Tetherless THz CV-QKD – Would it Work?

Xin Liu, Nan Wang, Chao Xu, Soon Xin Ng, Phuc V. Trinh, Shinya Sugiura, and Lajos Hanzo

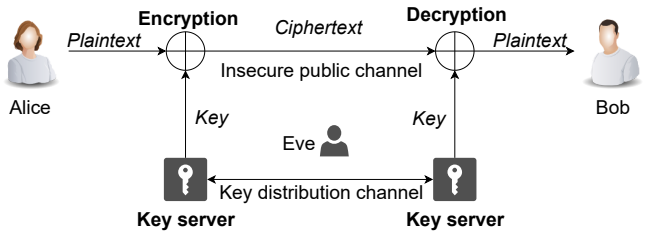
***Abstract*—Quantum key distribution (QKD) provides information-theoretic security by leveraging quantum mechanical principles, while Terahertz (THz) communications offer unprecedented data rates for next-generation networks. We sketch out an evolutionary pathway for bridging these domains by critically appraising THz-based continuous-variable QKD (CV-QKD) systems conceived for wireless environments like space-air-ground integrated networks (SAGINs) and vehicle-to-everything (V2X) scenarios, where time-varying frequency-selective fading poses critical challenges. To address these issues, we elaborate on the feasibility of THz based CV-QKD applications from a wireless perspective. Specifically, we commence by highlighting a typical CV-QKD protocol. Then present three sophisticated CV-QKD system designs. *Firstly*, we propose a codeword-based – rather than syndrome-based – reconciliation scheme capable of accommodating diverse forward error correction (FEC) codes, imposing a similar complexity on the transmitter and receiver. As a further improvement, we demonstrate that powerful irregular convolutional codes (IRCCs) attain a near-capacity performance, thus offering longer secure distance and/or improved secret key rate (SKR). *Secondly*, the secure boundaries derived for the optical and THz band – even down to microwave frequencies – demonstrate the feasibility of short-distance THz CV-QKD systems. Furthermore, multiple-input multiple-output (MIMO) schemes are harnessed for improving the SKR performance. *Thirdly*, an orthogonal time frequency space (OTFS) modem-based CV-QKD system is conceived for time-varying frequency-selective THz fading channels. Finally, we conclude by identifying several promising research directions for CV-QKD systems.**

I. Introduction

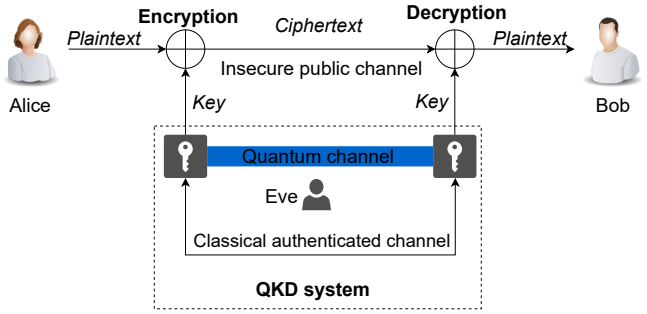
The historical development of cryptography can be traced back to the ancient Rome. One of the earliest and most well-documented encryption techniques, referred to as Caesar's cipher after Julius Caesar, was used for protecting sensitive military and political messages, as described by the Roman historian Suetonius. Specifically, this is a type of monoalphabetic substitution cipher used a shifted standard alphabet. Explicitly, each letter in the message is replaced by another letter via a fixed number of shifts, while the decryption process is the reverse operation, converting the encrypted message back to recover the original message. For example, with a left shift of 3, A would be replaced by D, B would become E, and so on. Although easily broken via brute-force attacks or by a frequency analysis-based attack, it laid the foundation for more sophisticated systems like Vigenere cipher and ultimately modern symmetric-key cryptography. In essence, the

Xin Liu, Nan Wang, Chao Xu, Soon Xin Ng, and Lajos Hanzo are with the School of Electronics and Computer Science, University of Southampton, SO17 1BJ Southampton, U.K. (e-mail: xl4a25@soton.ac.uk; nw1y22@soton.ac.uk; cx1g08@soton.ac.uk; sxn@ecs.soton.ac.uk; lh@soton.ac.uk).

Phuc V. Trinh and Shinya Sugiura are with the Institute of Industrial Science, The University of Tokyo, Tokyo 153-8505, Japan (e-mail: trinh@iis.u-tokyo.ac.jp; sugiura@iis.u-tokyo.ac.jp).



(a)



(b)

Fig. 1: Schematics of different secure communication systems: a) classical cryptosystem, b) QKD-based cryptosystem.

Caesar cipher symbolizes the birth of classical cryptography, bridging ancient secret-keeping practices and the mathematical foundations that define secure communication today.

Modern cryptography began with the standardization of the data encryption standard (DES) in 1977, which was derived from the Lucifer cipher developed by Horst Feistel and IBM in the early 1970s. Today, cryptographic systems are broadly classified into three categories [1], which are symmetric cryptography, asymmetric cryptography and secure hash algorithms, respectively. Albeit 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 computers, they may be endangered by the progress in advanced quantum computing techniques, such as Shor's powerful algorithm and Grover's search algorithm.

As a promising solution, quantum key distribution (QKD) plays a pivotal role in supporting highly secure next-generation (NG) communication. As shown in Fig. 1(a), in classical cryptography the communicating parties Alice and Bob exchange encrypted messages using pre-shared keys transmitted over insecure channels. By contrast, the QKD scheme shown in Fig. 1(b) allows Alice and Bob to generate a shared secret key securely over a quantum channel with some aid of an additional authenticated public channel used for the process of quantum basis comparison, eavesdropping detection and

error correction. Furthermore, the QKD-based cryptosystem is capable of eavesdropping detection based on the no-cloning theorem and Heisenberg's uncertainty principle, hence supporting ultimate information security.

While point-to-point QKD systems initially only supported a few user pairs, the field has witnessed remarkable progress since the first experimental demonstration in the UK (1997). Recently, a sophisticated measurement-device-independent (MDI) quantum network was conceived in Hefei (2016), followed by other continuous variable (CV) quantum networks in Shanghai (2016), Madrid (2018) and Cambridge (2019), as well as by the Bennett-Brassard-Mermin-1992 (BBM92) quantum network in Bristol (2020), etc [2]. Furthermore, apart from the terrestrial quantum network architecture, China's Micius satellite (2016) marked a 'quantum leap' forward in satellite-based quantum communication, establishing four quantum communication ground stations and an experimental quantum teleportation platform in space [3]. Therefore, this technological evolution paves the way for incorporating quantum communications into space-air-ground integrated networks (SAGINs) conceived for NG wireless coverage via integrating satellites, unmanned aerial vehicles, and manned aircraft along with the terrestrial infrastructure, providing a synergistic global quantum Internet alongside classical networks.

In contrast to discrete variable QKD (DV-QKD) regimes, such as the Bennett-Brassard-1984 (BB84) protocol, which map information onto discrete degrees of freedom (e.g., photon polarization or phase), CV-QKD protocols map information onto the quadrature components of electromagnetic fields. Hence CV-QKD may be seamlessly integrated with the existing operational network infrastructure by employing standard off-the-shelf homodyne/heterodyne detectors, eliminating the need for specialized single-photon DV-QKD detectors. As a further benefit, CV-QKD is capable of providing a higher key rate than its DV-QKD counterpart, since both homodyne and heterodyne detectors offer higher detection efficiency than their expensive yet limited-efficiency single-photon DV-QKD counterparts. Additionally, CV-QKD remains the only potentially viable QKD technique below the optical frequency bands. This is because as we progress from optical to THz and microwave frequencies, the photon energy becomes too low for direct single-photon detection. Furthermore, the significantly increasing thermal noise renders DV-QKD impractical due to its inherent sensitivity to noise and detection efficiency requirements.

In addition to optical CV-QKD, the Terahertz (THz) band has emerged as a promising candidate for CV-QKD in NG communication systems, as featured in Table I, offering both abundant bandwidth and enhanced resilience to atmospheric disturbances (e.g., dust, fog, turbulence) compared to free-space optical (FSO) links. Ottaviani *et al.* [4] demonstrated viable secret key rates (SKR) across 1–50 THz, with single-input single-output (SISO) systems achieving practical transmission distances ranging from meters to hundreds of meters at room temperature. Apart from the terrestrial CV-QKD scenarios, the THz band has also been considered for inter-satellite CV-QKD, paving the way for the quantum SAGIN paradigm. However, its performance hinges on a critical tradeoff: the quantum-state preparation thermal noise is reduced at higher THz frequencies (which improves the SKR), but the channel's transmissivity is reduced at higher frequencies (which degrades the SKR). To further boost the secure transmission distance, multiple-input and multiple-output (MIMO) and orthogonal frequency division multiplexing (OFDM) techniques are leveraged in the CV-QKD systems of [5], [6] in order to compensate the degradation caused by the high path-loss of the THz band and to mitigate the detrimental multipath effects of wireless channels, respectively.

While experimental implementations of CV-QKD have predominantly been realized at optical frequencies due to the relative technological maturity of photonic components, recent advances aim for expanding the operational spectrum. Notably, a 5 GHz-microwave-frequency CV-QKD system has been successfully demonstrated, albeit requiring cryogenic cooling conditions. Furthermore, emerging developments in THz device technology might eventually facilitate quantum communications in this band at room-temperature, but significant challenges remain. Recent breakthroughs listed in Table I include superconducting THz sources having enhanced radiation efficiency, improved radio-frequency (RF) quadrature measurements through Rydberg atomic sensors, graphene-based tunable metamaterial THz filters, THz microstrip antennas and plasmonic photoconductive detectors. Although huge challenges persist in optimizing THz sources, modulators, and detectors, these rapid advances hold the promise of supporting practical THz-band CV-QKD systems.

As the most relevant recent surveys, Kundu *et al.* [10] review wireless THz CV-QKD in the microwave-to-THz regime, discussing room-temperature feasibility, the promise of MIMO, and the associated hardware implementation challenges. As a further advance, Ottaviani *et al.* [4] present a tutorial-style feasibility analysis across 0.1–50 THz that quantifies the secure DR/RR regions under realistic thermal noise and molecular absorption conditions. Against this backdrop, in this treatise, we aim for sketching a future wireless pathway for CV-QKD from a wireless THz perspective. Therefore, the main contributions of this article are summarized below:

- **Codeword-based reconciliation:** We propose a generic reconciliation scheme referred to as codeword-based reconciliation scheme, to make the CV-QKD system more compatible with a wide range of forward error correction (FEC) schemes, including convolutional codes (CCs), irregular convolution codes (IRCCs), and low-density parity-check (LDPC) codes, just to name a few.
- **Secure-region characterization across diverse frequency bands:** We evaluate the feasibility of THz based CV-QKD by sketching the secure region via using both direct reconciliation (DR) and reverse reconciliation (RR), respectively.
- **Orthogonal time frequency space (OTFS)-based quantum transmission for time-varying THz channels:** We conceive an OTFS modulation based LDPC-coded reconciliation scheme operating in time-varying frequency-selective THz fading channels, and compare it to its OFDM-based counterpart.

TABLE I: Timeline of important milestones in CV-QKD from optical to THz bands and of device development.

Years	Development of CV-QKD THz	Development of THz Devices
2010	**DR** and **RR** were investigated and the secure region of CV-QKD from infrared to microwave was highlighted [7].	
2012	DR and RR using both homodyne and heterodyne detection were compared. The security of QKD at **various** electromagnetic **wavelengths** was considered.	
2014	**Two-way CV-QKD** at different wavelengths was investigated.	**Graphene-based** tunable metamaterial THz filters.
2016		**Cavity mode** enhancement of THz emission from equilateral triangular microstrip antennas was proposed.
2018	**THz CV-QKD** with Gaussian modulation system using DR and homodyne detection against collect Gaussian attacks [8].	**Plasmonic photoconductive detectors** were used for direct homodyne detection at THz frequencies [8]; **Carbon nanotubes and graphene-based** nano-antennas was proposed for the THz band.
2019	**Inter-satellite** CV-QKD at THz frequencies was analysed.	
2020	**THZ CV-QKD** was shown to be feasible and the SKR against realistic collective attacks was derived [4]. **Indoor channel modeling** for CV-QKD in the THz band was analyzed;	Indirect optical homodyne/heterodyne detectors can be used with the aid of **THz-to-optical converter** [4].
2021	**MIMO THz CV-QKD** was proposed for improving the SKR [5]; **OFDM CV-QKD** in THz band both under indoor environmnet and in inter-satellite links communication was investigated [6].	A **superconducting** THz sources technique was proposed.
2022		**Rydberg atomic** RF sensors were investigated for accurate RF quadrature measurement
2023	CV-QKD based on **simultaneous quantum and classical communication** in the THz band.	
2025	**OTFS-based CV-QKD** was conceived for time-varying frequency-selective THz fading scenarios [9].	**Rydberg atomic quantum receivers** for classical wireless communication and sensing.

- We conclude with a range of open CV-QKD research directions concerning both quantum transmission as well as the classical reconciliation techniques.

II. Typical CV-QKD Protocol

A. Conventional CV-QKD Protocol

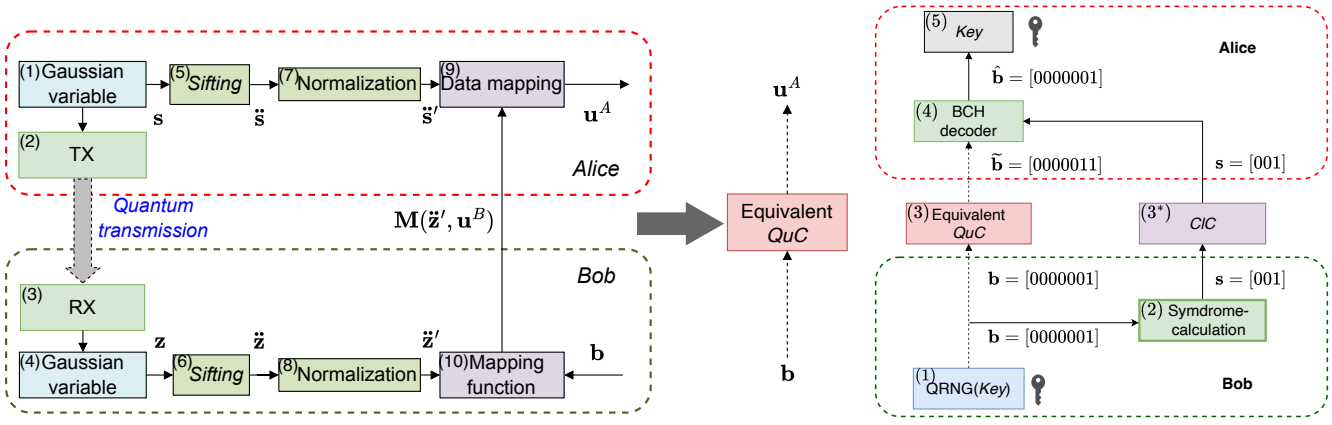
A standard CV-QKD system consists of two fundamental components: (1) quantum transmission stage and (2) the classical post-processing stage, which is mainly constituted by the sifting and reconciliation modules. Their complete functionalities are described as follows:

- ***Quantum transmission***: The quantum transmission phase begins with Alice generating a pair of independent Gaussian distributed random variables (GVs), denoted as $q_A, p_A \sim \mathcal{N}(0, V_s)$, where V_s is the variance of the initial GV. These variables represent the quadrature components of a coherent state $|s\rangle$, having the complex amplitude $s = q_A + jp_A$. Alice prepares and transmits this state through the quantum channel (QuC) (e.g., optical fibre or FSO link). As for eavesdropping modelling, it is assumed that Eve has full control over the QuC, including perfect channel state information. Therefore, Eve may inject some auxiliary signals, coupling them with Alice's signal via a beamsplitter-like interaction, thereby contaminating the QuC [4]. After receiving the corrupted GVs, Bob performs either homodyne or heterodyne detection, measuring to corrupted quadrature variables q'_A, p'_A. These measurements retain Gaussian statistics, but now include Eve's perturbations plus receiver noise.

  As illustrated in Fig. 2(a), Alice prepares the complex random GVs $\mathbf{s}$ of block (1) and maps them to quadratures. Then transmits them via the TX of block (2) through QuCs, which is denoted by the thick dashed-line arrow. Now Bob applies homodyne detection to the received signal in block (3) for obtaining the noise-contaminated decision variables $\mathbf{z}$ at the output of block (4).
- ***Sifting***: The so-called sifting operation is required for homodyne detection in order to ascertain, which specific randomly chosen quadrature of each GV coincides for both Alice and Bob. For example, in GV-based CV-QKD, Bob randomly measures one of the two quadratures, and then obtains either q'_A or p'_A based on a randomly generated bit stream to indicate which quadrature should be measured. Then Bob publicly communicates with Alice through an authenticated classical channel (ClC) to tell her which quadrature is measured for each GV. Hence Alice retains the corresponding quadrature GV at her side, i.e. either q_A or p_A. However, sifting is unnecessary for heterodyne detection, since both the in-phase and quadrature components are needed.

  So in the sifting step of the generic scheme in Fig. 2(a), Alice and Bob synchronize their bases in blocks (5) and (6) for reconciliation processing.
- ***Reconciliation***: The reconciliation process employs two distinct approaches: DR and RR [7].
  - In **DR**, Bob corrects his measured data to match Alice's original transmitted values, while Alice's data remains unchanged.
  - **RR** operates in the opposite direction, with Alice adjusting her data to correspond to Bob's measurements, while Bob's results remain unaltered.

  The key distinction lies in their performance limitations: DR requires a channel transmissivity of $T > 0.5$ to achieve a non-zero SKR, while RR imposes no such threshold. This fundamental difference makes RR the preferred choice in practical implementations, as it enables significantly longer secure transmission distances,



(a) (b)

Fig. 2: (a) Illustration of a generic CV-QKD system, which contains quantum transmission (thick dashed-line arrow) and classical post-processing (thin continuous-line arrows) and (b) the general syndrome-based BCH-coded RR.

particularly in lossy channel conditions where the transmissivity T may fall below 0.5 [7].

Hence, RR is harnessed for reconciliation in Fig. 2(a), where Bob first generates a random bit stream $\mathbf{b}$. Then the modulated binary data $\mathbf{u}^B$ is mapped to the normalized random variables $\ddot{\mathbf{z}}'$ (output of block (8)) using the mapping function[1] $\mathbf{M}(\ddot{\mathbf{z}}', \mathbf{u}^B)$ (output of block (10)) agreed by both Alice and Bob. Alice employs the agreed mapping function $\mathbf{M}(\ddot{\mathbf{z}}', \mathbf{u}^B)$ in block (9) to generate a noisy estimate $\mathbf{u}^A$ of Bob's modulated data based on the output $\ddot{\mathbf{s}}'$ from block (7). In light of this, these processes in blocks (1) to (10) establish an equivalent QuC, whose input is $\mathbf{b}$ and output is $\mathbf{u}^A$. This equivalent QuC that comprises the whole process of quantum transmission, sifting, normalization and mapping operation, is adopted in our analysis for clarity. When the QuC of Fig. 2(a) exhibits only attenuation but no fading (as in fibre-based CV-QKD where path loss can be compensated via power control), the equivalent QuC is adequately modelled by a binary-input additive white Gaussian noise (BI–AWGN) channel [11], [12]. In wireless THz CV-QKD, however, the QuC is subject to more hostile frequency-selective time-varying fading. To retain a tractable reconciliation interface, we compute the mapping function and the log-likelihood ratios (LLRs) using the *post-equalization* SNR. This THz-specific treatment makes the reconciliation directly applicable to wireless THz links, while retaining its FEC-agnostic property, allowing the employment of arbitrary FEC codes.

B. Conventional Syndrome-based Reconciliation

Briefly, the specific instance of Fig. 2(a), namely Fig. 2(b) illustrates a syndrome-based Bose-Chaudhuri-Hocquenghem (BCH)-coded RR example. The complete workflow comprises the following key modules:

- Bob randomly generates a bit stream $\mathbf{b}$ using a quantum random number generator (QRNG), and we view this as the key $\mathbf{b}$ at his side. The length of this is determined by the codeword length of the predefined parity check matrix (PCM), which is known at both sides. Let us consider a simple [7,4,1] BCH code as our rudimentary example, and assume that the bit stream generated by the QRNG in block (1) of Fig. 2(b) is $\mathbf{b} = [0000001]$. Then Bob treats this random bit stream as the key.
- Bob transmits this bit stream $\mathbf{b} = [0000001]$ through a QuC to Alice, which is modelled by the classical BI-AWGN channel constructed in Fig. 2(a) and represented by block (3) of Fig. 2(b). The channel-contaminated sequence received by Alice is denoted by $\tilde{\mathbf{b}} = [0000011]$, which is corrupted in the second to last bit position.
- Meanwhile, based on the QRNG output Bob calculates the syndrome, say $\mathbf{s} = [001]$ in block (2) and transmits it as side information to Alice through the authenticated ClC of block (3*), which is assumed to be perfectly noiseless and error-free.
- Alice takes the bit stream $\tilde{\mathbf{b}}$ inferred at the output of the QuC, which may or may not be a legitimate codeword, and forwards it to the BCH decoder (block (4) of Fig. 2(b)). The BCH decoder then corrects it with the aid of the syndrome bits she received through the ClC and gets the decoded results of $\hat{\mathbf{b}} = [0000001]$. Based on this, Alice acquires the decoded codeword as the final reconciled key shown in block (5). Observe that this is the same as Bob's bit stream $\mathbf{b}$, provided that there are no decoding errors.

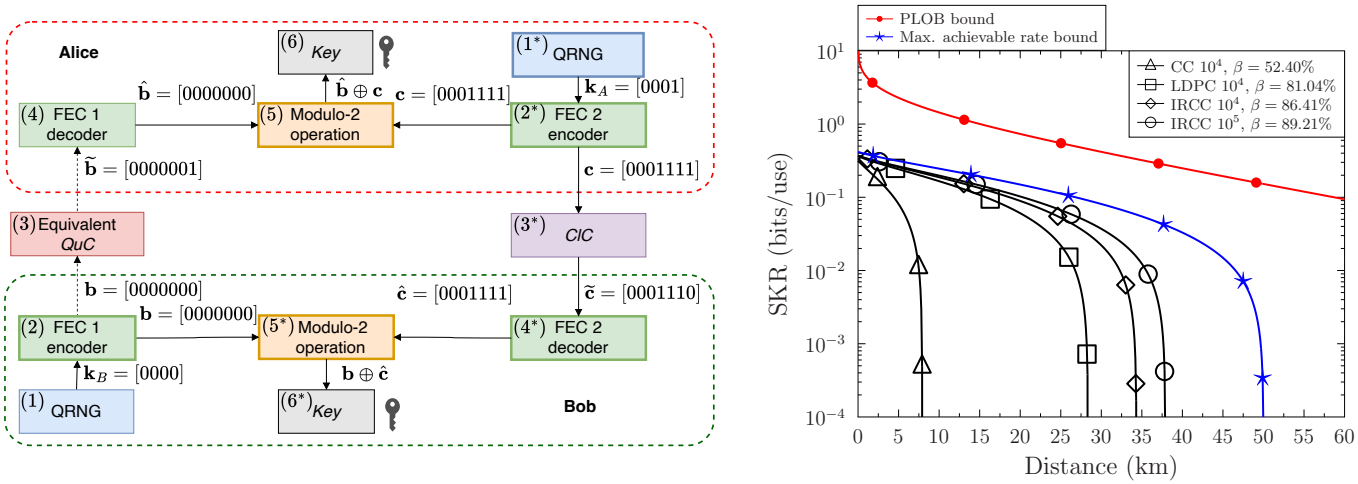
III. Improved CV-QKD

In this section, we present the improved CV-QKD system of Fig. 3 derived from Fig. 2.

A. Codeword-based Reconciliation Scheme

In optical fibre-based CV-QKD systems, the channel's transmissivity T is primarily determined by the fibre attenuation ac-

[1]This mapping function is used to calculate the noise between $\mathbf{b}$ and $\mathbf{u}^A$ based on the noise level in QuC.



(a) (b)

Fig. 3: (a) The codeword-based RR scheme and (b) SKR versus distance performance of different FEC codes. The Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound that represents the fundamental limit of SKR for any DV or CV point-to-point quantum communication protocol – regardless of the specific modulation scheme or reconciliation method used. By contrast, the maximum achievable rate bound characterizes near-error-free transmission, when aiming for obtaining the SKR of specific modulation and coding schemes. Attenuation loss α = 0.2 dB/km, room temperature T_e =296 K, detector efficiency η = 0.98, finite-size factor $N_{\text{privacy}} = 10^{12}$.

cording to $T = 10^{-\alpha\mathfrak{L}/10}$, where α (dB/km) is the attenuation coefficient and $\mathfrak{L}$ represents the transmission distance. This yields a Gaussian quantum transmission model $z = \sqrt{T}s + n$, where n represents the noise from different sources, which can be modelled as a BI-AWGN channel [11], [12]. Specifically, the output $\mathbf{u}^A$ in Fig. 2(a) is a channel-contaminated version of the input bit stream $\mathbf{b}$ in Fig. 2(a), hence the conventional quantum reconciliation then employs syndrome-based BCH coding, where Bob forwards the syndromes $\mathbf{s}$ in Fig. 2(b) as additional side information for Alice's BCH decoder of block (4) in Fig. 2(b) to correct errors.

While widely adopted, the conventional syndrome-based reconciliation scheme of Fig. 2(b) exhibits several fundamental constraints. Firstly, it requires FEC codes having well-defined syndrome structures, thereby excluding IRCCs, and polar codes from consideration. Secondly, the ClC used for transmitting the syndrome is typically assumed to be error-free in the literature. Practically, an arbitrary secondary FEC code is needed to protect the syndrome during its transmission over a realistic noisy ClC. This necessitates: (i) an FEC encoder at Bob's side before syndrome transmission from block (2) of Fig. 2(b), and (ii) a corresponding FEC decoder at Alice's side preceding the main reconciliation BCH decoder block (4) of Fig. 2(b). Consequently, these architectural requirements create an asymmetric computational burden, with Alice's processing complexity significantly exceeding Bob's. These limitations motivate the investigation of alternative reconciliation paradigms capable of supporting broader code families, while maintaining practical feasibility in realistic channel conditions.

In light of this, we advocate a generic codeword-based – rather than syndrome-based – reconciliation scheme that achieves near-capacity performance at a balanced-complexity. This solution is particularly advantageous for quantum-safe device-to-device (D2D) communication systems. As depicted in Fig. 3(a), our proposed scheme incorporates an equivalent QuC in block (3) that comprehensively models the quantum transmission, sifting, and mapping processes. The operational workflow of Fig. 3(a) proceeds as follows:

- In our example, both Bob and Alice generate a $k = 4$-bit random string using their QRNGs and encode them by two independent FEC encoders. We consider a simple [7,4,1] BCH code. The random uncoded bits of Bob and Alice are assumed to be $\mathbf{k}_B$=[0000] and $\mathbf{k}_A$=[0001], while their corresponding codewords are $\mathbf{b}$=[0000000] and $\mathbf{c}$=[0001111], respectively.
- Bob transmits his legitimate codeword $\mathbf{b}$ through the QuC (dashed lines), using the same general process as in block (3) of Fig. 2(b). The QuC of block (3) corrupts it to $\tilde{\mathbf{b}} = [0000001]$ and the FEC 1 decoder (block (4)) corrects it to $\hat{\mathbf{b}} = [0000000]$. Meanwhile, Alice transmits her legitimate codeword $\mathbf{c}$ generated by FEC 2 (block (2*)) through the ClC (block (3*)), which may inflict errors, yielding $\tilde{\mathbf{c}}$, but the FEC 2 decoder (block (4*)) corrects them to $\hat{\mathbf{c}}$.
- Explicitly, both Alice and Bob carry out error correction to get $\hat{\mathbf{b}}$=[0000000] and $\hat{\mathbf{c}}$=[0001111], respectively. Note that the encoders and decoders of FEC 1 and FEC 2 do not have to rely on the same code. However, for convenience, in our study, it is assumed that both the QuC and ClC adopt the same [7,4,1] BCH codes.
- Finally, the Modulo-2 operation is adopted at both Alice and Bob to obtain the final reconciled key for both of them, which are $\hat{\mathbf{b}} \oplus \mathbf{c}$ and $\mathbf{b} \oplus \hat{\mathbf{c}}$, respectively. In case of $\mathbf{b} = \hat{\mathbf{b}}$ and $\mathbf{c} = \hat{\mathbf{c}}$ they both have the same key.

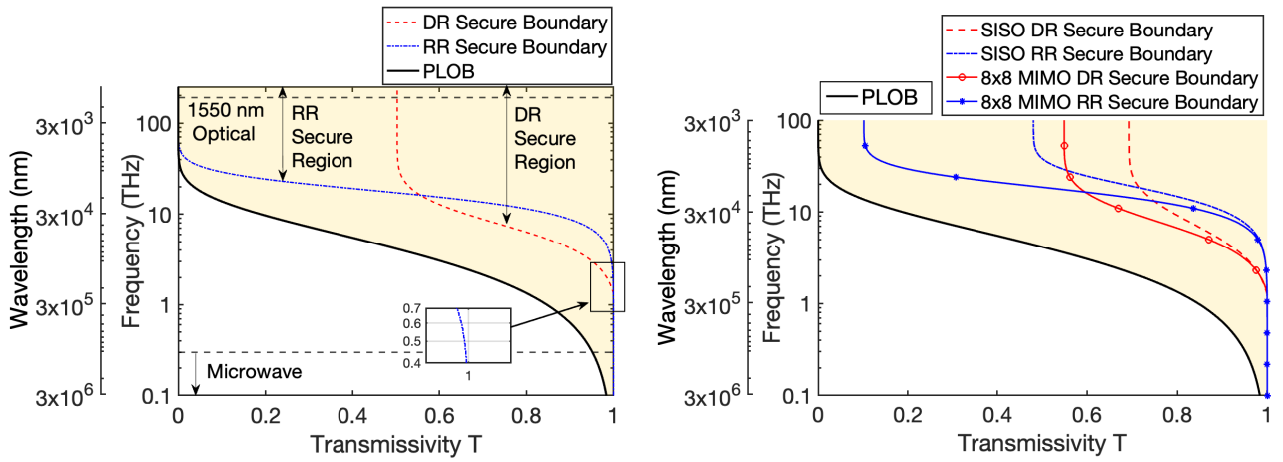


Fig. 4: Secure boundary comparison between DR and RR schemes: (a) SISO case with ideal reconciliation, (b) SISO and MIMO cases using realistic LDPC-coded reconciliation. Room temperature T_e =296 K, detector efficiency η = 0.98, finite-size factor N_{privacy} = 10^{12}. LDPC code: R_{LDPC}=0.5 and N_{LDPC} = 1024.

Fig. 3(b) demonstrates the SKR versus distance performance of a codeword-based reconciliation aided CV-QKD scheme for CC, LDPC and IRCC codes. An optical fibre quantum link[2] having $\alpha = 0.2$ dB/km attenuation is considered, where the coding-rate and codeword-length are set as 0.5 and 10^4, respectively. Furthermore, the effect of IRCC codeword-length is investigated by using two different codeword-lengths, i.e. 10^4 and 10^5. Firstly, the IRCC coded reconciliation achieves longer secure distance than the LDPC-coded system, which is followed by the CC-coded system associated with the same code-rate of 0.5 and codeword-length 10^4. Secondly, the SKR performance of a 10^5 long IRCC block is better than that of a block-length 10^4, as expected.

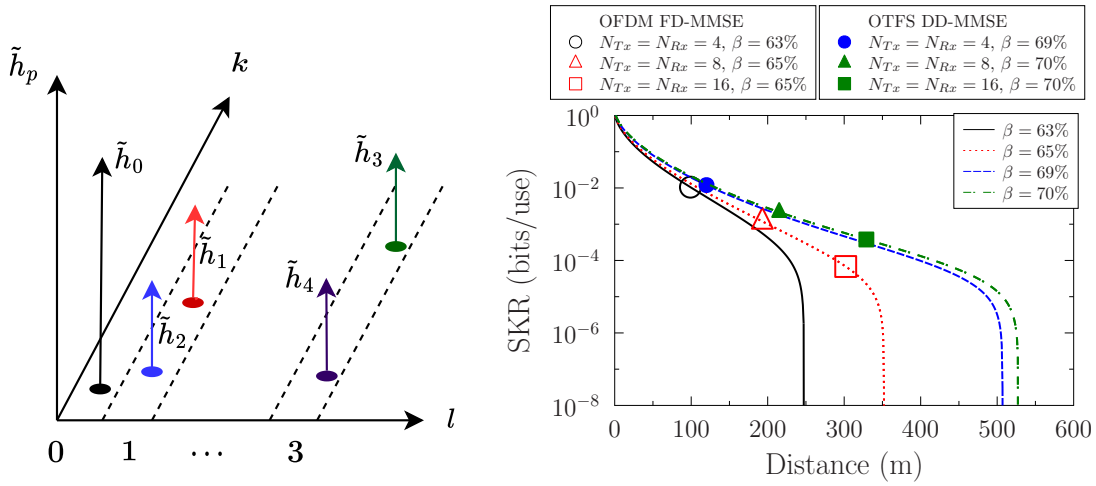
B. MIMO aided CV-QKD THz System

The investigation of CV-QKD protocols below the optical band – particularly in the microwave and THz regimes – presents compelling practical significance. These frequency ranges underpin ubiquitous wireless technologies, such as Wi-Fi, Bluetooth, and the emerging NG/THz communications, where quantum-safe security could address the critical vulnerabilities of classical communications. While optical CV-QKD benefits from mature photonic components, expanding to lower frequencies offers potential robustness against atmospheric disturbances, while supporting the Internet of Things (IoT) and NG networks. Nonetheless, moving from the optical band down to THz/mmWave frequencies generally alleviates the effects of path loss and the impact of fog, dust, atmospheric turbulence. However, the corresponding photon energy will decrease, while the room-temperature thermal background noise increases. It was demonstrated in [4], [5] that the variance of thermal noise characterized by $V_0 = 2\overline{n}+1$ with $\overline{n} = 1/[\exp(hf/k_BT_e)-1]$, where T_e is the temperature, h is Planck's constant, k_B is Boltzmann's constant and f is the frequency, will asymptotically decrease to 1 ($V_0 \to 1$) as f approaches to optical band, whereas at low-THz/microwave band $V_0 \gg 1$ [4], [5]. This frequency–noise trade-off is central to the design and feasibility of wireless THz CV-QKD. Therefore, we are inspired to characterize the security thresholds of CV-QKD systems by analysing the relationship between the operational frequencies (from microwave to optical bands) and channel transmissivity T, extending prior theoretical frameworks [4]. This comprehensive analysis reveals the operational boundaries of practical CV-QKD implementations relative to the theoretical maximum, providing critical insights for system design across different frequency regimes.

More specifically, Fig. 4(a) systematically compares the security thresholds of CV-QKD systems across the microwave to optical bands for both DR and RR based CV-QKD under ideal conditions, where a 0.5-rate LDPC code is considered and an ideal reconciliation efficiency is assumed, which is associated with 0 dB SNR required for achieving near-error-free transmission. Fig. 4(a) demonstrates that the PLOB bound defines the minimum transmissivity required for secure key generation across different frequencies, with the yellow boundary separating the secure (right) and insecure (left) operational regions. Furthermore, RR enables secure key distribution over the entire 0.1-200 THz range, although frequencies below 2 THz require extremely high transmissivity ($T \geq 0.999$), making practical implementation challenging. By contrast, DR exhibits significant limitations: it cannot operate below 1.3 THz, regardless of the transmissivity and it is restricted to $T > 0.5$ (the 3 dB limit) at higher frequencies, resulting in a much narrower secure region. These results highlight the superior adaptability of RR across the spectrum, while underscoring the stringent conditions required for low-frequency CV-QKD implementations.

Fig. 4(b) further demonstrates the benefits of MIMO techniques for CV-QKD systems by comparing the secure frequency-transmissivity regions of SISO and MIMO config-

[2]Although the case study is conducted on an optical-fibre quantum link, the proposed codeword-based reconciliation is equally applicable to the THz CV-QKD framework of Sec. III-C.



(a) (b)

Fig. 5: (a) The multipath channel in the DD domain and (b) the SKR versus distance performance comparison between MIMO aided OFDM and OTFS systems for different MIMO dimensions ($N_{Tx} \times N_{Rx}$) in a mobile scenario of $v = 30$ mph. Atmospheric loss α = 50 dB/km, Ricean factor K= 0 dB, the number of OFDM/OTFS symbols N=16, and the number of subcarriers M=64. Room temperature T_e =296 K, detector efficiency η = 0.98, finite-size factor $N_{\text{privacy}} = 10^{12}$. LDPC code: R_{LDPC} and N_{LDPC} = 1024.

urations under practical LDPC-coded DR/RR reconciliation, where a 0.5-rate LDPC code and 1024 code-length is harnessed, requiring 2.2 dB and 1.2 dB SNRs to achieve a target frame error rate of 10^{-1} for SISO and MIMO, respectively. The results show that while both the DR and RR schemes experience significant reductions in their secure regions due to their realistic non-ideal reconciliation efficiency owing to their practical LDPC implementation, an 8×8 MIMO system substantially expands the security boundaries, resulting in longer maximum secure transmission distance and improved SKR performance at relatively low carrier frequencies.

C. OTFS assisted CV-QKD THz System

Again, the feasibility of THz CV-QKD has been extensively studied and evaluated over the past decade. By leveraging classical techniques such as MIMO and OFDM, the SKR versus distance performance can be improved, despite the challenges posed by the high path-loss and frequency-selective fading in the THz band. However, in high-mobility SAGIN systems, OFDM suffers from excessive inter-carrier interference (ICI). By contrast, the recently developed OTFS waveform conveys information in the delay-Doppler (DD) domain, and converts the time-frequency (TF) fading into quasi-static DD domain fading. Consequently, Gaussian modulation is performed in the DD domain using OTFS. Accordingly, blocks (2) and (3) in Fig. 2(a) can be replaced by OTFS transmitters and receivers, along with THz QuCs[3]. As for the time-varying frequency-selective THz fading channel, it can be characterized in the DD domain as illustrated in Fig. 5(a). More specifically, in Fig. 5(a), we have $L = 4$ resolvable delay bins in the time-domain (TD). Additionally, there are $P = 5$ distinct paths differentiated by their delay and Doppler indices. Among these, $\tilde{h}_0$ represents the line-of-sight (LoS) path located in the $l = 0$th bin, while the other four non-line-of-sight (NLoS) paths arrive at the 1st and 3rd bins associated with different Doppler indices. The subsequent post-processing remains the same as in Fig. 3.

Fig. 5(b) compares the SKR versus distance performance of MIMO OFDM and MIMO-OTFS systems for different MIMO sizes in a time-varying frequency-selective THz channel, where the atmospheric path loss attenuation coefficient α is set to 50 dB/km at 15 THz. Moreover, due to the limited number of scatters and high attenuation of the THz band, the Ricean factor K is set to 0 dB. The 0.5-rate LDPC code length is N_{LDPC} = 1024, and the cyclic prefix (CP) length is $M_{\text{cp}} = L + 1$, where $L = 0, 1, 2$ for $M = 64$ subcarriers, and $P = L$ paths. The results of Fig. 5(b) show that the OTFS-based CV-QKD system achieves a longer secure transmission distance than its OFDM counterpart in a mobile scenario (v=30 mph), owing to its superior reconciliation efficiency. Additionally, increasing the MIMO beamforming gain enhances the secure transmission distance for both OFDM- and OTFS- based CV-QKD systems.

Furthermore, the complexities of OFDM/OTFS modulation/demodulation and detections are briefly discussed as follows:

- *Modulation/demodulation complexity*: For a frame of N OFDM symbols consisting of M subcarriers each, the complexity of fast Fourier transform (FFT) is $\mathcal{O}\left[MN \log_2(M)\right]$, while the 2D symplectic finite Fourier transform (SFFT) for OTFS has the complexity $\mathcal{O}\left[MN \log_2(MN)\right]$.

[3]It is widely acknowledged that particle-like behaviour of photons is gradually eroded in the THz RF band, where predominantly wave-like behaviour prevails [7]. However, sufficient non-zero SKR was still heralded in [7]. Hence a RF THz channel is considered in our treatise.

- *Detection complexity*: In high-mobility channels, the per-frame DD minimum mean squared error (DD-MMSE) of an OTFS system scales as $\mathcal{O}(M^3N^3)$, which is higher than that of the FD-MMSE of OFDM, namely $\mathcal{O}(M^3N)$. Accounting for the N_{bl} blocks required by LDPC coded reconciliation, the overall complexity over processing blocks becomes $\mathcal{O}(M^3N\,N_{bl})$ for OFDM and $\mathcal{O}(M^3N^3)$ for OTFS [9].

IV. Future Directions

A. Pareto-Optimal HARQ-Based CV-QKD System Design

In the reconciliation process, FEC codes are harnessed for mitigating the transmission-induced errors. To detect decoding failures, a classic cyclic redundancy check (CRC) verifies whether the decoded bit stream is correct. If decoding fails, post-processing resumes with a new randomly generated bit stream from either Alice or Bob, along with additional quantum transmissions. However, this approach leads to significant resource wastage. To enhance the error correction capability, automatic repeat request (ARQ) can be employed, but this introduces additional latency and reduced throughput – especially when longer blocks are used for near-capacity performance. To address this, *hybrid ARQ (HARQ)*[4] techniques can be leveraged for improving the block error rate (BLER) performance, while maintaining acceptable delay. To elaborate further, pure unprotected bits may be transmitted initially. If decoding fails, more and more parity check bits may be provided in subsequent transmissions. The receiver's FEC decoder then combines soft information from all transmissions for decoding. If successful, Alice and Bob proceed to privacy amplification, otherwise, additional redundancy bits are incrementally transmitted until either decoding success is declared or the maximum retransmission limit is reached.

In this ARQ-aided reconciliation context, a whole range of design options has to be explored. First of all, different FEC codes and ARQ schemes exhibit diverse CV-QKD trade-offs. Fig. 3(b) already indicated the pros and cons of CC, LDPC and IRCC codes, but polar codes tend to perform best for short, low-delay blocks. The family of other FEC codes, such as BCH, RS and multiple-component turbo codes must be characterized for determining their code-rate, block-length and complexity trade-offs. Their ability to lend themselves to Type-I and Type-II ARQ has not been documented in the literature of CV-QKD either.

Clearly, there is a huge range of trade-offs to be quantified as a function of the above parameters. This has to be handled in the context of non-dominated multi-component Pareto optimization characterizing the rich design-space of ARQ-aided CV-QKD systems. Briefly, the SKR may be improved upon increasing the FEC block-length or the number of LDPC/turbo decoding iterations, but only at the cost of increasing the latency and/or complexity plus power-dissipation. A plethora of similar trade-offs emerge. In the asymptotic limit of all parameters we arrive at a set of near-Pareto solutions. These solutions share the property that none of the system parameters can be improved without degrading at least one of the others, which is hence characteristic of the ultimate practical limits of CV-QKD systems.

[4]HARQ is implemented in the ClC for the reconciliation process. In light of this, an additional new security proof for CV-QKD is needed, when HARQ is applied.

B. Simultaneous Quantum and Classical Protocol Design

Simultaneous quantum and classical communication (SQCC) protocol design aims for intrinsically amalgamating the QKD process with classical communication. Existing SQCC implementations in the optical band demonstrate this dual functionality. For instance, coherent state-based SQCC [13] encodes both classical communication bits and Gaussian-modulated coherent states (GMCS) for CV-QKD to the same coherent state, which may be detected by a shared coherent receiver. This approach achieves both low-bit error rate (BER) classical communication and a practical SKR in single-mode fibres. As a further improvement, the advanced MDI SQCC protocol can mitigate eavesdropping risks associated with imperfect detectors. The simulation results of [14] confirm the feasibility of MDI-based SQCC over a 21 km optical fibre link using superposition modulation.

Building on our OTFS-based CV-QKD system proposed for time-varying frequency-selective fading scenarios, a multicarrier THz SQCC system is potentially capable of supporting both QKD and classical communication.

C. New Waveforms and Detectors for CV-QKD

Beyond the emerging OTFS waveform that is proposed for tackling the detrimental effects of doubly-dispersive fading of high-mobility scenarios, other promising waveforms are worthwhile considering for CV-QKD.

- *Chirp-domain affine frequency-division multiplexing (AFDM)*: Maps symbols from the affine Fourier transform domain to the TD. By optimizing its parameters to match the channel statistics, AFDM enhances DD orthogonality.
- *Orthogonal delay-Doppler division multiplexing (ODDM)*: It leverages orthogonal DD-plane pulses to achieve a compact and exact channel input-output relationship in the DD domain. ODDM enables perfect coupling between the modulated signal and DD channel, outperforming OTFS both in terms of out-of-band emission and BER.

Before THz devices reach maturity, optical-frequency homodyne/heterodyne detectors having low electronic noise can be adopted for THz via THz-to-optical converters [4]. On the other hand, as for the direct measurement of the received THz signals, the beamsplitters and plasmonic photoconductive detectors offer a viable solution [8]. Furthermore, Rydberg atomic quantum receivers exhibit exceptional sensitivity for accurate RF measurement thanks to (i) their precise phase/frequency resolution of weak RF electric fields and (ii) enhanced sensitivity in electric fields, particularly for detecting time-varying signals. Experimental studies in the classical domain have validated these attractive capabilities in the detection of amplitudes, phase, polarization, modulation, spatial direction, etc. Hence, they constitute a promising technology for direct homodyne/heterodyne detection at THz frequencies for CV-QKD.

D. Security Analysis of the Proposed CV-QKD Schemes

While our prior work [12] touched upon the security of codeword-based (FEC-agnostic) reconciliation, a full security proof based on wireless THz links remains to be completed. Furthermore, as part of the evolution from OFDM (FD modulation) to OTFS (DD-domain modulation), our design uses popular transforms (ISFFT/SFFT, equalization, and MIMO combining). Although such unitary/orthogonal operations should not increase Eve's accessible information, a dedicated proof under wireless THz conditions is warranted.

E. Testbed Verifications

Albeit there are a few pioneering research contributions related to wireless THz CV-QKD preceding our proposed OTFS-based THz CV-QKD scheme, such as the SISO/MIMO THz CV-QKD of [4], [5], and the reconfigurable intelligent surface (RIS)-assisted MMO THz CV-QKD of [15], this research area is still in its infancy. Testbed verifications are needed once the THz devices (THz detectors, antennas, etc) become mature enough to carry out experimental tests.

V. Conclusions

QKD offers information-theoretic security grounded in quantum mechanics and can benefit a wide range of verticals – including finance and banking, government and defence, cloud/data centres, and healthcare. Looking beyond fibre and FSO links, THz CV-QKD is envisioned for wireless environments such as SAGINs and vehicle-to-everything (V2X) applications, enabling high-throughput, secure connectivity. However, challenges such as balanced transmitter–receiver complexity requirements, transmission in different frequency bands, and time-varying frequency-selective fading scenarios may degrade the SKR performance. To address these challenges, we proposed three key innovations : 1) *Codeword-based* – rather than syndrome-based – FEC-coded reconciliation was advocated for balancing the transmitter-receiver complexity; 2) The *secure boundaries* of both DR and RR schemes were characterized right across the entire optical-to-microwave spectrum. MIMO techniques were exploited for further improving the secure regions of both DR and RR; 3) *OTFS* was harnessed to combat the time-varying frequency-selective fading in THz CV-QKD scenarios, demonstrating its superior Doppler resilience compared to its OFDM counterpart. Therefore, the SKR versus distance performance was improved. Future directions include HARQ-based reconciliation schemes, simultaneous quantum and classical protocol design as well as new waveforms and detectors for CV-QKD. Additionally, we touched upon the security analysis and testbed verifications tasks of the proposed schemes.

VI. Acknowledgement

The financial support of the following Engineering and Physical Sciences Research Council (EPSRC) projects is gratefully acknowledged: Platform for Driving Ultimate Connectivity (TITAN) under Grant EP/Y037243/1 and EP/X04047X/1; Robust and Reliable Quantum Computing (RoaRQ, EP/W032635/1); India-UK Intelligent Spectrum Innovation ICON UKRI-1859; PerCom (EP/X012301/1); EP/X01228X/1; EP/Y037243/1. The work of S. Sugiura was supported in part by the Japan Science and Technology Agency (JST) ASPIRE Program (Grant JPMJAP2345), and in part by the Japan Society for the Promotion of Science (JSPS) KAKENHI (Grant 24K21615).

References

[1] H. Delfs, H. Knebl, and H. Knebl, *Introduction to cryptography*. Springer, 2002, vol. 2.

[2] 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 Commun. Surv. Tutor.*, vol. 24, no. 2, pp. 839–894, 2022.

[3] 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.

[4] C. Ottaviani, M. J. Woolley, M. Erementchouk, J. F. Federici, P. Mazumder, S. Pirandola, and C. Weedbrook, "Terahertz quantum cryptography," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 483–495, 2020.

[5] N. K. Kundu, S. P. Dash, M. R. McKay, and R. K. Mallik, "MIMO Terahertz quantum key distribution," *IEEE Commun. Lett.*, vol. 25, no. 10, pp. 3345–3349, 2021.

[6] 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 Photon. J.*, vol. 13, no. 4, pp. 1–13, 2021.

[7] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Phys. Rev. Lett.*, vol. 105, no. 11, pp. 1–8, 2010.

[8] X. Liu, C. Zhu, N. Chen, and C. Pei, "Practical aspects of Terahertz wireless quantum key distribution in indoor environments," *Quant. Inf. Process.*, vol. 17, no. 11, pp. 1–20, 2018.

[9] X. Liu, C. Xu, S. X. Ng, and L. Hanzo, "OTFS-based CV-QKD systems for doubly selective THz channels," *IEEE Trans. Commun.*, vol. 73, no. 8, pp. 6274–6289, 2025.

[10] N. K. Kundu, M. R. McKay, and R. K. Mallik, "Wireless quantum key distribution at terahertz frequencies: Opportunities and challenges," *IET Quantum Commun.*, vol. 5, no. 4, pp. 450–461, 2024.

[11] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, no. 4, 2008, Art. no. 042325.

[12] 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 J. Commun. Soc.*, vol. 5, pp. 2089–2112, 2024.

[13] B. Qi, "Simultaneous classical communication and quantum key distribution using continuous variables," *Phys. Rev. A*, vol. 94, no. 4, p. 042340, 2016.

[14] D. Pan, S. X. Ng, D. Ruan, L. Yin, G. Long, and L. Hanzo, "Simultaneous two-way classical communication and measurement-device-independent quantum key distribution with coherent states," *Phys. Rev. A*, vol. 101, no. 1, p. 012343, 2020.

[15] S. Kumar, S. P. Dash, D. Ghose, and G. C. Alexandropoulos, "Ris-assisted MIMO CV-QKD at THz frequencies: Channel estimation and secret key rate analysis," *IEEE Trans. Commun.*, 2025, early access.

VII. Biographies

Xin Liu received the Ph.D. degree from the University of Southampton, Southampton, U.K., in 2025. He is now a Research Fellow with the Next Generation Wireless Research Group, University of Southampton. His research interests include quantum communications, channel coding and wireless communications.

Nan Wang is currently a Master's student studying at Imperial College London, majoring in Optics and Photonics. He was awarded a first-class Bachelor's degree in Electrical and

Electronic Engineering from the University of Southampton in 2025, and also received the National Grid Company Prize that same year.

Chao Xu [Senior Member, IEEE] is currently a Senior Lecturer with Next Generation Wireless Research Group, University of Southampton. He was the recipient of the Best M.Sc. Student in Broadband and Mobile Communication Networks by the IEEE Communications Society UK and RI Chapter in 2009, 2012 Chinese Government Award for Outstanding Self-Financed Student Abroad, 2017 Dean's Award, Faculty of Physical Sciences and Engineering, University of Southampton, 2023 Marie Sklodowska-Curie Actions Global Postdoctoral Fellowships with the highest evaluation score of 100/100.

Soon Xin Ng [Senior Member, IEEE] received the Ph.D. degree in telecommunications from the University of Southampton (2002). He is a Senior Member of the IEEE, a Fellow of the Higher Education Academy in the UK, a Chartered Engineer and a Fellow of the IET. He is currently a Professor at the University of Southampton. For further details please see https://generic.wordpress.soton.ac.uk/sxn/about.

Phuc V. Trinh [Senior Member, IEEE] received the Ph.D. degree from the University of Aizu, Japan, in 2017. He is currently a Project Research Associate with the Institute of Industrial Science, The University of Tokyo, Japan. His research interests include optical and wireless communications for space, aerial, and terrestrial networks.

Shinya Sugiura [Senior Member, IEEE] received the Ph.D. degree from the University of Southampton, U.K., in 2010. Since 2018, he has been with the Institute of Industrial Science, The University of Tokyo, Japan, where he is currently a full Professor. He is an Editor for IEEE TWC, IEEE TCOM, and IEEE WCL.

Lajos Hanzo [Life Fellow, IEEE] received Honorary Doctorates from the Technical University of Budapest (2009) and Edinburgh University (2015). He is a Foreign Member of the Hungarian Science-Academy, Fellow of the Royal Academy of Engineering (FREng), of the IET, of EURASIP and holds the IEEE Eric Sumner Technical Field Award. For further details please see http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos˙Hanzo.