Guest Editorial Advances in Quantum Communications, Computing, Cryptography, and Sensing

Soon Xin Ng, Andrea Conti, Gui-Lu Long, Peter Muller, Akbar Sayeed, Jinhong Yuan, and Lajos Hanzo

I. Motivation

SEVEN decades after the foundation of classical information theory and the invention of the transistor that launched the digital communication and computing revolutions, we are entering a new era of quantum information science and engineering (QISE). Despite holding its impressive sway for nearly 60 years, the celebrated Moore's law is beginning to hit physical limits, as the ever-shrinking transistor size is making it necessary to account for quantum effects. Concurrently, the growing demand for high-rate processing is imposing unsustainable power and heat dissipation requirements. Thus, there is an urgent need to develop quantum information processing systems that can circumvent the limitations of existing technology.

Quantum computing paradigms have been investigated since the 1980s and foundational advances have shown that harnessing the unique quantum mechanical concepts of superposition and entanglement can lead to capabilities that are beyond the reach of classical systems [1]. Several physical platforms for realizing quantum bits, or qubits, have been explored [2]. One of the most promising technologies relies on superconducting qubits, which is under investigation by D-Wave [3], IBM [4], Google [5], and Rigetti [6], while another is based on trapped ions explored by other groups and startups, such as IonQ [7]. A chip with 1024 qubits, suitable for quantum annealing algorithms, is commercially available from D-Wave, while IBM and Google recently announced their gate-based architectures with 50-100 qubits. Furthermore, the recent launch of the Micius quantum-enabled satellite [8] heralds a major advance in long-range secure quantum communication. Several efforts are aimed at developing quantum networks and at exploiting quantum effects for sensing with unprecedented resolution and sensitivity. These advances also underscore the daunting technical challenges that have to be overcome to realize the full potential of QISE.

A. The Race for Scientific and Technological Leadership in QISE Is On!

Chinese scientists have demonstrated satellite-based quantum entanglement distribution over a record-distance of 1200 km [9]–[11]. The Canadian company D-Wave [3] has sold its quantum annealing computer to both Google and NASA, and Google [5] and Intel [12] are also developing their own quantum computers. IBM's cloud-based quantum computing platform [13] has been made available for collaborative research, and Amazon is beginning to offer clould-based access to quantum computers from Rigetti [6], IonQ [7], and D-Wave [3] through its *Amazon Bracket* program, as part of Amazon Web Service [14]. While there is a rapid evolution in quantum computing technologies, there is a growing realization that building of a fully fault-tolerant universal quantum computer is possibly decades away. At the same time, noisy intermediate-scale quantum (NISQ) technologies are expected to be available in the near future, opening up the possibility of many exciting applications [15].

Given the recent rapid advances in quantum computing, communication, sensing, and related technologies, an intense worldwide interest and competition in QISE is emerging with very substantial investments by governments and industries around the world. For example, the University of New South Wales in Sydney has received a 75 Million Australian Dollar government grant and even larger investments have been made by the Canadian government in the Institute of Quantum Computing at the University of Waterloo. In Europe, the Commissioner for the Digital Economy and Society outlined the plan to launch a 1 Billion Euro Flagship initiative on quantum technology. As part of this momentum, the EU's 34 Million Euro QUANTERA project [16] coordinates the quantum research of 26 countries. The British Government invested 300 Million GBP into the so-called quantum hubs [17]. The U.S. investments in QISE got a major boost recently under the umbrella of the *National Quantum Initiative Act* [18], passed in December 2018 that involves research and coordination across multiple agencies, including the National Science Foundation (NSF), Department of Energy, and the National Institute

The work of Lajos Hanzo was supported in part by the Engineering and Physical Sciences Research Council Projects EP/N004558/1, EP/P034284/1, EP/P034284/1, and EP/P003990/1 (COALESCE), of the Royal Society's Global Challenges Research Fund Grant and in part by the the European Research Council's Advanced Fellow Grant QuantCom. The work of Soon Xin Ng was supported by the Engineering and Physical Sciences Research Council Project EP/L018659/1.

Soon Xin Ng and Lajos Hanzo are with the School of Electronic and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K.

Andrea Conti is with the Department of Engineering and CNIT, University of Ferrara, 44121 Ferrara, Italy.

Gui-Lu Long is with the Department of Physics, Tsinghua University, Beijing 100084, China.

Peter Muller is with IBM Research–Zurich, 8803 Rueschlikon, Switzerland.

Akbar Sayeed is with the Department of Electrical and Computer Engineering, University of Wisconsin–Madison, Madison, WI 53706 USA.

Jinhong Yuan are with the School of Electrical Engineering and Telecommunications, University of New South Wales Sydney, Kensington, 2052 NSW, Australia

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSAC.2020.2973529

of Standards and Technology. In particular, NSF's recent investments in QISE are highlighted by the flagship *Quantum Leap* program [19] including the latest solicitation for the establishment of the *Quantum Leap Challenge Institutes*.

Given the cross-disciplinary nature of challenges in quantum information technology, and the worldwide attention it is enjoying, this is a unique and timely opportunity for the signal processing, communications, information science, and networking communities to get engaged in this emerging research frontier. In this spirit, this special issue is aimed at promoting foundational, algorithmic, and experimental advances in QISE spanning communications, cryptography, computing, and sensing, as well as fostering new avenues for cross-disciplinary research. The topics of interest in the call for papers included, but were not limited to:

- Quantum communications
- Quantum state preparation
- Quantum information theory
- Quantum modulation and coding
- Quantum algorithms and applications
- Quantum key distribution
- Entanglement distillation and purification
- Experimental results and demonstrations
- Prototypes and testbeds
- Quantum networks and architectures
- Quantum secure direct communication
- Modeling and simulation of quantum information processing systems
- Quantum detection and estimation
- Role of entanglement in encoding and decoding of information
- Quantum sensing and measurements

The articles in this special issue address many of these topics and represent complementary contributions towards solving the currently sparsely populated jigsaw puzzle of the opportunities and challenges in QISE. Topically, the articles may be broadly categorized into three groups:

1) quantum channels, coding, and sensing;
2) secure communication and cryptography; and
3) entanglement distribution and quantum networking.

The contributions of the articles in the three groups are briefly summarized in Sections II-IV and the keywords from their abstracts are illustrated in the word cloud in Fig. 1.

Fig. 1. A word cloud representing the frequency of various keywords in the collective titles of the articles in this special issue.

II. Quantum Channels, Coding, and Sensing

The classical work on quantum detection and estimation theory by Helstrom is a very useful and comprehensive reference [20]. A 1998 snapshot of the quantum information theory is captured by [21] in the special issue of the *IEEE Transactions on Information Theory* marking the 50th anniversary of Shannon's seminal work. A gentle introduction to the topics in this section, including the deleterious effects of quantum decoherence, is provided in [22]. An historic perspective on the duality of classical and quantum error correction codes is offered in [23], along with an easy-reading introduction to quantum channels. Quantum error correction adapting to channel characteristics was studied in [24]. The use of non-classical quantum states for quantum pulse position modulation was explored in [25]. Let us now briefly review the contributions that fall into this category.

A. Discrete Weyl Channels With Markovian Memory

Rehman *et al.* address the problem of calculating the capacity of the quantum discrete Weyl channel in the presence of correlated noise across multiple channel uses. This study is motivated by the analytical intractability of the Holevo bound for general quantum channels. The authors succeeded in generalizing specific instances of discrete Weyl channels, which exhibit the unique behavior that the optimal signal states transition from a product state to a maximally entangled state as the level of channel correlation increases. The authors show that this behavior is true for a general class of discrete Weyl channels in which the product state is optimal in the memoryless case.

B. Transmission of Classical Information Over Noisy Quantum Channels–A Spectrum Approach

In this article, Lindsey analyzes hybrid communication systems in which classical information (bits) is communicated over noisy quantum channels. A two-parameter model for the Quantum Noise-Energy Spectral Density (QN-ESD) is developed using a framework for operator-valued noise processes and the corresponding Quantum Noise-Autocorrelation Function is also characterized. Using this model, three disjoint regions in the electromagnetic spectrum are characterized whose boundaries are determined by two frequency dependent design parameters. The first region (below 62.5 GHz) represents the classical communication regime with symmetric QN-ESD. The other two regions represent a transition classical-to-electro-optical communication regime (from 62.5 GHz to 62.5 THz), and the optical communications regime (above 62.5 THz), and exhibit noticeable QN-ESD asymetries in frequency. Channel capacities in the three regions are quantified using various metrics, including bits/photon and bits/s. The results enable optimizing quantum communication techniques for optical links.

C. Channel Coding of a Quantum Measurement

In this article, Kechrimparis *et al.* address the problem of preserving the optimality of a quantum measurement by viewing it as a channel coding problem. Specifically, they consider a measurement over a channel and devise operations to be carried out both before and after transmission over the channel to preserve the optimality of the measurement. A protocol is proposed for preserving a quantum measurement over an arbitrary channel that uses only local operations and classical communication, and yet, in contrast to channel coding, does not require a larger Hilbert space. It is also shown that with the aid of the proposed protocol, a measurement can be preserved both for pairs of qubit states as well as for ensembles of equally probable states. The theoretical results of the article are supported by simulations carried out on the IBM quantum computer.

D. Quantum Data-Syndrome Codes

The success of quantum error correction in terms of protecting quantum states directly depends on the reliability of the measured error syndromes. Ashikhmin *et al.* address how to obtain reliable error syndromes using imperfect physical circuits. In particular, the so-called syndrome measurement and quantum data-syndrome codes are proposed for making the syndrome of quantum stabilizer codes robust against measurement errors. The syndrome measurement codes protect the syndromes with the aid of linearly dependent redundant stabilizer measurements. As a further innovation, the data-syndrome codes generalize this idea for simultaneous correction of both the data qubits and syndrome bit errors. It is demonstrated that if the stabilizers of a code have a small spread of weights, then the syndrome measurement codes attain a substantial performance gain over the repeated syndrome measurement approach. An upper bound for the minimum distance of the codes is derived. Finally, the authors propose a family of Calderbank-Steane-Shor type quantum data-syndrome codes based on classical cyclic codes, which include the classical Steane code and the quantum Golay code.

E. Use of CdTe Quantum Dots as Heat Resistant Temperature Sensor for Bearing Rotating Elements Monitoring

Zhang *et al.* argue that in recent years, quantum dot (QD) based temperature sensors and noncontact thermal monitoring methods using CdTe QDs as the temperature sensor have attracted widespread attention due to their many advantages, such as high accuracy, wide measurement range, high resolution and good dynamic response. The authors present a study on the thermal monitoring of bearings rotating by a QD-based sensor under the extreme conditions of high temperature. For practical realization, a temperature measurement technology for QDs is proposed for improved sensor performance. Specifically, to improve the performance of QDs, the influence of their preparation process on the temperature-dependent photoluminescence spectra of CdTe QDs is investigated. The fluorescence intensity and the highest tolerable temperature of CdTe QDs are optimized by controlling the preparation process. The authors optimize the QD sensor synthesis process to yield highly stable QD-based sensors. A pair of techniques are proposed and compared for incorporating the QDs in both inorganic and in organic polymers. Using a rolling bearing experimental rig, it is demonstrated that the temperature of the bearing cage at different rotation speeds can be accurately captured by using the proposed QD sensor.

III. Secure Communication and Cryptography

One of the most well-established applications of QISE, even beginning to see commercialization, is Quantum Key Distribution (QKD), which is capable of supporting perfectly secure communications by establishing private random cryptographic keys between a pair of users. One of the most well-known implementation of QKD, often referred to as discrete variable QKD (DV-QKD) relies on mapping the bits of the secret key on the detection of single photons. Continuous-variable QKD (CV-QKD) protocols, such as the Gaussian-modulated technique proposed by Grosshans and Grangier in 2002, constitutes an alternative QKD implementation, which relies on employing coherent communication techniques and maps the bits of the secret key onto the (continuous-valued) quadrature components of an optical field. Given its specific characteristics, CV-QKD is generally suitable for relatively short distances over low-loss links. On the other hand, DV-QKD is more robust, hence it is more suitable for longer distances. The research and development of QKD technology has greatly accelerated since the recent demonstration of satellite-based QKD over a distance of 1200 km by Chinese scientists from the University of Science and Technology (USTC) in Hefei [9]. Similar reports have also emerged from Russia. An easy-reading tutorial and predictive outlook on continuous-valued QKD may be found in [26]. The secure key throughput of QKD protocols with intermittent relays was studied in [27].

A. Fundamental Limits of Quantum-Secure Covert Communication Over Bosonic Channels

In this article, Bullock *et al.* consider the fundamental limits of quantum-secure covert communication over a thermal noise bosonic channel, where the adversary also has quantum-mechanical capabilities. Specifically, they derive an explicit expression for quantifying the constant in the square root law (SRL) which governs the fundamental limit of quantum-secure communications. The authors also show that coherent binary phase shift keying, which succeeds in achieving the Holevo bound in the con-covert scenario of the low signal-to-noise ratio regime, is actually sub-optimal in the covert case. On the other hand, coherent quadrature phase shift keying achieves the optimal value of the constant derived in the article.

B. Terahertz Quantum Cryptography

In this article, Ottaviani *et al.* analyze the potential and performance of secure QKD in Terahertz (THz) communication links. Specifically, the achievable secret key rates are derived under realistic attacks. Based on their results the authors argue that in the 0.1–1-THz range the critical impairment tends to be

the thermal noise, whereas at higher frequencies spanning the 1–50-THz range the critical impairment is atmospheric absorption. They also outline a potential hardware implementation of the proposed THz QKD schemes.

C. Quantum Fingerprinting Over AWGN Channels With Power-Limited Optical Signals

In this article, Lipka *et al.* consider the problem of quantum fingerprinting, which can be used for generating secret keys for secure communication, in the practically relevant regime of extremely low power (less than one photon per unit time and unit bandwidth) and unlimited bandwidth in optical channels with additive white Gaussian noise (AWGN). The authors identify a specific noise parameter, which allows them to separate a near-noiseless fingerprinting regime from a noise-contaminated one, where the impact of AWGN is significant. In the latter noise-limited scenario, the results of the article demonstrate the advantages of quantum fingerprinting over classical methods.

D. Discrete-Modulation Continuous-Variable Quantum Key Distribution Enhanced by Quantum Scissors

Recent advances have shown that the so-called quantum scissors acting as non-deterministic amplifiers are capable of enhancing the performance of Gaussian-modulated CV-QKD in long-distance operation, even in the face of unfriendly propagation scenarios. In this article, Ghalaii *et al.* study the rate-versus-distance behavior of a discrete-modulation based CV-QKD system that uses quantum scissors at its receiver. This work also extends the applicability of quantum scissors to quantum repeaters by supporting a non-Gaussian CV-QKD protocol relying on discrete modulation schemes. A realistic analysis considering a non-deterministic linear amplifier at the receiver, along with a physical realization of the non-deterministic linear amplifier, is used for assessing the practicality of the proposed repeater setups. The results show that the use of quantum scissors in the receiver of the proposed discrete modulation CV-QKD protocols can succeed in achieving adequate secret key rates even in the face of unfriendly propagation scenarios.

E. Error Tolerance Bound in QKD-Based Quantum Private Query

Recognizing that QKD protocols are extremely sensitive to channel-induced impairments, in this contribution, Wei *et al.* propose a practical protocol which is capable of operating in the face of realistic noisy channels while still protecting the privacy of both communicating parties. An upper bound on the attainable error resilience is also obtained while striking a compelling trade-off among the conflicting design objectives of reliability, database security, and user privacy.

IV. Entanglement Distribution and Quantum Networking

Quantum networking is an emerging field for exploiting the unique properties of quantum mechanics to support end-to-end generation of entangled quantum states across distant nodes in a network [28]. In quantum communication networks, the transmission of long-distance, long-lived entanglement remains an open technical challenge. A key problem is overcoming the losses in the physical transmission links. One option for establishing long distance quantum communication is to construct a chain of intermediate quantum repeater nodes between the source and destination. Furthermore, sophisticated quantum repeater protocols need to be developed for mitigating the errors introduced by the channels, which may be partly addressed through quantum error correction codes. In the absence of coding, the losses may be dealt with by heralded entanglement generation, while the error probability may be reduced by entanglement distillation (see e.g., [29]). Despite all these potential approaches, practical realization of quantum repeaters remains an open technical challenge.

In light of the substantial advances in classical network coding, a natural question is whether the quantum version of network coding does exist at all? Since cloning of quantum bits is impossible due to fundamental laws of quantum mechanics, the very existence of quantum network coding (QNC) was questioned in [30]. However, further studies of QNC have shown that, given the availability of extra resources such as pre-shared entanglement [31]–[38] or the abundance of low-cost classical communications [30], [39]–[42], QNC is feasible. Nonetheless, there are numerous questions and a paucity of answers in quantum networking. The following contributions in this special issue advance the state-of-the-art of global entanglement distribution and quantum networking.

A. Global Entanglement Distribution With Multi-Mode Non-Gaussian Operations

In this article, He *et al.* address the problem of global entanglement distribution in optical quantum communication links using multi-mode non-Gaussian operators. While non-Gaussian operations are known to capable of increasing the level of entanglement, previous studies have been limited to single-mode operation. Specifically, the authors propose a framework for multi-mode photon catalysis and apply it to the problem of continuous variable entanglement distribution in quantum-enabled optical satellite links. They also compare the performance of the multi-mode photon catalysis approach to that of multi-mode photon addition and photon subtraction. Their results show that multi-mode photon catalysis is the superior non-Gaussian operation, regardless of whether it is applied at the transmitter or receiver. However, the performance gain attained depends on the level of squeezing of the initial state in the photon addition scenario and on the channel loss in the photon subtraction case.

B. Optimal Remote Entanglement Distribution

In this article, Dai *et al.* consider the problem of entanglement swapping and distribution in a quantum network. Imperfect quantum repeater nodes are assumed to facilitate the swapping and distribution. The authors propose a protocol for remote entanglement distribution that maximizes the entanglement distribution rate. The network is represented as a graph and the problem of remote entanglement distribution

is formulated as a linear programming problem. A closed-form solution is provided for attaining the maximum entanglement distribution rate for the special case of a homogeneous repeater chain.

C. What Criterion Can We Get From Precise Entanglement Witnesses?

Entanglement constitutes one of the most unique properties of quantum systems and the detection and quantification of entanglement is an important topic in Quantum information theory. A criterion for entanglement detection in two-qubit systems was proposed by Wootters, based on a concurrence metric. In this article, Chen studies the connection between Wootters formula and the concept of matched entanglement witness for a three-qubit system and proposes a generalization of Wootters formula for a four-qubit system.

D. Local Equivalence of Multipartite Entanglement

In this contribution, Qiao *et al.* study a long-standing open problem–the degree of the generators of invariant polynomial rings–which play an important role in characterizing multipartite entanglement. They derive explicit upper bounds on the degree of the generators of invariant polynomial rings, and propose a systematic approach for developing a complete characterization of invariant polynomial rings. Finally, an application of the results to the problem of multipartite entanglement is provided.

E. Quantum Switch for the Quantum Internet: Noiseless Communications Through Noisy Channels

In this article, Caleffi and Cacciapuoti study the role of a quantum switch in quantum networks that enables the propagation of quantum information simultaneously over multiple channels in a quantum superposition. They quantify the performance gain that can be achieved by employing a quantum switch for enhancing the entanglement distribution process during quantum teleportation. Their analysis reveals that, under certain conditions (detailed in the article), through the use of a quantum switch, the quantum teleportation process starts to behave like a noiseless communication process with a probability that increases with the noise level affecting the underlying communication channels under superposition.

F. Self-Testing of Symmetric Three-Qubit States

Due to the essential role played by symmetry in the field of quantum entanglement, it is of high importance to explore the properties of symmetric states. Self-testing refers to a device-independent technique for identifying the state of an uncharacterized quantum device. The information sought entails the number of measurements, the number of outputs for each measurement and the statistics of each measurement. Earlier results on self-testing for multipartite states have remained limited to one or two states. In this article, Li *et al.* propose self-testing schemes for a large family of symmetric three-qubit states.

G. Entanglement Verification in Quantum Networks With Tampered Nodes

In this article, Amoretti and Carretta study the problem of entanglement verification across the quantum memories of any two nodes of a quantum network. Such verification schemes may be used for detecting the presence of attackers that may compromize a node in a network. In particular, two-party Bell pairs stored in the quantum memories of two distant nodes of the quantum network are investigated. Three scenarios are considered in their attack model. In their most disruptive scenario, the attacker is assumed to be capable of completely taking over certain nodes, including their quantum memories. The authors propose a pair of entanglement verification protocols for a quantum network, which are capable of limiting the malicious actions of even the most powerful attackers.

H. Quantum Queuing Delay

In this article, Dai *et al.* propose a tractable model for analyzing the queuing delay of quantum information, which is one of the critical issues in transmitting quantum information across quantum networks. Aiming to be consistent with physical realizations and practical constraints, the authors advocate a model that employs a dynamic programming formalism and accounts for a range of practical aspects, including the finite memory size. Using this model, the authors develop a cognitive-memory-based policy for memory management by characterizing and exploiting specific quantum properties. An upper bound is derived for the average queue length corresponding to the proposed cognitive-memory-based policy. The key result is that the proposed policy is capable of exponentially reducing the average queuing delay as a function of the memory size. The near-optimality of the developed policy is validated by both the theoretical analysis and simulations.

I. Efficient Computation of the Waiting Time and Fidelity in Quantum Repeater Chains

In the contribution, Brand *et al.* aim for fully characterizing the behavior of an important class of entanglement distribution protocols conceived for transmission over repeater chains in a quantum communication network. They propose a pair of efficient algorithms for determining both the generation-time and the fidelity of the first generated entangled pair of nodes in a quantum repeater chain. The first probabilistic algorithm analyzes refined versions of repeater chain protocols, including intermediate entanglement distillation. On the other hand, the second algorithm computes the waiting time distribution and is faster than the first one. In contrast to the exponentially increasing execution time of existing algorithms, the run time of the proposed algorithms increases only polynomially with the number of segments in the chain. This enables the authors to analyze repeater chains of thousands of segments by employing their proof-of-principle implementation. Thus, the proposed techniques may serve as useful practical tools for analyzing large-scale quantum repeater topologies in the design of the future quantum internet.

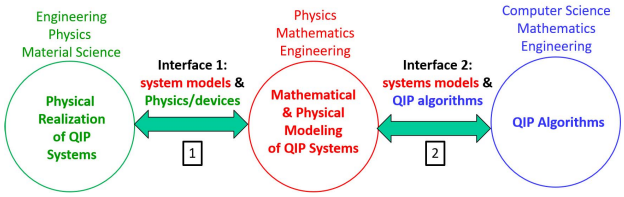

Fig. 2. Cross-disciplinary research challenges and opportunities in QISE.

V. A Glimpse of Open Research Issues and Closing Remarks

Inevitably, the 19 contributions in this special issue only provide a glimpse of the vast body of contemporary debates in the open literature on QISE. There are many outstanding challenges and technical questions that need to be addressed to realize the potential of QISE. The field of QISE is inherently cross-disciplinary in nature drawing on tools from physics, materials science, device engineering, signal processing, communication and information theory, computer science, mathematics, and systems engineering. A conceptual schematic of a quantum information processing (QIP) system is illustrated in Fig. 2 and highlights three components: 1) physical hardware realization; 2) mathematical system model; and 3) QIP techniques and algorithms. Signal processing and communications researchers, the main audience of *IEEE JSAC*, can fruitfully engage in QISE through mathematical modeling of QIP systems and their interactions with physical hardware realizations on the one hand, and the development of QIP algorithms on the other. These pathways are also evident in many of the articles in this special issue and we need to grow the involvement of this research community to accelerate innovation in this exciting research frontier [43].

Some open research issues relevant to the scope of this special issue are briefly discussed below.

- Currently, there is a huge variety of models used by different parts of the QISE research community, that are critically dependant on the envisioned underlying physical implementation. However, there is a paucity of experimentally justified models which would be very useful making the theoretical and simulation-based investigations more realistic. In the context of algorithm development, a promising starting point may be to develop and validate a model for the open-access IBM computer.
- The so-called depolarizing channel model is often used for the design of quantum error correction codes, which captures bit-flips, phase-flips, or both on the qubits. However, there are no widely accepted models for characterizing the errors imposed by other operations, such as quantum gates.
- The availability of experimentally validated channel models would greatly facilitate the design of improved quantum error correction codes, such as powerful topological codes [44]–[46], for enhancing the fidelity of quantum computers and for extending their coherence time. However, these quantum codes need high-fidelity qubits, which are not possible with the low fidelity of currently available quantum computing hardware platforms. Hence the motivation for NISQ computing [15] with current hardware and the need for fully fault-tolerant quantum codes which are capable of avoiding avalanche-like error-proliferation.
- Space-to-ground optical satellite links encounter harsher propagation (due to atmospheric effects) degradation than free-space optical links and optic-fiber links [26]. Thus, space-ground quantum communication using satellites is currently quite immature, despite substantial research efforts [47]–[51].
- Despite their relative maturity, the existing physical realizations of QKD solutions only achieve modest secrete key generation rates that need to be significantly improved. This is due to the probabilistic nature of existing approaches for generating entangled states. Another limitation of the existing QKD protocols is that they require both a classical and a quantum channel. By contrast, the so-called quantum secure direct communication protocol only needs a single channel [52]–[56] and thus deserves further research, especially since it is also potentially capable of dispensing with quantum memory.
- Due to channel degradations, typically there is a mismatch between the secret keys extracted by the communicating parties, which has to be corrected by an appropriate quantum error correction code using the so-called information reconciliation process. However, currently, there is no systematic approach for choosing the most appropriate reconciliation codes and processes.
- The field of CV-QKD has attracted vigorous theoretical research interest [57]–[61], but hitherto no experimental verification has been reported in the open literature.
- The design of quantum secure multi-party quantum networks requires just as much attention, as enhancing the fidelity of quantum hardware. Leveraging mature elements of operational classical-domain networking solutions in the design of quantum communication networks also deserves further attention from the research community.

In closing we note that, despite the promising and spectacular advances in the theory and practice of QISE, there is a healthy degree of skepticism across the research community regarding the future practicality of some of the applications of QISE, especially fully fault-tolerant quantum computers. As the same time, there is a growing realization that while universal quantum computing may be a distant goal, research and technological advances along the way may lead to compelling QISE applications in other areas such as simulation of quantum systems, communications, security, sensing, and metrology. We hope that the readers enjoy the varied contributions in this special issue in this fascinating research area. We invite and encourage our colleagues to contribute their own proposals for growing the community and advancing the state-of-the-art of QISE!

Acknowledgment

The Editors would like to thank all the authors who submitted their valuable contributions to this special issue. They received 63 submissions and were able to accept only

19 of them. The submissions provided both the Reviewers and the Editors with a fascinating snapshot of the range of ongoing research in the area of QISE. They are equally grateful to all the Reviewers, who were very responsive to the repeated reminders about staying on schedule. Their critical comments and suggestions to the authors contributed substantially to the quality of the final product. They are also indebted to Prof. R. Boutaba, the Editor-in-Chief of JSAC, J. Bruttin, and the Senior Editor, Prof. A. Yener, for the encouragement they have provided.

REFERENCES

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[2] G. Popkin, "Quest for qubits," *Science*, vol. 354, no. 6316, pp. 1090–1093, Dec. 2016.
[3] *D-Wave Systems*. Accessed: Feb. 1, 2020. [Online]. Available: https://dwavesys.com
[4] *IBM Quantum Computing*. Accessed: Feb. 1, 2020. [Online]. Available: https://ibm.com/quantum-computing/
[5] *Google Quantum Computing*. Accessed: Feb. 1, 2020. [Online]. Available: https://9to5google.com/guides/quantum-computing/
[6] *Rigetti*. Accessed: Feb. 1, 2020. [Online]. Available: https://www.rigetti.com/
[7] *IonQ*. Accessed: Feb. 1, 2020. [Online]. Available: https://ionq.com/
[8] (Jan. 19, 2018). *Real-World Intercontinental Quantum Communications Enabled By the Micius Satellite*. [Online]. Available: https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html
[9] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, Sep. 2017.
[10] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, Jun. 2017.
[11] J.-G. Ren *et al.*, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, pp. 70–73, Sep. 2017.
[12] *Intel Quantum Computing*. Accessed: Feb. 1, 2020. [Online]. Available: https://www.intel.com/content/www/us/en/research/quantum-computing.html
[13] *IBM Quantum Computing Cloud Platform*. Accessed: Feb. 1, 2020. [Online]. Available: https://quantum-computing.ibm.com/composer
[14] *Amazon Bracket*. Accessed: Feb. 1, 2020. [Online]. Available: https://aws.amazon.com/braket/
[15] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 2018.
[16] *The QUANTERA Project*. Accessed: Feb. 1, 2020. [Online]. Available: https://www.quantera.eu/
[17] *The United Kingdom National Quantum Technologies Programme*. Accessed: Feb. 1, 2020. [Online]. Available: http://uknqt.epsrc.ac.uk/
[18] *The United States National Quantum Initiative Act*. Accessed: Feb. 1, 2020. [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/6227
[19] *The United States National Science Foundation's Quantum Leap Program*. Accessed: Feb. 1, 2020. [Online]. Available: https://www.nsf.gov/news/special reports/big ideas/quantum.jsp
[20] H. P. Yuen, "Quantum detection and estimation theory," *Proc. IEEE*, vol. 66, no. 2, pp. 268–269, Jun. 1978.
[21] C. Bennett and P. Shor, "Quantum information theory," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2724–2741, Oct. 1998.
[22] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum Internet (invited paper)," 2019, *arXiv:1907.06197*. [Online]. Available: http://arxiv.org/abs/1907.06197
[23] Z. Babar *et al.*, "Duality of quantum and classical error correction codes: Design principles and examples," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 970–1010, 1st Quart., 2019.
[24] A. S. Fletcher, P. W. Shor, and M. Z. Win, "Channel-adapted quantum error correction for the amplitude damping channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5705–5718, Dec. 2008.
[25] S. Guerrini, M. Chiani, M. Z. Win, and A. Conti, "Quantum pulse position modulation with photon-added coherent states," in *Proc. IEEE Workshop Quantum Commun. Inf. Technol. (QCIT), Global Telecomm. Conf.*, Waikoloa, HI, USA, Dec. 2019, pp. 1–5.
[26] 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 Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 881–919, 1st Quart., 2019.
[27] S. Guerrini, M. Chiani, and A. Conti, "Secure key throughput of intermittent trusted-relay QKD protocols," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, UAE, Dec. 2018, pp. 1–5.
[28] S. Wehner, D. Elkouss, and R. Hanson, "Quantum Internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, Oct. 2018, Art. no. eaam9288.
[29] L. Ruan, W. Dai, and M. Z. Win, "Adaptive recurrence quantum entanglement distillation for two-Kraus-operator channels," *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 5, May 2018, Art. no. 052332.
[30] D. Leung, J. Oppenheim, and A. Winter, "Quantum network communication—The butterfly and beyond," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3478–3490, Jul. 2010.
[31] M. Mahdian and R. Bayramzadeh, "Perfect K-pair quantum network coding using superconducting qubits," *J. Supercond. Novel Magn.*, vol. 28, no. 2, pp. 345–348, Feb. 2015.
[32] J. Li, X.-B. Chen, G. Xu, Y.-X. Yang, and Z.-P. Li, "Perfect quantum network coding independent of classical network solutions," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 115–118, Feb. 2015.
[33] T. Satoh, K. Ishizaki, S. Nagayama, and R. Van Meter, "Analysis of quantum network coding for realistic repeater networks," *Phys. Rev. A, Gen. Phys.*, vol. 93, no. 3, Mar. 2016, Art. no. 032302.
[34] T. Shang, X.-J. Zhao, and J.-W. Liu, "Quantum network coding based on controlled teleportation," *IEEE Commun. Lett.*, vol. 18, no. 5, pp. 865–868, May 2014.
[35] T. Satoh, F. Le Gall, and H. Imai, "Quantum network coding for quantum repeaters," *Phys. Rev. A, Gen. Phys.*, vol. 86, no. 3, Sep. 2012, Art. no. 032331.
[36] A. Jain, M. Franceschetti, and D. A. Meyer, "On quantum network coding," *J. Math. Phys.*, vol. 52, no. 3, 2011, Art. no. 032201.
[37] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, "From quantum multiplexing to high-performance quantum networking," *Nature Photon.*, vol. 4, no. 11, pp. 792–796, Nov. 2010.
[38] M. Hayashi, "Prior entanglement between senders enables perfect quantum network coding with modification," *Phys. Rev. A, Gen. Phys.*, vol. 76, no. 4, Oct. 2007, Art. no. 040301.
[39] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rotteler, "Constructing quantum network coding schemes from classical nonlinear protocols," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2011, pp. 109–113.
[40] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rotteler, "Perfect quantum network communication protocol based on classical network coding," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2686–2690.
[41] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Roetteler, "General scheme for perfect quantum network coding with free classical communicationn," in *Proc. Int. Colloq. Automat., Lang., Program.*, in Lecture Notes in Computer Science, vol. 5555, 2009, pp. 622–633.
[42] H. V. Nguyen *et al.*, "Towards the quantum Internet: Generalised quantum network coding for large-scale quantum communication networks," *IEEE Access*, vol. 5, pp. 17288–17308, 2017.
[43] A. Sayeed, "From millimeter-wave to quantum communication: A call for cross-disciplinary research and innovation," in *Proc. IEEE Conf. Comput., Netw., Commun. (ICNC)*, Honolu, HI, USA, Feb. 2019, pp. 1–26. [Online]. Available: https://dune.ece.wisc.edu/wp-content/uploads/sites/605/2019/03/icnc2019_final.pdf
[44] D. Chandra, Z. Babar, S. X. Ng, and L. Hanzo, "Near-hashing-bound multiple-rate quantum turbo short-block codes," *IEEE Access*, vol. 7, pp. 52712–52730, 2019.
[45] D. Chandra, Z. Babar, H.-V. Nguyen, D. Alanis, P. Botsinis, S.-X. Ng, and L. Hanzo, "Quantum topological error correction codes are capable of improving the performance of clifford gates," *IEEE Access*, vol. 7, pp. 121501–121529, 2019.
[46] D. Chandra, Z. Babar, H.-V. Nguyen, D. Alanis, P. Botsinis, S.-X. Ng, L. Hanzo, "Quantum topological error correction codes—The classical-to-quantum isomorphism perspective," *IEEE Access*, vol. 6, pp. 13729–13757, 2018.
[47] S. Nauerth *et al.*, "Air-to-ground quantum communication," *Nature Photon.*, vol. 7, no. 5, pp. 382–386, May 2013.
[48] J.-Y. Wang *et al.*, "Direct and full-scale experimental verifications towards ground–satellite quantum key distribution," *Nature Photon.*, vol. 7, no. 5, pp. 387–393, May 2013.
[49] J.-P. Bourgoin *et al.*, "Free-space quantum key distribution to a moving receiver," *Opt. Express*, vol. 23, no. 26, p. 33437, Dec. 2015.
[50] D. E. Bruschi, T. C. Ralph, I. Fuentes, T. Jennewein, and M. Razavi, "Spacetime effects on satellite-based quantum communications," *Phys. Rev. D, Part. Fields*, vol. 90, no. 4, Aug. 2014, Art. no. 045041.
[51] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *NPJ Quantum Inf.*, vol. 3, no. 1, Dec. 2017, Art. no. 30.

[52] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 3, Jul. 2002, Art. no. 032302.
[53] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A, Gen. Phys.*, vol. 69, no. 5, May 2004, Art. no. 052319.
[54] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Phys. Rev. A, Gen. Phys.*, vol. 68, no. 4, Oct. 2003, Art. no. 042317.
[55] C. Zheng and G. Long, "Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs," *Sci. China Phys. Mech. Astron.*, vol. 57, no. 7, pp. 1238–1243, Jul. 2014.
[56] P.-H. Niu, Z.-R. Zhou, Z.-S. Lin, Y.-B. Sheng, L.-G. Yin, and G.-L. Long, "Measurement-device-independent quantum communication without encryption," *Sci. Bull.*, vol. 63, no. 20, pp. 1345–1350, Oct. 2018.
[57] N. Hosseinidehaj and R. Malaney, "Gaussian entanglement distribution via satellite," *Phys. Rev. A, Gen. Phys.*, vol. 91, no. 2, Feb. 2015, Art. no. 022304.
[58] N. Hosseinidehaj and R. Malaney, "Quantum key distribution over combined atmospheric fading channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 7413–7419.
[59] N. Hosseinidehaj and R. Malaney, "Entanglement generation via non-Gaussian transfer over atmospheric fading channels," *Phys. Rev. A, Gen. Phys.*, vol. 92, no. 6, Dec. 2015, Art. no. 062336.
[60] N. Hosseinidehaj and R. Malaney, "CV-MDI quantum key distribution via satellite," *Quantum Inf. Comput.*, vol. 17, pp. 361–379, Mar. 2017.
[61] N. Hosseinidehaj and R. Malaney, "CV-QKD with Gaussian and non-Gaussian entangled states over satellite-based channels," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–7.