\overline{m},:]\right\|^2}$, and $\frac{\left\|\widetilde{\mathbf{H}}^{\varrho\prime}[\kappa,\kappa]\right\|^2}{\left\|\widetilde{\mathbf{G}}^{\varrho}[\kappa,:]\right\|^2}$.

The calculations of I_{AB}, and χ_{BE} are similar to those in [79, 83, 84, 96, 105, 111]. To elaborate further, similar to [105], the total amount of noise between Alice and Bob ξ_{total} can be expressed as $\xi_{\text{total}} = \xi_{\text{line}} + \xi_{\text{det}}$, where $\xi_{\text{line}} = \frac{1-T}{T}W$ represents the impairment imposed by Eve, and W is the variance of the channel's noise [83]. Furthermore, $T = 10^{-\alpha\mathfrak{L}/10}$ represents the distance-dependent path loss, where α and $\mathfrak{L}$ represent the attenuation and distance between Alice and Bob, respectively. Moreover, $\xi_{\text{det}} = \frac{1-\eta}{\eta T}S$ is the homodyne detector's noise, where η represents the detection efficiency and S stands for the variance of the trusted detector's noise [79]. After taking the effect of imperfect detection stated above into account, the variance of Bob's received signal based on the single-tap equalization as shown in Eq. (4.5) can be represented as

$$\begin{aligned}V_B &= \eta T\left(\|\overline{h}\|^2 V_A + \xi_{\text{total}}\right) \\ &= \eta T\|\overline{h}\|^2 V_A + \eta\left(1-T\right)W + \left(1-\eta\right)S,\end{aligned} \tag{4.48}$$

where $V_A = V_0 + V_s$ is the total variance of Alice's side, which contains the modulation variance V_s and the thermal noise variance V_0. The variance of the thermal noise is given by $V_0 = 2\bar{n}+1$ with $\bar{n} = \left[\exp\left(\hbar f_c/k_B T_e\right)\right]^{-1}$, where $\hbar$ is Planck's constant, k_B is Boltzmann's constant, f_c is the carrier frequency and T_e is the environmental temperature in Kelvin. Furthermore, a more general expression may be formulated for the

[8]It is assumed that the strongest attack [54], namely the so-called collective attack is used. Accordingly, Eve performs an optimal collective measurement on the collection of the stored ancilla after the key distillation procedure. Therefore, the Holevo information between Eve and Bob is harnessed as the evaluation metric for this kind of attack.

SNR at Bob's side, which is used in Eq. (4.7) based on Eq. (4.29), and it is harnessed in Eq. (4.18) based on Eq. (4.30), where FD and DD MMSE detectors are adopted for OFDM and OTFS respectively. This is as follows

$$\begin{aligned} V_B &= \eta T \left(\mathrm{Y} V_A + \xi_{\text{total}} \right) \\ &= \eta T \mathrm{Y} V_A + \eta \left(1 - T \right) W + \left(1 - \eta \right) S. \end{aligned} \tag{4.49}$$

We make the worst-case assumption that Eve can acquire perfect CSI knowledge and accordingly set $W = 1 + \frac{T(1-\mathrm{Y})V_0}{1-T}$, which is similar to that in [96]. Therefore, the mutual information between Alice and Bob can be obtained as follows:

$$\begin{aligned} I_{AB} =& \frac{1}{2} \log_2 \left[1 + \frac{\eta T \mathrm{Y} V_s}{\eta T V_0 + \eta \left(1 - T \right) + \left(1 - \eta \right) S} \right] \\ =& \frac{1}{2} \log_2 \left[\frac{\eta T (\mathrm{Y} V_s + V_0) + \eta \left(1 - T \right) + \left(1 - \eta \right) S}{\eta T V_0 + \eta \left(1 - T \right) + \left(1 - \eta \right) S} \right], \end{aligned} \tag{4.50}$$

where the second term in $\log_2(\cdot)$ represents the receiver's SNR after equalization. Note that, V_s is adjustable in order to match the SNR required at the receiver by compensating the effect of fading channel gain Y and loss T. Therefore we can rewrite $V_s' = \mathrm{Y} V_s$ and $V_A' = V_s' + V_0$.

On the other hand, the Holevo information between Bob and Eve can be calculated as follows [59, 127]

$$\chi_{BE} = S(\rho_{AB}) - S\left(\rho_{A|B}\right), \tag{4.51}$$

where $S(\cdot)$ is the von Neumann entropy defined in [59, 127]. In light of this, the covariance matrix related to the information between Alice and Bob, i.e. the mode of ρ_{AB} after transmission through the quantum channel can be expressed as [59, 127]

$$\begin{aligned} \mathbf{V}_{AB} &= \begin{pmatrix} V_A' \mathbf{I}_2 & \sqrt{\eta T \left({V_A'}^2 - 1 \right)} \mathbf{Z} \\ \sqrt{\eta T \left({V_A'}^2 - 1 \right)} \mathbf{Z} & V_B \mathbf{I}_2 \end{pmatrix} \\ &= \begin{pmatrix} a \mathbf{I}_2 & c \mathbf{Z} \\ c \mathbf{Z} & b \mathbf{I}_2 \end{pmatrix}, \end{aligned} \tag{4.52}$$

where we have:

$$\mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{4.53}$$

representing a pair of Pauli matrices. Therefore, the required symplectic eigenvalues of ρ_{AB} are given by [59, 127]

$$v_{1,2}^2 = \frac{1}{2} \left(\Delta \pm \sqrt{\Delta^2 - 4D^2} \right), \tag{4.54}$$

where

$$\begin{aligned} \Delta &= a^2 + b^2 - 2c^2, \\ D &= ab - c^2. \end{aligned} \tag{4.55}$$

As for the symplectic eigenvalue of $\rho_{A|B}$, it can be shown that [59, 127]:

$$v_3 = \sqrt{a\left(a - \frac{c^2}{b}\right)}. \tag{4.56}$$

Hence, the Holevo information can be formulated as

$$\chi_{BE} = G(v_1) + G(v_2) - G(v_3), \tag{4.57}$$

where v_1, v_2 and v_3 are symplectic eigenvalues and $G(*) = \left(\frac{*+1}{2}\right) \cdot \log_2\left(\frac{*+1}{2}\right) - \left(\frac{*-1}{2}\right) \cdot \log_2\left(\frac{*-1}{2}\right)$. Upon substituting Eq. (4.50) and Eq. (4.57) into Eq. (4.46), the corresponding SKR can be obtained.

Note that, the SKR analysis derived for MIMO scenarios obeys the same process as that for SISO scenarios, since the technique of analog precoding and combining is only used for providing a beanforming gain, but the input-output relationship is similar to that in the SISO case. In light of this, the SKR for MIMO scenarios can be derived using the process of Eq. (4.46), Eq. (4.50), and Eq. (4.51) with the aid of Eq. (4.39), Eq. (4.40) and Eq. (4.45) to derive the SNR at Bob's side.

4.5 Performance Analysis

In this section, a comparison between ABF-assisted OFDM and OTFS in classical communications is conducted followed by a comprehensive parametric study of both THz OFDM and OTFS based CV-QKD. Explicitly, firstly the BER performance comparisons are presented for both OFDM and OTFS based multicarrier-based systems associated with different MIMO dimensions of $N_{Tx} \times N_{Rx}$ in classical communications. Then our BLER performance comparisons are presented for different multicarrier-based CV-QKD quantum transmission systems associated with a variety of different parameters, including the number of subcarriers M, FEC block length N_{FEC} and MIMO dimension $N_{Tx} \times N_{Rx}$. Moreover, the SKR versus distance as a key performance indicator will be analyzed.

The simulation parameters are summarized in Table 4.3, which are selected based on the seminal papers in the open literature [79, 83, 105, 133, 163]. Specifically, the attenuation coefficient α associated with the atmospheric path loss is set to 50 dB/km at 15 THz

Table 4.3: Simulation parameters.

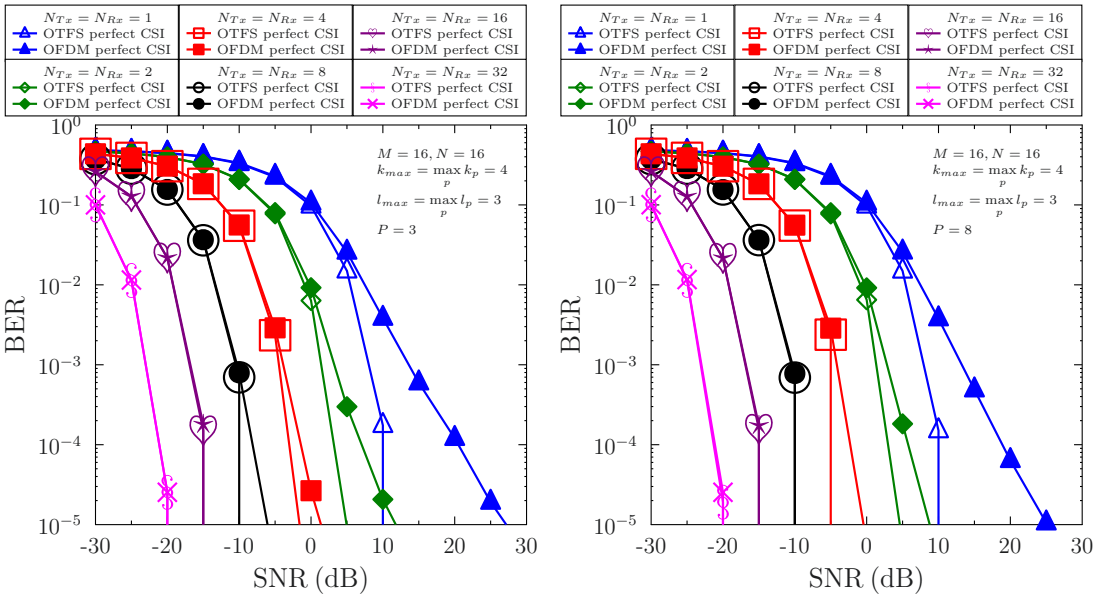
Parameter	Symbol	Value
Parameters for OFDM/OTFS		
The number of subcarrier	M	16,32,64
The number of symbol	N	16
Subcarrier spacing	Δf	2 MHz
Carrier frequency	f_c	15 THz
Maximum delay	τ_{max}	20 ns
Speed	v	0,30 mph
Parameters for MIMO		
The number of transmitter antennas	N_{Tx}	1,4,8,16,32
The number of receiver antennas	N_{Rx}	1,4,8,16,32
Parameters for LDPC		
Coding rate	R	0.5
Code length	N_{FEC}	1024
Parameters for the QuC		
Ricean factor	K	0 dB
Atmospheric loss	α	50 dB/km

[79, 83][9]. Moreover, due to the limited number of scatterers and high attenuation of the THz band [133, 136, 163], based on [136] we set the Ricean factor K to 0 dB. The FEC code length of $N_{\text{FEC}} = 1024$ and the coding rate of $R = 0.5$ are the same as in [105]. The CP length M_{cp} is set to $M_{cp} = L + 1$, where we have $L = \lceil \tau_{max} M \Delta f \rceil = 1, 2, 3$ for $M = 16, 32, 64$, respectively, and $P = L$.

4.5.1 OFDM vs. OTFS in Classical Communication

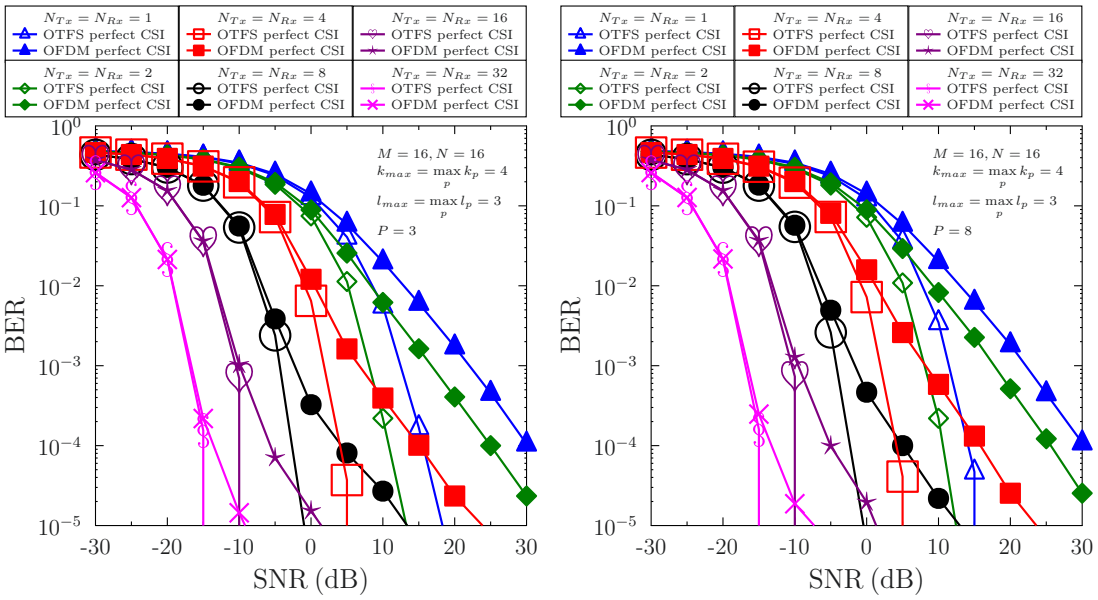
Fig. 4.6 portrays our BER performance comparison between ABF-assisted MIMO OFDM and OTFS systems in classical communications with perfect CSI under different MIMO sizes in mobile scenarios. Firstly, it is demonstrated that the BER of OTFS system significantly outperforms that of OFDM system in SISO cases, and the OFDM system performs comparably to the OTFS system upon increasing the MIMO size from 1×1 to 32×32, since the beamforming gain becomes dominating, as evidenced by Fig. 4.6(a)-(d). Secondly, it can be observed by comparing Fig. 4.6(a) and Fig. 4.6(c) as well as by comparing Fig. 4.6(b) and Fig. 4.6(d) that the BER performance is improved, as the Ricean K factor increases. Thirdly, it can also be observed from Fig. 4.6(b) and Fig. 4.6(d) that the BER performances associated with $P = 8$ are nearly the same as those associated with $P = 4$ in Fig. 4.6(a) and Fig. 4.6(c), since the effect of the number of paths on both the OFDM and OTFS systems is insignificant as only LoS is used for ABF.

[9] In contrast to the THz wireless communication range spanning from 0.1 to 10 THz, the THz range investigated in the literature of QKD is wider, ranging from 0.1 to 50 THz [24, 79]. Therefore, the frequency set in our paper is chosen in line with [79], which exhibits low atmospheric loss and low thermal noise. Higher THz carrier frequencies are generally preferred for QKD, because the lower the frequency, the higher the thermal noise, which degrades the secure communication distance.



(a) K=6 dB, P=3

(b) K=6 dB, P=8



(c) K=-6 dB, P=3

(d) K=-6 dB, P=8

Figure 4.6: Performance comparison between **ABF-assisted MIMO OFDM and OTFS systems in classical communications with perfect CSI** and with different MIMO sizes in **mobile** scenario ($k_{max} = \max_p k_p = 4$), where $M = 16$ and $N = 16$ are used and we have: (a) K=6 dB, P=3, (b) K=6 dB, P=8, (c) K=-6 dB, P=3, (d) K=-6 dB, P=8.

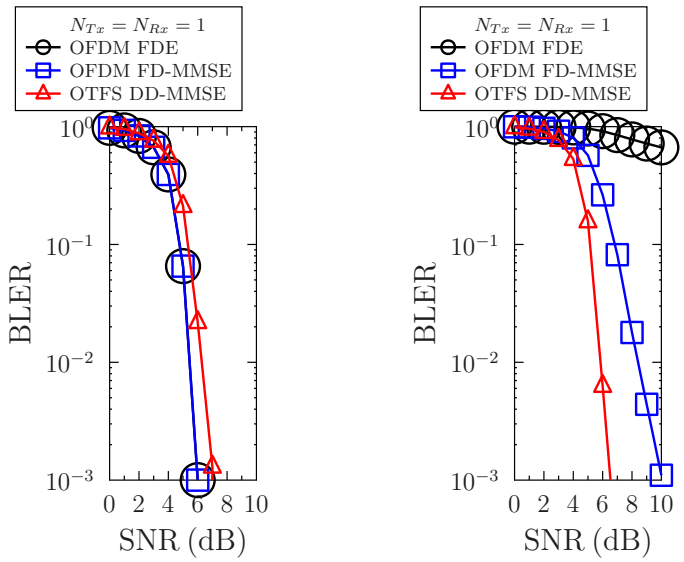


Figure 4.7: Performance comparison between **SISO OFDM and OTFS-LDPC CV-QKD systems with perfect CSI** in both (a) **stationary** ($v = 0$ m/s) and (b) **mobile** ($v = 30$ mph) scenarios, where $M = 64$ and $N = 16$ are used.

4.5.2 OFDM vs. OTFS in CV-QKD

Fig. 4.7 provides our performance comparison between the OFDM and OTFS schemes employed by our LDPC-aided CV-QKD arrangement, where the user mobility is set to $v = 0$ mph for time-invariant fading and $v = 30$ mph for time-varying fading, respectively. Fig. 4.7 (a) demonstrates that all of the three detectors of OFDM FDE, OFDM FD-MMSE and OTFS DD-MMSE achieve comparable performance, which is expected in the absence of mobility. However, Fig. 4.7 (b) evidences that in the mobile scenario associated with a user speed of $v = 30$ mph, the conventional OFDM single-tap FDE performs the worst, as OFDM subcarrier orthogonality no longer holds. As a remedy, the OFDM FD-MMSE scheme exhibits an improved performance in Fig. 4.7 (b), but OTFS DD-MMSE achieves the best performance in time-varying THz channels, as evidenced by Fig. 4.7 (b).

Fig. 4.8 portrays our performance comparison between the OFDM and OTFS schemes employed by our LDPC-aided CV-QKD system using different numbers of subcarriers M in time-varying fading. Fig. 4.8 demonstrates that the BLER of our OFDM FD-MMSE based system using $M = 64$ performs better than that with $M = 32$ due to a higher gain obtained for more subcarrier. Nonetheless, the proposed OTFS scheme always performs the best in time-varying fading channels, as evidenced by Fig. 4.8.

Fig. 4.9 characterizes the effect of the FEC block length N_{FEC} on the BLER performance in the mobile ($v = 30$ mph) scenario. It demonstrates that the BLERs of the OFDM/OTFS detectors improve upon increasing N_{FEC}. More explicitly, take the OTFS

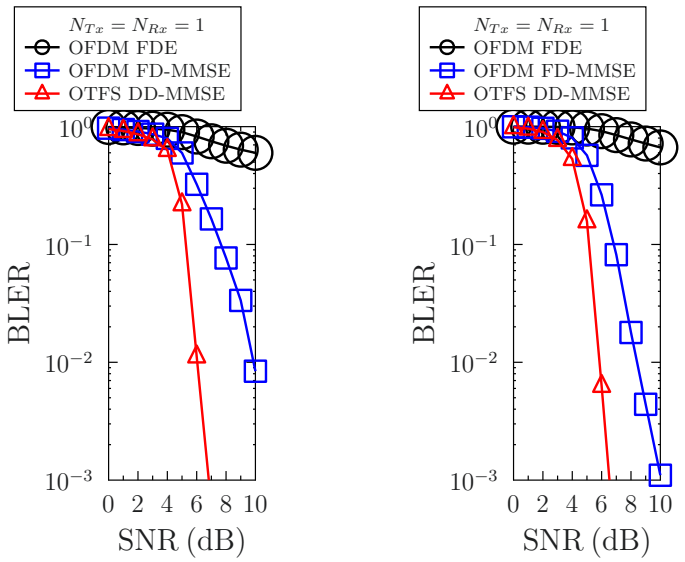


Figure 4.8: Performance comparison between **SISO OFDM and OTFS-LDPC CV-QKD systems with perfect CSI** in **mobile** scenario ($v = 30$ mph), where $N = 16$ and different number of subcarriers are used: (a) $M = 32$, (b) $M = 64$.

DD-MMSE detection as an example. The SNR threshold to achieve a BLER of 10^{-3} decreases from 8.0 dB, to 7.0 dB and to 6.5 dB with N_{FEC} increasing from 256, 512 to 1024. Nonetheless, we note that the delay will also be increased with N_{FEC}, especially when an Automatic Repeat Request (ARQ) mechanism is taken into account for re-transmission if the decoding fails.

Fig. 4.10 illustrates the effect of the MIMO size $N_{Tx} \times N_{Rx}$ on the BLER performance in a mobile (v=30 mph) scenario. Firstly, similarly to the SISO results of Fig. 4.7 (b), OTFS using DD-MMSE performed the best in MIMO systems, followed by OFDM with FD-MMSE and OFDM with single-tap FDE, as evidenced by Fig. 4.10. Secondly, Fig. 4.10 demonstrates that the BLER performance improves for all of the three OTFS/OFDM detectors, as the MIMO size increases. Specifically, it can be observed that the SNR threshold at a BLER of 10^{-1} is reduced from -6.8 dB, -12.8 dB, -18.9 dB to -24.8 dB with the increase of MIMO size from 4, 8, 16, to 32. In order to investigate the effect of different parameters on the SKR, the pair of BLER and β, namely (BLER, β), are summarized in Table 4.4 and Table 4.5 for both the stationary and mobile scenarios. We note that the BLER results of OFDM FDE recorded for both the SISO and MIMO based mobile scenarios are absent in Table 4.4 and Table 4.5 owing to their error floors, as evidenced by Figs. 4.7-4.10. Based on this, Fig. 4.11 portrays the performances of the SKR versus distance for the SISO OFDM and OTFS based LDPC-aided systems using different numbers of subcarriers M in both stationary and mobile scenarios. The modulation variance is always kept at the optimal value, in the same way as in [71]. The

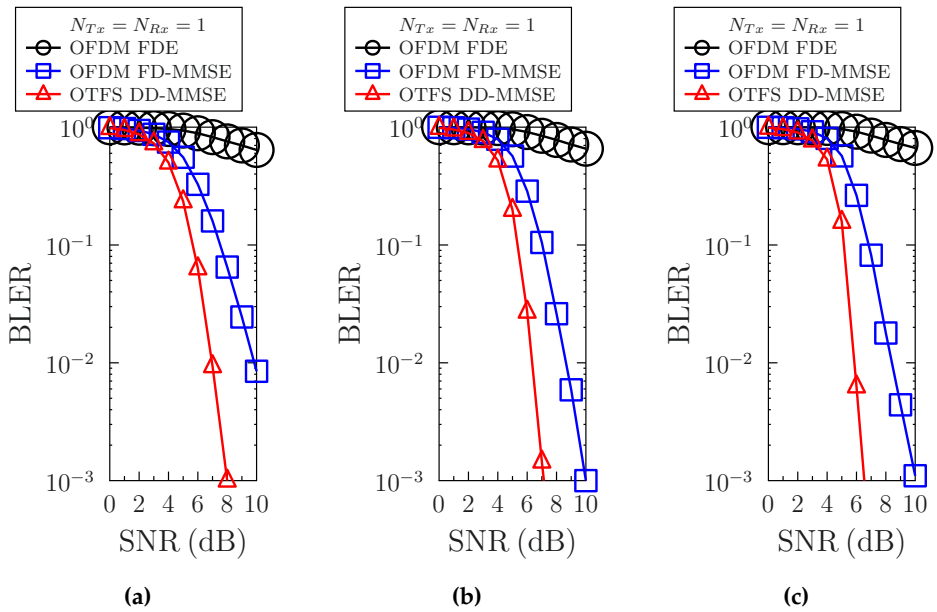


Figure 4.9: Performance comparison between **SISO OFDM and OTFS-LDPC systems with perfect CSI** with different block lengths of LDPC codes in **mobile** scenario ($v = 30$ mph), where $M = 64$ and $N = 16$ are used and we have: (a) $N_{\text{FEC}} = 256$, (b) $N_{\text{FEC}} = 512$, (c) $N_{\text{FEC}} = 1024$.

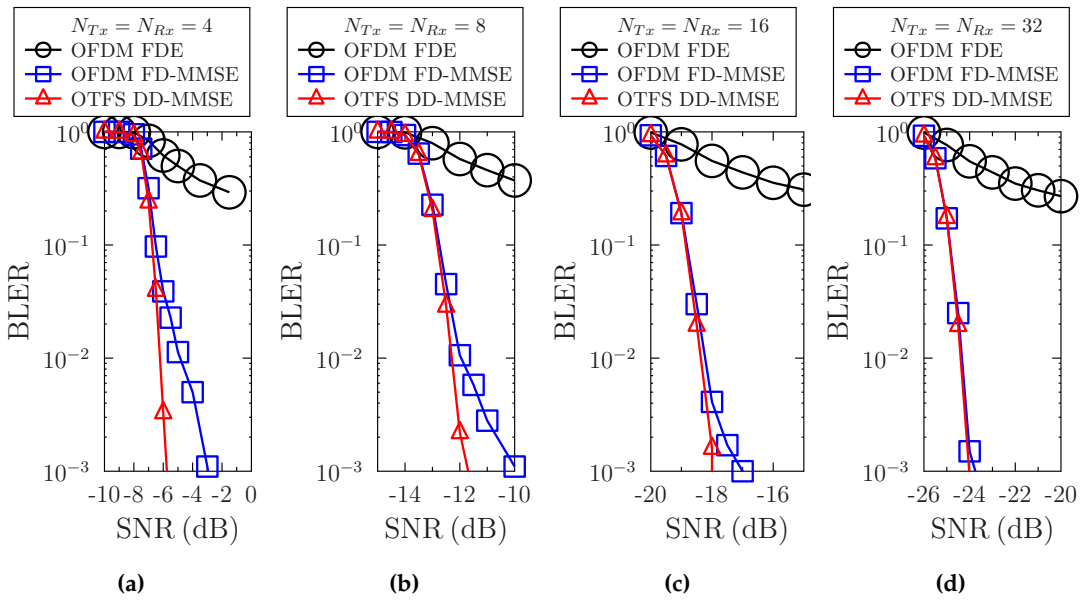


Figure 4.10: Performance comparison between **MIMO OFDM and OTFS-LDPC systems with perfect CSI** with different MIMO size in **mobile** scenario ($v = 30$ mph), where $M = 64$ and $N = 16$ are used and we have: (a) $N_{Tx} = N_{Rx} = 4$, (b) $N_{Tx} = N_{Rx} = 8$, (c) $N_{Tx} = N_{Rx} = 16$, (d) $N_{Tx} = N_{Rx} = 32$.

Table 4.4: Reconciliation efficiency comparison of different detection methods used in OFDM/OTFS CV-QKD system under different M and $N_{Tx} \times N_{Rx}$. The reconciliation efficiencies are calculated from Eq. (4.47) at the BLER threshold that equals to $\mathbf{10^{-1}}$, together with the corresponding SNRs. Note that both the stationary and mobile scenarios are considered with $v = 0, 30$ mph.

	$N_{Tx} \times N_{Tx}$	M	OFDM FDE		OFDM FD-MMSE		OTFS DD-MMSE	
			SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$
SISO ($v = 0$ mph)	1×1	16	5.2	62.10	5.2	62.10	5.2	70.41
	1×1	32	4.8	52.18	4.8	52.30	5.4	54.38
	1×1	64	4.8	54.16	4.8	54.48	5.4	54.72
MIMO ($v = 0$ mph)	4×4	64	-6.8	64.79	-6.8	65.01	-6.8	69.78
	8×8	64	-12.8	65.90	-12.8	65.61	-12.8	70.05
	16×16	64	-18.8	65.73	-18.8	64.39	-18.8	69.84
	32×32	64	-24.8	65.54	-24.8	65.54	-24.8	69.63
SISO ($v =$ 30 mph)	1×1	16	-	-	5.2	62.10	5.2	70.41
	1×1	32	-	-	7.5	38.94	5.2	55.56
	1×1	64	-	-	6.8	43.51	5.2	56.61
MIMO ($v =$ 30 mph)	4×4	64	-	-	-6.5	63.25	-6.7	68.81
	8×8	64	-	-	-12.75	65.43	-12.8	70.05
	16×16	64	-	-	-18.8	65.73	-18.9	70.87
	32×32	64	-	-	-24.8	65.54	-24.8	69.63

Table 4.5: Reconciliation efficiency comparison of different detection methods used in OFDM/OTFS CV-QKD system under different M and $N_{Tx} \times N_{Rx}$. The reconciliation efficiencies are calculated from Eq. (4.47) at the BLER threshold that equals to $\mathbf{10^{-2}}$, together with the corresponding SNRs. Note that both the mobile scenario is considered with $v = 30$ mph.

	$N_{Tx} \times N_{Tx}$	M	OFDM FDE		OFDM FD-MMSE		OTFS DD-MMSE	
			SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$
MIMO ($v =$ 30 mph)	4×4	64	-	-	-5	51.49	-6.25	64.53
	8×8	64	-	-	-12.0	58.81	-12.3	65.18
	16×16	64	-	-	-18.25	60.74	-18.4	65.92
	32×32	64	-	-	-24.4	61.86	-24.4	65.73

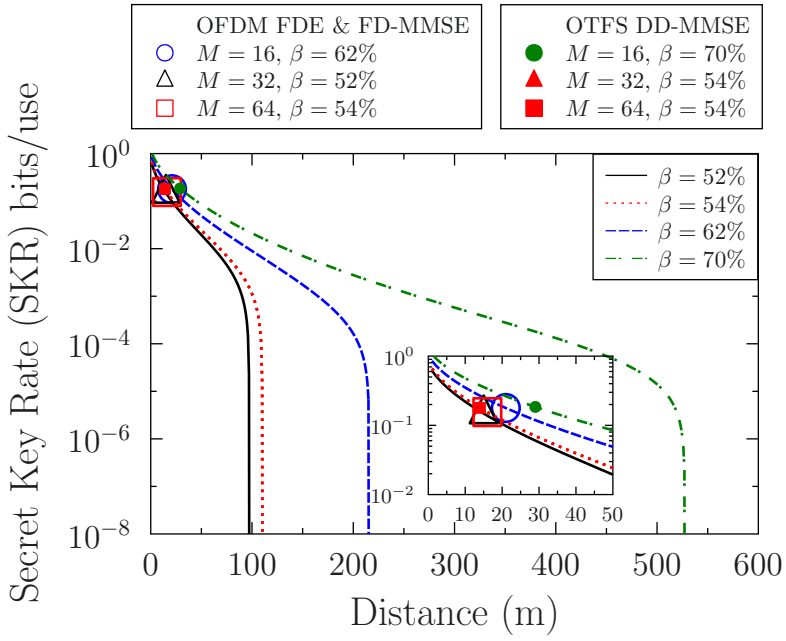
other parameters are as follows [79, 83]: atmospheric loss $\alpha = 50$ dB/km; room temperature $T_e = 296$ K; detector efficiency $\eta = 0.98$; detector's noise variance $S = 1$; $N_{\text{privacy}} = 10^{12}$. In Fig. 4.11 (a), there are four asymptotic theoretical SKR curves for different reconciliation efficiencies, which are 52%, 54%, 62%, and 70%, respectively. More explicitly, for the OFDM FDE and FD-MMSE based systems, they have the same reconciliation efficiency at the same setting, i.e. $\beta = 62\%$, 52%, 54% for $M = 16$, 32, 64, respectively. For the OTFS DD-MMSE based one, the corresponding reconciliation efficiencies are $\beta = 70$, 54, 54% for $M = 16$, 32, 64, respectively. Therefore, as expected, similar SKR performance can be achieved under these six different modes, as shown in Fig. 4.11 (a), indicating around 20 meters of secure transmission distance. By contrast, in Fig. 4.11 (b), both the reconciliation efficiencies of the OFDM FD-MMSE with $M = 32$ and 64 decreased from 52%, 54% in Fig. 4.11 (a) to 39%, 44% in Fig. 4.11 (b). The corresponding efficiencies of the rest of the other modes remain the same. Therefore, there is a secure distance gap between the OFDM FD-MMSE based system and the OTFS

DD-MMSE based scheme, indicating that the OTFS-based scheme using DD-MMSE detection outperforms the OFDM-based scheme relying on FD-MMSE detection in a mobile scenario.

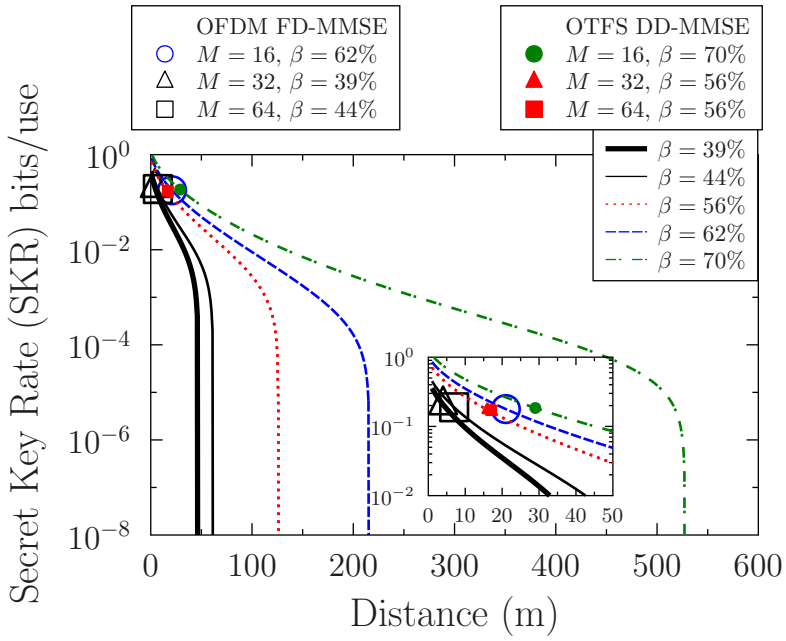
Fig. 4.12 (a) and Fig. 4.12 (b) demonstrate the SKR versus distance comparison between our MIMO OFDM and OTFS LDPC-aided systems using different detectors and MIMO sizes in both stationary and mobile scenarios, respectively. In Fig. 4.12 (a), there are two asymptotic theoretical SKR curves associated with different reconciliation efficiencies, which are 65% and 70%, respectively. Firstly, Fig. 4.12 (a) demonstrates that longer secure transmission distance is achieved by the OTFS-based CV-QKD system than by its OFDM counterpart in a stationary scenario as the OTFS-based CV-QKD system can provide higher reconciliation efficiencies than its OFDM counterpart, which can be seen in Table 4.4. Explicitly, the secure transmission distance of our OTFS system is around 120 meters (blue filled circle) in 4×4 MIMO setting, whereas the corresponding secure transmission distance of our OFDM system is around 110 meters (black circle) in 4×4 MIMO setting. Secondly, Fig. 4.12 (a) also confirms that the increased MIMO beamforming gain is capable of increasing the secure transmission distance for both OFDM and OTFS based CV-QKD systems. More explicitly, upon increasing the MIMO size from 4×4 to 8×8, 16×16 and 32×32, the secure transmission distance of OTFS-based system can be extended from 120 meters (blue filled circle), to 210 (blue filled triangle), 330 (blue filled square) and 450 meters (blue filled diamond), respectively, whereas the corresponding secure transmission distance of our OFDM system can be extended from 110 meters (black circle), to 190 meters (black triangle) and 300 meters (black square) in 4×4, 8×8 and 16×16 MIMO settings, respectively. However, for the OFDM system, the secure transmission distance can only be achieved by increasing the MIMO size to 16×16. This is because the low reconciliation efficiency of the OFDM-based system cannot support longer secure transmission distance, even though the larger MIMO 32×32 reduces the required SNR, as shown in Table 4.4.

Furthermore, in Fig. 4.12 (b), there are four asymptotic theoretical SKR curves having different reconciliation efficiencies, which are 63%, 65%, 69% and 70%, respectively. Similar conclusions can be made in doubly selective THz fading channels as that from Fig. 4.12 (a). This is evidenced by our simulation results. More explicitly, the secure transmission distance of our OTFS system is around 120 meters (blue filled circle), 210 meters (green filled triangle), 330 meters (green filled square) and 450 meters (green filled diamond) in 4×4, 8×8, 16×16 and 32×32 MIMO settings, respectively, whereas the corresponding secure transmission distance of our OFDM sytem is around 100 meters (black circle), 190 meters (red triangle) and 300 meters (red square) in 4×4, 8×8 and 16×16 MIMO settings, respectively.

To further investigate the effect of reconciliation efficiency on the secure transmission distance, Fig. 4.13 is portrayed based on the values in Table 4.5, where the reconciliation efficiencies in a mobile scenario are collected based on the SNR threshold at a BLER of

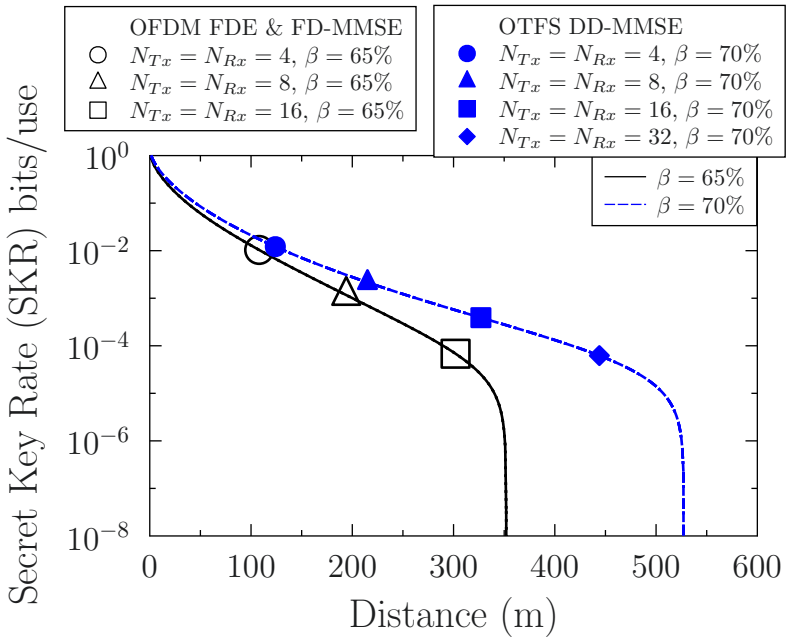


(a)

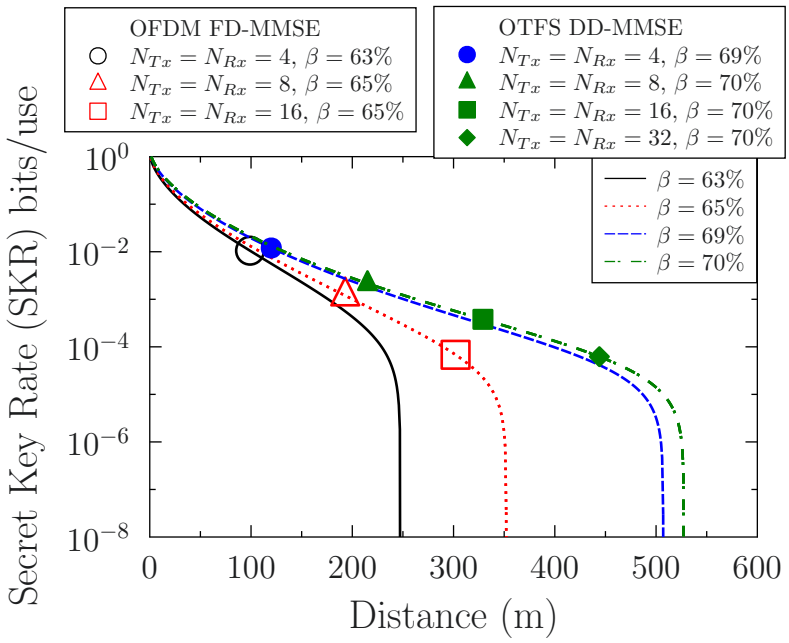


(b)

Figure 4.11: The SKR versus distance comparison between **SISO OFDM and OTFS-LDPC systems with perfect CSI** using different detections and different number of subcarriers M with BLER equals to $\mathbf{10^{-1}}$ in Table 4.4, where $N = 16$, $f_c = 15$ THz, $N_{\text{FEC}} = 1024$ and $R = 0.5$ are used in the following scenarios: (a) $v = 0$ mph, (b) $v = 30$ mph.



(a)



(b)

Figure 4.12: The SKR versus distance comparison between **MIMO OFDM and OTFS-LDPC systems with perfect CSI** using different detections and different MIMO sizes with BLER equals to $\mathbf{10^{-1}}$ in Table 4.4, where $M = 64$, $N = 16$, $f_c = 15$ THz, $N_{\text{FEC}} = 1024$ and $R = 0.5$ are used in the following scenarios: (a) $v = 0$ mph, (b) $v = 30$ mph.

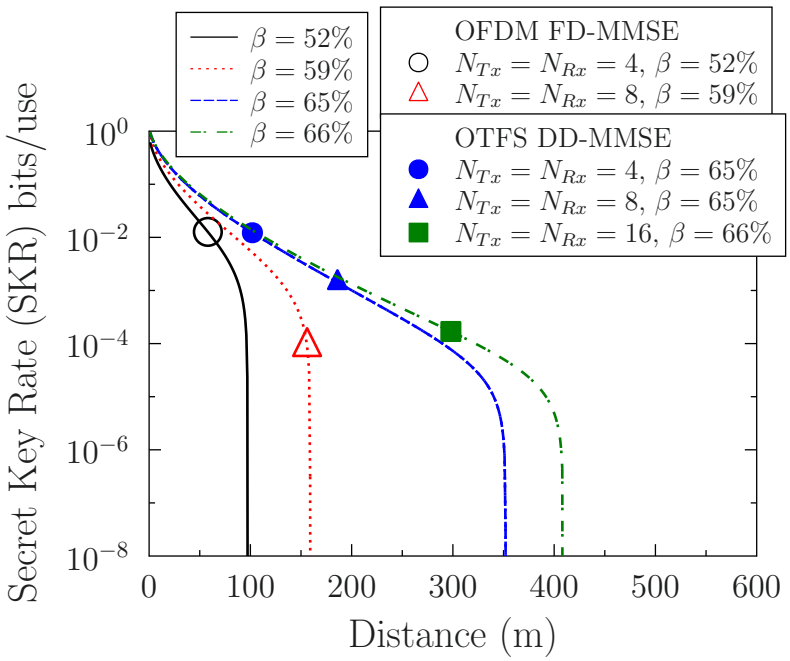


Figure 4.13: The SKR versus distance comparison between **MIMO OFDM and OTFS-LDPC systems with perfect CSI** using different detections and different MIMO sizes with BLER equals to $\mathbf{10^{-2}}$ in Table 4.5, where $M = 64$, $N = 16$, $f_c = 15$ THz, $N_{\text{FEC}} = 1024$ and $R = 0.5$ are used in the mobile scenario with $v = 30$ mph.

10^{-2}. As shown in Fig. 4.13, all the reconciliation efficiencies are lower than those in Fig. 4.12 (b), since the SNRs threshold are higher than those in Fig. 4.12 (b), which can be seen by comparing Table 4.4 and Table 4.5. More explicitly, the reconciliation efficiencies are 65%, 65% and 66% for OTFS-based systems in 4×4, 8×8 and 16×16 MIMO settings, whereas the reconciliation efficiencies are 52% and 59% for OFDM-based systems in 4×4 and 8×8 MIMO settings. Therefore, the corresponding secure transmission distances for both OFDM and OTFS-based systems seen in Fig. 4.13 for different MIMO settings are shorter than those in Fig. 4.12 (b), indicating that the value of reconciliation efficiency plays a vital role in providing a long secure transmission distance.

4.6 Conclusions

An OFDM/OTFS based LDPC assisted MDR CV-QKD system was conceived for transmission over time-variant frequency-selective THz channels. **Firstly**, it was demonstrated that the BLER is the same under three different OFDM/OTFS detectors in stationary ($v = 0$ mph) cases. The BLER of our OTFS DD-MMSE based system is the best, followed by that of the OFDM FD-MMSE based method. The BLER of OFDM using FDE detection is the worst in mobile ($v = 30$ mph) scenarios. **Secondly**, we

Table 4.6: A summary of SKR vs. distance based on Fig. 4.11 and Fig. 4.12, where $M = 64$, $N = 16$.

	$N_{Tx} \times N_{Tx}$	OFDM FDE		OFDM FD-MMSE		OTFS DD-MMSE	
		$\beta(\%)$	Max. distance(m)	$\beta(\%)$	Max. distance(m)	$\beta(\%)$	Max. distance(m)
MIMO ($v = 0$ mph)	1×1	54.16	15	54.48	15	54.72	15
	4×4	64.79	110	65.01	110	69.78	120
	8×8	65.90	190	65.61	190	70.05	210
	16×16	65.73	300	64.39	300	69.84	330
	32×32	65.54	-	65.54	-	69.63	450
MIMO ($v = 30$ mph)	1×1	-	-	43.51	7	56.61	17
	4×4	-	-	63.25	100	68.81	120
	8×8	-	-	65.43	190	70.05	210
	16×16	-	-	65.73	300	70.87	330
	32×32	-	-	65.54	-	69.63	450

investigated the effect of FEC block length. It was demonstrated that all the BLER performances are improved under all three different detectors upon increasing of the block length. However, the delay will be increased for a higher block length, especially when an ARQ mechanism is adopted for retransmissions if the decoding fails. **Thirdly**, it was demonstrated that the BLER performance will be improved upon increasing the MIMO size, thanks to the improved beamforming gain achieved by the MIMO OFDM/OTFS proposed for quantum transmission. **Lastly**, an SKR versus distance performance comparison was conducted, which is summarized in Table 4.6. It was demonstrated that the OTFS-based system offers higher SKR and longer secure transmission distance than the OFDM-based system in both stationary and mobile ($v = 30$ mph) scenarios. Moreover, increasing the MIMO size can enhance the secure transmission distance for both the OFDM- and OTFS-based systems.

Chapter 5

Hybrid Beamforming Assisted OTFS-Based CV-QKD Systems for Doubly Selective THz Channels

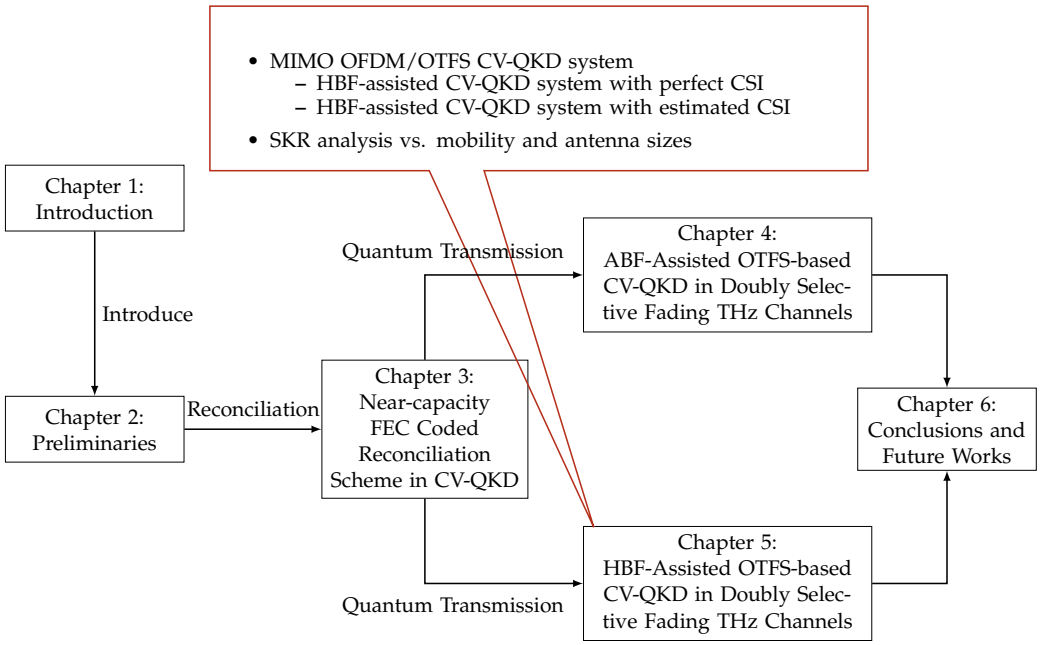


Figure 5.1: The outline of this thesis with the highlight of Chapter 5.

5.1 Introduction

In Chapter 4, an ABF MIMO OFDM/OTFS based and LDPC assisted MDR CV-QKD system was conceived for transmission over time-varying frequency-selective THz channels [164]. It was demonstrated that the OTFS-based system offers higher SKR and

Table 5.1: Novel contributions of this work in comparison to the state-of-the-art THZ CV-QKD schemes.

Contributions	**This work**	[69, 90–93, 95, 97]	[96]	[94, 98]	[79, 81]	[83]	[86]
Optical fibre		✓					
FSO				✓			
Terahertz	✓		✓		✓	✓	✓
SISO	✓	✓	✓	✓	✓		✓
MIMO	✓					✓	✓
Analog beamforming	✓					✓	✓
Frequency selective	✓	✓	✓	✓			
Time-invariant fading	✓	✓	✓	✓	✓	✓	✓
Time-varying fading	✓						
OFDM	✓	✓	✓	✓			
OTFS	✓						
SVD	✓						
Channel estimation	✓						

longer secure transmission distance than the OFDM-based system in both stationary and mobile ($v = 30$ mph) scenarios. As a further improvement of the ABF-assisted MIMO OFDM/OTFS CV-QKS system, hybrid beamforming is proposed in this Chapter which requires that full CSI is available at both the transmitter (CSI-T) and receiver (CSI-R). In light of this, a variety of channel estimation methods are conceived for MIMO OFDM/OTFS in order to provide CSI-T and CSI-R for HBF. Table 5.1 boldly contrasts the novelty of this chapter to the literature. To elaborate, the novel contributions of this work are as follows:

- Firstly, multi-carrier OFDM and OTFS based LDPC assisted CV-QKD reconciliation schemes have been designed and studied in the face of time-varying and frequency-selective THz scenarios, where a HBF technique is conceived for improving the quantum transmission distance attained in the face of severe THz path loss.

- Secondly, MIMO- OFDM and OTFS channel estimation techniques have been conceived both for the conventional TF domain and for the state-of-the-art DD domain. It is demonstrated that under the idealistic conditions of perfect CSI, the beamforming gain provided by sufficiently large number of antennas makes OFDM and OTFS perform comparably, even in doubly selective fading environments. However, the OFDM-based system relying on realistic channel estimation can only work in stationary scenarios since they suffer from high error-floors in mobile cases.

- Finally, we apply the proposed MIMO OFDM and MIMO OTFS channel estimation methods to both analog and hybrid beamforming aided THz CV-QKD systems. Our analysis and simulation results demonstrate that the proposed OTFS-based CV-QKD is capable of outperforming its OFDM counterpart in terms of SKR, when the user mobility is increased. Moreover, our performance results

also demonstrate that the proposed beamforming scheme is capable of improving secure CV-QKD transmission for both OTFS and OFDM in doubly-selective THz fading environments.

The structure of this chapter is described in Fig. 5.1 and the rest of this chapter is organized as follows. Our MIMO OFDM/OTFS CV-QKD system is conceived in Section 5.2, which introduces the CV-QKD system model, OFDM and OTFS quantum transmission, the modified MDR decoding in doubly selective THz channels and the complexity analysis. The MIMO OFDM/OTFS channel estimation algorithms of our CV-QKD system are proposed in Section 5.3, which is followed by the SKR analysis in Section 5.4. Our simulation results are presented in Section 5.6. Finally, our conclusions are offered in Section 5.7.

5.2 System Model of MIMO OFDM/OTFS Based CV-QKD

In this section, both the MIMO OFDM and MIMO OTFS systems operating in doubly selective THz channels are introduced, which are followed by the MDR decoding and complexity analysis of our MIMO OFDM/OTFS CV-QKD systems. Note that the CV-QKD system model and the SISO OFDM/OTFS based quantum transmission process used in this Chapter are the same as those in Chapter 4, which were presented in Section 4.2.1 and Section 4.2.2.

5.2.1 MIMO OFDM in Doubly Selective THz Channels using Hybrid Beamforming

For a MIMO THz scheme using N_{Tx} TAs and N_{Rx} RAs, the TD fading matrix is modelled by [158, 162]:

$$\begin{aligned}\mathbf{H}_{n,m,l} =& \sqrt{N_{Tx}N_{Rx}} \cdot \\ & \sum_{p=0}^{P_l-1} \widetilde{h}_p \omega_{MN}^{k_p(nM+m-l_p)} \mathbf{a}_{Rx}(\theta_{Rx,p}) \mathbf{a}_{Tx}^H(\theta_{Tx,p}),\end{aligned} \tag{5.1}$$

where there are P_l paths falling into the lth TDL. The AoD and AoD $\theta_{Tx,p}$ and $\theta_{Rx,p}$ are Laplacian distributed with means $\overline{\theta}_{Tx}$, $\overline{\theta}_{Rx}$ and variances $\sigma_{\theta_{Tx}}$, $\sigma_{\theta_{Rx}}$, where $\overline{\theta}_{Tx}$ and $\overline{\theta}_{Rx}$ are uniformly distributed over $[0, 2\pi)$. We adopt ULAs at both the transmitter and the receiver, where the antenna response vectors are given by:

$$\begin{aligned}\mathbf{a}_{Tx}(\theta_{Tx,p}) = \frac{1}{\sqrt{N_{Tx}}} \Big[1, e^{j\frac{2\pi d \sin(\theta_{Tx,p})}{\lambda}}, e^{j2\frac{2\pi d \sin(\theta_{Tx,p})}{\lambda}}, \cdots, \\ e^{j\frac{(N_{Tx}-1)2\pi d \sin(\theta_{Tx,p})}{\lambda}}\Big]^T,\end{aligned} \tag{5.2}$$

$$\mathbf{a}_{Rx}(\theta_{Rx,p}) = \frac{1}{\sqrt{N_{Rx}}}\Big[1, e^{j\frac{2\pi d\sin(\theta_{Rx,p})}{\lambda}}, e^{j2\frac{2\pi d\sin(\theta_{Rx,p})}{\lambda}}, \cdots, e^{j\frac{(N_{Rx}-1)2\pi d\sin(\theta_{Rx,p})}{\lambda}}\Big]^T, \tag{5.3}$$

respectively. In Eq. (5.2) and Eq. (5.2) λ is the wavelength of the signal and $d = \lambda/2$ denotes the aperture domain sample spacing. Thereafter, we adopt HBF for our MIMO OFDM scheme operating in doubly selective THz channels under the assumption that the CSI is available at both Alice and Bob. In light of this, the analog beamformed fading channel is formulated as:

$$\mathbf{H}^{RF}_{n,m,l} = \left(\mathbf{W}^{Rx,RF}\right)^H \mathbf{H}_{n,m,l}\mathbf{W}^{Tx,RF}, \tag{5.4}$$

where $\mathbf{W}^{Tx,RF} \in \mathcal{C}^{N_{Tx}\times N_s}$ and $\mathbf{W}^{Rx,RF} \in \mathcal{C}^{N_{Rx}\times N_s}$ are constituted by N_s columns of $\mathbf{A}_{Tx}$ and $\mathbf{A}_{Rx}$ that correspond to the first N_s largest channel gain of $\widetilde{h}_p$, respectively, while N_s represents the number of the data streams. Furthermore, $\mathbf{A}_{Tx}$ and $\mathbf{A}_{Rx}$ representing the antenna response in matrix form are given by $\mathbf{A}_{Tx} = \big[\mathbf{a}_{Tx}(\theta_{Tx,0}), \mathbf{a}_{Tx}(\theta_{Tx,1}), ..., \mathbf{a}_{Tx}(\theta_{Tx,P-1})\big]$ and $\mathbf{A}_{Rx} = [\mathbf{a}_{Rx}(\theta_{Rx,0}), \mathbf{a}_{Rx}(\theta_{Rx,1}), ..., \mathbf{a}_{Rx}(\theta_{Rx,P-1})]$, respectively. The analog Transmit Precoder (TPC) and Receive Combiner (RC) matrices should satisfy $\left\{\left\{\left\|\mathbf{W}^{Tx,RF}[t,\mu]\right\| = \frac{1}{\sqrt{N_{Tx}}}\right\}_{t=1}^{N_{Tx}}\right\}_{\mu=1}^{N_s}$ and $\left\{\left\{\left\|\mathbf{w}^{Rx,RF}[r,\nu]\right\| = \frac{1}{\sqrt{N_{Tx}}}\right\}_{r=1}^{N_{Rx}}\right\}_{\nu=1}^{N_s}$.

Therefore, the signal obtained by the receiver's ν-th RF chain after analog combining is modelled as[1]

$$\begin{aligned} y^{\nu}_{n,m} &= \sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1} h^{RF_{\nu,\mu}}_{n,m,l} s^{\mu}_{n,<m-l>_M} \\ &+ \sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1} h^{RF_{\nu,\mu}}_{n,m,l} s0^{\mu}_{n,<m-l>_M} + \sqrt{1-T}s_{E}{}^{\nu}_{n,m} \\ &= \sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1} h^{RF_{\nu,\mu}}_{n,m,l} s^{\mu}_{n,<m-l>_M} + v^{\nu}_{n,m}, \end{aligned} \tag{5.5}$$

where $h^{RF_{\nu,\mu}}_{n,m,l} = \mathbf{H}^{RF}_{n,m,l}[\nu,\mu]$. The TD matrix form is given by

$$\mathbf{y}^{\nu}_{n} = \sqrt{T}\sum_{\mu=0}^{N_s-1}\mathbf{H}^{RF_{\nu,\mu}}_{n}\mathbf{s}^{\mu}_{n} + \mathbf{v}^{\nu}_{n}, \tag{5.6}$$

where $\mathbf{y}^{\nu}_{n} = [y^{\nu}_{n,0}, y^{\nu}_{n,1}, \cdots, y^{\nu}_{n,M-1}]^T$, $\mathbf{H}^{RF_{\nu,\mu}}_{n}[r,c] = h^{RF_{\nu,\mu}}_{n,r,<r-c>_M}$, $\mathbf{s}^{\mu}_{n} = [s^{\mu}_{n,0}, s^{\mu}_{n,1}, \cdots, s^{\mu}_{n,M-1}]^T$ and $\mathbf{v}^{\nu}_{n} = [v^{\nu}_{n,0}, v^{\nu}_{n,1}, \cdots, v^{\nu}_{n,M-1}]^T$. Then the FD received signal at the ν-th RF chain can

[1] As in a MIMO scenario, the technique of analog precoding and combining is only used for providing a beamforming gain, but the input-output relationship is consistent with the aforementioned SISO OFDM and OTFS systems. Hence, a similar beam splitter model can be extended to their MIMO counterparts, which is shown in Eq. (5.5) and Eq. (5.17).

be obtained by applying the DFT, yielding:

$$\begin{aligned}\overline{y}_{n,\overline{m}}^{\nu} &= \frac{1}{\sqrt{M}}\sum_{m=0}^{M-1} y_{n,m}^{\nu}\omega_M^{-m\overline{m}} \\ &= \frac{\sqrt{T}}{\sqrt{M}}\sum_{m=0}^{M-1}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1} h_{n,m,l}^{RF_{\nu,\mu}} s_{n,<m-l>_M}^{\mu}\omega_M^{-m\overline{m}} + \overline{v}_{n,\overline{m}}^{\nu}.\end{aligned} \tag{5.7}$$

The FD matrix form is given by

$$\overline{\mathbf{y}}_n^{\nu} = \mathbf{F}_M\mathbf{y}_n^{\nu} = \sqrt{T}\sum_{\mu=0}^{N_s-1}\overline{\mathbf{H}}_n^{RF_{\nu,\mu}}\overline{\mathbf{s}}_n^{\mu} + \overline{\mathbf{v}}_n^{\nu}, \tag{5.8}$$

where $\overline{\mathbf{y}}_n^{\nu} \in \mathcal{C}^{M\times 1}$, $\overline{\mathbf{s}}_n^{\mu} = \mathbf{F}_M\mathbf{s}_n^{\mu} \in \mathcal{C}^{M\times 1}$, $\overline{\mathbf{v}}_n^{\nu} = \mathbf{F}_M\mathbf{v}_n^{\nu} \in \mathcal{C}^{M\times 1}$, while $\overline{\mathbf{H}}_n^{RF_{\nu,\mu}} = \mathbf{F}_M\mathbf{H}_n^{RF_{\nu,\mu}}\mathbf{F}_M^H \in \mathcal{C}^{M\times M}$ is no longer diagonal in time-varying frequency-selective fading. Following this, the full matrix form is expressed as

$$\overline{\mathbf{y}}_n = \sqrt{T}\overline{\mathbf{H}}_n^{RF}\overline{\mathbf{s}}_n + \overline{\mathbf{v}}_n, \tag{5.9}$$

where $\overline{\mathbf{y}}_n \in \mathcal{C}^{N_sM\times 1}$, $\overline{\mathbf{H}}_n^{RF} \in \mathcal{C}^{N_sM\times N_sM}$, $\overline{\mathbf{s}}_n \in \mathcal{C}^{N_sM\times 1}$ and $\overline{\mathbf{v}}_n \in \mathcal{C}^{N_sM\times 1}$.

Based on Eq. (5.9), SVD technique can be applied to the analog beamformed fading channels, which gives us

$$\overline{\mathbf{H}}_n^{RF} = \overline{\mathbf{U}}_n^{RF}\overline{\mathbf{\Sigma}}_n^{RF}(\overline{\mathbf{V}}_n^{RF})^H, \tag{5.10}$$

where both $\overline{\mathbf{U}}_n^{RF} \in \mathcal{C}^{N_sM\times N_sM}$ and $\overline{\mathbf{V}}_n^{RF} \in \mathcal{C}^{N_sM\times N_sM}$ are unitary matrices, and the r_n^{FD} non-zero singular values of the rank r_n^{FD} matrix $\overline{\mathbf{H}}_n^{RF}$ can be expressed as follows:

$$\overline{\mathbf{\Sigma}}_n^{RF} = \begin{bmatrix} \text{diag}\left\{\varsigma_{n,1},\varsigma_{n,2},...,\varsigma_{n,r_n^{FD}}\right\} & \mathbf{0}_{r_n^{FD}\times\left(N_sM-r_n^{FD}\right)} \\ \mathbf{0}_{\left(N_sM-r_n^{FD}\right)\times r_n^{FD}} & \mathbf{0}_{\left(N_sM-r_n^{FD}\right)\times\left(N_sM-r_n^{FD}\right)} \end{bmatrix}. \tag{5.11}$$

Based on the singular values in Eq. (5.11), we retain the first $N_{s,n}^{FD}$ singular values of $\overline{\mathbf{H}}_n^{RF}$, which are no less than 0.1, i.e. $\varsigma_{n,n_s^{FD}} \geq 0.1$ with $n_s^{FD} \in [1, N_{s,n}^{FD}]$, $N_{s,n}^{FD} \leq r_n^{FD} \leq N_sM$. Then we apply Water Filling (WF) to them. In light of this, firstly, the average beamforming gain based on the $N_{s,n}^{FD}$ retained singular values can be derived as

$$\overline{\varsigma}_n = \sqrt{\frac{1}{N_{s,n}^{FD}}\sum_{n_s^{FD}=1}^{N_{s,n}^{FD}}\varsigma_{n,n_s^{FD}}^2}. \tag{5.12}$$

Secondly, the first $N_{s,n}^{FD}$ columns of $\overline{\mathbf{V}}_n^{RF}$ and $\overline{\mathbf{U}}_n^{RF}$ are exploited as the digital TPC matrix $\overline{\mathbf{W}}_n^{Tx,BB}$ and RC matrix $\overline{\mathbf{W}}_n^{Rx,BB}$, respectively, i.e. $\overline{\mathbf{W}}_n^{Tx,BB} = \overline{\mathbf{V}}_n^{RF}[:, 1:N_{s,n}^{FD}] \in \mathcal{C}^{N_sM\times N_{s,n}^{FD}}$ and $\left\|\overline{\mathbf{W}}^{Tx,BB}\right\|^2 = N_{s,n}^{FD}$, while $\overline{\mathbf{W}}_n^{Rx,BB} = \overline{\mathbf{U}}_n^{RF}[:, 1:N_{s,n}^{FD}] \in \mathcal{C}^{N_sM\times N_{s,n}^{FD}}$ and $\left\|\overline{\mathbf{W}}^{Rx,BB}\right\|^2 = N_{s,n}^{FD}$. Thirdly, the digital TPC matrices are updated based on the average beamforming gain in Eq. (5.12) for WF, which gives

$$\overline{\mathbf{W}}_{\text{WF},n}^{Tx,BB} = \overline{\mathbf{W}}_n^{Tx,BB}\overline{\varsigma}_n\left[\text{diag}\left\{\frac{1}{\varsigma_{n,1}},\frac{1}{\varsigma_{n,2}},...,\frac{1}{\varsigma_{n,N_{s,n}^{FD}}}\right\}\right]. \tag{5.13}$$

Therefore, at the transmitter, the data-carrying symbols are modulated in the FD as $\overline{\mathbf{x}}_n \in \mathcal{C}^{N_{s,n}^{FD}\times 1}$ and then the subcarriers are precoded as

$$\overline{\mathbf{s}}_n = \overline{\mathbf{W}}_{\mathrm{WF},n}^{Tx,BB}\overline{\mathbf{x}}_n. \tag{5.14}$$

At the receiver, digital RC is applied to $\overline{\mathbf{y}}_n$ of Eq. (5.9), which gives

$$\overline{\mathbf{r}}_n = \left(\overline{\mathbf{W}}_n^{Rx,BB}\right)^H \overline{\mathbf{y}}_n = \sqrt{T}\overline{\varsigma}_n\overline{\mathbf{x}}_n + \left(\overline{\mathbf{W}}_n^{Rx,BB}\right)^H \overline{\mathbf{v}}_n. \tag{5.15}$$

Therefore, the data streams are equalized in the FD as follows:

$$\overline{\mathbf{z}}_n = \overline{\mathbf{r}}_n/\overline{\varsigma}_n. \tag{5.16}$$

5.2.2 MIMO OTFS in Doubly Selective THz Channel using Hybrid Beamforming

As for OTFS based on the OFDM Frame CP structure, the receiver's ν-th RF chain signal after the analog RC is expressed as follows:

$$\begin{aligned} y_{n,m}^{\nu} &= \sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1} h_{n,m,l}^{RF_{\nu,\mu}} s_{<nM+m-l>_{MN}}^{\mu} \\ &+ \sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1} h_{n,m,l}^{RF_{\nu,\mu}} s0_{<nM+m-l>_{MN}}^{\mu} + \sqrt{1-T}s_{E_{n,m}}^{\nu} \\ &= \sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1} h_{n,m,l}^{RF_{\nu,\mu}} s_{<nM+m-l>_{MN}}^{\mu} + v_{n,m}^{\nu}. \end{aligned} \tag{5.17}$$

After carrying out the DFT and SFFT at the receiver's ν-th RF chain, the DD-domain signal is given by

$$\widetilde{y}_{k,l}^{\nu} = \sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{p=0}^{P-1} \widetilde{h}_p^{RF_{\nu,\mu}}\widetilde{T}(k,l,k_p,l_p)\widetilde{s}_{<k-k_p>_N,<l-l_p>_M}^{\mu} + \widetilde{v}_{k,l}^{\nu}, \tag{5.18}$$

where we have

$$\widetilde{h}_p^{RF_{\nu,\mu}} = \sqrt{N_{Tx}N_{Rx}}\widetilde{h}_p \cdot \left[\left(\mathbf{W}^{Rx,RF}\right)^H \mathbf{a}_{Rx}\left(\theta_{Rx},p\right)\mathbf{a}_{Tx}^H\left(\theta_{Tx},p\right)\mathbf{W}^{Tx,RF}\right][\nu,\mu]. \tag{5.19}$$

The DD-domain input-output relationship cast in matrix form is hence given by

$$\widetilde{\mathbf{y}}^{\nu} = \sqrt{T}\sum_{\mu=0}^{N_s-1}\widetilde{\mathbf{H}}^{RF_{\nu,\mu}}\widetilde{\mathbf{s}}^{\mu} + \widetilde{\mathbf{v}}^{\nu}, \tag{5.20}$$

where we have $\widetilde{\mathbf{y}}^{\nu} \in \mathcal{C}^{MN\times 1}$, $\widetilde{\mathbf{y}}^{\nu}[\kappa] = \widetilde{y}_{k,l}$, $\widetilde{\mathbf{s}}^{\mu} \in \mathcal{C}^{MN\times 1}$, $\widetilde{\mathbf{s}}^{\mu}[\kappa] = \widetilde{s}_{k,l}$, $\widetilde{\mathbf{v}}^{\nu} \in \mathcal{C}^{MN\times 1}$, $\widetilde{\mathbf{v}}^{\nu}[\kappa] = \widetilde{v}_{k,l}$, $k = \lfloor\frac{\kappa}{M}\rfloor$, $l = \kappa - kM$, $\widetilde{\mathbf{H}}^{RF_{\nu,\mu}} \in \mathcal{C}^{MN\times MN}$, $\widetilde{\mathbf{H}}^{RF_{\nu,\mu}}[\kappa,\iota] = \widetilde{h}_p^{RF_{\nu,\mu}}\widetilde{T}(k,l,k_p,l_p)$.

Furthermore, the full matrix form is given by

$$\widetilde{\mathbf{y}} = \sqrt{T}\widetilde{\mathbf{H}}^{RF}\widetilde{\mathbf{s}} + \widetilde{\mathbf{v}}, \tag{5.21}$$

where $\widetilde{\mathbf{y}} \in \mathcal{C}^{N_sMN\times 1}$, $\widetilde{\mathbf{H}}^{RF} \in \mathcal{C}^{N_sMN\times N_sMN}$, $\widetilde{\mathbf{s}} \in \mathcal{C}^{N_sMN\times 1}$ and $\widetilde{\mathbf{v}} \in \mathcal{C}^{N_sMN\times 1}$. Similar to its use in OFDM, the SVD is applied to $\widetilde{\mathbf{H}}^{RF}$, which gives

$$\widetilde{\mathbf{H}}^{RF} = \widetilde{\mathbf{U}}^{RF}\widetilde{\mathbf{\Sigma}}^{RF}(\widetilde{\mathbf{V}}^{RF})^H, \tag{5.22}$$

where both $\widetilde{\mathbf{U}}^{RF} \in \mathcal{C}^{N_sMN\times N_sMN}$ and $\widetilde{\mathbf{V}}^{RF} \in \mathcal{C}^{N_sMN\times N_sMN}$ are unitary matrices, and the r^{DD} non-zero singular values of the rank r^{DD} matrix $\widetilde{\mathbf{H}}^{RF}$ can be expressed as follows:

$$\widetilde{\mathbf{\Sigma}}^{RF} = \begin{bmatrix} \text{diag}\left\{\vartheta_1, \vartheta_2, ..., \vartheta_{r^{DD}}\right\} & \mathbf{0}_{r^{DD}\times\left(N_sMN-r^{DD}\right)} \\ \mathbf{0}_{\left(N_sMN-r^{DD}\right)\times r^{DD}} & \mathbf{0}_{\left(N_sMN-r^{DD}\right)\times\left(N_sMN-r^{DD}\right)} \end{bmatrix}. \tag{5.23}$$

Based on the singular values in Eq. (5.23), we take the first N_s^{DD} singular values of $\widetilde{\mathbf{H}}^{RF}$, which are no less than 0.1, i.e. $\vartheta_{n_s^{DD}} \geq 0.1$ with $n_s^{DD} \in [1, N_s^{DD}]$, $N_s^{DD} \leq r^{DD} \leq N_sMN$. Then we apply water-filling to them. In light of this, firstly, the average beamforming gain based on the N_s^{DD} singular values can be formulated as:

$$\overline{\vartheta} = \sqrt{\frac{1}{N_s^{DD}}\sum_{n_s^{DD}=1}^{N_s^{DD}} \vartheta_{n_s^{DD}}^2}. \tag{5.24}$$

Secondly, the first N_s^{DD} columns of $\widetilde{\mathbf{V}}^{RF}$ and $\widetilde{\mathbf{U}}^{RF}$ are harnessed as the digital TPC matrix $\widetilde{\mathbf{W}}^{Tx,BB}$ and RC matrix $\widetilde{\mathbf{W}}^{Rx,BB}$, respectively, i.e. $\widetilde{\mathbf{W}}^{Tx,BB} = \widetilde{\mathbf{V}}^{RF}[:, 1 : N_s^{DD}] \in \mathcal{C}^{N_sMN\times N_s^{DD}}$ and $\left\|\widetilde{\mathbf{W}}^{Tx,BB}\right\|^2 = N_s^{DD}$, while $\widetilde{\mathbf{W}}^{Rx,BB} = \widetilde{\mathbf{U}}^{RF}[:, 1 : N_s^{DD}] \in \mathcal{C}^{N_sMN\times N_s^{DD}}$ and $\left\|\widetilde{\mathbf{W}}^{Rx,BB}\right\|^2 = N_s^{DD}$. Thirdly, the digital TPC matrices are updated based on the average beamforming gain in Eq. (5.24) of WF, which gives

$$\widetilde{\mathbf{W}}_{\text{WF}}^{Tx,BB} = \widetilde{\mathbf{W}}^{Tx,BB}\overline{\vartheta}\left[\text{diag}\left\{\frac{1}{\vartheta_1}, \frac{1}{\vartheta_2}, ..., \frac{1}{\vartheta_{N_s^{DD}}}\right\}\right]. \tag{5.25}$$

Therefore, at the transmitter, the data-carrying symbols are modulated in the DD as $\widetilde{\mathbf{x}} \in \mathcal{C}^{N_s^{DD}\times 1}$ and then the subcarriers are precoded as

$$\widetilde{\mathbf{s}} = \widetilde{\mathbf{W}}_{\text{WF}}^{Tx,BB}\widetilde{\mathbf{x}}. \tag{5.26}$$

At the receiver, the digital RC is applied to $\widetilde{\mathbf{y}}$ of Eq. (5.21), which gives

$$\widetilde{\mathbf{r}} = \left(\widetilde{\mathbf{W}}^{Rx,BB}\right)^H\widetilde{\mathbf{y}} = \sqrt{T}\overline{\vartheta}\widetilde{\mathbf{x}} + \left(\widetilde{\mathbf{W}}^{Rx,BB}\right)^H\widetilde{\mathbf{v}}. \tag{5.27}$$

Hence, the DD-domain data-carrying symbols are normalized as

$$\widetilde{\mathbf{z}} = \widetilde{\mathbf{r}}/\overline{\vartheta}. \tag{5.28}$$

5.2.3 MDR Decoding for OFDM/OTFS in Doubly Selective THz Channels

As portrayed in Fig. 4.2, the MDR process [105, 121] is employed for enhancing the CV-QKD performance in THz quantum channels after the OFDM- and OTFS- based quantum transmission and detection. However, the conventional MDR found in [75, 160] generally assumes a BI-AWGN channel, where the noise variance of LLR computation is uniform across all received Gaussian variables. By contrast, the OFDM FD-SVD decision variables $\bar{\mathbf{z}}_n$ in Eq. (5.16) exhibit different noise variances across different OFDM symbols for each sub-channel in the presence of doubly selective fading. By contrast, the OTFS DD-SVD decision variables $\widetilde{\mathbf{z}}$ in Eq. (5.28) have a noise variance that is always the same for each sub-channel in doubly selective fading. In light of this, the same modified MDR scheme associated with a new mapping schemes is adopted in order to provide reliable LLRs, which is elaborated on in Algorithm 4 of Chapter 4.

Therefore, the LLR calculation associated with FD-SVD detection of Eq. (5.16) in OFMD transmission can be obtained as

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\left\|\ddot{\mathbf{x}}_i\right\|\left\|\ddot{\mathbf{z}}_i\right\|}{\sqrt{D}} \frac{\left\|\overline{\varsigma}_n^{\varrho}\right\|^2}{\left\|\overline{\mathbf{W}}_{\varrho,n}^{Rx,BB}[:, n_s^{FD}]\right\|^2 N_0/2} \mathbf{u}_i^A[d], \tag{5.29}$$

where the modulated/demodulated symbols of the ith segment can be denoted as $\ddot{\mathbf{x}}_i = \mathfrak{Re}\left[\bar{\mathbf{x}}_i^{\mathrm{MDR}}\right] = \mathfrak{Re}\left[\bar{x}_{i,0}^{\mathrm{MDR}}, \cdots, \bar{x}_{i,d}^{\mathrm{MDR}}, \cdots, \bar{x}_{i,D-1}^{\mathrm{MDR}}\right]^T$ and $\ddot{\mathbf{z}}_i = \mathfrak{Re}\left[\bar{\mathbf{z}}_i^{\mathrm{MDR}}\right] = \mathfrak{Re}\left[\bar{z}_{i,0}^{\mathrm{MDR}}, \cdots, \bar{z}_{i,d}^{\mathrm{MDR}}, \cdots, \bar{z}_{i,D-1}^{\mathrm{MDR}}\right]^T$ along with $i = \lfloor n/D \rfloor \cdot N_s^{FD} + n_s^{FD} + \varrho\left(N/D \cdot N_s^{FD}\right)$ and $d = \mathrm{rem}(n, D)$, while $n = 0, 1, ..., N-1$, $n_s^{FD} = 0, 1, ..., N_s^{FD} - 1$ and $\varrho = 0, 1, ..., N_{bl} - 1$. Moreover, $\bar{x}_{i,d}^{\mathrm{MDR}} = \bar{x}_{n,n_s^{FD}}^{\varrho}$ and $\bar{z}_{i,d}^{\mathrm{MDR}} = \bar{z}_{n,n_s^{FD}}^{\varrho}$ represent the dth element in the ith segment of $\bar{s}_i^{\mathrm{MDR}}$ and $\bar{z}_i^{\mathrm{MDR}}$, respectively. The ith segment of noise term can be denoted as $\ddot{\mathbf{v}}_i = \mathfrak{Re}\left[\bar{v}_{i,0}^{\mathrm{MDR}}, \cdots, \bar{v}_{i,d}^{\mathrm{MDR}}, \cdots, \bar{v}_{i,D-1}^{\mathrm{MDR}}\right]^T$ with $\bar{v}_{i,d}^{\mathrm{MDR}} = \overline{v}_{n,n_s^{FD}}^{\varrho}$. Hence, the variance of each element of the noise becomes $\frac{\left\|\overline{\mathbf{W}}_{\varrho,n}^{Rx,BB}\left[:, n_s^{FD}\right]\right\|^2 N_0/2}{\left\|\overline{\varsigma}_n^{\varrho}\right\|^2}$.

In OTFS transmission, similar to Eq. (5.29), the LLR calculation associated with the DD-SVD detection of Eq. (5.28) in OTFS transmission can be obtained as

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\left\|\ddot{\mathbf{x}}_i\right\|\left\|\ddot{\mathbf{z}}_i\right\|}{\sqrt{D}} \frac{\left\|\overline{\vartheta}^{\varrho}\right\|^2}{\left\|\widetilde{\mathbf{W}}_{\varrho}^{Rx,BB}[:, n_s^{DD}]\right\|^2 N_0/2} \mathbf{u}_i^A[d], \tag{5.30}$$

where the modulated/demodulated symbols for the ith segment can be denoted as $\ddot{\mathbf{x}}_i = \mathfrak{Re}\left[\widetilde{\mathbf{x}}_i^{\mathrm{MDR}}\right] = \mathfrak{Re}\left[\widetilde{x}_{i,0}^{\mathrm{MDR}}, \cdots, \widetilde{x}_{i,d}^{\mathrm{MDR}}, \cdots, \widetilde{x}_{i,D-1}^{\mathrm{MDR}}\right]^T$, and $\ddot{\mathbf{z}}_i = \mathfrak{Re}\left[\widetilde{\mathbf{z}}_i^{\mathrm{MDR}}\right] = \mathfrak{Re}\left[\widetilde{z}_{i,0}^{\mathrm{MDR}}, \cdots, \widetilde{z}_{i,d}^{\mathrm{MDR}}, \cdots, \widetilde{z}_{i,D-1}^{\mathrm{MDR}}\right]^T$ with $i = n_s^{DD} + \lfloor \varrho/D \rfloor \cdot N_s^{DD}$ and $d = \mathrm{rem}(\varrho, D)$, where $\varrho = 0, 1, ..., N_{bl} - 1$. Moreover, $\widetilde{x}_{i,d}^{\mathrm{MDR}} = \widetilde{x}_{n_s^{DD}}^{\varrho}$ and $\widetilde{z}_{i,d}^{\mathrm{MDR}} = \widetilde{z}_{n_s^{DD}}^{\varrho}$ represent the dth element in the ith segment of $\widetilde{x}_i^{\mathrm{MDR}}$ and $\widetilde{z}_i^{\mathrm{MDR}}$, respectively. The ith segment of the noise term can

be denoted as $\ddot{\mathbf{v}}_i = \mathfrak{Re}\left[\widetilde{v}_{i,0}^{\mathrm{MDR}}, \cdots, \widetilde{v}_{i,d}^{\mathrm{MDR}}, \cdots, \widetilde{v}_{i,D-1}^{\mathrm{MDR}}\right]^T$ along with $\widetilde{v}_{i,d}^{\mathrm{MDR}} = \widetilde{v}_{n_s^{DD}}^{\varrho}$. Hence the variance of each element of the noise $\ddot{\mathbf{v}}_i$ becomes $\frac{\left\|\widetilde{\mathbf{W}}_{\varrho}^{Rx,BB}\left[:, n_s^{DD}\right]\right\|^2 N_0/2}{\left\|\overline{\vartheta}^{\varrho}\right\|^2}$.

Note that the accuracy of the LLRs of Eq. (5.29) may be affected by the MDR process in mobile scenarios, which will degrade the corresponding SKR performance. To elaborate further, since it is assumed in our MDR process that the fading gains of all elements in a segment are identical, the LLR calculation for a segment will assign the same fading value to each element. However, in time-variant channels, the FD channel $\overline{\mathbf{H}}_n^{RF}$ will fluctuate with time, therefore the average beamforming gain $\overline{\varsigma}_n^{\varrho}$ obtained for each element in a segment will differ from each other, which degrades the accuracy of the LLR calculation of Eq. (5.29). By contrast, the accuracy of LLR calculation of Eq. (5.30) remains unaffected by the MDR process in mobile scenarios, because the DD domain channel $\widetilde{\mathbf{H}}^{RF}$ does not fluctuate with time.

5.2.4 Complexity Analysis for OFDM/OTFS in Doubly Selective THz Channels

Clearly, the SVD calculations dominate the computational complexities of both the OFDM- and OTFS-based transceivers. To elaborate further, the complexity of FD-SVD in Eq. (5.10) for a single OFDM symbol associated with $\overline{\mathbf{H}}_n^{RF} \in \mathcal{C}^{M\times M}$ is $\mathcal{O}(M^3)$ [165–167]. Hence the complexity of a block is $\mathcal{O}(M^3N)$. By contrast, for an OTFS-based system associated with $\widetilde{\mathbf{H}}^{RF} \in \mathcal{C}^{MN\times MN}$, the complexity of a DD-SVD in Eq. (5.22) for a single OTFS block is $\mathcal{O}(M^3N^3)$. Therefore, the complexity of the FD-SVD of OFDM is lower than that of DD-SVD of OTFS. Note that both detectors perform similarly in a stationary scenario. Hence, the FD-SVD of OFDM is the better choice in stationary scenarios.

However, in high-mobility scenarios, the total complexity for a block of N_{bl} OFDM or OTFS symbols required for completing the MDR process with the aid of LDPC codes is $\mathcal{O}(M^3NN_{bl})$ and $\mathcal{O}(M^3N^3)$ for OFDM and OTFS, respectively. This is because in time-variant channels, the FD matrix $\overline{\mathbf{H}}_n^{RF}$ will change with time, which means that the digital beamforming of OFDM has to be updated for each OFDM symbol, where the SVD calculations required for updating the digital beamforming have to be repeated. By contrast, the digital beamforming of OTFS does not have to be updated, owing to the fact that the DD-domain fading representation is time-invariant. In light of this, the complexity of OTFS becomes lower than that of OFDM when we have $N_{bl} > N^2$, which is the case for a large number of blocks combined with powerful LDPC codes having long frame lengths for the sake of achieving a near-capacity performance.

5.3 MIMO OFDM/OTFS Channel Estimation in CV-QKD Systems

In this section, MIMO OFDM/OTFS channel estimation algorithms are proposed for estimating the time-varying frequency-selective MIMO THz channels in CV-QKD systems. Fig. 5.2 illustrates three different channel estimation techniques, namely FD, TD and DD-domain estimations, respectively. The FD estimation in Fig. 5.2(a) arranges the pilot symbols in both FD and TD with suitable spacings, which can be viewed as the "horizontal comb" and the "vertical comb". In contrast to FD estimation, Fig. 5.2(b) shows the TD estimation via placing the TD pilot symbols at the beginning of each transmitted frame. Moreover, as for the DD-domain estimation shown in Fig. 5.2(c), the pilot symbols are inserted into DD index grids. For OFDM channel estimation, it is better to opt for TD channel estimation, because TD estimation performs better than FD estimation in the face of ICI [168], while the DD-domain channel estimation is the natural choice for OTFS systems.

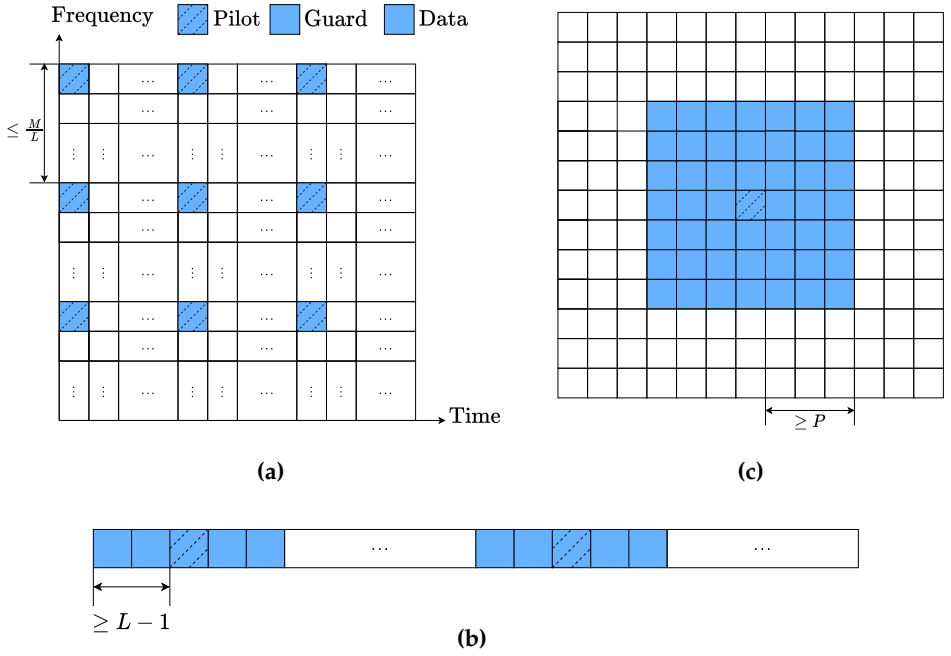


Figure 5.2: Schematic illustration of (a) FD, (b) TD and (c) DD-domain channel estimation techniques.

5.3.1 MIMO OFDM Doubly Selective Channel Estimation

For MIMO OFDM, the fading channels are inherently assumed to be time-invariant. Hence the TF-domain channel estimation algorithm conceived for MIMO OFDM is detailed as follows. Firstly, the input-output relationship between the uth TA of the

transmitter and the vth RA of the receiver is modelled as follows

$$\mathbf{y}^{CE_{v,u}} = \mathbf{H}^{CE_{v,u}}\mathbf{s}^{CE_{v,u}} + \mathbf{v}^{CE_{v,u}}, \tag{5.31}$$

where $\mathbf{y}^{CE_{v,u}} \in \mathcal{C}^{L\times 1}$ represents the received contaminated pilot symbols. Furthermore, $\mathbf{s}^{CE_{v,u}} \in \mathcal{C}^{L\times 1}$ represents the pilot symbols, which takes part of the Direc delta impulse-based CP inserted in the TD of Fig. 5.2(a). More specifically, the Direc delta pulse-based CP is expressed as [168]

$$s_{0,m} = \begin{cases} \rho_{\mathrm{p}}^{\mathrm{TD}}, & m = 0 \\ 0, & m = \pm 1, \pm 2, \ldots, \pm \mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}} \end{cases}, \tag{5.32}$$

where the power of the pilot impulse $\rho_{\mathrm{p}}^{\mathrm{TD}}$ aims for ensuring that the transmission power obeys $\sum_{\forall m} \|s_{0,m}\|^2 = 2\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}} + 1$, while the zeros in Eq. (5.32) are referred to as guard intervals in Fig. 5.2(a). To make sure that there is no interference when carrying out TD convolution represented in the matrix form of Eq. (5.31), the number of guard intervals $\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}}$ should be no less than $L-1$, i.e. $\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}} \geq L-1$. In our work, we set $\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}} = L-1$. Therefore the pilot symbols $\mathbf{s}^{CE_{v,u}}$ used in Eq. (5.31) are $\mathbf{s}^{CE_{v,u}} = [s_{0,0}, s_{0,1}, \ldots, s_{0,L-1}]$. Moreover, $\mathbf{H}^{CE_{v,u}} \in \mathcal{C}^{L\times L}$ represents the $L \times L$ CIR matrix in TD, which is expressed as

$$\mathbf{H}^{CE_{v,u}} = \begin{bmatrix} h_{0,v,u} & h_{L-1,v,u} & \cdots & h_{2,v,u} & h_{1,v,u} \\ h_{1,v,u} & h_{0,v,u} & \cdots & h_{3,v,u} & h_{2,v,u} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ h_{L-2,v,u} & h_{L-3,v,u} & \cdots & h_{0,v,u} & h_{L-1,v,u} \\ h_{L-1,v,u} & h_{L-2,v,u} & \cdots & h_{1,v,u} & h_{0,v,u} \end{bmatrix}, \tag{5.33}$$

where $h_{l,v,u}, \forall l \in [0, L-1]$ are the L CIR taps and $h_{l,v,u} = \sqrt{N_{Tx}N_{Rx}} \cdot \sum_{\forall l_p = l} \widetilde{h}_p \Big[\sqrt{N_{Rx}}\, \mathbf{a}_{Rx}(\theta_{Rx}, p) \sqrt{N_{Rx}} \mathbf{a}_{Tx}^H(\theta_{Tx}, p) \Big][v,u]$. Secondly, based on Eq. (5.31), the L CIR taps can be estimated as $\widehat{h}_{l,v,u}$ that contains the AoA and AoD information. More explicitly, since the TD CE pilot symbol is a Dirac Delta signal, $y^{CE_{v,u}}$ can be directly used as the noise-contaminated estimated CIR $\widehat{h}_{l,v,u}$. Thirdly, the full channel matrix containing all the $\widehat{h}_{l,v,u}$ values of the different antenna pairs for the lth delay tap is constructed as follows

$$\widehat{\mathbf{H}}_l = \begin{bmatrix} \widehat{h}_{l,1,1} & \widehat{h}_{l,1,2} & \cdots & \widehat{h}_{l,1,N_{Tx}} \\ \widehat{h}_{l,2,1} & \widehat{h}_{l,2,2} & \cdots & \widehat{h}_{l,2,N_{Tx}} \\ \vdots & \vdots & \ddots & \vdots \\ \widehat{h}_{l,N_{Rx},1} & \widehat{h}_{l,N_{Rx},2} & \cdots & \widehat{h}_{l,N_{Rx},N_{Tx}} \end{bmatrix}. \tag{5.34}$$

Based on Eq. (5.34), the dominant AoA $\widehat{\theta}_{Rx,p}$ and AoD $\widehat{\theta}_{Tx,p}$ and channel gain of $\widehat{\widetilde{h}}_p$ for the lth delay tap, i.e. $l_p = l$, can be obtained, as described in Algorithm 5. Therefore,

Algorithm 5: MIMO OFDM channel estimation algorithm.

Input: $\mathbf{y}^{CE_{v,u}}$ for $u/v = 0, 1, ..., N_{Tx-1}/N_{Rx-1}$.

Output: AoA and AoD $\widehat{\theta}_{Rx,p}, \widehat{\theta}_{Tx,p}$, and channel gain $\widehat{\widehat{h}}_p$ with $l_p = l$ for all the delay taps.

`// Obtain channel gain` $\widehat{h}_{l,v,u}$

for *All the* (v, u) *antenna pairs* **do**
  Get $\widehat{h}_{l,v,u}$ for L delay taps.
end

`// Obtain` $\widehat{\theta}_{Rx,p}$, $\widehat{\theta}_{Tx,p}$, `and` $\widehat{\widehat{h}}_p$ `with` $l_p = l$

for *All the L delay taps* **do**
  Construct $\widehat{\mathbf{H}}_l$ based on Eq. (5.34) using $\widehat{h}_{l,v,u}$.
  Define the objective function:

$$J\left(\theta_{Rx,p}, \theta_{Tx,p}\right) = \mathbf{a}_{Rx}^{H}\left(\theta_{Rx,p}\right) \cdot \widehat{\mathbf{H}}_l \cdot \mathbf{a}_{Tx}\left(\theta_{Tx,p}\right). \tag{5.36}$$

  The estimation of AoA/AoD can be obtained by:

$$\left(\widehat{\theta}_{Rx,p}, \widehat{\theta}_{Tx,p}\right) = \arg \max_{\substack{\forall \theta_{Rx,p}=0^\circ,1^\circ,...,90^\circ \\ \forall \theta_{Tx,p}=0^\circ,1^\circ,...,90^\circ}} J\left(\theta_{Rx,p}, \theta_{Tx,p}\right) \tag{5.37}$$

  based on the orthogonality of two different steering vectors, which obey:

$$\begin{aligned} \mathbf{a}_{Rx}^{H}\left(\theta_{Rx,p}\right) \mathbf{a}_{Rx}\left(\theta_{Rx,p}\right) &= 1, \\ \mathbf{a}_{Tx}^{H}\left(\theta_{Tx,p}\right) \mathbf{a}_{Tx}\left(\theta_{Tx,p}\right) &= 1. \end{aligned} \tag{5.38}$$

  The channel gain can be obtained by:

$$\widehat{\widehat{h}}_p = \frac{J_{\max}}{N_{Rx} N_{Tx}}. \tag{5.39}$$

end

`// Reconstruct the channel in TD`

Reconstruct the channel in TD after channel estimation, which is expressed as in Eq. (5.35).

`// Update the analog beamformed fading channel`

if *For ABF-based systems* **then**
  Update the analog beamformed fading channel $\widehat{h}_{n,m,l}^{RF}$ based on Eq. (4.34),
else if *For HBF-based systems* **then**
  Update the analog beamformed fading channel $\widehat{\mathbf{H}}_{n,m,l}^{RF}$ based on Eq. (5.4).
end

the reconstructed channel in TD after channel estimation can be expressed as

$$\widehat{\mathbf{H}}_{n,m,l} = \sqrt{N_{Tx} N_{Rx}} \cdot \widehat{\widehat{h}}_p \mathbf{a}_{Rx}(\widehat{\theta}_{Rx,p}) \mathbf{a}_{Tx}^{H}(\widehat{\theta}_{Tx,p}),\ l_p = l. \tag{5.35}$$

5.3.2 MIMO OTFS Doubly Selective Channel Estimation

In this section, we conceive the DD-domain channel estimation for MIMO OTFS based on each single antenna pair in order to obtain the AoA/AoD, delay and Doppler indices and channel gain for each path. The detailed procedure is shown in Algorithm 6. Firstly, the input-output relationship between the uth TA of the transmitter and the vth RA of the receiver is modelled as follows:

$$\widetilde{\mathbf{y}}^{CE_{v,u}} = \widetilde{\mathbf{H}}^{CE_{v,u}} \widetilde{\mathbf{s}}^{CE_{v,u}} + \widetilde{\mathbf{v}}^{CE_{v,u}}, \tag{5.40}$$

where we have $\widetilde{\mathbf{y}}^{CE_{v,u}} \in \mathcal{C}^{MN\times 1}$, $\widetilde{\mathbf{H}}^{CE_{v,u}} \in \mathcal{C}^{MN\times MN}$, $\widetilde{\mathbf{s}}^{CE_{v,u}} \in \mathcal{C}^{MN\times 1}$ and $\widetilde{\mathbf{v}}^{CE_{v,u}} \in \mathcal{C}^{MN\times 1}$. Furthermore, $\widetilde{\mathbf{H}}^{CE_{v,u}}[\kappa,\iota] = \widetilde{h}_{p,v,u}\widetilde{T}(k,l,k_p,l_p)$ and $\widetilde{h}_{p,v,u} = \sqrt{N_{Tx}N_{Rx}}\widetilde{h}_p \cdot \Big[\sqrt{N_{Rx}}\mathbf{a}_{Rx}(\theta_{Rx},p)$ $\sqrt{N_{Tx}}\mathbf{a}_{Tx}^H(\theta_{Tx},p)\Big][v,u]$, since neither analog beamforming nor digital beamforming is used during the channel estimation process. Moreover, $\widetilde{\mathbf{s}}^{CE_{v,u}}$ represents the DD-domain pilot symbol, which is a Dirac delta impulse transmitted in the DD-domain of Fig. 5.2(b). The elements of $\widetilde{\mathbf{s}}^{CE_{v,u}}$ are set as [168]

$$\widetilde{\mathbf{s}}^{CE_{v,u}}[\kappa] = \begin{cases} \rho_{\mathrm{p}}^{\mathrm{DD}}, & \kappa = \kappa_{\mathrm{p}} \\ 0, & \kappa = \kappa_{\mathrm{p}} \pm 1, \kappa_{\mathrm{p}} \pm 2, \ldots, \kappa_{\mathrm{p}} \pm \mathcal{N}_{\mathrm{guard}}^{\mathrm{DD}} \\ \widetilde{s}_{k,l}, & \text{otherwise} \end{cases} \tag{5.41}$$

where the power of the pilot impulse $\rho_{\mathrm{p}}^{\mathrm{DD}}$ is adjusted for maintaining the constant OTFS frame power of MN. The guard interval has to obey $\mathcal{N}_{\mathrm{guard}}^{\mathrm{DD}} \geq P$. Secondly, the estimated Delay and Doppler index $\widehat{l}_p, \widehat{k}_p$ and channel gain $\widehat{\widetilde{h}}_{p,v,u}$ that contains the AoA and AoD information are obtained based on the SISO OTFS channel estimation algorithm of [158]. Thirdly, a new channel matrix containing all the $\widehat{\widetilde{h}}_{p,v,u}$ values of the different antenna pairs for the pth path is constructed as follows

$$\widehat{\widetilde{\mathbf{H}}}_p = \begin{bmatrix} \widehat{\widetilde{h}}_{p,1,1} & \widehat{\widetilde{h}}_{p,1,2} & \cdots & \widehat{\widetilde{h}}_{p,1,N_{Tx}} \\ \widehat{\widetilde{h}}_{p,2,1} & \widehat{\widetilde{h}}_{p,2,2} & \cdots & \widehat{\widetilde{h}}_{p,2,N_{Tx}} \\ \vdots & \vdots & \ddots & \vdots \\ \widehat{\widetilde{h}}_{p,N_{Rx},1} & \widehat{\widetilde{h}}_{p,N_{Rx},2} & \cdots & \widehat{\widetilde{h}}_{p,N_{Rx},N_{Tx}} \end{bmatrix}. \tag{5.42}$$

Based on Eq. (5.42), the estimated AoA $\widehat{\theta}_{Rx,p}$ and AoD $\widehat{\theta}_{Tx,p}$ and channel gain $\widetilde{h}_p$ can be obtained, as detailed in Algorithm 6.

Algorithm 6: MIMO OTFS channel estimation algorithm.

Input: $\widetilde{\mathbf{y}}^{CE_{v,u}}$ for $u/v = 0, 1, ..., N_{Tx-1}/N_{Rx-1}$

. **Output:** Delay and Doppler index $\widehat{l}_p, \widehat{k}_p$, AoA and AoD $\widehat{\theta}_{Rx,p}, \widehat{\theta}_{Tx,p}$, and channel gain $\widehat{\widetilde{h}}_p$ for all the paths.

`// Obtain` $\widehat{l}_p, \widehat{k}_p$ `and channel gain` $\widehat{\widetilde{h}}_{p,v,u}$

for *All the* (v, u) *antenna pairs* **do**

  Get $\widehat{l}_p, \widehat{k}_p, \widehat{\widetilde{h}}_{p,v,u}$ for $\widehat{P}$ paths based on SISO OTFS channel estimation in [158].

end

`// Obtain` $\widehat{\theta}_{Rx,p}, \widehat{\theta}_{Tx,p}$, `and` $\widehat{\widetilde{h}}_p$

for *All the* $\widehat{P}$ *paths* **do**

  Construct $\widehat{\widetilde{\mathbf{H}}}_p$ based on Eq. (5.42) using $\widehat{\widetilde{h}}_{p,v,u}$.

  Define the objective function:

$$J\left(\theta_{Rx,p}, \theta_{Tx,p}\right) = \mathbf{a}_{Rx}^{H}\left(\theta_{Rx,p}\right) \cdot \widehat{\widetilde{\mathbf{H}}}_p \cdot \mathbf{a}_{Tx}\left(\theta_{Tx,p}\right). \tag{5.43}$$

  The estimation of AoA/AoD can be obtained by:

$$\left(\widehat{\theta}_{Rx,p}, \widehat{\theta}_{Tx,p}\right) = \arg \max_{\substack{\forall \theta_{Rx,p}=0^\circ,1^\circ,...,90^\circ \\ \forall \theta_{Tx,p}=0^\circ,1^\circ,...,90^\circ}} J\left(\theta_{Rx,p}, \theta_{Tx,p}\right) \tag{5.44}$$

  based on the orthogonality of two different steering vectors, which obey:

$$\mathbf{a}_{Rx}^{H}\left(\theta_{Rx,p}\right)\mathbf{a}_{Rx}\left(\theta_{Rx,p}\right) = 1, \quad \mathbf{a}_{Tx}^{H}\left(\theta_{Tx,p}\right)\mathbf{a}_{Tx}\left(\theta_{Tx,p}\right) = 1. \tag{5.45}$$

  The channel gain can be obtained by:

$$\widehat{\widetilde{h}}_p = \frac{J_{\max}}{N_{Rx}N_{Tx}}. \tag{5.46}$$

end

`// Reconstruct the analog beamformed fading gain for each path`

if *For ABF-based systems* **then**

  Reconstruct the analog beamformed fading gain $\widehat{\widetilde{h}}_p^{RF}$ for each path p based on Eq. (4.43),

else if *For HBF-based systems* **then**

  Reconstruct the analog beamformed fading gain $\widehat{\widetilde{h}}_p^{RF_{v,\mu}}$ for each path p based on Eq. (5.19).

end

5.4 Secret Key Rate Analysis

The definition of SKR is expressed as follows [65][2]

$$K_{\text{finite}} = \gamma \left(1 - P_B\right) \left[\beta I_{AB} - \chi_{BE} - \triangle \left(N_{\text{privacy}}\right)\right], \tag{5.47}$$

where γ denotes the fraction of the key extractions in the total number of data exchanged by Alice and Bob, while P_B represents the BLER in the reconciliation step. Furthermore, I_{AB} is the classical mutual information between Alice and Bob based on their shared correlated data, and χ_{BE} represents the Holevo information that Eve can extract from the information of Bob[3]. Finally, $\triangle \left(N_{\text{privacy}}\right)$ represents the finite-size offset factor associated with the finite-size N_{privacy}. As for $\beta \in [0,1]$, it represents the reconciliation efficiency, which is defined as [59, 74]

$$\begin{aligned} \beta = \frac{R^{\text{eff}}}{C} &= \frac{R^{\text{eff}}}{\mathbb{E}\left[0.5 \log_2\left(1 + \text{SNR}^{Rx}\right)\right]} \\ &= \frac{R^{\text{eff}}}{\mathbb{E}\left[0.5 \log_2\left(1 + 1/N_0^{Rx}\right)\right]}. \end{aligned} \tag{5.48}$$

R^{eff} represents the transmission rate, where we have $R^{\text{eff}} = \left(1 - \frac{M_{cp}}{M}\right) \cdot R$ for OFDM transmission and $R^{\text{eff}} = \left(1 - \frac{M_{cp}}{MN}\right) \cdot R$ for OTFS transmission, while R is the coding rate, and C is the one-dimensional Shannon capacity [108, 128]. Furthermore, SNR^{Rx} represents the receive SNR after equalization at the receivers, which can be expressed as $\text{SNR}^{Rx} = 1/N_0^{Rx} = 1/N_0\text{Y}$. The noise variance N_0^{Rx} equals to $\frac{\left\|\overline{\mathbf{W}}_{\varrho,n}^{Rx,BB}\left[:,n_s^{FD}\right]\right\|^2 N_0}{\left\|\overline{\varsigma}_n^{\varrho}\right\|^2}$ and $\frac{\left\|\widetilde{\mathbf{W}}_{\varrho}^{Rx,BB}\left[:,n_s^{DD}\right]\right\|^2 N_0}{\left\|\overline{\vartheta}^{\varrho}\right\|^2}$ based on Eq. (5.29) and Eq. (5.30), when FD-SVD of OFDM and DD-SVD of OTFS receivers are used, respectively, and the corresponding coefficient Y equals to $\frac{\left\|\overline{\varsigma}_n^{\varrho}\right\|^2}{\left\|\overline{\mathbf{W}}_{\varrho,n}^{Rx,BB}\left[:,n_s^{FD}\right]\right\|^2}$, and $\frac{\left\|\overline{\vartheta}^{\varrho}\right\|^2}{\left\|\widetilde{\mathbf{W}}_{\varrho}^{Rx,BB}\left[:,n_s^{DD}\right]\right\|^2}$.

The calculations of I_{AB}, and χ_{BE} are similar to those in [79, 83, 84, 96, 105, 111]. To elaborate further, similar to [105], the total amount of noise between Alice and Bob ξ_{total} can be expressed as $\xi_{\text{total}} = \xi_{\text{line}} + \xi_{\text{det}}$, where $\xi_{\text{line}} = \frac{1-T}{T} W$ represents the impairment imposed by Eve, and W is the variance of the channel's noise [83]. Furthermore, $T = 10^{-\alpha \mathfrak{L}/10}$ represents the distance-dependent path loss, where α and $\mathfrak{L}$ represent the attenuation and distance between Alice and Bob, respectively. Moreover, $\xi_{\text{det}} = \frac{1-\eta}{\eta T} S$

[2]Note that Eq. (5.47) is the normalized SKR based on the bandwidth. As for the unnormalized SKR, it can be expressed based on Eq. (5.47) as $K_{\text{finite}}^{\text{UN}} = B \cdot K_{\text{finite}}$, where B represents the bandwith of the multi-carrier systems considered and we have $B = M\Delta f$. In this work, normalized SKR results are used.

[3]It is assumed that the strongest attack [54], namely the so-called collective attack is used. Accordingly, Eve performs an optimal collective measurement on the collection of the stored ancilla after the key distillation procedure. Therefore, the Holevo information between Eve and Bob is harnessed as the evaluation metric for this kind of attack.

is the homodyne detector's noise, where η represents the detection efficiency and S stands for the variance of the trusted detector's noise [79]. After taking the effect of imperfect detection stated above into account, the variance of Bob's received signal based on the HBF and detection as shown in Eq. (5.16) and Eq. (5.28) can be represented as

$$\begin{aligned} V_B &= \eta T \left(\mathrm{Y} V_A + \xi_{\text{total}} \right) \\ &= \eta T \mathrm{Y} V_A + \eta \left(1 - T \right) W + \left(1 - \eta \right) S. \end{aligned} \tag{5.49}$$

where $V_A = V_0 + V_s$ is the total variance of Alice's side, which contains the modulation variance V_s and the thermal noise variance V_0. The variance of the thermal noise is given by $V_0 = 2\bar{n} + 1$ with $\bar{n} = \left[\exp\left(\hbar f_c / k_B T_e \right) \right]^{-1}$, where $\hbar$ is Planck's constant, k_B is Boltzmann's constant, f_c is the carrier frequency and T_e is the environmental temperature in Kelvin. We make the worst-case assumption that Eve can acquire perfect CSI knowledge and accordingly set $W = 1 + \frac{T(1-\mathrm{Y})V_0}{1-T}$, which is similar in [96]. Therefore, the mutual information between Alice and Bob can be obtained as follows:

$$\begin{aligned} I_{AB} =& \frac{1}{2} \log_2 \left[1 + \frac{\eta T \mathrm{Y} V_s}{\eta T V_0 + \eta \left(1 - T \right) + \left(1 - \eta \right) S} \right] \\ =& \frac{1}{2} \log_2 \left[\frac{\eta T (\mathrm{Y} V_s + V_0) + \eta \left(1 - T \right) + \left(1 - \eta \right) S}{\eta T V_0 + \eta \left(1 - T \right) + \left(1 - \eta \right) S} \right], \end{aligned} \tag{5.50}$$

where the second term in $\log_2(\cdot)$ represents the receiver's SNR after equalization. Note that, V_s is adjustable in order to match the required SNR at receiver's side by compensating the effect of fading channel gain Y and loss T, therefore we can rewrite $V_s' = \mathrm{Y} V_s$ and $V_A' = V_s' + V_0$.

On the other hand, the Holevo information between Bob and Eve can be calculated as follows [59, 127]

$$\chi_{BE} = S(\rho_{AB}) - S\big(\rho_{A|B}\big), \tag{5.51}$$

where $S(\cdot)$ is the von Neumann entropy defined in [59, 127]. In light of this, the covariance matrix related to the information between Alice and Bob, i.e. the mode of ρ_{AB} after transmission through the quantum channel can be expressed as [59, 127]

$$\begin{aligned} \mathbf{V}_{AB} &= \begin{pmatrix} V_A' \mathbf{I}_2 & \sqrt{\eta T \left({V_A'}^2 - 1 \right)} \mathbf{Z} \\ \sqrt{\eta T \left({V_A'}^2 - 1 \right)} \mathbf{Z} & V_B \mathbf{I}_2 \end{pmatrix} \\ &= \begin{pmatrix} a \mathbf{I}_2 & c \mathbf{Z} \\ c \mathbf{Z} & b \mathbf{I}_2 \end{pmatrix}, \end{aligned} \tag{5.52}$$

where

$$\mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{5.53}$$

are the two Pauli matrices. Therefore, the required symplectic eigenvalues of ρ_{AB} are given by [59, 127]

$$v_{1,2}^2 = \frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4D^2}\right), \tag{5.54}$$

where

$$\begin{aligned} \Delta &= a^2 + b^2 - 2c^2, \\ D &= ab - c^2. \end{aligned} \tag{5.55}$$

As for the symplectic eigenvalue of $\rho_{A|B}$, it can be shown that [59, 127]:

$$v_3 = \sqrt{a\left(a - \frac{c^2}{b}\right)}. \tag{5.56}$$

Hence, the Holevo information can be calculated as

$$\chi_{BE} = G(v_1) + G(v_2) - G(v_3), \tag{5.57}$$

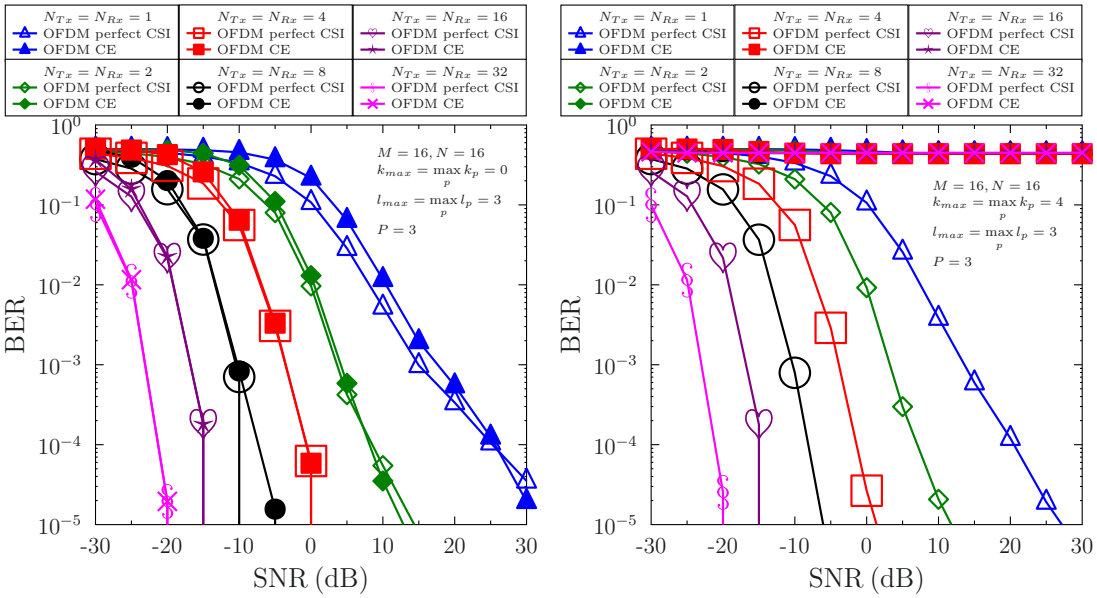
where v_1, v_2 and v_3 are symplectic eigenvalues and $G(*) = \left(\frac{*+1}{2}\right) \cdot \log_2\left(\frac{*+1}{2}\right) - \left(\frac{*-1}{2}\right) \cdot \log_2\left(\frac{*-1}{2}\right)$. Upon substituting Eq. (5.50) and Eq. (5.57) into Eq. (5.47), the corresponding SKR can be obtained.

5.5 Performance Analysis of ABF-Assisted Systems Relying on Imperfect Channel Estimation

In this section, before we delve into the performance analysis of HBF-assisted systems in Section 5.6, the performance analysis of ABF-assisted systems relying on realistic imperfect channel estimation is carried out in terms of BER performance comparisons between OFDM and OTFS in classical communications both with perfect and imperfect CSI. The BLER performance comparisons between the OFDM and OTFS CV-QKD systems both with perfect and imperfect CSI were demonstrated in Section 4.5.2.

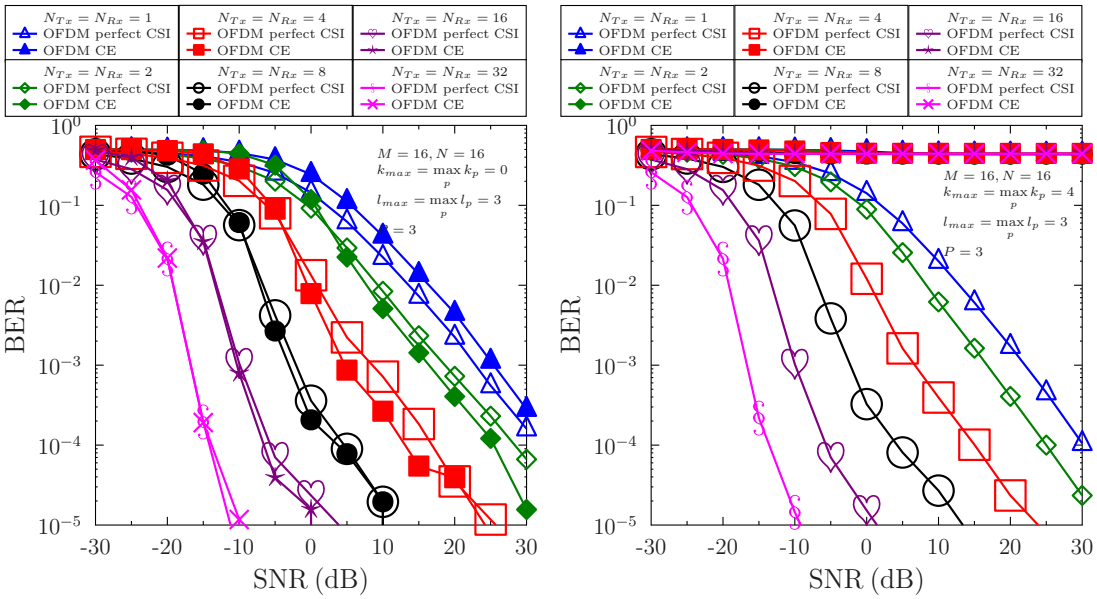
5.5.1 OFDM vs. OTFS in Classical Communication

Fig. 5.3 demonstrates our comparison between ABF-assisted MIMO OFDM systems with both perfect and estimated CSI based on Algorithm 5, where different MIMO sizes as well as both stationary and mobile scenarios are investigated. It is demonstrated by Fig. 5.3(a) and Fig. 5.3(c) that the BER performance associated with estimated CSI is very close to that with perfect CSI in the SISO case. Furthermore, the BER with estimated CSI is almost the same as that with perfect CSI when increasing the MIMO size from 1×1 to 32×32 in a stationary scenario for both $K = 6$ dB and $K = -6$ dB, since the channel estimation for MIMO OFDM is trivial in stationary cases. By contrast,



(a) K=6 dB, $k_{max} = \max_p k_p = 0$

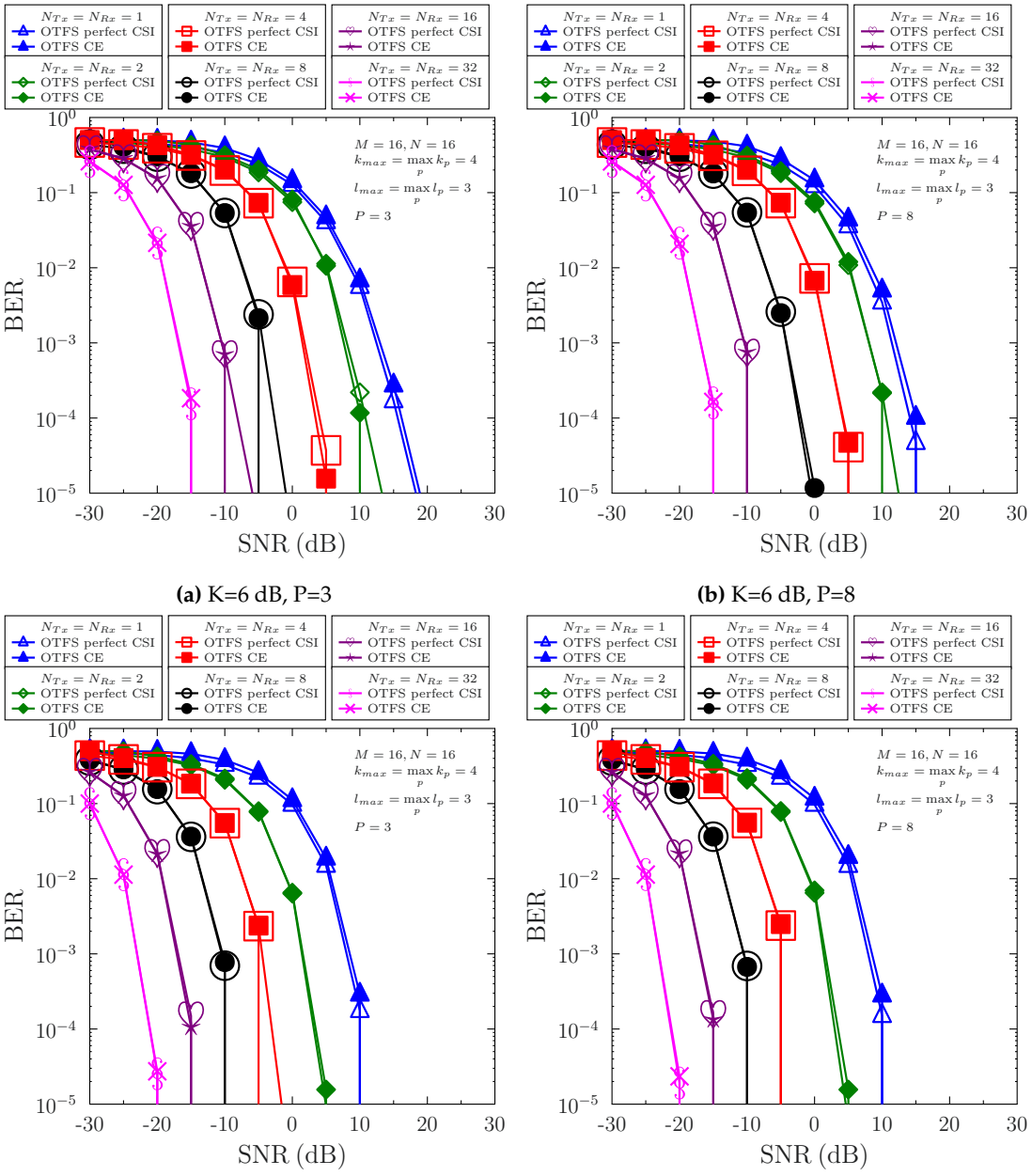
(b) K=6 dB, $k_{max} = \max_p k_p = 4$



(c) K=-6 dB, $k_{max} = \max_p k_p = 0$

(d) K=-6 dB, $k_{max} = \max_p k_p = 4$

Figure 5.3: Performance comparison between **ABF-assisted MIMO OFDM systems with both perfect and estimated CSI** and with different MIMO sizes in both **stationary** and **mobile** scenarios, where $M = 16$ and $N = 16$ are used and we have: (a) K=6 dB, $k_{max} = \max_p k_p = 0$, (b) K=6 dB, $k_{max} = \max_p k_p = 4$, (c) K=-6 dB, $k_{max} = \max_p k_p = 0$, (d) K=-6 dB, $k_{max} = \max_p k_p = 4$.



(a) K=6 dB, P=3

(b) K=6 dB, P=8

(c) K=-6 dB, P=3

(d) K=-6 dB, P=8

Figure 5.4: Performance comparison between **ABF assisted MIMO OTFS systems with both perfect and estimated CSI** and with different MIMO sizes in **mobile** scenario ($k_{max} = \max_p k_p = 4$), where $M = 16$ and $N = 16$ are used and we have: (a) K=6 dB, P=3, (b) K=6 dB, P=8, (c) K=-6 dB, P=3, (d) K=-6 dB, P=8.

the BER results of estimated CSI seen in Fig. 5.3(b) and Fig. 5.3(d) exhibit irreducible error floors, regardless of the value of the Ricean K and of the number of antennas. This is due to the fact that in a mobility scenario, the TF-domain channel estimation algorithm suffers from the time-varying fluctuation of fading channels, where the inter-channel interference becomes too severe to extract accurate CSI. Furthermore, there is no time interpolation in our channel estimation benchmark for OFDM.

In contrast to the channel estimation performance illustrated in Fig. 5.3, ABF-assisted MIMO OTFS using the proposed DD-domain channel estimation algorithm does not suffer from error floors in Fig. 5.4. It is demonstrated in Fig. 5.4 that the BER performances relying on estimated channel CSI based on Algorithm 6 are comparable to those with perfect channel CSI even in mobile cases, for a high Ricean $K = 6$ dB and low Ricean $K = -6$ dB. This is owing to the fact that OTFS transforms time-varying frequency-selective fading in the TF domain into quasi-static fading in the DD domain, which allows accurate channel estimation even in high-mobility scenarios.

5.5.2 OFDM vs. OTFS in CV-QKD

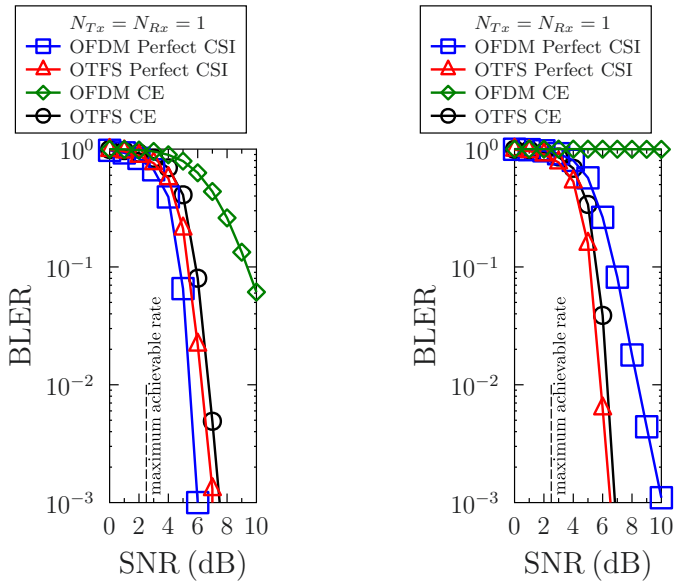


Figure 5.5: ABF CE: Performance comparison between **SISO OFDM and OTFS-LDPC CV-QKD systems with estimated CSI** in both (a) **stationary** ($v = 0$ mph) and (b) **mobile** ($v = 30$ mph) scenarios, where $M = 64$ and $N = 16$ are used.

To further investigate the effect of channel estimation on the BLER performance of the ABF-assisted OFDM/OTFS CV-QKD systems conceived in Chapter 4, Fig. 5.5 portrays our BLER performance comparison between the OFDM and OTFS schemes employed by our LDPC-aided CV-QKD system relying on estimated CSI in stationary and mobile scenarios. Fig. 5.5(a) demonstrates that the BLER performance of OTFS associated with

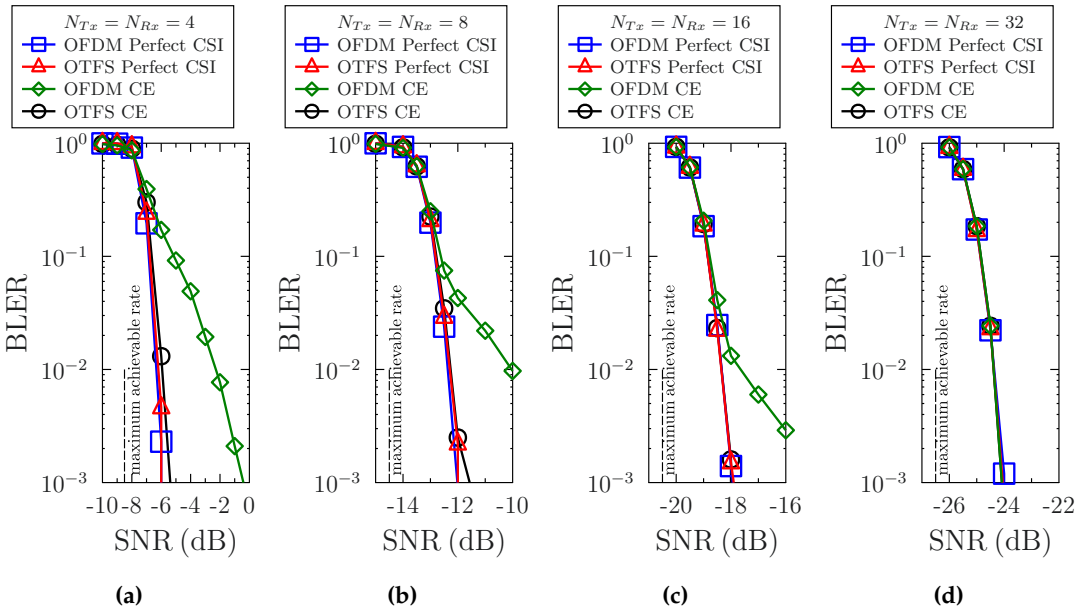


Figure 5.6: ABF CE: Performance comparison between **MIMO OFDM and OTFS-LDPC systems with estimated CSI** with different MIMO size in **mobile** scenario ($v = 0$ mph), where $M = 64$ and $N = 16$ are used and we have: (a) $N_{Tx} = N_{Rx} = 4$, (b) $N_{Tx} = N_{Rx} = 8$, (c) $N_{Tx} = N_{Rx} = 16$, (d) $N_{Tx} = N_{Rx} = 32$.

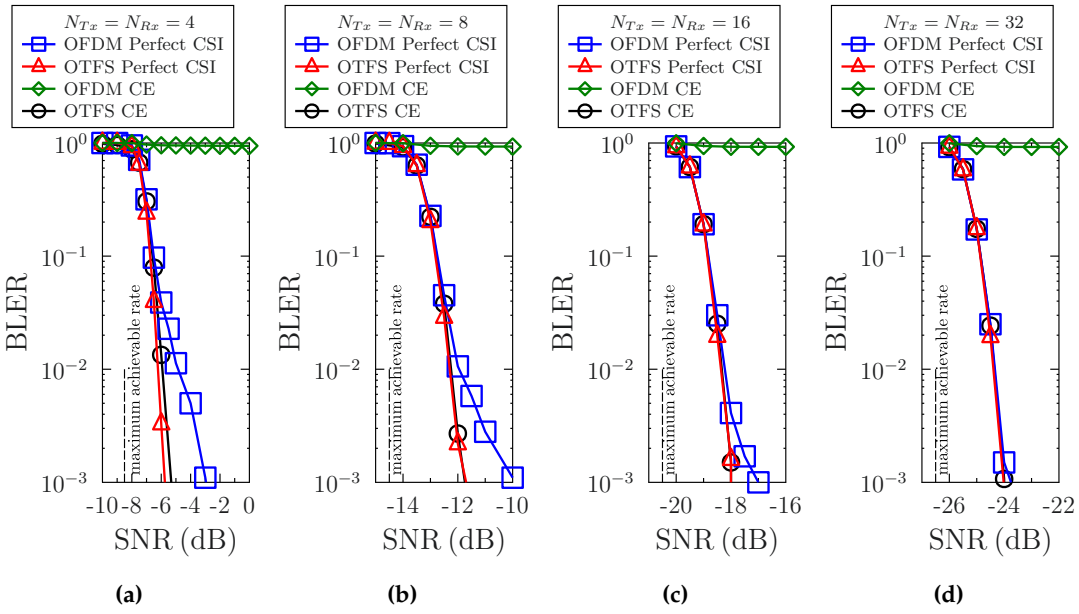


Figure 5.7: ABF CE: Performance comparison between **MIMO OFDM and OTFS-LDPC systems with estimated CSI** with different MIMO size in **mobile** scenario ($v = 30$ mph), where $M = 64$ and $N = 16$ are used and we have: (a) $N_{Tx} = N_{Rx} = 4$, (b) $N_{Tx} = N_{Rx} = 8$, (c) $N_{Tx} = N_{Rx} = 16$, (d) $N_{Tx} = N_{Rx} = 32$.

estimated CSI approaches the performance with perfect CSI, whilst there is a substantial gap between the BLER performance of OFDM with estimated CSI and with perfect CSI. This leads to a severe degradation of the corresponding reconciliation efficiency. Therefore, the maximum secure transmission distance is much shorter than before in the OFDM based CV-QKD system. Furthermore, as shown in Fig. 5.5(b) for mobile cases, the performance of OTFS with estimated CSI remains the same as that with perfect CSI, whilst there is a high error-floor for OFDM with estimated CSI. Hence, the OFDM-based system fails to achieve an adequate SKR and secure distance for CV-QKD.

Fig. 5.6 and Fig. 5.7 present on performance comparison between MIMO OFDM and OTFS based CV-QKD systems with estimated CSI in stationary and mobile scenarios, respectively. It is demonstrated in Fig. 5.6 and Fig. 5.7 that the performance of OTFS associated with estimated CSI remains the same as that with perfect CSI in both stationary and mobile scenarios. Therefore, the same reconciliation efficiencies and SKR versus distance can be achieved for OTFS based system associated with estimated CSI as that with perfect CSI. By contrast, for the OFDM based system operating in stationary cases, the performance associated with estimated CSI is gradually improved upon increasing the MIMO size from 1×1 to 32×32, as evidenced by Fig. 5.6. On the other hand, it is illustrated in Fig. 5.7 that the OFDM system with estimated CSI cannot perform adequately in mobile case due to the high error-floor. This is due to the fact that in a mobile scenario, the TF-domain channel estimation benchmark algorithm, operating without time interpolation suffers from the time-varying fluctuation of fading channels, where the inter-channel interference prevents the systems from extracting accurate CSI.

5.6 Performance Analysis of Hybrid Beamforming-Assisted Systems

In this section, a comparison between HBF-assisted OFDM and OTFS systems in classical communications is conducted, followed by a comprehensive parametric study of both THz OFDM and OTFS based CV-QKD. Explicitly, firstly the BER performance comparisons are presented for both OFDM and OTFS based multicarrier-based systems associated with a MIMO dimension of $N_{Tx} \times N_{Rx}$ in classical communications. Then, our BLER performance comparisons are presented for different multicarrier-based CV-QKD quantum transmission systems associated with a vehicle velocity v and MIMO dimension $N_{Tx} \times N_{Rx}$. Moreover, the SKR versus distance as a key performance indicator will be analyzed.

Table 5.2: Simulation parameters.

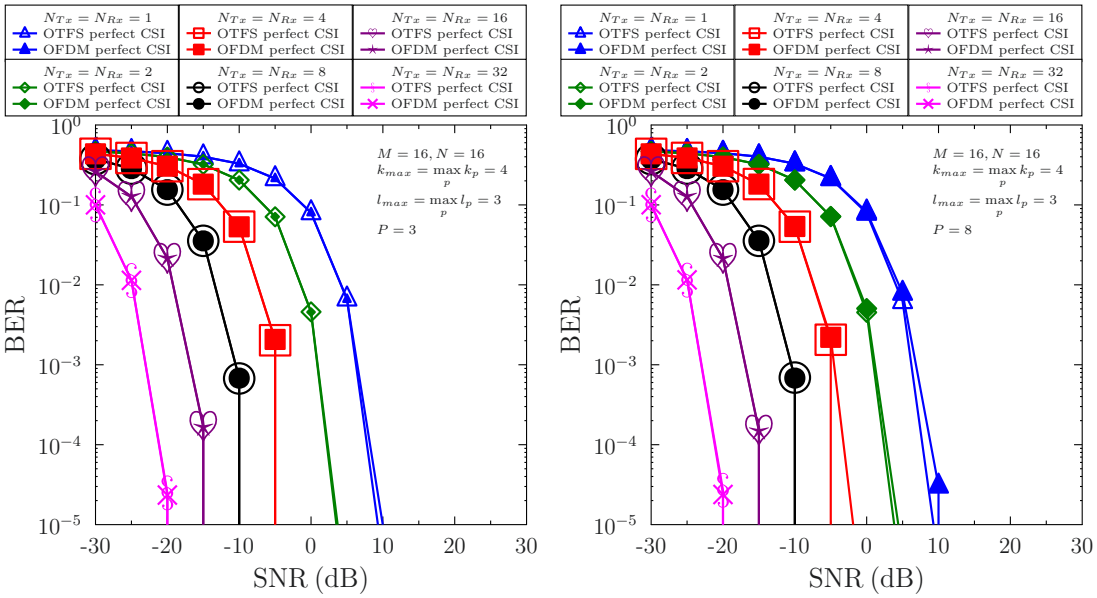
Parameter	Symbol	Value
Parameters for OFDM/OTFS		
The number of subcarrier	M	64
The number of symbol	N	16
Subcarrier spacing	Δf	2 MHz
Carrier frequency	f_c	15 THz
Maximum delay	τ_{max}	20 ns
Speed	v	0,30 mph
Parameters for MIMO		
The number of transmitter antennas	N_{Tx}	1,4,8
The number of receiver antennas	N_{Rx}	1,4,8
Parameters for LDPC		
Coding rate	R	0.5
Code length	N_{FEC}	1024
Parameters for the QuC		
Ricean factor	K	0 dB
Atmospheric loss	α	50 dB/km

The simulation parameters are summarized in Table 5.2, which are selected based on the seminal papers in the open literature [79, 83, 105, 133, 163]. Specifically, the attenuation coefficient α associated with the atmospheric path loss is set to 50 dB/km at 15 THz [79, 83][4]. Moreover, due to the limited number of scatterers and high attenuation of the THz band [133, 136, 163], based on [136] we set the Ricean factor K to 0 dB. The FEC code length of $N_{\text{FEC}} = 1024$ and the coding rate of $R = 0.5$ are the same as in [105]. The CP length M_{cp} is set to $M_{cp} = L + 1$, where we have $L = \lceil \tau_{max} M \Delta f \rceil = 1, 2, 3$ for $M = 16, 32, 64$, respectively, and $P = L$.

5.6.1 OFDM vs. OTFS in Classical Communication

Fig. 5.8 portrays our BER performance comparison between HBF assisted MIMO OFDM and OTFS systems in classical communications with perfect CSI under different MIMO sizes in mobile scenarios. Firstly, it is demonstrated that the BER of OFDM is comparable to that of OTFS. Secondly, it can be observed by comparing Fig. 5.8(a) and Fig. 5.8(c) as well as by comparing Fig. 5.8(c) and Fig. 5.8(d) that the BER performance is improved, as the Ricean K factor increases. Thirdly, it can also be observed from Fig. 5.8(b) and Fig. 5.8(d) that OTFS significantly outperforms OFDM for $N_{Tx} = N_{Rx} = 1$, when the number of paths is increased to $P = 8$. This is due to the improved multipath diversity gain that can be achieved by OTFS. However, as N_{Tx} and N_{Rx} increase, the beamforming gain dominates, which results in OTFS and OFDM perform comparably, as evidenced by Fig. 5.8(a)-(d).

[4]In contrast to the THz wireless communication range spanning from 0.1 to 10 THz, the THz range investigated in the literature of QKD is wider, ranging from 0.1 to 50 THz [24, 79]. Therefore, the frequency set in our paper is chosen in line with [79], which exhibits low atmospheric loss and low thermal noise. Higher THz carrier frequencies are generally preferred for QKD, because the lower the frequency, the higher the thermal noise, which degrades the secure communication distance.



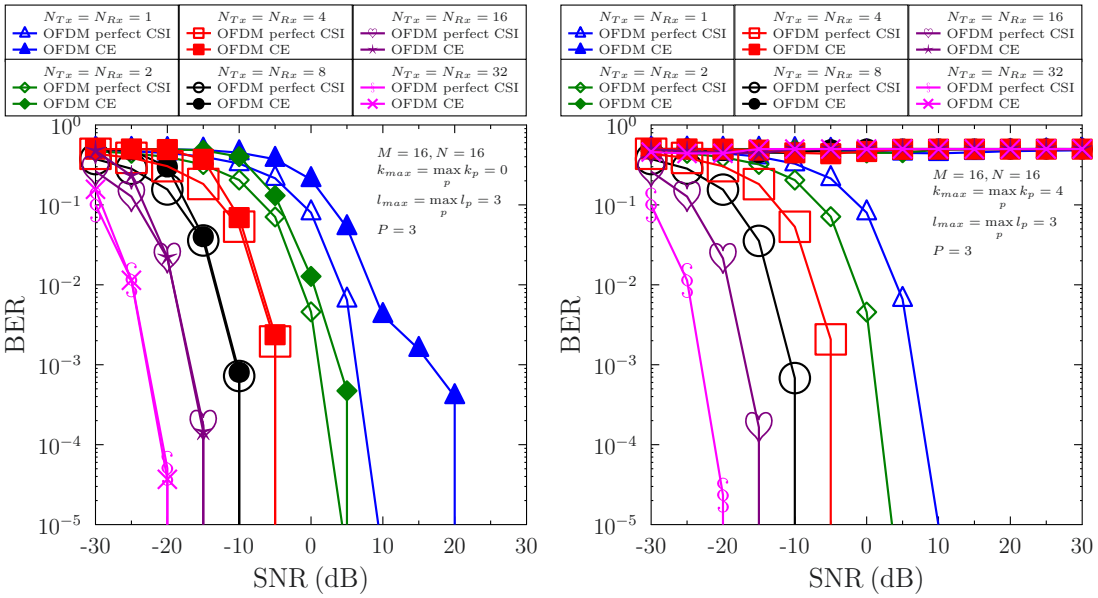
(a) K=6 dB, P=3

(b) K=6 dB, P=8

(c) K=-6 dB, P=3

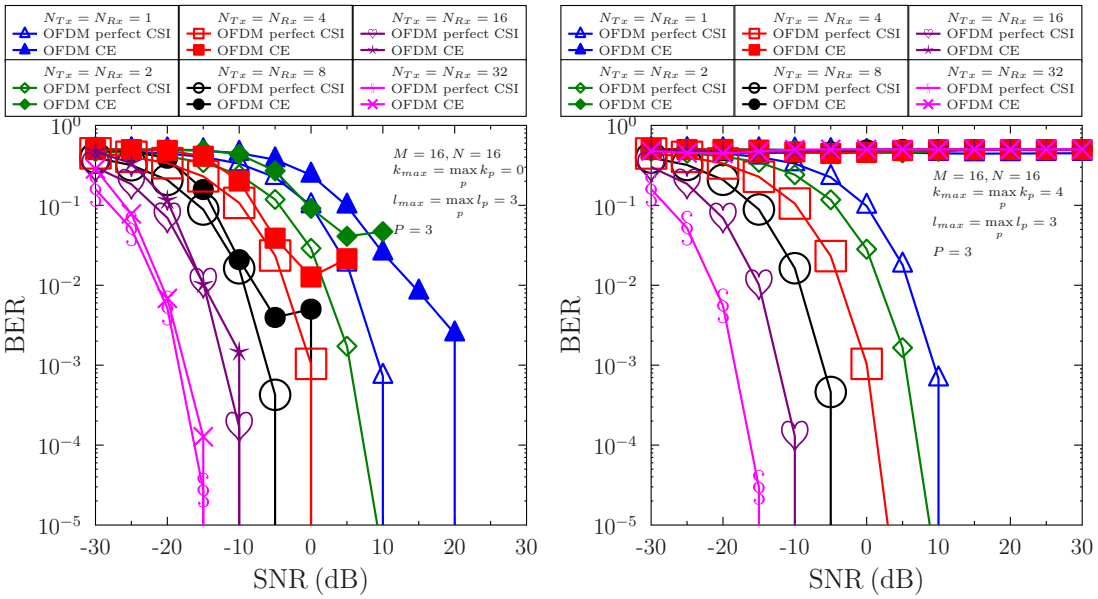
(d) K=-6 dB, P=8

Figure 5.8: Performance comparison between **HBF assisted MIMO OFDM and OTFS systems in classical communications with perfect CSI** and with different MIMO sizes in **mobile** scenario ($k_{max} = \max_p k_p = 4$), where $M = 16$ and $N = 16$ are used and we have: (a) K=6 dB, P=3, (b) K=6 dB, P=8, (c) K=-6 dB, P=3, (d) K=-6 dB, P=8.



(a) K=6 dB, $k_{max} = \max_p k_p = 0$

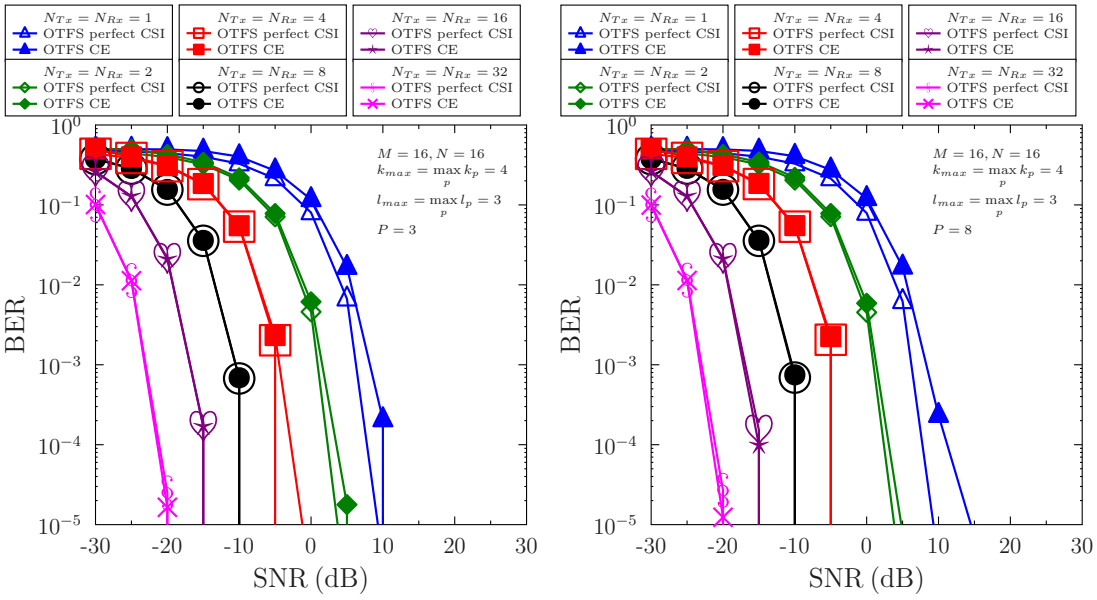
(b) K=6 dB, $k_{max} = \max_p k_p = 4$



(c) K=-6 dB, $k_{max} = \max_p k_p = 0$

(d) K=-6 dB, $k_{max} = \max_p k_p = 4$

Figure 5.9: Performance comparison between **HBF assisted MIMO OFDM systems with both perfect and estimated CSI** and with different MIMO sizes in both **stationary** and **mobile** scenarios, where $M = 16$ and $N = 16$ are used and we have: (a) K=6 dB, $k_{max} = \max_p k_p = 0$, (b) K=6 dB, $k_{max} = \max_p k_p = 4$, (c) K=-6 dB, $k_{max} = \max_p k_p = 0$, (d) K=-6 dB, $k_{max} = \max_p k_p = 4$.



(a) K=6 dB, P=3

(b) K=6 dB, P=8

(c) K=-6 dB, P=3

(d) K=-6 dB, P=8

Figure 5.10: Performance comparison between **HBF assisted MIMO OTFS systems with both perfect and estimated CSI** and with different MIMO sizes in **mobile** scenario ($k_{max} = \max_p k_p = 4$), where $M = 16$ and $N = 16$ are used and we have: (a)K=6 dB, P=3, (b) K=6 dB, P=8, (c) K=-6 dB, P=3, (d) K=-6 dB, P=8.

Fig. 5.9 portrays our comparison between HBF assisted MIMO OFDM systems with both perfect and estimated CSI based on Algorithm 5, where different MIMO sizes are investigated in both stationary and mobile scenarios. It is demonstrated by Fig. 5.9(a) that the BER performance with estimated CSI gradually approaches to that with perfect CSI upon increasing the MIMO size from 1×1 to 32×32 in a stationary scenario for $K = 6$ dB, since the channel estimation of MIMO OFDM is accurate in stationary cases. But the channel estimation performance degrades for $N_{Tx} = N_{Rx} \leq 8$ at $K = -6$ dB in Fig. 5.9(c), owing to the increased multipath interference. Nonetheless, in the stationary scenario, the BER results of perfect CSI and estimated CSI become comparable for $N_{Tx} = N_{Rx} > 8$, which is a benefit of the increased beamforming gain that compensates for CSI estimation errors, as demonstrated by Fig. 5.9(c). By contrast, the BER results of estimated CSI seen in Fig. 5.9(b) and Fig. 5.9(d) exhibits irreducible error floors, regardless of the value of Ricean K and the number of antennas. This is due to the fact that in mobile scenarios, the TF-domain channel estimation algorithm suffers from the time-varying fluctuation of fading channels, where the inter-channel interference prevents the systems from extracting accurate CSI. Furthermore, there is no time interpolation in our channel estimation benchmark for OFDM.

In contrast to the channel estimation performance illustrated in Fig. 5.9, HBF assisted MIMO OTFS using the proposed DD-domain channel estimation algorithm does not suffer from error floors, as seen in Fig. 5.10. Explicitly, it is demonstrated in Fig. 5.10 that the BER associated with estimated channel CSI based on Algorithm 6 approaches the performance of perfect channel CSI even in mobile scenarios for both high Ricean $K = 6$ dB and low Ricean $K = -6$ dB. This is a benefit of the fact that OTFS transforms the time-varying frequency-selective fading in the TF domain into quasi-static fading in the DD domain, which once again makes channel estimation quite accurate even in high-mobility scenarios.

5.6.2 OFDM vs. OTFS in CV-QKD

Fig. 5.11 provides our performance comparison between the OFDM and OTFS schemes employed by our LDPC-aided CV-QKD systems relying on idealistic perfect CSI, where the user velocity is set to $v = 0$ m/s for time-invariant fading and $v = 30$ mph for time-varying fading, respectively. Fig. 5.11 (a) demonstrates that both the detectors of the OFDM FD-SVD and OTFS DD-SVD based CV-QKD systems achieve a comparable performance in stationary scenario, which is expected in the absence of doubly selective fading. However, Fig. 5.11 (b) shows that in a mobile scenario associated with a user speed of $v = 30$ mph, the OTFS DD-SVD based CV-QKD system outperforms the OFDM FD-SVD based system in time-varying THz channels.

Fig. 5.12 illustrates the effect of the MIMO size $N_{Tx} \times N_{Rx}$ on the BLER performance in a mobile (v=30 mph) scenario, where idealistic perfect CSI is assumed. Firstly, it

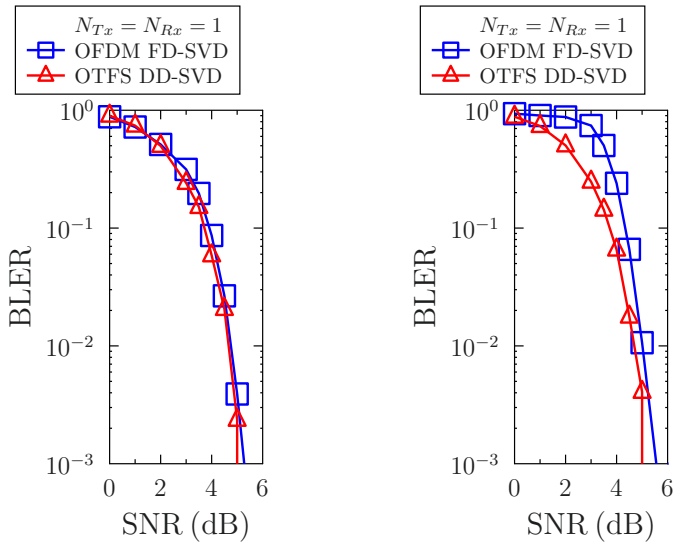


Figure 5.11: Performance comparison between **SISO OFDM and OTFS-LDPC CV-QKD systems with perfect CSI** in both (a) **stationary** ($v = 0$ mph) and (b) **mobile** ($v = 30$ mph) scenarios, where $M = 64$ and $N = 16$ are used.

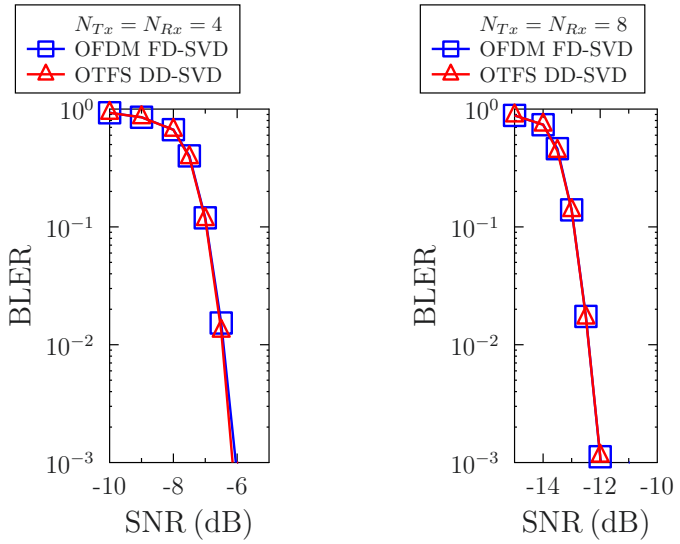


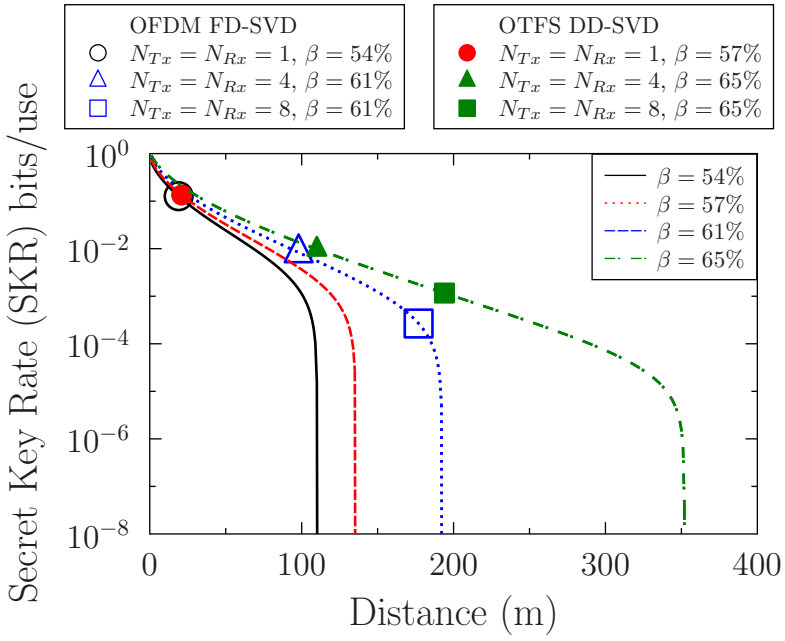
Figure 5.12: Performance comparison between **MIMO OFDM and OTFS-LDPC systems with perfect CSI** with different MIMO size in **mobile** scenario ($v = 30$ mph), where $M = 64$ and $N = 16$ are used and we have: (a) $N_{Tx} = N_{Rx} = 4$, (b) $N_{Tx} = N_{Rx} = 8$.

Table 5.3: Reconciliation efficiency comparison of different detection methods used in OFDM/OTFS CV-QKD system under different M and $N_{Tx} \times N_{Rx}$. The reconciliation efficiencies are calculated from Eq. (5.48) at the BLER threshold that equals to 0.1, together with the corresponding SNRs. Note that both the stationary and mobile scenarios are considered with $v = 0, 30$ mph.

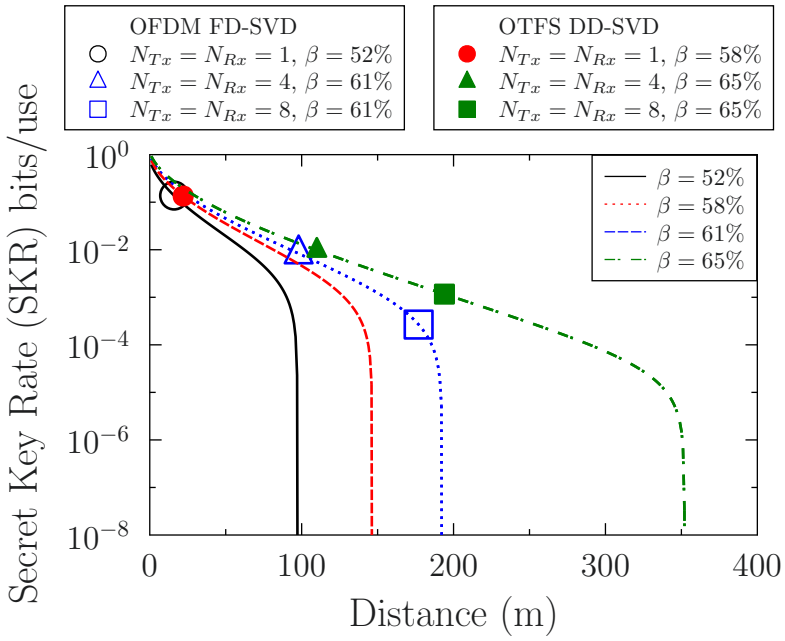
	$N_{Tx} \times N_{Tx}$	OFDM FD-SVD		OTFS DD-SVDE	
		SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$
$v =$ 0 mph	1×1	3.85	54.17	3.75	57.44
	4×4	-6.9	60.95	-6.9	65.08
	8×8	-12.8	61.28	-12.8	65.38
$v =$ 30 mph	1×1	4.4	52.30	3.75	57.80
	4×4	-6.9	60.93	-6.9	65.08
	8×8	-12.8	61.44	-12.8	65.23

is demonstrated that the OFDM FD-SVD based CV-QKD system achieves the same performance as the OTFS DD-SVD based system even in mobile cases, since the beamforming gain obtained by our MIMO assists in mitigating the gap between OTFS and OFDM observed in SISO case, as shown in Fig.5.11 (b). Secondly, Fig. 5.12 demonstrates that the BLER performance improves for both the OTFS and OFDM detectors, as the MIMO size increases. Specifically, it can be observed from Fig. 5.12(a) and (b) that the SNR required for a BLER of 10^{-1} is reduced from -6.9 dB to -12.8 dB with the increase of MIMO size from 4 to 8.

In order to investigate the effect of different parameters on the SKR, the parameter pair of BLER and β, denoted by (BLER, β), are summarized in Table 5.3 for both stationary and mobile scenarios. Based on this, Fig. 5.13 portrays our SKR versus distance comparison between our MIMO OFDM and OTFS LDPC-aided systems using different detectors and MIMO sizes in both stationary and mobile scenarios. The modulation variance is always kept at the optimal value, in the same way as in [71]. The other parameters are as follows [79, 83]: atmospheric loss $\alpha = 50$ dB/km; room temperature $T_e = 296$ K; detector efficiency $\eta = 0.98$; detector's noise variance $S = 1$; $N_{\text{privacy}} = 10^{12}$. In Fig. 5.13 (a), there are four asymptotic theoretical SKR curves associated with different reconciliation efficiencies, which are 54%, 57%, 61% and 65%, respectively. Firstly, Fig. 5.13 (a) demonstrates that in a stationary scenario, the OFDM and OTFS-based systems achieve comparable SKR performance in the SISO case. However, in the MIMO case, longer secure transmission distance is achieved by the OTFS-based CV-QKD system than by its OFDM counterpart, since the OTFS-based CV-QKD system associated with frame-based CP overhead can provide higher reconciliation efficiencies than its OFDM counterpart, which can be seen in Table 5.3. Secondly, Fig. 5.13 (a) also confirms that the increased MIMO beamforming gain attained is capable of increasing the secure transmission distance for both OFDM and OTFS based CV-QKD. More explicitly, upon increasing the antenna size from 1×1, 4×4, 8×8, the secure transmission distance of our OTFS-based system can be extended from 20 meters (red filled circle), to 120 meters (green filled triangle) and 190 meters (green filled square),



(a)



(b)

Figure 5.13: The SKR versus distance comparison between **MIMO OFDM and OTFS-LDPC systems with perfect CSI** using different detections and different MIMO sizes with BLER equals to 10^{-1} in Table 5.3, where $M = 64$, $N = 16$, $f_c = 15$ THz, $N_{\text{FEC}} = 1024$ and $R = 0.5$ are used in the following scenarios: (a) $v = 0$ mph, (b) $v = 30$ mph.

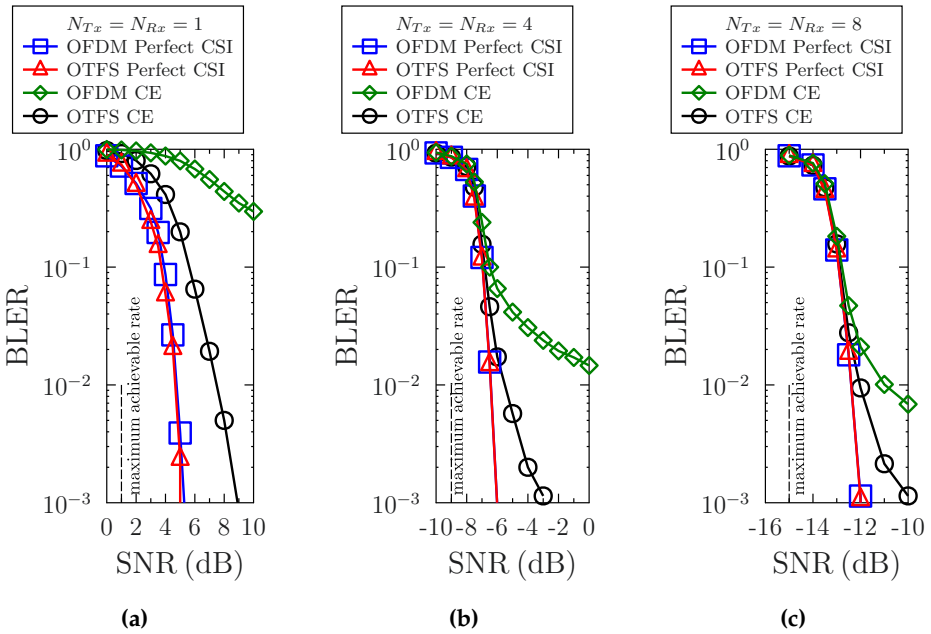


Figure 5.14: SVD-WF CE: Performance comparison between **OFDM and OTFS-LDPC CV-QKD systems with estimated CSI** with different MIMO sizes in **stationary** scenarios, where $M = 64$ and $N = 16$ are used and we have: (a) $N_{Tx} = N_{Rx} = 1$, (b) $N_{Tx} = N_{Rx} = 4$, (c) $N_{Tx} = N_{Rx} = 8$.

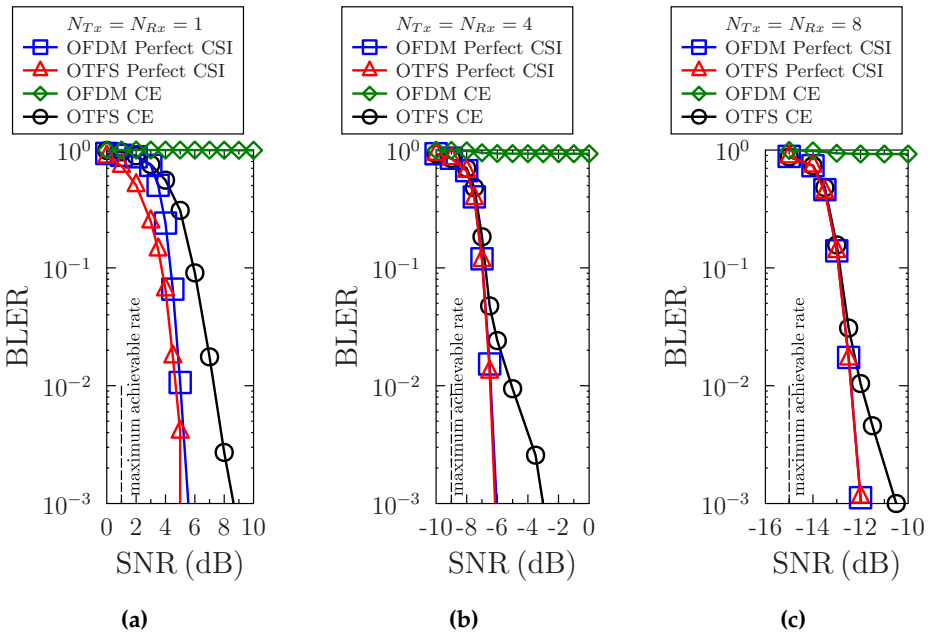


Figure 5.15: SVD-WF CE: Performance comparison between **OFDM and OTFS-LDPC CV-QKD systems with estimated CSI** with different MIMO sizes in **mobile** scenarios ($v = 30$ mph), where $M = 64$ and $N = 16$ are used and we have: (a) $N_{Tx} = N_{Rx} = 1$, (b) $N_{Tx} = N_{Rx} = 4$, (c) $N_{Tx} = N_{Rx} = 8$.

respectively, whereas the corresponding secure transmission distance of our OFDM system can be extended from 20 meters (black circle), to 100 meters (blue triangle) and 170 meters (blue square), respectively.

Furthermore, in Fig. 5.13(b), there are four asymptotic theoretical SKR curves having different reconciliation efficiencies defined in Eq. (2.62), which are 52%, 58%, 61% and 65%, respectively. Similar conclusions can be made in doubly selective THz fading channels as seen from Fig. 5.13(a). More explicitly, the secure transmission distance of our OTFS-based system is around 20 meters (red filled circle), 120 meters (green filled triangle) and 190 meters (green filled square) in 1×1, 4×4, 8×8 antenna settings, respectively. By contrast, the corresponding secure transmission distance of our OFDM system is around 16 meters (black circle), 100 meters (blue triangle) and 170 meters (blue square) in 1×1, 4×4, 8×8 antenna setting, respectively.

To further investigate the effect of channel estimation on the BLER performance, Fig. 5.14 portrays our BLER performance comparison between the OFDM and OTFS schemes employed by our LDPC-aided CV-QKD system with estimated CSI in a stationary scenario. Fig. 5.14(a) demonstrates that there is almost no BLER performance gap for OTFS between the estimated CSI and perfect CSI SISO case, whilst there is a high BLER floor for OFDM with estimated CSI. Furthermore, the BLER performance of OFDM and OTFS with estimated CSI is gradually improved upon increasing the MIMO sizes from 1×1 to 8×8 as evidenced by Fig. 5.14(b) and (c).

By contrast, Fig. 5.15 presents our performance comparison between MIMO OFDM and OTFS based CV-QKD systems with estimated CSI in mobile scenarios. It is observed that the performance of OTFS with estimated CSI exhibits the same trend as that in Fig. 5.14, where the corresponding BLER performance of OTFS with estimated CSI is gradually improved when increasing the MIMO sizes. Therefore, similar reconciliation efficiencies and SKR versus distance can be achieved for OTFS based systems with estimated CSI as that with perfect CSI in both stationary and mobile scenarios. However, the OFDM system with estimated CSI does not perform adequately in mobile cases. This is due to the fact that in a mobile scenario, the TF-domain channel estimation benchmark algorithm, operating without time interpolation suffers from the time-varying fluctuation of fading channels, where the inter-channel interference prevents the systems from extracting accurate CSI.

5.7 Conclusions

Multi-carrier OFDM and OTFS based LDPC assisted CV-QKD reconciliation schemes have been designed and studied in the face of time-varying and frequency-selective THz scenarios, where **HBF** were utilized to improve the quantum transmission distance attained in the face of severe THz path loss. **Firstly**, it was demonstrated that the

Table 5.4: A summary of SKR vs. distance based on Fig. 5.13, where $M = 64$, $N = 16$.

	$N_{Tx} \times N_{Tx}$	OFDM FD-SVD		OTFS DD-SVD	
		$\beta(\%)$	Max. distance(m)	$\beta(\%)$	Max. distance(m)
MIMO ($v = 0$ mph)	1×1	54.17	20	57.44	20
	4×4	60.95	100	65.08	120
	8×8	61.28	170	65.38	190
MIMO ($v = 30$ mph)	1×1	52.30	16	57.80	20
	4×4	60.93	100	65.08	120
	8×8	61.44	170	65.23	190

OFDM FD-SVD based CV-QKD system with perfect CSI achieves comparable BLER performance to the OTFS DD-SVD based system even in mobile ($v = 30$ mph) scenarios, since the beamforming gain mitigates the gap between OTFS and OFDM observed in SISO cases, provided that perfect CSI is available at both the transmitter and receiver. **Secondly**, it was demonstrated that the BLER performance is improved upon increasing the MIMO size, thanks to the improved beamforming gain achieved by the MIMO OFDM/OTFS scheme proposed for quantum transmission. **Thirdly**, an SKR versus distance performance comparison was conducted, which is summarized in Table 5.4. It was demonstrated that the OTFS-based system associated with frame-based CP overhead offers higher SKR and longer secure transmission distance than the OFDM-based system in both stationary and mobile ($v = 30$ mph) scenarios. Moreover, increasing the MIMO size enhances the secure transmission distance for both the OFDM- and OTFS-based systems. **Lastly**, the effect of channel estimation on the OFDM- and OTFS-based systems was investigated. It was demonstrated that the OTFS system with estimated CSI performs similarly to that with perfect CSI in both stationary and mobile scenarios. Therefore, similar reconciliation efficiencies and SKR vs. distance performance can be achieved for OTFS based systems with estimated CSI as that with perfect CSI. However, the OFDM-based system with estimated CSI cannot achieve adequate SKR and secure distance for CV-QKD in mobile cases due to its BLER.

Chapter 6

Conclusions and Future Work

In this concluding chapter, we commence by summarizing our conclusions in Section 6.1, while a range of promising future research directions will be discussed in Section 6.2.

6.1 Conclusions

Chapter 1 In Section 1.1, we presented the motivation of quantum communication and argued that QKD plays an important role in constructing a more secure communication environment compared to some classic cryptography algorithms, by way of detecting the presence of eavesdropping. In light of this, QKD-based research has flourished in both the quantum physics and communication societies. Therefore, a historical review of QKD-based research has been provided in Section 1.2, which was followed by the outline of the thesis in Section1.3 and the novel contributions in Section 1.4.

Chapter 2 In this chapter, we provided a rudimentary introduction to QKD protocols. In Section 2.2, the syndrome-based decoding process was reviewed with the aid of Hamming and LDPC coded examples, followed by brief reviews of the DV-QKD and CV-QKD systems in Section 2.3 and Section 2.4, respectively. Both the quantum transmission and classic reconciliation schemes have been introduced with an emphasis on LDPC-coded reconciliation schemes. Thereafter, a comprehensive parametric study of LDPC-coded reconciliation in CV-QKD systems was conducted in Section 2.4.3. Specifically, as seen in Fig. 2.6(a) and Fig.2.17(a), the BLER performance is gradually improved with the increase of the code length of LDPC codes. The corresponding coding gains associated with different LDPC codes having different code lengths are tabulated in Table 2.4, along with the associated coding gains

in Fig. 2.18. Furthermore, the computational complexities of LDPC decoding associated with different code lengths and code rates are tabulated in Table 2.5, and they are portrayed in Fig. 2.20. Section 2.4.4.3 introduced the calculation of SKR and demonstrated the importance of reconciliation efficiency for the SKR versus distance performance. More specifically, it is demonstrated in Fig.2.21 and Fig.2.22 that a longer LDPC code has a better BLER performance, hence it provides higher reconciliation efficiency, thus offering higher SKR and longer secure transmission distances. As a further investigation, both SISO and MIMO THz CV-QKD systems have been introduced with an emphasis on the quantum transmission part in Section 2.5 and Section 2.6. It can be concluded from Fig. 2.24, Fig. 2.26 and Fig. 2.28 that both the thermal noise variance level, the absorption coefficient and the path loss associated with different frequency bands have a significant impact on the SKR versus distance performance of THz CV-QKD systems.

Chapter 3 In this chapter, the codeword based reconciliation concept was proposed as the general reconciliation scheme illustrated in Fig. 3.5 that can be applied in conjunction with diverse FEC codes, as detailed in Section 3.2. This is a significant improvement, because the popular syndrome-based LDPC-coded reconciliation scheme can only be applied for FEC codes that possess syndromes like Systems A and B shown in Fig. 3.2 and Fig. 3.3. Furthermore, in contrast to the general assumption that the classical authenticated channel is error-free and noiseless, a realistic ClC has been considered in System B, as shown in Fig. 3.3, which may contain errors. In Section 3.3, the SKR calculation is derived for the FEC-coded reconciliation scheme of CV-QKD system in fibre transmission. In Section 3.4, we investigated the performance of our QKD systems when the classical authenticated channel is modelled either as an AWGN channel or a Rayleigh channel. It is demonstrated in Fig. 3.7 and Fig. 3.8 that when the ClC quality is sufficiently high, the QKD system will have a relatively low BLER. An error floor is exhibited by the system, when the ClC has errors due to employing a weak channel code or when the ClC quality is too low. More specifically, we have investigated LDPC codes, plus CC and IRCC assisted CV-QKD schemes. It was demonstrated in Fig. 3.14 and Fig. 3.16 that the IRCC-aided system performs best among them, followed by the LDPC codes, whilst the CC code performs the worst. In light of this, the SKR versus distance performance of different FEC codes using optical fibre as the QuC has been compared. It was demonstrated in Fig. 3.15 that near-capacity FEC codes such as IRCC can provide higher reconciliation efficiency, hence they can offer a longer secure transmission distance, which is summarized in Table 3.5.

Chapter 4 In this chapter, an OFDM/OTFS based LDPC assisted MDR CV-QKD system was conceived for transmission over time-variant frequency-selective THz channels, as detailed in Section 4.2. Furthermore, ABF technique is harnessed in our MIMO OFDM/OTFS based CV-QKD systems communicating in THz channels, which attains a high beamforming gain,as detailed in Section 4.3. In Section 4.4, the SKR calculation is derived for the ABF OFDM/OTFS based LDPC assisted CV-QKD systems in THz transmission. Our performance analysis was conducted in Section 4.5 in terms of the BLER versus SNR and SKR versus distance. Firstly, it was demonstrated in Fig.4.7 that the BLER is similar under three different OFDM/OTFS detectors in stationary ($v = 0$ mph) cases. The BLER of our OTFS DD-MMSE based system is the best, followed by that of the OFDM FD-MMSE based method. The BLER of OFDM using FDE detection is the worst in mobile ($v = 30$ mph) scenarios as shown in Fig. 4.7. Secondly, we investigated the effect of FEC block length. It was demonstrated in Fig. 4.9 that all the BLER performances are improved under all three different detectors upon increasing the block length. However, the delay will be increased for larger block length, especially when an ARQ mechanism is adopted for retransmissions, if the decoding fails. Thirdly, it was demonstrated in Fig. 4.10 that the BLER performance will be improved upon increasing the MIMO size, thanks to the improved beamforming gain achieved by the MIMO OFDM/OTFS scheme proposed for quantum transmission. Lastly, an SKR versus distance performance comparison was conducted, which is summarized in Table 4.6. It was demonstrated in Fig. 4.12 that the OTFS-based system offers higher SKR and longer secure transmission distance compared to the OFDM-based system in both stationary and mobile ($v = 30$ mph) scenarios. Moreover, increasing the MIMO size can enhance the secure transmission distance for both the OFDM- and OTFS-based systems.

Chapter 5 In this chapter, HBF OTFS/OFDM based and LDPC assisted CV-QKD reconciliation schemes have been established and studied in the face of time-varying and frequency-selective THz scenarios. The corresponding system model is introduced in Section 5.2. In order to fulfil the pre-condition that the full CSI is available at both the transmitter and receiver, a variety of channel estimation methods are conceived for MIMO OFDM/OTFS in order to facilitate CSI-T and CSI-R for HBF in Section 5.3. In Section 5.4, the SKR calculation is derived for the HBF OFDM/OTFS based LDPC assisted CV-QKD systems in THz transmission. Our performance analysis was conducted in Section 5.6 in terms of the BLER versus SNR and SKR versus distance. Firstly, it was demonstrated in Fig. 5.11 that the OFDM FD-SVD based CV-QKD system having perfect CSI achieves comparable BLER performance to the OTFS DD-SVD based system even in mobile ($v = 30$ mph)

scenarios, since the beamforming gain obtained via MIMO setting can effectively bridge the gap between OTFS and OFDM observed in a SISO case, provided that perfect CSI is available at both the transmitter and receiver. Secondly, it was demonstrated in Fig. 5.12 that the BLER performance is improved upon increasing the MIMO size, thanks to the improved beamforming gain achieved by the MIMO OFDM/OTFS scheme proposed for quantum transmission. Thirdly, an SKR versus distance performance comparison was conducted, which is summarized in Table 5.4. It was demonstrated in Fig. 5.13 that the OTFS-based system associated with frame-based CP overhead offers higher SKR and longer secure transmission distance compared to the OFDM-based system in both stationary and mobile ($v = 30$ mph) scenarios. Moreover, increasing the MIMO size can enhance the secure transmission distance for both the OFDM- and OTFS-based systems. Lastly, the effect of channel estimation on the OFDM- and OTFS-based systems was investigated. It was demonstrated in Fig. 5.14 and Fig. 5.15 that the OTFS system with estimated CSI performs closely to that with perfect CSI in both stationary and mobile scenarios. Therefore, the same reconciliation efficiencies and SKR vs. distance can be achieved for OTFS based system with estimated CSI as that with perfect CSI. However, the OFDM-based system with estimated CSI cannot achieve adequate SKR and secure distance for CV-QKD in mobile cases due to the high BLER.

6.2 Future work

In this section, we will briefly discuss a range of potential future research directions.

6.2.1 HARQ-based CV-QKD Systems Design

Table 6.1: Potential novel contributions of this potential work in comparison to the state-of-the-art schemes.

Contributions	**Potential work**	[169, 170]	[171]	[172]	[173, 174]	[175, 176]	[177]
DV-QKD		✓	✓	✓		✓	✓
CV-QKD	✓				✓		
ARQ retransmission					✓		
Blind reconciliation (BR)		✓	✓	✓		✓	✓
Symmetric BR			✓				
Asymmetric BR		✓		✓		✓	✓
HARQ	✓						
LDPC codes-based	✓	✓	✓			✓	✓
Polar codes-based				✓			✓
Adaptive step sizes	✓					✓	✓
FSO					✓		
THz	✓						
Codeword based reconciliation scheme	✓						

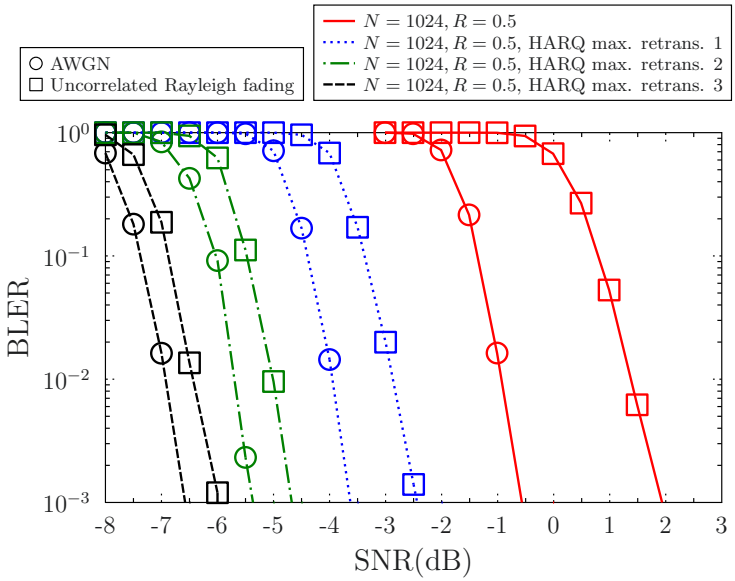


Figure 6.1: BLER performance comparison with Type I HARQ with CCB in classical communication associated with different channels. Three different maximum numbers of retransmission are set, which are 1, 2 and 3, respectively.

As demonstrated in Fig. 4.9 of Chapter 4, the BLER performance is improved upon increasing of the block length. However, the delay will be increased with larger block length, especially when an ARQ mechanism is adopted for retransmissions, when the decoding fails. On the other hand, shorter block length can provide lower delay at the cost of BLER performance degradation. Therefore, it is worthwhile exploiting Hybrid ARQ (HARQ) techniques to provide a better BLER performance while keeping the delay to an acceptable level. Table 6.1 summarizes the research related to ARQ and Blind Reconciliation (BR) found in the open literature. Furthermore, to incorporate the classical HARQ technique into our proposed codeword based reconciliation scheme of Chapter 3, some potential novel contributions for this piece of future work are also listed in Table 6.1. In light of this, some initial results in terms of the BLER performance are portrayed in Fig. 6.1 for Type I HARQ along with Chase Combining (CCB) . As seen in Fig. 6.1, the BLER performance can be improved by the application of Type I HARQ combined with CCB. Furthermore,upon increasing the number of retransmissions, HARQ with CCB offers a notable improvement due the diversity gain provided by the CCB technique. However, both the effective transmission rate and delay have to be taken into account. Therefore, it is worthwhile investigating other more advanced HARQ schemes.

6.2.2 RIS-assisted OTFS CV-QKD Systems

Reconfigurable Intelligent Surfaces (RIS) have drawn considerable attention as a benefit of enhancing the performance of future wireless communication systems [178, 179].

Some recent contributions have also investigated the application of optical RISs in order to relax the LoS requirement for classical FSO communication systems harnessed for high data rate communication in urban environments [180, 181]. Furthermore, RIS techniques have also been studied in quantum communications, especially in CV-QKD systems [182–187]. To elaborate further, an RIS-assisted NLoS FSO quantum communication system that can be used for both DV-QKD and CV-QKD protocols even if the LoS link is blocked was studied in [182], and the achievable SKR for both protocols has been characterized. To accurately characterize the optical beam propagation, an analytical channel model based on extended Huygens-Fresnel principles for representing both the atmospheric turbulence effects and the hovering fluctuation of low-altitude platforms was developed in [183]. Furthermore, [184] derived a novel model of the quantum noise and losses experienced by quantum states for transmission over FSO channels, where the joint optimization of entanglement distribution and RIS placement problem is formulated and solved. Apart from the RIS-assisted CV-QKD systems used in FSO channels, RIS-assisted CV-QKD systems operating in THz channels have also been investigated [185, 186], where eavesdropping is considered both in the direct Alice to Bob channel, the channel between Alice and the RIS, and between the RIS and Bob. Moreover, the limited quantum memory effect has been taken into account, as well as the effect of channel estimation [186]. In light of this, it is feasible to conceive a RIS-assisted OTFS based CV-QKD system in THz scenarios, where both blockage and high-mobility are considered.

6.2.3 Near-field THz CV-QKD Systems

In classic performance evaluation it is typically assumed that the receiver is exposed to far-field propagation in form of plane waves. By contrast, in the near-field spherical propagation takes place. Hence, near-field THz propagation modelling has been investigated in [188, 189]. Since the corresponding Rayleigh distance grows with the array size, as well as with the reduction of the wavelength, this has been investigated in [190, 191]. Therefore, it is worthwhile considering near-field THz CV-QKD systems, since the transmission distance is limited in the THz bands.

Bibliography

[1] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang *et al.*, "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Science China Information Sciences*, vol. 64, no. 1, pp. 1–74, 2021.

[2] 3GPP. [Online]. Available: https://www.3gpp.org

[3] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1853–1888, 2012.

[4] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum search algorithms for wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1209–1242, 2019.

[5] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design," *IEEE Access*, vol. 1, pp. 94–122, 2013.

[6] D. Maslov, Y. Nam, and J. Kim, "An outlook for quantum computing [point of view]," *Proceedings of the IEEE*, vol. 107, no. 1, pp. 5–10, 2019.

[7] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 126–132, 2020.

[8] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021.

[9] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks," *IBM Journal of Research and Development*, vol. 38, no. 3, pp. 243–250, 1994.

[10] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback, "Report on the development of the advanced encryption standard (AES)," *Journal of Research of the National Institute of Standards and Technology*, vol. 106, no. 3, p. 511, 2001.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[12] M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[13] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the Theory and Application of Cryptographic Techniques*. Springer, 1985, pp. 417–426.

[14] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[15] H. Mani, "Error reconciliation protocols for continuous-variable quantum key distribution," *Ph.D dissertation, Technical University of Denmark*, 2021.

[16] R. A. Mollin, *An introduction to cryptography*. CRC Press, 2000.

[17] D. Pan, K. Li, D. Ruan, S. X. Ng, and L. Hanzo, "Single-photon-memory two-step quantum secure direct communication relying on einstein-podolsky-rosen pairs," *IEEE Access*, vol. 8, pp. 121 146–121 161, 2020.

[18] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings of the 35th IEEE Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

[19] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219.

[20] ——, "Quantum mechanics helps in searching for a needle in a haystack," *Physical review letters*, vol. 79, no. 2, pp. 325–328, 1997.

[21] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 881–919, 2019.

[22] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 281–291, 2020.

[23] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the Qinternet," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.

[24] Z. Wang, R. Malaney, and J. Green, "Inter-satellite quantum key distribution at Terahertz frequencies," in *Proceedings of IEEE International Conference on Communications (ICC)*, 2019, pp. 1–7.

[25] S. P. Kish, E. Villaseñor, R. Malaney, K. A. Mudge, and K. J. Grant, "Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-earth channel," *Quantum Engineering*, vol. 2, no. 3, p. e50, 2020.

[26] M. Fujiwara, R. Nojima, T. Tsurumaru, S. Moriai, M. Takeoka, and M. Sasaki, "Long-term secure distributed storage using quantum key distribution network with third-party verification," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–11, 2022.

[27] A. Stanco, F. B. L. Santagiustina, L. Calderaro, M. Avesani, T. Bertapelle, D. Dequal, G. Vallone, and P. Villoresi, "Versatile and concurrent FPGA-based architecture for practical quantum communication systems," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–8, 2022.

[28] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[29] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[30] W. Grice, M. Olama, A. Lee, and P. G. Evans, "Quantum key distribution applicability to smart grid cybersecurity systems," *IEEE Access*, vol. 13, pp. 17 398–17 413, 2025.

[31] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Dec 1984, pp. 175–179.

[32] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

[33] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Physical Review Letters*, vol. 68, no. 5, pp. 557–559, 1992.

[34] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, pp. 3121–3124, 1992.

[35] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, no. 14, pp. 3018–3021, 1998.

[36] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, 2003, Article no. 057901.

[37] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical Review Letters*, vol. 92, no. 5, 2004, Article no. 057901.

[38] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, 2018.

[39] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Physical Review X*, vol. 8, p. 031043, Aug 2018.

[40] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical Review Letters*, vol. 88, no. 5, 2002, Article no. 057902.

[41] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, . f. T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Physical Review Letters*, vol. 93, no. 17, p. 170504, 2004.

[42] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Physical Review Letters*, vol. 102, May 2009, Article no. 180504.

[43] Y. Bian, Y.-C. Zhang, C. Zhou, S. Yu, Z. Li, and H. Guo, "High-rate point-to-multipoint quantum key distribution using coherent states," *arXiv preprint arXiv:2302.02391*, 2023.

[44] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[45] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, no. 2, 2020, Article no. 025002.

[46] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2014.

[47] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: principle, security and implementations," *Entropy*, vol. 17, no. 9, pp. 6072–6092, 2015.

[48] H. Ge, A. Tomita, A. Okamoto, and K. Ogawa, "Analysis of the effects of the two-photon temporal distinguishability on measurement-device-independent quantum key distribution," *IEEE Transactions on Quantum Engineering*, vol. 4, pp. 1–8, 2023.

[49] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future," *Applied Physics Reviews*, vol. 11, no. 1, 2024.

[50] K. Sulimany, G. Pelc, R. Dudkiewicz, S. Korenblit, H. S. Eisenberg, Y. Bromberg, and M. Ben-Or, "High-dimensional coherent one-way quantum key distribution," *NPJ Quantum Information*, vol. 11, no. 1, p. 16, 2025.

[51] H. Yu, S. Sciara, M. Chemnitz, N. Montaut, B. Crockett, B. Fischer, R. Helsten, B. Wetzel, T. A. Goebel, R. G. Krämer *et al.*, "Quantum key distribution implemented with d-level time-bin entangled photons," *Nature Communications*, vol. 16, no. 1, p. 171, 2025.

[52] C. Bennett, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore*, 1984, pp. 175–179.

[53] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, no. 13, 2012, Article no. 130503.

[54] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Reviews of Modern Physics*, vol. 84, no. 2, pp. 621–669, 2012.

[55] Y.-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution using squeezed states," *Physical Review A*, vol. 90, no. 5, p. 052325, 2014.

[56] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, 2003.

[57] M. Navascués, F. Grosshans, and A. Acin, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," *Physical Review Letters*, vol. 97, no. 19, 2006, Article no. 190502.

[58] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 81, no. 6, 2010, Article no. 062343.

[59] F. Laudenbach, C. Pacher, C. H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with gaussian modulation—The theory of practical implementations," *Advanced Quantum Technologies*, vol. 1, no. 1, pp. 1–37, 2018.

[60] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[61] K. Zhang, X.-Q. Jiang, Y. Feng, R. Qiu, and E. Bai, "High efficiency continuous-variable quantum key distribution based on quasi-cyclic LDPC codes," in *Proceedings of the 5th IEEE International Conference on Communication, Image and Signal Processing (CCISP)*, 2020, pp. 38–42.

[62] Y. Guo, X. Wang, C. Xie, and D. Huang, "Free-space continuous-variable quantum key distribution in atmospheric channels based on low-density parity-check codes," *Laser Physics Letters*, vol. 17, no. 4, 2020, Article no. 045203.

[63] M. Shirvanimoghaddam, S. J. Johnson, and A. M. Lance, "Design of raptor codes in the low SNR regime with applications in quantum key distribution," in *Proceedings of the IEEE International Conference on Communications (ICC)*. IEEE, 2016, pp. 1–6.

[64] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Key reconciliation with low-density parity-check codes for long-distance quantum cryptography," *arXiv preprint arXiv:1702.07740*, 2017.

[65] ——, "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography," *NPJ Quantum Information*, vol. 4, no. 1, 2018.

[66] K. Gümüş, T. A. Eriksson, M. Takeoka, M. Fujiwara, M. Sasaki, L. Schmalen, and A. Alvarado, "A novel error correction protocol for continuous variable quantum key distribution," *Scientific reports*, vol. 11, no. 1, p. 10465, 2021.

[67] X. Wen, Q. Li, H. Mao, X. Wen, and N. Chen, "Rotation based slice error correction protocol for continuous-variable quantum key distribution and its implementation with polar codes," *arXiv preprint arXiv:2106.06206*, 2021.

[68] B.-Y. Tang, C.-Q. Wu, W. Peng, B. Liu, and W.-R. Yu, "Polar-code-based information reconciliation scheme with the frozen-bit erasure strategy for quantum key distribution," *Physical Review A*, vol. 107, no. 1, 2023, Article no. 012612.

[69] W. Zhao, Y. Guo, D. Huang, and L. Zhang, "Continuous-variable quantum key distribution with orthogonal frequency division multiplexing modulation," *International Journal of Theoretical Physics*, vol. 57, no. 10, pp. 2956–2967, 2018.

[70] Y. Kim, C. Suh, and J.-K. K. Rhee, "Reconciliation with polar codes constructed using Gaussian approximation for long-distance continuous-variable quantum key distribution," in *Proceedings of the IEEE International Conference on Information and Communication Technology Convergence (ICTC)*, 2017, pp. 301–306.

[71] C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, and H. Guo, "Continuous-variable quantum key distribution with rateless reconciliation protocol," *Phys. Rev. Appl.*, vol. 12, no. 5, 2019, Article no. 054013.

[72] M. B. Asfaw, X. Q. Jiang, M. Zhang, J. Hou, and W. Duan, "Performance analysis of raptor code for reconciliation in continuous variable quantum key distribution." IEEE, 2019, pp. 463–467.

[73] M. Zhang, H. Hai, Y. Feng, and X.-Q. Jiang, "Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution," *Quantum Information Processing*, vol. 20, no. 10, pp. 1–17, 2021.

[74] C. Zhou, X. Y. Wang, Z. G. Zhang, S. Yu, Z. Y. Chen, and H. Guo, "Rate compatible reconciliation for continuous-variable quantum key distribution using Raptor-like LDPC codes," *Science China Physics, Mechanics & Astronomy*, vol. 64, no. 6, 2021, Article no. 260311.

[75] M. Zhang, Y. Dou, Y. Huang, X. Q. Jiang, and Y. Feng, "Improved information reconciliation with systematic polar codes for continuous variable quantum key distribution," *Quantum Information Processing*, vol. 20, no. 10, pp. 1–16, 2021.

[76] X. Ai and R. Malaney, "Optimised multithreaded CV-QKD reconciliation for global quantum networks," *IEEE Transactions on Communications*, vol. 70, no. 9, pp. 6122–6132, 2022.

[77] H. Sarieddeen, M.-S. Alouini, and T. Y. Al-Naffouri, "An overview of signal processing techniques for Terahertz communications," *Proceedings of the IEEE*, vol. 109, no. 10, pp. 1628–1665, 2021.

[78] H. Chen, H. Sarieddeen, T. Ballal, H. Wymeersch, M.-S. Alouini, and T. Y. Al-Naffouri, "A tutorial on Terahertz-band localization for 6G communication systems," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1780–1815, 2022.

[79] C. Ottaviani, M. J. Woolley, M. Erementchouk, J. F. Federici, P. Mazumder, S. Pirandola, and C. Weedbrook, "Terahertz quantum cryptography," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 3, pp. 483–495, 2020.

[80] Y. He, Y. Mao, D. Huang, Q. Liao, and Y. Guo, "Indoor channel modeling for continuous variable quantum key distribution in the Terahertz band," *Optics Express*, vol. 28, no. 22, pp. 32 386–32 402, 2020.

[81] X. Liu, C. Zhu, N. Chen, and C. Pei, "Practical aspects of Terahertz wireless quantum key distribution in indoor environments," *Quantum Information Processing*, vol. 17, no. 11, pp. 1–20, 2018.

[82] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Physical Review Letters*, vol. 105, no. 11, pp. 1–8, 2010.

[83] N. K. Kundu, S. P. Dash, M. R. McKay, and R. K. Mallik, "MIMO Terahertz quantum key distribution," *IEEE Communications Letters*, vol. 25, no. 10, pp. 3345–3349, 2021.

[84] N. K. Kundu, S. P. Dash, M. R. Mckay, and R. K. Mallik, "Channel estimation and secret key rate analysis of MIMO Terahertz quantum key distribution," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3350–3363, 2022.

[85] N. K. Kundu, M. R. McKay, A. Conti, R. K. Mallik, and M. Z. Win, "MIMO Terahertz quantum key distribution under restricted eavesdropping," *IEEE Transactions on Quantum Engineering*, vol. 4, pp. 1–15, 2023.

[86] M. Zhang, S. Pirandola, and K. Delfanazari, "Millimeter-waves to Terahertz SISO and MIMO continuous variable quantum key distribution," *IEEE Transactions on Quantum Engineering*, vol. 4, pp. 1–10, 2023.

[87] M. Gabay and S. Arnon, "Quantum key distribution by a free-space MIMO system," *Journal of Lightwave Technology*, vol. 24, no. 8, pp. 3114–3120, 2006.

[88] R. Jaentti, R. Di Candia, R. Duan, and K. Ruttik, "Multiantenna Quantum Backscatter Communications," *in Proceedings of IEEE Globecom Workshops (GC Wkshps), 2017*, vol. 2018-Janua, pp. 1–6, 2017.

[89] M. Lanzagorta and J. Uhlmann, "Virtual modes for quantum illumination." IEEE, 2018, pp. 1–4.

[90] L. Gyongyosi and S. Imre, "Adaptive multicarrier quadrature division modulation for long-distance continuous-variable quantum key distribution," *Quantum Information and Computation XII*, vol. 9123, no. May 2014, pp. 52–66, 2014.

[91] S. Bahrani, M. Razavi, and J. A. Salehi, "Orthogonal frequency-division multiplexed quantum key distribution," *Journal of Lightwave Technology*, vol. 33, no. 23, pp. 4687–4698, 2015.

[92] L. Gyongyosi, "Diversity extraction for multicarrier continuous-variable quantum key distribution," in *24th European Signal Processing Conference (EUSIPCO)*. EURASIP, 2016, pp. 478–482.

[93] H. Zhang, Y. Mao, D. Huang, J. Li, L. Zhang, and Y. Guo, "Security analysis of orthogonal-frequency-division-multiplexing-based continuous-variable quantum key distribution with imperfect modulation," *Physical Review A*, vol. 97, no. 5, pp. 1–9, 2018.

[94] W. Zhao, Q. Liao, D. Huang, and Y. Guo, "Performance analysis of the satellite-to-ground continuous-variable quantum key distribution with orthogonal frequency division multiplexed modulation," *Quantum Information Processing*, vol. 18, no. 1, pp. 1–22, 2019.

[95] L. Gyongyosi, "Singular value decomposition assisted multicarrier continuous-variable quantum key distribution," *Theoretical Computer Science*, vol. 801, pp. 35–63, 2020.

[96] C. Liu, C. Zhu, X. Liu, M. Nie, H. Yang, and C. Pei, "Multicarrier multiplexing continuous-variable quantum key distribution at Terahertz bands under indoor environment and in inter-satellite links communication," *IEEE Photonics Journal*, vol. 13, no. 4, pp. 1–13, 2021.

[97] H. Wang, Y. Pan, Y. Shao, Y. Pi, T. Ye, Y. Li, T. Zhang, J. Liu, J. Yang, L. Ma, W. Huang, and B. Xu, "Performance analysis for OFDM-based multi-carrier continuous-variable quantum key distribution with an arbitrary modulation protocol," *Optics Express*, vol. 31, no. 4, p. 5577, 2023.

[98] L. Gyongyosi and S. Imre, "Secret key rates of free-space optical continuous-variable quantum key distribution," *International Journal of Communication Systems*, vol. 32, no. 18, 2019.

[99] Y.-J. Lin and M. Jarrahi, "Heterodyne Terahertz detection through electronic and optoelectronic mixers," *Reports on Progress in Physics*, vol. 83, no. 6, 2020, Art. no. 066101.

[100] K. Ikamas, D. B. But, and A. Lisauskas, "Homodyne spectroscopy with broadband Terahertz power detector based on 90-nm silicon cmos transistor," *Applied Sciences*, vol. 11, no. 1, p. 412, 2021.

[101] R. Cattaneo, E. A. Borodianskyi, A. A. Kalenyuk, and V. M. Krasnov, "Superconducting Terahertz sources with 12% power efficiency," *Physical Review Applied*, vol. 16, no. 6, 2021, Article no. L061001.

[102] J. R. Rain, P. Cai, A. Baekey, M. A. Reinhard, R. I. Vasquez, A. C. Silverman, C. L. Cain, and R. A. Klemm, "Wave functions for high-symmetry, thin microstrip antennas, and two-dimensional quantum boxes," *Physical Review A*, vol. 104, no. 6, p. 062205, 2021.

[103] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature communications*, vol. 8, no. 1, 2017, Article no. 15043.

[104] L. Hanzo, O. Alamri, M. El-Hajjar, and N. Wu, *Near-capacity multi-functional MIMO systems: Sphere-packing, iterative detection and cooperation*. John Wiley & Sons, 2009.

[105] X. Liu, C. Xu, Y. Noori, S. X. Ng, and L. Hanzo, "The road to near-capacity CV-QKD reconciliation: An FEC-agnostic design," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 2089–2112, 2024.

[106] R. Tanner, "A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 533–547, 1981.

[107] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman, "Efficient erasure correcting codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 569–584, 2001.

[108] W. Ryan and S. Lin, *Channel codes: Classical and modern*. Cambridge University Press, 2009.

[109] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Transactions on Information Theory*, vol. 47, pp. 498–519, 2001.

[110] X. Ai, R. Malaney, and S. X. Ng, "Quantum key reconciliation for satellite-based communications," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.

[111] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," *Physical Review A — Atomic, Molecular, and Optical Physics*, vol. 86, no. 2, 2012, Article no. 022318.

[112] R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," *Physical Review Letters*, vol. 97, no. 19, pp. 1–4, 2006.

[113] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," *arXiv preprint quant-ph/0306141*, 2003.

[114] C. Fabre and N. Treps, "Modes and states in quantum optics," *Reviews of Modern Physics*, vol. 92, no. 3, p. 035005, 2020.

[115] D. A. Miller, "Waves, modes, communications, and optics: a tutorial," *Advances in Optics and Photonics*, vol. 11, no. 3, pp. 679–825, 2019.

[116] R. Dändliker, "The concept of modes in optics and photonics," in *Education and Training in Optics and Photonics*. Optica Publishing Group, 1999, p. GP193.

[117] *Color figures from Rappaport et al ., Millimeter Wave Wireless*.

[118] N. K. Kundu, M. R. McKay, and R. K. Mallik, "Wireless quantum key distribution at terahertz frequencies: Opportunities and challenges," *IET Quantum Communication*, 2024.

[119] U. Leonhardt, "Quantum physics of simple optical instruments," *Reports on Progress in Physics*, vol. 66, no. 7, p. 1207, 2003.

[120] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Physical Review Letters*, vol. 105, p. 110501, Sep 2010.

[121] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 77, no. 4, 2008, Articel no. 042325.

[122] R. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, 1962.

[123] M. P. Fossorier, M. Mihaljevic, and H. Imai, "Reduced complexity iterative decoding of low-density parity check codes based on belief propagation," *IEEE Transactions on Communications*, vol. 47, no. 5, pp. 673–680, 1999.

[124] M. Baldi, G. Cancellieri, A. Carassai, and F. Chiaraluce, "LDPC codes based on serially concatenated multiple parity-check codes," *IEEE Communications Letters*, vol. 13, no. 2, pp. 142–144, 2009.

[125] S. Shao, P. Hailes, T. Y. Wang, J. Y. Wu, R. G. Maunder, B. M. Al-Hashimi, and L. Hanzo, "Survey of Turbo, LDPC, and Polar Decoder ASIC Implementations," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2309–2333, 2019.

[126] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Problemy Peredachi Informatsii*, vol. 9, no. 3, pp. 3–11, 1973.

[127] A. S. Holevo, M. Sohma, and O. Hirota, "Capacity of quantum Gaussian channels," *Physical Review A*, vol. 59, no. 3, pp. 1820–1828, 1999.

[128] T. Richardson and R. Urbanke, *Modern coding theory*. Cambridge University Press, 2008.

[129] R. Steele and L. Hanzo, *Mobile radio communications: Second and third generation cellular and WATM systems: 2nd*. IEEE Press-John Wiley, 1999.

[130] C. Liu, C. Zhu, X. Liu, M. Nie, H. Yang, and C. Pei, "Multicarrier multiplexing continuous-variable quantum key distribution at Terahertz bands under indoor environment and in inter-satellite links communication," *IEEE Photonics Journal*, vol. 13, no. 4, pp. 1–13, 2021.

[131] International Telecommunication Union, "Attenuation by atmospheric gases," ITU Radiocommunication Sector, Geneva, Switzerland, Tech. Rep. Recommendation ITU-R P.676-10, Sept. 2013.

[132] R. ITU-RP.676-10, "Attenuation by atmospheric gases and related effects," *International Telecommunication Union, Geneva, Switzerland*, Sep 2013. [Online]. Available: https://www.itu.int/rec/R-REC-P.676

[133] C. Han and Y. Chen, "Propagation modeling for wireless communications in the Terahertz band," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 96–101, 2018.

[134] C. Lin and G. Y. Li, "Antenna subarray partitioning with interference cancellation for multi-user indoor terahertz communications," in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2015, pp. 1–6.

[135] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, 2018.

[136] K. Guan, D. He, B. Ai, Y. Chen, C. Han, B. Peng, Z. Zhong, and T. Kuerner, "Channel characterization and capacity analysis for THz communication enabled smart rail mobility," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4065–4080, 2021.

[137] H. Mani, T. Gehring, P. Grabenweger, B. Ömer, C. Pacher, and U. L. Andersen, "Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution," *Physical Review A*, vol. 103, p. 062419, Jun 2021.

[138] M. Bloch, A. Thangaraj, and S. W. McLaughlin, "Efficient reconciliation of correlated continuous random variables using LDPC codes," *arXiv preprint cs/0509041*, 2005.

[139] Z. Cao, X. Chen, G. Chai, K. Liang, and Y. Yuan, "Rate-adaptive polar-coding-based reconciliation for continuous-variable quantum key distribution at low signal-to-noise ratio," *Physical Review Applied*, vol. 19, 2023, Article no. 044023.

[140] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Physical Review A*, vol. 76, no. 4, 2007, Article no. 042305.

[141] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a gaussian modulation," *Physical Review A*, vol. 84, no. 6, p. 062317, 2011.

[142] C. Xu, P. Zhang, R. Rajashekar, N. Ishikawa, S. Sugiura, Z. Wang, and L. Hanzo, ""Near-perfect" finite-cardinality generalized space-time shift keying," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 9, pp. 2146–2164, 2019.

[143] C. Xu, N. Ishikawa, R. Rajashekar, S. Sugiura, R. G. Maunder, Z. Wang, L.-L. Yang, and L. Hanzo, "Sixty years of coherent versus non-coherent tradeoffs and

the road from 5G to wireless futures," *IEEE Access*, vol. 7, pp. 178 246–178 299, 2019.

[144] V. K. Ralegankar, J. Bagul, B. Thakkar, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, "Quantum cryptography-as-a-service for secure UAV communication: Applications, challenges, and case study," *IEEE Access*, vol. 10, pp. 1475–1492, 2022.

[145] N. Alshaer, A. Moawad, and T. Ismail, "Reliability and security analysis of an entanglement-based QKD protocol in a dynamic Ground-to-UAV FSO communications system," *IEEE Access*, vol. 9, pp. 168 052–168 067, 2021.

[146] M. Wang, Z. Yan, and V. Niemi, "UAKA-D2D: Universal authentication and key agreement protocol in D2D communications," *Mobile networks and Applications*, vol. 22, pp. 510–525, 2017.

[147] M. Wang and Z. Yan, "Security in D2D communications: A review," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 1199–1204.

[148] R. G. Maunder and L. Hanzo, "Near-capacity irregular variable length coding and irregular unity rate coding," *IEEE Transactions on Wireless Communications*, vol. 8, no. 11, pp. 5500–5507, 2009.

[149] N. Wu and L. Hanzo, "Near-capacity irregular-convolutional-coding-aided irregular precoded linear dispersion codes," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 6, pp. 2863–2871, 2009.

[150] M. El-Hajjar and L. Hanzo, "EXIT charts for system design and analysis," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 127–153, 2013.

[151] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Transactions on Communications*, vol. 49, no. 10, pp. 1727–1737, 2001.

[152] C. Xu, S. Sugiura, S. X. Ng, P. Zhang, L. Wang, and L. Hanzo, "Two decades of MIMO design tradeoffs and reduced-complexity MIMO detection in near-capacity systems," *IEEE Access*, vol. 5, pp. 18 564–18 632, 2017.

[153] S. X. Ng and L. Hanzo, "On the MIMO channel capacity of multidimensional signal sets," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 2, pp. 528–536, 2006.

[154] R. Hadani, S. Rakib, M. Tsatsanis, A. Monk, A. J. Goldsmith, A. F. Molisch, and R. Calderbank, "Orthogonal time frequency space modulation," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, 2017, pp. 1–6.

[155] Z. Wei, W. Yuan, S. Li, J. Yuan, G. Bharatula, R. Hadani, and L. Hanzo, "Orthogonal time-frequency space modulation: A promising next-generation waveform," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 136–144, 2021.

[156] S. K. Mohammed, "Derivation of OTFS modulation from first principles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 7619–7636, 2021.

[157] C. Xu, X. Zhang, P. Petropoulos, S. Sugiura, R. G. Maunder, L.-L. Yang, Z. Wang, J. Yuan, H. Haas, and L. Hanzo, "Optical OTFS is capable of improving the bandwidth-, power- and energy-efficiency of optical OFDM," *IEEE Transactions on Communications*, vol. 72, no. 2, pp. 938–953, 2024.

[158] C. Xu, L. Xiang, J. An, C. Dong, S. Sugiura, R. G. Maunder, L.-L. Yang, and L. Hanzo, "OTFS-aided RIS-assisted SAGIN systems outperform their OFDM counterparts in doubly selective high-doppler scenarios," *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 682–703, 2023.

[159] C. Xu, L. Xiang, S. Sugiura, R. G. Maunder, L.-L. Yang, D. Niyato, G. Y. Li, R. Schober, and L. Hanzo, "Noncoherent orthogonal time frequency space modulation," *IEEE Transactions on Wireless Communications*, vol. 23, no. 8, pp. 10 072–10 090, 2024.

[160] Z. Cao, X. Chen, G. Chai, K. Liang, and Y. Yuan, "Rate-adaptive polar-coding-based reconciliation for continuous-variable quantum key distribution at low signal-to-noise ratio," *Physical Review Applied*, vol. 19, no. 4, 2023, Article no. 044023.

[161] G. Surabhi and A. Chockalingam, "Low-complexity linear equalization for OTFS modulation," *IEEE communications letters*, vol. 24, no. 2, pp. 330–334, 2019.

[162] B. Ning, Z. Tian, W. Mei, Z. Chen, C. Han, S. Li, J. Yuan, and R. Zhang, "Beamforming technologies for ultra-massive MIMO in Terahertz communications," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 614–658, 2023.

[163] J. Tan and L. Dai, "Wideband channel estimation for THz massive MIMO," *China Communications*, vol. 18, no. 5, pp. 66–80, 2021.

[164] X. Liu, C. Xu, S. X. Ng, and L. Hanzo, "OTFS-based CV-QKD systems for doubly selective THz channels," *IEEE Transactions on Communications*, 2025, accepted.

[165] G. H. Golub and C. Reinsch, "Singular value decomposition and least squares solutions," in *Handbook for Automatic Computation: Volume II: Linear Algebra*. Springer, 1971, pp. 134–151.

[166] E. Angerson, Z. Bai, J. Dongarra, A. Greenbaum, A. McKenney, J. Du Croz, S. Hammarling, J. Demmel, C. Bischof, and D. Sorensen, "LAPACK: A portable linear algebra library for high-performance computers," in *Proceedings of the 1990 ACM/IEEE Conference on Supercomputing*, 1990, pp. 2–11.

[167] T. Peken, S. Adiga, R. Tandon, and T. Bose, "Deep learning for SVD and hybrid beamforming," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, pp. 6621–6642, 2020.

[168] C. Xu, L. Xiang, J. An, C. Dong, S. Sugiura, R. G. Maunder, L.-L. Yang, and L. Hanzo, "OTFS-aided RIS-assisted SAGIN systems outperform their OFDM counterparts in doubly selective high-doppler scenarios," *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 682–703, 2022.

[169] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Blind reconciliation," *Quantum Information and Computation*, vol. 12, no. 9-10, pp. 791–812, 2012.

[170] ——, "Key reconciliation for high performance quantum key distribution," *Scientific Reports*, vol. 3, pp. 3–8, 2013.

[171] E. O. Kiktenko, A. S. Trushechkin, C. C. Lim, Y. V. Kurochkin, and A. K. Fedorov, "Symmetric Blind Information Reconciliation for Quantum Key Distribution," *Physical Review Applied*, vol. 8, no. 4, pp. 1–12, 2017.

[172] E. O. Kiktenko, A. O. Malyshev, and A. K. Fedorov, "Blind Information Reconciliation With Polar Codes for Quantum Key Distribution," *IEEE Communications Letters*, vol. 25, no. 1, pp. 79–83, 2020.

[173] N. D. Nguyen, H. T. T. Pham, V. V. Mai, and N. T. Dang, "Comprehensive performance analysis of satellite-to-ground FSO/QKD systems using key retransmission," *Optical Engineering*, vol. 59, no. 12, pp. 1–25, 2020.

[174] N. D. Nguyen, H. T. Phan, H. T. Pham, V. V. Mai, and N. T. Dang, "Reliability improvement of satellite-based quantum key distribution systems using retransmission scheme," *Photonic Network Communications*, vol. 42, no. 1, pp. 27–39, 2021.

[175] L. Liu, J. L. Niu, C. R. Fan, X. T. Feng, and C. Wang, "High-dimensional measurement-device-independent quantum secure direct communication," *Quantum Information Processing*, vol. 19, no. 11, pp. 1–5, 2020.

[176] N. Borisov, I. Petrov, and A. Tayduganov, "Asymmetric Adaptive LDPC-Based Information Reconciliation for Industrial Quantum Key Distribution," *Entropy*, vol. 25, no. 1, 2023.

[177] J. Xie, C. Jiang, J. Lin, Z. L. Jiang, J. Wang, and J. Fang, "Blind reconciliation based on inverse encoding of polar codes with adaptive step sizes for quantum key distribution," *Quantum Information Processing*, vol. 21, no. 10, pp. 1–15, 2022.

[178] Z. Chen, B. Ning, C. Han, Z. Tian, and S. Li, "Intelligent reflecting surface assisted Terahertz communications toward 6G," *IEEE Wireless Communications*, vol. 28, no. 6, pp. 110–117, 2021.

[179] M. Di Renzo, A. Zappone, M. Debbah, M.-S. Alouini, C. Yuen, J. De Rosny, and S. Tretyakov, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2450–2525, 2020.

[180] H. Ajam, M. Najafi, V. Jamali, B. Schmauss, and R. Schober, "Modeling and design of IRS-assisted multilink FSO systems," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3333–3349, 2022.

[181] V. Jamali, H. Ajam, M. Najafi, B. Schmauss, R. Schober, and H. V. Poor, "Intelligent reflecting surface assisted free-space optical communications," *IEEE Communications Magazine*, vol. 59, no. 10, pp. 57–63, 2021.

[182] N. K. Kundu, M. R. McKay, R. Murch, and R. K. Mallik, "Intelligent reflecting surface-assisted free space optical quantum communications," *IEEE Transactions on Wireless Communications*, 2023.

[183] P. V. Trinh, S. Sugiura, C. Xu, and L. Hanzo, "Optical RISs improve the secret key rate of free-space QKD in HAP-to-UAV scenarios," *arXiv preprint arXiv:2408.06106*, 2024.

[184] M. Chehimi, M. Elhattab, W. Saad, G. Vardoyan, N. K. Panigrahy, C. Assi, and D. Towsley, "Reconfigurable intelligent surface (RIS)-assisted entanglement distribution in FSO quantum networks," *arXiv preprint arXiv:2401.10823*, 2024.

[185] S. Kumar and S. P. Dash, "RIS-assisted THz MIMO wireless system in the presence of direct link for CV-QKD with limited quantum memory," *arXiv preprint arXiv:2410.16731*, 2024.

[186] S. Kumar, S. P. Dash, D. Ghose, and G. C. Alexandropoulos, "Ris-assisted MIMO CV-QKD at THz frequencies: Channel estimation and SKR analysis," *arXiv preprint arXiv:2412.18771*, 2024.

[187] M. Chehimi, M. Elhattab, W. Saad, G. Vardoyan, N. K. Panigrahy, C. Assi, and D. Towsley, "Reconfigurable intelligent surface (RIS)-assisted entanglement distribution in FSO quantum networks," *IEEE Transactions on Wireless Communications*, 2025.

[188] D. Bodet, V. Petrov, S. Petrushkevich, and J. M. Jornet, "Sub-Terahertz near field channel measurements and analysis with beamforming and Bessel beams," *Scientific Reports*, vol. 14, no. 1, p. 19675, 2024.

[189] V. Petrov, D. Moltchanov, and J. M. Jornet, "Accurate channel model for near field Terahertz communications beyond 6G," in *Proceedings of IEEE 25th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE, 2024, pp. 781–785.

[190] C. Han, Y. Chen, L. Yan, Z. Chen, and L. Dai, "Cross far-and near-field wireless communications in Terahertz ultra-large antenna array systems," *IEEE Wireless Communications*, 2024.

[191] Y. Wang, S. Sun, and C. Han, "Far-and near-field channel measurements and characterization in the Terahertz band using a virtual antenna array," *IEEE Communications Letters*, 2024.