On the Road to Quantum Communications

Daryus Chandra, Panagiotis Botsinis, Dimitrios Alanis, Zunaira Babar, Soon-Xin Ng and Lajos Hanzo

***Abstract*—Moore's Law has prevailed since 1965, predicting that the integration density of chips will be doubled approximately every 18 months or so, which has resulted in nano-scale integration associated with 7 nm technologies at the time of writing. At this scale however we are about to enter the transitory range between classical and quantum physics. Based on the brilliant proposition by Feynman a new breed of information bearers was born, where the quantum bits are mapped for example to the spin of an electron. As a benefit, the alluring properties of the nano-scale quantum world have opened up a whole spate of opportunities in signal processing and communications, as discussed in this easy-reading discourse requiring no background in quantum physics.**

I. Introduction

The Internet has revolutionized our lives. This revolution was catalyzed by the groundbreaking discoveries of information theory, followed by the evolution of integrated circuit technology, which has broadly speaking followed the predictions of Moore's Law ever since 1965. This trend has gradually led to nano-scale integration, where encountering quantum effects is no longer avoidable. The processing of quantum-domain information has to obey the basic postulates of quantum physics, where a so-called quantum bit or *qubit* may be represented as the *superposition* of a logical zero and a logical one. More explicitly, we could visualize this superposition as a coin spinning in a box, hence being in an equiprobable superposition of 'head' and 'tail', so that we can avoid the somewhat unpalatable reference to the famous Schrödinger cat analogy. Metaphorically speaking, we have to carry out all quantum signal processing operations, while the coin is still spinning in the box, because once it has stopped, we can no longer 'manipulate' or process it in the quantum-domain - it has 'collapsed' back into the classical domain. Therefore upon lifting the lid of the box, we can reveal the resultant classical-domain outcome, which is either 'head' or 'tail'.

Another property of the above-mentioned qubits is that they cannot be copied, because trying to copy them would result again in their collapse to the classical domain, hence precluding their further processing in the quantum domain. Instead, the so-called *entanglement* operation has to be used. Intriguingly, entangled qubits have the property that if we change the spin of the electron representing the qubit, that of its entangled pair is also changed at the same instant. However, it has to be mentioned that at the time of writing entanglement has only been demonstrated in practice by relying on classical-domain preparatory operations carried out before the entanglement is established, which had to obey the speed of light. Upon entangling large vectors of qubits, representing the quantum-domain operands parallel processing becomes feasible, hence it also becomes possible to construct so-called quantum computers capable of solving various classically intractable problems. Having said that, these bespoke quantum computers can still be outperformed in certain tasks by classical computers, but they are eminently suitable for tailor-made tasks, which cannot be efficiently solved by classical computers [1]. In parallel to these alluring developments, next-generation communication systems aim for realizing flawless telepresence. It has also been predicted that the number of devices connected to the Internet has outnumbered the entire human population of planet Earth. In this context, the power of superposition and entanglement may be harnessed for efficiently solving various problems, which have hitherto been deemed to be unsolvable in our lifetime.

A striking example demonstrating the power of quantum computing is Grover Quantum Search Algorithm (QSA), which is capable of finding a single solution in an unstructured database having N elements at a complexity order of $\mathcal{O}(\sqrt{N})$, whilst its classical full-search-based counterpart requires on the order of $\mathcal{O}(N)$ cost-function evaluations (CFEs). As wonderful as it sounds, quantum computers also impose a massive threat on classical security and privacy. The most popular public cryptosystem, known as the Rivest-Shamir-Adleman (RSA) algorithm, heavily relies on the hardness of the so-called integer factorization problem. Although this problem is impractical to solve using the current classical computers, this will no longer be the case when a fully functioning quantum computer is available. For instance, the time required for breaking a 2048-bit public key can be reduced from billions of years required by classical computers to a matter of minutes by employing a quantum computer [2].

Fortunately, quantum information processing also provides a wonderful solution for mitigating this emerging threat. Quantum key distribution (QKD) [3]–[5] constitutes one of the already commercialized quantum technologies. QKD circumvents the problem of the impractical, but absolutely secure one-time pad secret key distribution of classical communication. Therefore, QKD will remain provably secure in the face of the physical security attacks that may be carried out by quantum computers. Another impressive development has suggested that it is also possible to directly transmit classical information totally securely over quantum channels, whilst relying on the so-called quantum secure direct communication (QSDC) protocol [6]. This field of finding a novel scheme for securely transmitting classical information using quantum-domain techniques is widely referred to as *quantum cryptography*.

At the time of writing, quantum technologies gradually

The authors are with the School of Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, UK (email: {dc3c18, sxn, lh}@soton.ac.uk).

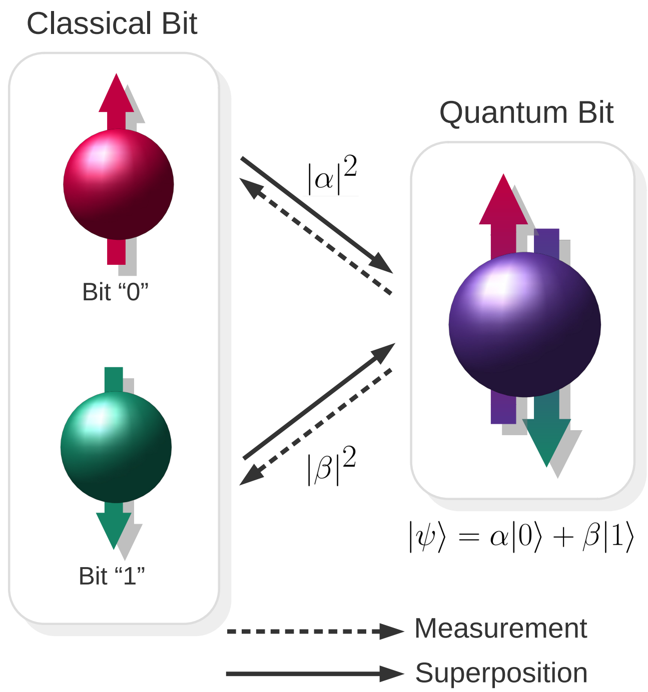


Fig. 1: A quantum bit or *qubit* can be in a *superposition* of two values or states at the same time. However, this superposition will collapse after measurement with a certain probability for each value "0" and "1".

approach maturity, and hence the exchange of quantum information will become inevitable and eventually ubiquitous. Connecting multiple quantum computers using quantum links potentially offers the capability of outperforming a single quantum computer by creating a larger distributed quantum computer. One of the key requirements for creating such a system is the capability to maintain seamless quantum links among the quantum computers. The vital resource required in this architecture is the so-called maximally-entangled quantum state relying on the Einstein-Podolski-Rosen (EPR) electron-pairs, potentially facilitating an instantaneous action at a distance. This entangled pair is created in a unique superposition state so that any operation applied to one of the particles will immediately affect the other particle, even if they are separated by a great distance - again, provided that the appropriate preparatory entanglement operations have been carried out. Boldly and explicitly, this does not 'violate' the speed of light, because these preparatory communications actions of course have to obey the speed of light, regardless whether they rely on optical fiber or free-space optical links. As quantum technologies become more prevalent in mainstream publications, several questions have emerged concerning what quantum technologies can offer in the realms of communication engineering. Although we have already touched upon them briefly, we would like to elaborate a little further on some promising applications for motivating further research.

II. Quantum-Based Communication

Again, in contrast to classical bits, which can only assume a value of "0" or "1" in any time interval, a qubit can hold both values simultaneously in a form of superposition as shown in Fig. 1. Therefore, N qubits in a state of superposition can be used to hold all the 2^N classical bit combinations simultaneously. Another highly relevant property of quantum information in this context is the *no-cloning theorem*, which we have briefly alluded to above by stating that upon trying to observe the qubits they collapse to the classical domain. In scientific parlance this dictates that no unitary operation can perform a perfect copying operation of a qubit found in an unknown superposition state to another auxiliary qubit. These two properties, in addition to the entanglement, can be exploited for developing several novel communication protocols.

Quantum key distribution (QKD) [3], [4] constitutes one of the most well-known quantum communications protocols, albeit in all truth QKD only represents a secret key negotiation protocol. By relying on the no-cloning theorem and on the fact that the action of 'measurement' or observation collapses the superposition of quantum states to the classical domain, sharing the so-called 'one-time pad' secret key now becomes plausible. The seminal QKD proposal is commonly referred to as the Bennett-Brassard protocol (BB84) [3], which is based on the 'prepare-and-measure' protocol, while the E91 protocol [4] is based on pre-shared EPR electron-pairs.

One of the features of a qubit is that it can be used to convey either quantum information or classical information. While the QKD protocol can be used for the exchange of the classical one-time pad secret key, **quantum superdense coding** [7] supports the secure transmission of classical information through pre-shared EPR electron-pair. This was an early demonstration that instead of acting as the medium of exchanging the secret key, the pre-shared maximally-entangled quantum state can also be used for directly transferring confidential classical information. This ingenious concept was then ultimately further developed by the proposal of **quantum-secure direct communication (QSDC)** [6], which constitutes a fully-fledged confidential quantum-based classical communications protocol, rather than being a pure secret key negotiation procedure. Given the increasing number of mobile devices communicating by broadcasting information, the secrecy and the privacy of the information becomes more crucial than ever. Quantum cryptography may pave the way for providing unbreachable physical layer security for next-generation communication. Naturally, there are numerous open challenges in the way of wide-spread QSDC, such as its limited attainable rate and distance, as well as its reliance on quantum memory, which future research has to tackle. It is also important to highlight that the underlying security-proofs of both the QKD and QSDC protocols are based on the classical information-theoretic physical layer security definitions.

To expound a little further, the direct transfer of quantum information over a quantum channel faces the following challenge. Due to the no-cloning theorem, any quantum information that is lost during its transmission cannot be

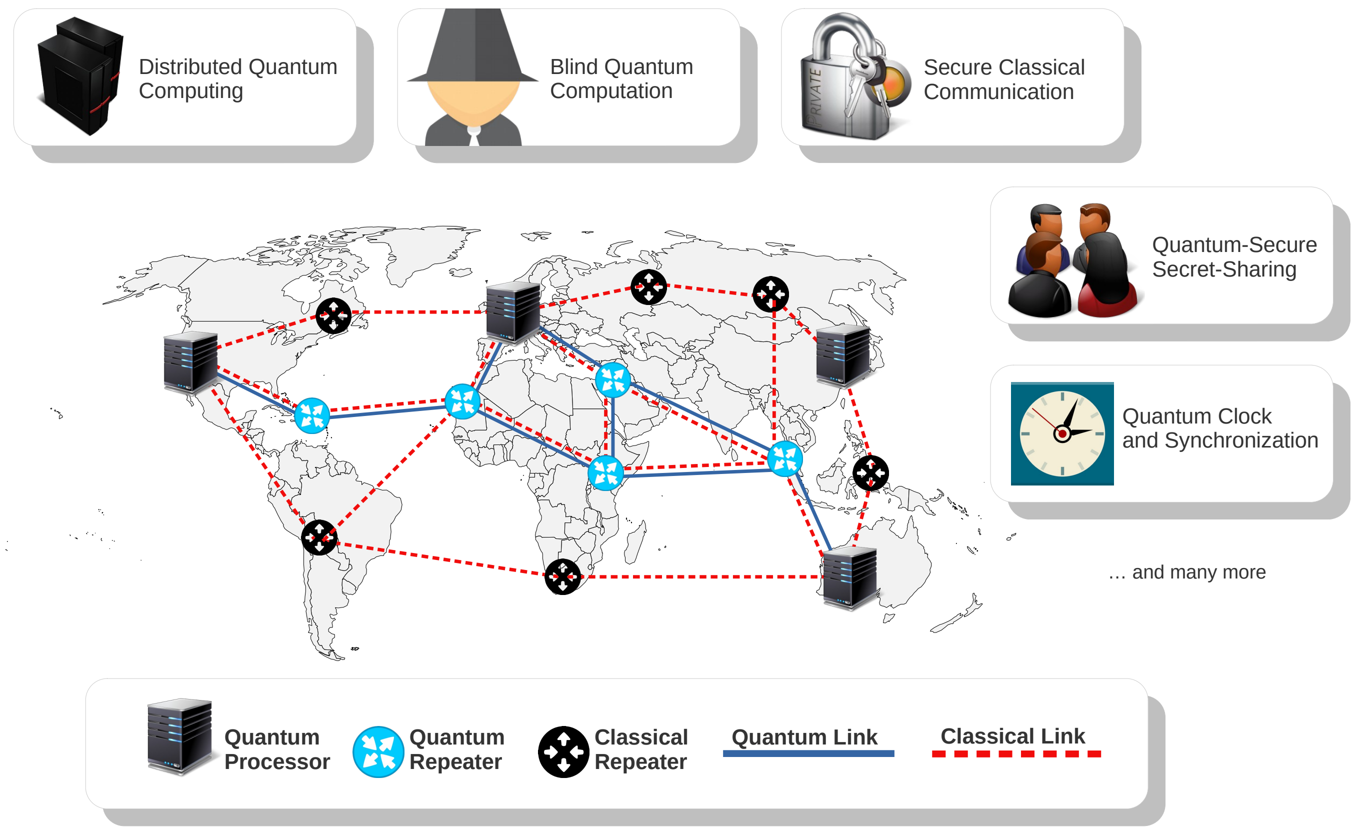


Fig. 2: Stylized vision of the Quantum Internet of the near future, which will rely on a combination of both classical and quantum devices.

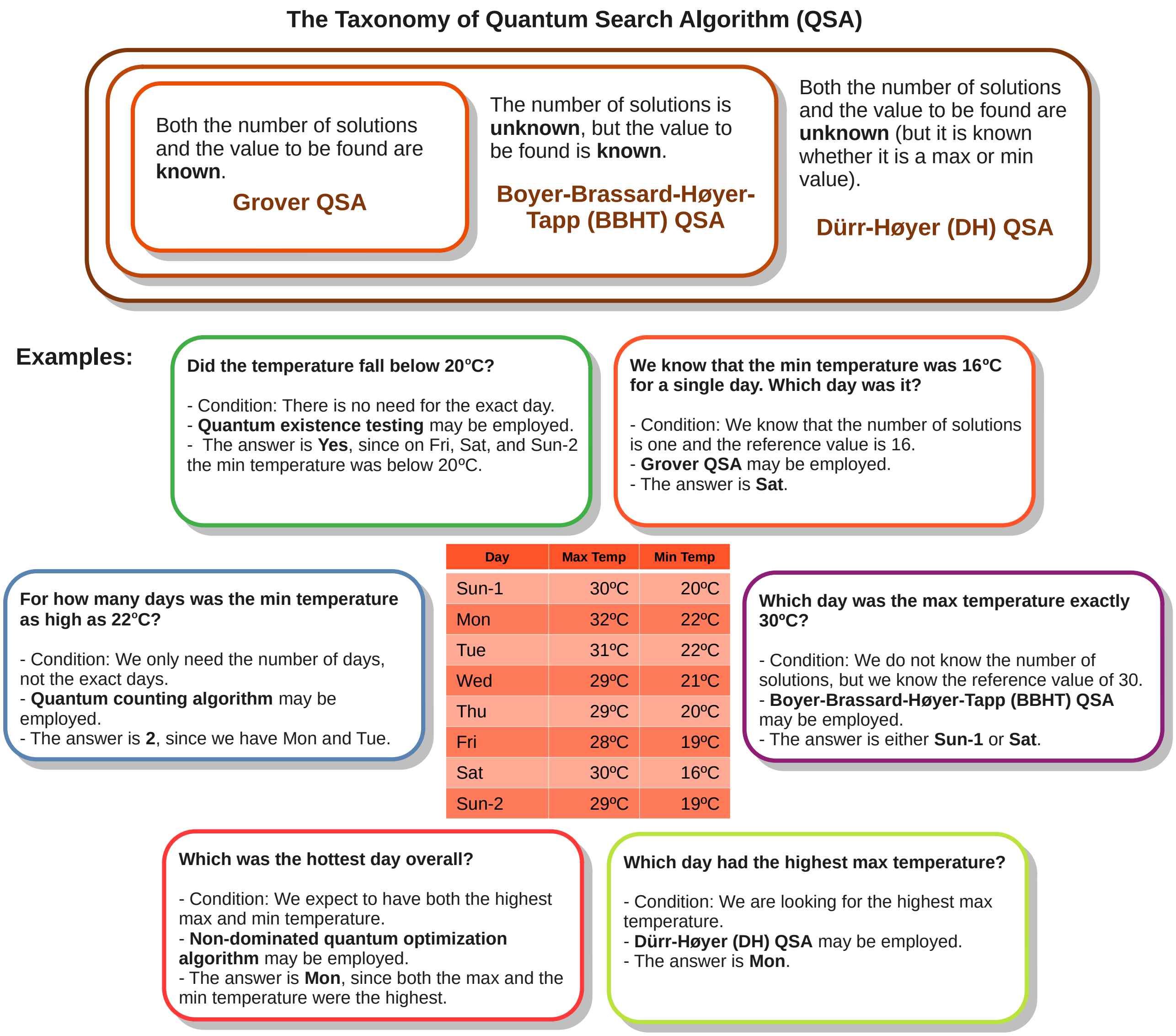
readily replaced. Hence the traditional method of ensuring a reliable transmission by sending multiple copies of the same information is no longer feasible. However, the properties of quantum mechanics allow us to transfer quantum information without sending it through the quantum channel with the aid of **quantum teleportation** [8]. The transfer of quantum information can be replaced by the joint action of an EPR electron-pair and classical communication. The employment of quantum teleportation is promising for the following reason. Multiple copies of EPR electron-pairs can be generated, hence an error-control procedure commonly referred to as **entanglement distillation** can be invoked for improving the integrity of quantum communications.

Therefore, a paradigm shift is taking shape concerning the role of repeaters and network coding. For a quantum network, both **quantum repeaters** and **quantum network coding** are indispensable for the reliable distribution of the EPR pairs across multiple nodes in the context of long-distance transmissions. While in classical networks the operation of the repeater is often based on the decode-and-forward mechanism, in the quantum domain the role of the repeater is to maintain connectivity in the form of the seamless generation and sharing of EPR electron-pairs between quantum nodes. To support this functionality, each quantum repeater may rely on the capability of performing **entanglement swapping** and **entanglement distillation**. This, in turn, will hinge on several novel network utilization metrics, which must be considered during the quantum network design of the near future.

The long-term goal in the exploration of quantum computation and communication is to conceive the perfectly secure **Quantum Internet** [9], which is an emerging concept in the landscape of quantum engineering, as portrayed in the stylized illustration of Fig. 2. The concept is reminiscent of that of the classical Internet, interconnecting multiple quantum nodes in the quantum network. The Quantum Internet will facilitate the perfectly secure exchange of quantum information, whilst supporting a plethora of other compelling applications such as distributed quantum computation, blind quantum computation, quantum-secure secret-sharing, and many more [10], [11]. For example, multiple inter-connected quantum computers can jointly act as a distributed quantum computer and can perform more advanced computational tasks than a single quantum computer. However, there are numerous other attractive applications that cannot even be predicted at the time of writing.

III. Quantum-Search-Aided Wireless Communications

The inherent parallelism of quantum information processing equips quantum computers with immense computational power. It has been shown theoretically that there are several classes of problems that can be solved very efficiently by quantum computers, such as integer factorization, finding solutions



Day	Max Temp	Min Temp
Sun-1	30ºC	20ºC
Mon	32ºC	22ºC
Tue	31ºC	22ºC
Wed	29ºC	21ºC
Thu	29ºC	20ºC
Fri	28ºC	19ºC
Sat	30ºC	16ºC
Sun-2	29ºC	19ºC

Fig. 3: The taxonomy of QSAs and their hypothetical use cases on weather data.

in large unstructured databases, and large-scale optimization problems, just to name a few. For instance, as we have mentioned briefly earlier, QSAs are capable of finding the correct solution in unstructured databases at a significantly reduced number of CFEs compared to the classical full-search based method. In order to form a clearer picture concerning the taxonomy and the potential applications of various QSAs, please refer to Fig. 3. However, the most intriguing question is, how we can exploit the beneficial computational speed-up attained by QSAs in solving the huge gamut of large-scale problems routinely found in classical wireless communications. Hence, this section will be dedicated to a number of applications, which have been shown to be capable of solving diverse problems arising in classical communication [12].

Quantum-Search-Aided Multi-User Detection [14]. The practical realization of the optimal full-search-based solution for classical wireless communication problems, such as the maximum-likelihood multiuser detector (ML-MUD), is hindered by its potentially excessive computational complexity. To circumvent this impediment, Grover's QSA may be invoked by exploiting the inherent parallelism of quantum information processing for approaching the ML-MUD's performance at a significantly lower number of cost function evaluations (CFEs). More explicitly, a derivative of Grover's QSA - namely the Durr-Høyer QSA - is capable of finding the correct solution with almost 100% probability after only evaluating on the order of $\mathcal{O}(\sqrt{N})$ CFEs, as opposed to the classical full-search-based solution requiring on the order of $\mathcal{O}(N)$ CFEs.

Quantum-Search-Aided Multi-Objective Routing [15], [16]. The emergence of the Internet of things (IoT) has motivated the development of the so-called self-organizing networks (SONs). Compared to conventional networks, SONs may act autonomously for achieving the best possible network performance. Thus, the underlying routing protocols should be capable of striking a delicate compromise amongst a range of conflicting quality-of-service (QoS) requirements. However, as the network size increases in terms of the number of nodes, finding the optimal solution typically becomes a non-polynomial-hard (NP-hard) search problem. Moreover, the employment of single-component objective functions relying on pure capacity or sum-rate maximization, on power or energy minimization or alternatively on dely or complexity minimization do not necessarily lead to attractive well-balanced system design. As a remedy, the concept of Pareto optimality comes to rescue in the context of multi-component optimization, which is capable of amalgamating various potentially conflicting design objectives. In this scenario, the Pareto front represents the collection of all optimal solutions, where none of the parameters involved in the objective function can be improved without degrading at least one of the others, as exemplified by the power versus bit-error ratio (BER) trade-off, just to mention one of them. Although a plethora of bio-inspired algorithms may be tailored specifically for solving multi-objective optimization problems, they often fail to generate all the optimal solutions constituting the Pareto front. As an attractive alternative, a quantum-aided multi-objective optimization algorithm may be invoked, which is capable of finding all Pareto optimal routes at a dramatically reduced number of CFEs. The complexity of finding the best route can be reduced to the order of $\mathcal{O}(N)$ and $\mathcal{O}(N\sqrt{N})$ CFEs in the best- and the worst-case scenarios, respectively, which corresponds to a substantial complexity reduction from the order of $\mathcal{O}(N^2)$ CFEs imposed by the classical full-search-based solution.

Quantum-Search-Aided Non-Coherent Detection [17]. With the proliferation of wireless devices in support of ubiquitous connectivity, solving large-dimensional search problems, such as cooperative multicell processing in areas of high user density - such as airports, train stations, and densely-populated metropolitan areas - imposes a major challenge. In these scenarios, an accurate estimation of every single channel gains is required for performing a coherent detection. However, every time the Doppler frequency is doubled, the pilot overhead used for sampling the channel's complex-valued envelope also has to be doubled. Consequently, both the pilot overhead and the detection complexity escalate rapidly as the Doppler frequency increases. Hence, a differentially encoded modulation scheme relying on non-coherent detection constitutes an attractive design alternative, since it may be invoked for mitigating the pilot overhead required for channel estimation, albeit naturally, at the cost of some performance erosion. As a beneficial solution, quantum-search-aided multiple-symbol differential detection may be employed for matching the performance of the classical full-search-based multiple-symbol differential detectors, despite requiring a significantly reduced number of CFEs.

Joint Quantum-Search-Aided Channel Estimation and Data Detection [18]. Joint channel estimation and multi-user detection (MUD) is capable of approaching the performance of perfect channel estimation by iteratively exchanging soft extrinsic information between these two components of the receiver. A quantum-aided repeated-weighted boosting search (QRWBS) algorithm may be readily combined with a quantum-search-aided MUD for performing iterative channel estimation and data detection in the uplink of MIMO-aided orthogonal frequency-division multiplexing (OFDM) systems. As an additional benefit, this powerful system is capable of operating in rank-deficient scenarios, where the number of receive antenna elements (AEs) at the base station (BS) is lower than the number of users transmitting in the uplink. Furthermore, the QRWBS-based channel estimation is capable of outperforming its classical counterpart, despite requiring a substantially lower number of CFEs, which is an explicit benefit of invoking iterative information exchange between the MUD, the channel estimator, and the channel decoders at the BS's receiver.

Quantum-Search-Aided Localization [19]. For various compelling applications of the next-generation communication technology - as exemplified by assisted living and the assignment of users to radio-frequency (RF) as well as to visible light communication (VLC) and narrow-beam millimeter-wave (mm-Wave) access points - the position of the users has to be accurately estimated. Furthermore, indoor localization may be used for creating new applications, such as personalized marketing and shopping experience. Therefore, there is a mutually beneficial relationship in the development of indoor localization, VLC, as well as mm-Wave and THz systems. However, the computational complexity of carrying out full-search based finger-printing based localization for numerous VLC-based and mm-Wave-based localization may become excessive. This is because it requires the knowledge of the entire room's topology, which has to be partitioned into numerous finely-grained tiles of a virtual grid. In this context, quantum-search-aided localization algorithm may be invoked for achieving the same localization accuracy as the classical full-search-based solution at substantially reduced number of CFEs.

Suffice to say in conclusion of this section that many more attractive applications can be found in the literature and some others are yet to be discovered. Quantum technology has opened new avenues for solving problems that previously were excessively complex to solve. This gives us the perfect timing to revisit the hitherto unsolved problems of the classical signal processing and communications domain - QSAs might provide the long-awaited answers.

IV. Quantum Decoherence

The gravest challenge in constructing a large-scale quantum computer is how to mitigate the deleterious effects of quantum decoherence, which inevitably affects the results of quantum computation or communication tasks, just like the Brownian motion of electrons imposes the ubiquitous Gaussian noise in the classical receivers. Completely isolating the qubits from any environmental influence is practically impossible, hence the mitigation of these effects is paramount. The deleterious circuit-impairments imposed by quantum decoherence

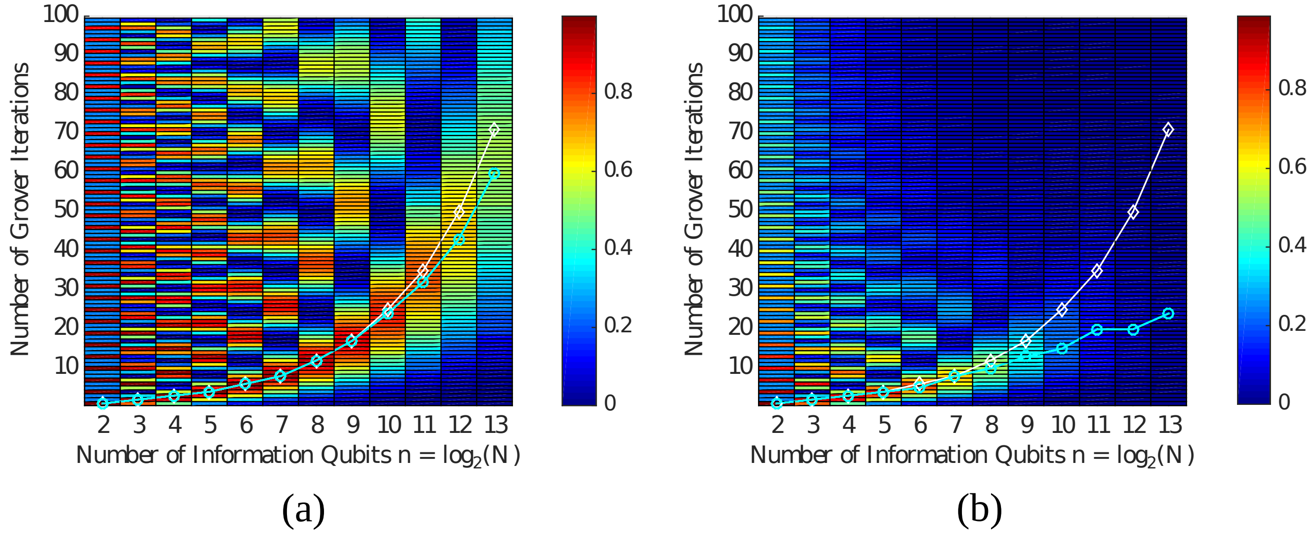


Fig. 4: The color map portraying the success probability of Grover QSA finding the correct solution in the face of quantum depolarizing channel, where the values of the depolarizing probability are given by (a) $p = 10^{-3}$ and (b) $p = 10^{-2}$. The white line represents the scenario of an ideal Grover QSA obtaining the correct solution with a probability of ≈ 1, while the blue line represents the maximum probability values of obtaining the correct solution for imperfect Grover QSA [13].

are typically modeled by the so-called quantum depolarizing 'channel', even though this does not actually entail transmission over a communications channel. After all, the classic Gaussian 'channel' is also a simple abstraction representing the undesired effects of the above-mentioned Brownian motion of electrons. The demonstration of the quantum depolarizing channel effects inflicted on the performance of Grover QSA is portrayed in Fig. 4. Observe from Fig. 4 that as the depolarizing probability increases, the success probability of finding the corrrect solution tends towards $\frac{1}{2^N}$, which is equivalent to the random decisions of the classical full-search-based method operating in the face of an excessively hostile channel. Hence as expected, the advantage of QSAs will erode in the face of excessive quantum decoherence [13].

The employment of quantum error-correction codes (QECC) is one of the most potent design alternatives of mitigating the decoherence. Even though error correction has been shown to perform well in the classical domain, implementing the QECCs imposes its own challenges. Indeed, any error correction procedure - both classical and quantum - depends on attaching redundancy to the information, which will be invoked at the decoder for error correction [20]. In the classical domain, the effect of noise in the encoder and decoder circuitry may be deemed negligible in comparison to the noise inflicted by the transmission channel. However, in the quantum domain both the QECC encoder and decoder circuitry impose more substantial imperfections, which simply cannot be ignored. A further challenge is that we additionally have to deal with the specific quantum-domain phenomenon of error proliferation, because a single quantum-gate error encountered by a quantum encoder may in fact precipitate multiple component errors, rather than simply passing on its input errors without proliferating them. This motivates the design of inherently fault-tolerant quantum computation, which is capable of correcting both the self-inflicted errors imposed by its own encoder and decoder as well as the errors caused by the quantum channel.

V. Challenges and Open Problems

Quantum signal processing relies on delicate quantum particles, such as photons and electrons. Hence, any interaction with the surrounding environment will compromise the integrity of the desired operation. An immeasurable amount of effort has been invested in trying to minimize the presence of decoherence by perfecting the hardware implementation of the qubits as well as by developing sophisticated error correction procedures. Many of the QECC techniques are rooted in their classical counterparts. However, to achieve an excellent error correction performance, long QECC codewords are required, which have to rely on a large number of qubits [20]. The problem with this approach is that at the time of writing most quantum circuits have a shorter coherence time than the time required for carrying out the decoding of long QECCs. Hence, low-complexity yet powerful short codes are required for mitigating the effects of short coherence times.

Another aspect requiring substantial attention is to find meaningful applications, where the unique benefits of quantum computing may be exploited, even if they only have the modest capability of handling just a few hundred qubits [21]. To elaborate a little further, quantum search, factorization, and optimization algorithms tend to require thousands to millions of qubits. Therefore, an intriguing idea is to connect many medium-sized quantum computers with the aid of the Quantum Internet relying on teleportation protocols for creating more powerful quantum computers. Some attractive applications are constituted by the variational quantum eigensolver

(VQE) and the quantum approximate optimization algorithm (QAOA) [22].

Finally, to fully realize the Quantum Internet, a whole suite of quantum computers relying on superconducting, trapped ion, nuclear magnetic resonance, optical, and other technologies have to be benchmarked. Furthermore, the entire gamut of quantum links, such as free space terrestrial, satellite, fiber optic, and other connections will have to be further developed. Similarly, sophisticated protocols, such as for example, routing, multiple access, as well as repeat-and-request solutions will require massive standardization efforts. Indeed, the road to the perfecty secure quantum communications era is inevitably a rocky one, which requires the collaboration of the entire IEEE community. This is why about half-a-dozen IEEE Societies have formed a New Initiative in Quantum Engineering (https://qce.quantum.ieee.org) and the new multi-disciplinary open access journal of quantum engineering (https://quantum.ieee.org/publications). **Valued Colleague, we invite you to join this exhilarating multi-disciplinary journey to solve some of the above-mentioned problems of true frontier-research into Communications v2.0.**

References

[1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, pp. 505–510, 2019; DOI: 10.1038/s41586-019-1666-5

[2] R. Van Meter, K. M. Itoh, and T. D. Ladd, *Architecture-Dependent Execution Time of Shor's Algorithm*, pp. 183–188. World Scientific, 2008, DOI: 10.1142/9789812814623_0029

[3] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, 1984; https://doi.org/10.48550/arXiv.2003.06557

[4] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, vol. 67, no. 6, 1991; DOI:https://doi.org/10.1103/PhysRevLett.67.661

[5] L. Gyongyosi, L. Bacsardi, and S. Imre, "A survey on quantum key distribution," *Infocommunications journal 11 (2), 14-21*, vol. 11, no. 2, pp. 14–21, 2019; DOI: 10.36244/ICJ.2019.2.2

[6] Z. Sun, L. Song, Q. Huang, L. Yin, G. L. Long, J. Lu, and L. Hanzo, "Toward Practical Quantum Secure Direct Communication: A Quantum-Memory-Free Protocol and Code Design," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5778–5792, 2020; DOI: 10.1109/TCOMM.2020.3006201

[7] C. H. Bennett and S. J. Wiesner, "Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States," *Physical Review Letters*, vol. 69, no. 20, 1992; DOI:https://doi.org/10.1103/PhysRevLett.69.2881

[8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," *Physical Review Letters*, vol. 70, no. 13, 1993; DOI:https://doi.org/10.1103/PhysRevLett.70.1895

[9] M. Caleffi, D. Chandra, D. Cuomo, S. Hassanpour, and A. S. Cacciapuoti, "The Rise of the Quantum Internet," *Computer*, vol. 53, no. 6, pp. 67–72, 2020; DOI: 10.1109/MC.2020.2984871

[10] R. Van Meter and S. J. Devitt, "The Path to Scalable Distributed Quantum Computing," *Computer*, vol. 49, no. 9, pp. 31–42, 2016; DOI: 10.1109/MC.2016.291

[11] J. F. Fitzsimons, "Private Quantum Computation: An Introduction to Blind Quantum Computing and Related Protocols," *npj Quantum Information*, vol. 3, no. 1, pp. 1–11, 2017; https://doi.org/10.1038/s41534-017-0025-3

[12] 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, 2018; DOI: 10.1109/COMST.2018.2882385

[13] P. Botsinis, Z. Babar, D. Alanis, D. Chandra, H. V. Nguyen, S. X. Ng, and L. Hanzo, "Quantum Error Correction Protects Quantum Search Algorithms Against Decoherence," *Scientific Reports*, vol. 6, no. 1, pp. 1–13, 2016; DOI: https://doi.org/10.1038/srep38095

[14] 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 2013, Vol. 1; DOI 10.1109/ACCESS.2013.2259536

[15] D Alanis, P Botsinis, Z Babar, H.V. Nguyen, D. Chandra, S-X. Ng. L. Hanzo: A Quantum-Search-Aided Dynamic Programming Framework for Pareto Optimal Routing in Wireless Multihop Networks, IEEE Transactions on Communications, 2018, Vol. 66, Issue 8; DOI: 10.1109/TCOMM.2018.2803068

[16] D Alanis, P Botsinis, Z Babar, H.V. Nguyen, D. Chandra, S-X. Ng. L. Hanzo: Quantum-Aided Multi-Objective Routing Optimization Using Back-Tracing-Aided Dynamic Programming Dimitrios Alanis;Panagiotis Botsinis;Zunaira Babar;Hung Viet Nguyen;Daryus Chandra;Soon Xin Ng;Lajos Hanzo, IEEE Transactions on Vehicular Technology, 2018, Vol. 67, Issue 8; DOI: 10.1109/TVT.2018.2822626

[17] D Alanis, P Botsinis, Z Babar, S-X. Ng. L. Hanzo: Noncoherent Quantum Multiple Symbol Differential Detection for Wireless Systems IEEE Access, 2015, Vol 3; DOI: 10.1109/ACCESS.2015.2432015

[18] D Alanis, P Botsinis, Z Babar, S-X. Ng. L. Hanzo: Joint Quantum-Assisted Channel Estimation and Data Detection IEEE Access, 2016, Vol 4, DOI: 10.1109/ACCESS.2016.2591903

[19] P. Botsinis, D. Alanis, S Feng, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, R Zhang and L. Hanzo, Quantum-Assisted Indoor Localization for Uplink mm-Wave and Downlink Visible Light Communication Systems, IEEE Access, 2017, Vol 5 DOI: 10.1109/ACCESS.2017.2733557

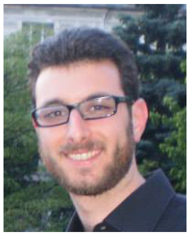
[20] Z. Babar, D. Chandra, H. V. Nguyen, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Duality of Quantum and Classical Error Correction Codes: Design Principles and Examples," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 970–1010, 2018; DOI: https://doi.org/10.5258/SOTON/D0616

[21] J. Preskill, "Quantum Computing in the NISQ Era and Beyond," *Quantum*, vol. 2, no. 79, pp. 1–20, 2018; Doi: https://doi.org/10.22331/q-2018-08-06-79

[22] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. Obrien, "A Variational Eigenvalue Solver on A Photonic Quantum Processor," *Nature Communications*, vol. 5, 2014; DOI: https://doi.org/10.1038/ncomms5213

Daryus Chandra received the B.Eng. and M.Eng. degrees from Universitas Gadjah Mada (UGM), Indonesia, in 2013 and 2014, respectively, and the Ph.D. degree from the University of Southampton, UK, in 2020. Currently, he is a research fellow at the University of Southampton.

Panagiotis Botsinis received the M.Eng. degree from the National Technical University of Athens (NTUA), Greece, in 2010 and the M.Sc. (Hons) and Ph.D. degrees from the University of Southampton, UK, in 2011 and 2015, respectively. Currently, he is a wireless system engineer at Apple Inc., Germany. He is a member of the Technical Chamber of Greece.



Dimitrios Alanis received the M.Eng. degree from the Aristotle University of Thessaloniki, Greece, in 2011 and the M.Sc. and Ph.D. degrees from the University of Southampton in 2012 and 2017, respectively. Currently, he is a wireless system engineer at Apple Inc., Germany.

Zunaira Babar received B.Eng. degree from the National University of Science and Technology (NUST), Pakistan, in 2008, and the M.Sc. (Hons) and Ph.D. degrees from the University of Southampton, UK, in 2011 and 2015, respectively. Currently, she is a senior algorithm engineer at VIAVI Solutions Inc., UK.

Soon Xin Ng (SMIEEE) received the B.Eng. degree (First Class) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, UK, in 1999 and 2002, respectively. Since 2003, he has been an academic staff at the same university and he is currently a Professor of Next Generation Communications.

Lajos Hanzo (FREng, FIEEE) received his doctorate in 1983 and since 1986 he has been with the University of Southampton. He holds honorary doctorates from the Technical University of Budapest (2009) and the University of Edinburgh (2015). He is a Foreign Member of the Hungarian Academy of Sciences.