AUTHOR QUERIES

AUTHOR PLEASE ANSWER ALL QUERIES

PLEASE NOTE: We cannot accept new source files as corrections for your article. If possible, please annotate the PDF proof we have sent you with your corrections and upload it via the Author Gateway. Alternatively, you may send us your corrections in list format. You may also upload revised graphics via the Author Gateway.

Carefully check the page proofs (and coordinate with all authors); additional changes or updates WILL NOT be accepted after the article is published online/print in its final form. Please check author names and affiliations, funding, as well as the overall article for any errors prior to sending in your author proof corrections.

AQ:1 = Please note that "Sensing and" and "Realities and" were changed to "Sensing, and" and "Realities, and," respectively, in the article title and body text to be in compliance with style guidelines.
AQ:2 = Please confirm or add details for any funding or financial support for the research of this article.
AQ:3 = Please provide the expansions of the acronyms QCS, UKRI, and CENTRIC for your funding agency. Providing the correct acknowledgment will ensure proper credit to the funder.
AQ:4 = Please provide the full current affiliation details (department name, name of university/institution, city, state/country, and zip/postal code) for all the authors.
AQ:5 = Please supply index terms/keywords for your article. To download the IEEE Taxonomy, go to http://www.ieee.org/documents/taxonomy_v101.pdf.
AQ:6 = The abbreviation PQC has been used for the terms "Parameterized quantum circuit" and "Postquantum cryptography." Please confirm which one has to be followed.
AQ:7 = The abbreviation QECC has been used for the terms "Quantum error correction code" and "quantum error correction coding." Please confirm which one has to be followed.
AQ:8 = Please provide the reference number for the author "Gordon Moore" in the sentence "Back in 1965, Gordon Moore hypothesized that the…"
AQ:9 = Please provide the reference number for the author "Richard Feynman" in the sentence "As a further advance, Richard Feynman suggested that the ubiquitous…"
AQ:10 = Please note that Fig. 8 has been processed as Fig. 7 (Continued.) as per style and the remaining figures were renumbered to maintain sequential order. Please check and confirm.
AQ:11 = The in-text citations of "Figs. 9 and 10" are out of order and are not sequential. Fig. 9 should be cited before Fig. 10. Please update in-text citations so that all figures are cited in sequential order.
AQ:12 = Please provide the appropriate section number for the phrases "previous sections, earlier sections, previous subsection, and next subsections."
AQ:13 = Please provide the expansions for the acronyms SWAP, DWDM, QKDP, and 3GPP.
AQ:14 = Please check and validate the sentence "At the core of QML lies the optimization of the free parameter…"
AQ:15 = Please check and validate the sentence "Indeed, one could argue that if E attempts to observe…"
AQ:16 = Please provide the "Conclusion" for this article.
AQ:17 = Please provide the department name for Refs. [29] and [325].
AQ:18 = Please provide the organization name and organization location for Ref. [253].
AQ:19 = Please note that Refs. [293], [338], [358], and [374] are same as [386], [390], [366], and [407], respectively, in your submitted manuscript. Hence, we have deleted Refs. [386], [390], [366], and [407] and have renumbered the subsequent references. This change will also be reflected in the citations present in the body text.
AQ:20 = Please specify the degree names for the author Lajos Hanzo.
AQ:21 = Please provide the location (city, country) for Technical University of Budapest, Edinburgh University, VIAVI Marconi Labs, Quantum Motion Company, and MIT.
AQ:22 = Please provide the city name for National University of Science and Technology, Universitas Gadjah Mada (UGM), Photonic Inc., University of Nis, Tyco Telecommunications, and National Technical University of Athens.
AQ:23 = Please confirm the location (city, country) for University of Cambridge, University of Oxford, University of Bristol, University of the West of England, The University of Arizona, Technical University of Munich, Sharif University of Technology, University of Waterloo, University of Leeds, King's College London, and New Jersey Institute of Technology.
AQ:24 = Please check and confirm whether the year 2017 provided for the author Zhenyu Cai is correct.
AQ:25 = Please provide the year of completion when the author Balint Koczor received the Ph.D. degree.
AQ:26 = Please specify the organization name and location (city, country) where the author Soon Xin Ng was a Postdoctoral Research Fellow.

Quantum Information Processing, Sensing, and Communications: Their Myths, Realities, and Futures

AQ:1

By Lajos Hanzo, *Life Fellow IEEE*, Zunaira Babar, *Senior Member IEEE*, Zhenyu Cai, Daryus Chandra, Ivan B. Djordjevic, *Fellow IEEE*, Balint Koczor, Soon Xin Ng, *Senior Member IEEE*, Mohsen Razavi, and Osvaldo Simeone, *Fellow IEEE*

ABSTRACT | The recent advances in quantum information processing, sensing, and communications are surveyed with the objective of identifying the associated knowledge gaps and formulating a roadmap for their future evolution. Since the operation of quantum systems is prone to the deleterious effects of decoherence, which manifests itself in terms of bit-flips, phase-flips, or both, the pivotal subject of quantum error mitigation is reviewed both in the presence and absence of quantum coding. The state of the art, knowledge gaps, and future evolution of quantum machine learning (QML) are also discussed, followed by a discourse on quantum radar systems and briefly hypothesizing about the feasibility of integrated sensing and communications (ISAC) in the quantum domain (QD). Finally, we conclude with a set of promising future research ideas in the field of ultimately secure quantum communications with the objective of harnessing ideas from the classical communications field.

KEYWORDS | XXXXX.

AQ:5

AQ:2 Received 30 December 2023; revised 27 April 2024; accepted 25 November 2024. The work of Lajos Hanzo was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) Projects under Grant EP/Y037243/1, Grant EP/W016605/1, Grant EP/X01228X/1, Grant EP/Y026721/1, Grant EP/W032635/1, Grant EP/Y037243/1, and Grant EP/X04047X/1; and in part by the European Research Council's Advanced Fellow Grant QuantCom under Grant 789028. The work of Zhenyu Cai was supported in part by the EPSRC QCS Hub under Grant EP/T001062/1; in part by EPSRC Projects Robust and Reliable Quantum Computing (RoaRQ) under Grant EP/W032635/1; in part by Software Enabling Early Quantum Advantage (SEEQA) under Grant EP/Y004655/1; and in part by the Junior Research Fellowship from St John's College, Oxford. The work of Ivan B. Djordjevic was supported in part by the Science and Technology Center New Frontiers of Sound through the National Science Foundation (NSF) under Grant 2242925 and in part by NSF under Grant 2244365. The work of Balint Koczor was supported in part by the University of Oxford for a Glasstone Research Fellowship, in part by Lady Margaret Hall Oxford for a Research Fellowship, in part by UKRI for the Future Leaders Fellowship Project titled Theory to Enable Practical Quantum Advantage under Grant MR/Y015843/1, in part by the EPSRC Projects RoaRQ under Grant EP/W032635/1, and in part by SEEQA under Grant EP/Y004655/1. The work of Osvaldo Simeone was supported in part by the European Union's Horizon Europe Project CENTRIC under Grant 101096379, in part by the Open Fellowship of the EPSRC under Grant EP/W024101/1, and in part by the EPSRC Project under Grant EP/X011852/1. *(Corresponding author: Lajos Hanzo.)*

AQ:3 The authors are with ??? (e-mail: lh@ecs.soton.ac.uk).

AQ:4 Digital Object Identifier 10.1109/JPROC.2024.3510394

NOMENCLATURE

AO	Adaptive optics.
AWGN	Additive white Gaussian noise.
BBS	Balanced beam splitter.
CD	Classical domain.
CDMA	Code division multiple access.
CF	Cost function.
CI	Configuration interaction.
COMP	Cooperative multicell processing.
CPU	Central processing unit.
CSS	Calderbank–Shor–Steane.
CV	Continuous variable.
DFG	Difference frequency generation.
DFRC	Dual-function radar communication.
DV	Discrete variable.
EA	Entanglement-assisted.
EV	Echo verification.

EXIT	Extrinsic information transfer.
FPQTD	Fully parallel quantum turbo decoder.
FSO	Free-space optical.
GRAND	Guessing random additive noise decoding.
HPC	Hypergraph product code.
ISAC	Integrated sensing and communications.
LADAR	Laser detection and ranging.
LDGM	Low-density generator matrix.
LEO	Low Earth orbit.
LPC	Lifted-product code.
LTE	Long-term evolution.
MDI	Measurement-device-independent.
MIMO	Multiple-input multiple-output.
MMD	Maximum mean discrepancy.
MUD	Multiuser detection.
MU-MIMO	Multiuser MIMO.
MUT	Multiuser transmission.
NISC	Near-term intermediate-scale computer.
NISQ	Noisy intermediate scale quantum.
NTN	Nonterrestrial networking.
OFDM	Orthogonal frequency-division multiplexing.
OPA	Optical parametric amplifier.
OPC	Optical phase conjugation.
OSD	Ordered-statistic decoding.
PC	Phase-conjugated.
PCM	Parity-check matrix.
PEC	Probabilistic error cancellation.
PPLN	Periodically poled LiNbO3.
PSCC	Phase-sensitive cross correlation.
PQC	Parameterized quantum circuit.
PQC	Postquantum cryptography.
QAOA	Quantum approximate optimization algorithm.
QBCH	Quantum Bose–Chaudhuri–Hocquenghem.
QBER	Quantum bit error ratio.
QC	Quasi-cyclic.
QCC	Quantum convolutional code.
QCNN	Quantum convolutional neural networks.
QD	Quantum domain.
QEC	Quantum error correction.
QECC	Quantum error-correction code.
QEM	Quantum error mitigation.
QGAN	Quantum generative adversarial network.
QI	Quantum illumination.
QIrCC	Quantum irregular convolutional code.
QKD	Quantum key distribution.
QLDPC	Quantum low-density parity check.
QM	Quantum memory.
QML	Quantum machine learning.
QNC	Quantum network code.
QNN	Quantum neural network.
QPC	Quantum polar code.
QPU	Quantum processor unit.
QRM	Quantum Reed–Muller.
QRS	Quantum Reed–Solomon.
QSBC	Quantum short-block code.
QSC	Quantum stabilizer code.
QSDC	Quantum-secured direct communications.
QTC	Quantum turbo code.
QTECC	Quantum topological error-correction code.
QURC	Quantum unity-rate code.
RF	Radio frequency.
SC	Spatially coupled.
SM	Spatial multiplexing.
SPDC	Spontaneous parametric downconversion.
SNR	Signal-to-noise ratio.
STC	Space–time code.
SV	Symmetry verification.
TMSV	Two-mode squeezed vacuum.
URLLC	Ultrareliable low-latency communication.
VL	Visible light.
WDM	Wavelength-division multiplexing.
VQE	Variational quantum eigensolver.
ZNE	Zero-noise extrapolation.

I. INTRODUCTION

Back in 1965, Gordon Moore hypothesized that the integration density of microelectronics chips would be doubled every 18 months or so and—perhaps somewhat surprisingly—this prediction has remained valid ever since. As a result, at the time of writing, the integration density of chips has reached nanometer scales; hence, the quantum effects may no longer be ignored by chip designers. As a further advance, Richard Feynman suggested that the ubiquitous bits conveying digital information could, in fact, be mapped not only to a pair of distinct voltage levels, but also either to a pair of different electron charges or to the up- and down-oriented spin of an electron for QD information processing. Naturally, this QD representation has its pros and cons because the resultant quantum bits abbreviated as qubits no longer obey the laws of classical physics—instead, they are governed by the laws of quantum physics. What are these?

To elaborate briefly, a qubit may be in the so-called superposition of a logical one and a logical zero. We may be able to interpret this by referring to a coin spinning in a closed box, which might be deemed to be in the equiprobable superposition of head and tail, representing a logical zero and one. Based on these qubits, we may construct arbitrarily long strings of qubits as the operands of quantum information processing. However, when this hypothetical coin stops spinning and we lift the lid of the box, we can reveal/observe the qubit, which will be either in a state of logical zero or logical one. We might say that upon its "observation," the qubits fall back into the CD and they may no longer be "processed or manipulated" in the QD. Another salient QD feature is that the qubits must not be copied, which is formulated in terms of the so-called no-cloning theorem of quantum physics. The qubits may be processed by unitary operators or quantum gates, which are the QD counterparts of classical gates.

A. Applications of QD Information Processing

At the time of writing, the most prominent QD applications are in the field of quantum communications since QKD is already a commercial off-the-shelf reality. By contrast, quantum computing is still in its infancy because the most capable quantum computer commercialized by DWave only handles 2048 qubits.

1) Quantum Information Processing and Its Applications: However, even the powerful quantum computers of the future are not expected to outperform classical computers in all tasks—they are more suitable for carrying out rather specific tasks at a high speed by exploiting their true parallel processing capability. This fact also motivates the design of so-called NISCs, where bespoke quantum circuits are harnessed for evaluating a particularly demanding CF, and the results are then fed into a classical computer for further processing. This might be deemed reminiscent of having a powerful external quantum processor. One of the main impediments of quantum computers is their very limited so-called coherence time, which limits the number of operations/actions that may be carried out before avalanche-like error proliferation sets in. The above-mentioned NISC philosophy mitigates this decoherence problem by forwarding the CF value to a classical computer before catastrophic decoherence occurs. Another potent QD error mitigation technique is constituted by the family of QEC codes (QECCs). The design of these QECs may be deemed to be reminiscent of CD error correction codes, provided that the so-called simplectic conditions exploited in [1], [2], [3], and [4] are satisfied.

When quantum computers capable of running large-scale quantum search algorithms become widely available, numerous large-scale search problems of wireless communications that have hitherto been deemed to have excessive complexity may be solved more efficiently than ever before, as detailed, for example, in [5], [6], and [7]. These may be exemplified by multiple-symbol-based differential detection [8], MUD [8], multiobjective Pareto optimization of large-scale routing problems [9], [10], localization problems [11], as well as network coding solutions [12].

2) Quantum Key Distribution: In the 5G advanced and 6G era, there is more emphasis on information security than ever before. Hence, QKD networks are proliferating at a fast pace, which are capable of providing an extremely high level of information security, because if an eavesdropper (Eve) tampers with the confidential key negotiation protocol, it may be detected with a near-unity probability. Furthermore, as mentioned above, observation of the qubits by an Eve results in destroying the confidential quantum state, and as a result, the qubits collapse back into the CD, as detailed in great depth with the aid of tutorial examples in [14] and [15]. Once the secret key has been negotiated and agreed by the communicating parties, it can be readily applied in a similar way to the classic crypto systems, where in its simplest form, the modulo two connection of the information bits and the key bits are transmitted over the channel. Suffice to say, however, that a severe limitation of this concept is that the secret key has to be at least as long as the data sequence, which represents a 100% security overhead. Furthermore, in the interest of high security, the key has to be changed rather frequently to avoid its potential long-term observation by Eves. However, the most severe limitation of QKD networks is that as the transmission distance is increased, the maximum attainable key rate is reduced due to the attenuation of the channel because the quantum signal must not be amplified. This phenomenon is reminiscent of the reduced bitrate versus distance trend of classical systems. As a remedy, similar to classical systems, so-called trusted relaying may be used for extending the distance, but this trusted relay must be accommodated in protected premises to avoid tampering with them. We note at this stage that given the similarity of the QKD-based and CD encryption procedures, it is becoming realistic to incorporate QKD-based key negotiation in the next-generation (NG) wireless systems.

3) Vision of the Qinternet: At the time of writing, the research of the interdisciplinary subject of quantum science and engineering is attracting substantial investment right across the globe. Many of the IEEE societies—including the Computer, the Communications, Signal Processing, and Antennas and Propagation Society, just to name a few—have joined forces in creating IEEE TRANSACTIONS ON QUANTUM ENGINEERING and also support the recently created conference referred to as the IEEE Quantum Week. Their broad vision is to make the creation of the *quantum Internet* (Qinternet) [16] a reality, which is portrayed in the stylized illustration of Fig. 1. It is expected to support both ultimate information security as well as eavesdropping detection, neither of which is feasible in the classical Internet. Numerous hitherto nonexistent services might be created [17], [18], but "quantum-leaps" are required in quantum engineering to make this vision a reality.

Fig. 2 provides an overview of this article. In Sections II–VI, we embark on critically appraising the state of the art in the critical components of quantum coding, QEM, QML, quantum radar, and QKD along the evolutionary road of creating the Qinternet. Based on this analysis, we then identify the knowledge gaps and speculate about the future roadmap of filling these gaps.

Section II is dedicated to the central topic of mitigating QD impairments by quantum coding, while Section III explores QEM without coding. Section IV puts QML under the magnifier glass, followed by Section V devoted to the radically new quantum radar subject area. Although QKD solutions are now an off-the-shelf commercial reality, numerous open problems exist in architecting the global Qinternet, as discussed in Section VI. Finally, in Section VII, we hypothesize about the next steps along the road leading

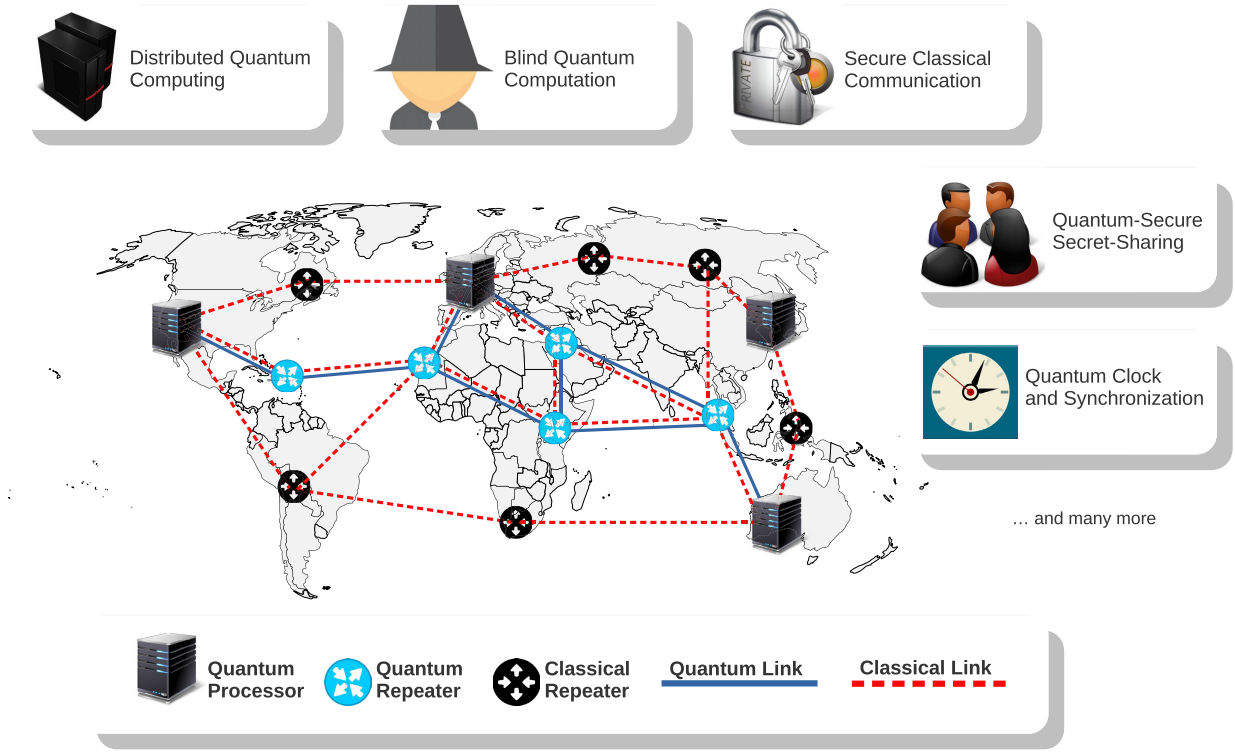

Fig. 1. ***Stylized vision of the Qinternet of the near future, which will rely on a combination of both classical and quantum devices (©Chandra et al. [13]).***

to the construction of an ultimately secure quantum communications system.

Let us now delve into deeper technical details concerning the relationship between classical as well as QEC coding.

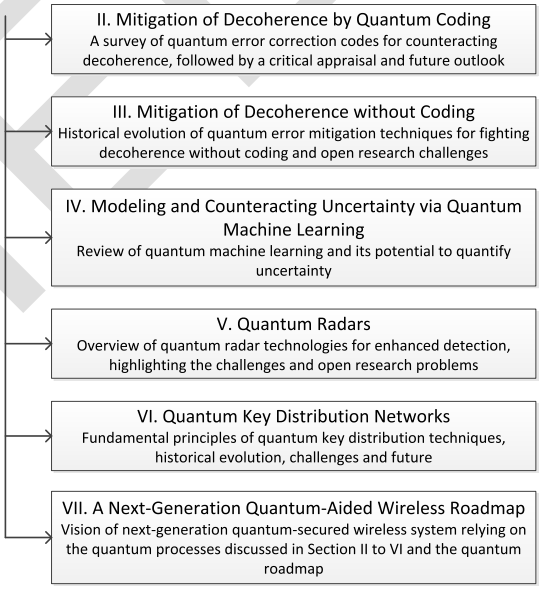

Fig. 2. ***Structure of this article.***

II. MITIGATION OF DECOHERENCE BY QUANTUM CODING

The Myth: Quantum coding is readily capable of eliminating the deleterious effects of quantum decoherence.

The Reality: Only short, low-complexity quantum codes—such as topological codes—may be implemented at the current state of the art, which is unable to approach the ultimate performance limit of the hashing bound.

The Future: The hardware of quantum codes also suffers from decoherence effects, but this is typically assumed to be flawless at this early stage. Future investigations have to incorporate the imperfections of the coding hardware as well.

Abstract: QEC codes (QECCs) can be constructed from the known classical coding paradigm by exploiting the inherent isomorphism between the classical and quantum regimes, while also addressing the challenges imposed by the strange laws of quantum physics. In this spirit, we provide insights into the duality of quantum and classical coding theory, thus aiming to bridge the gap between them. Explicitly, we survey the rich history of both classical as well as quantum codes, followed by a critical appraisal of QECCs, as exemplified by the family of dual-containing and nondual-containing CSS codes, non-CSS codes, and EA codes. Finally, we provide an outlook on the potential evolution of QECCs.

A. State of the Art

The deleterious effects of quantum decoherence can be completely characterized by amplitude-damping and phase-damping channel models. Explicitly, amplitude damping models the loss of qubit energy, for example, when the excited state of a qubit decays due to the spontaneous emission of a photon or when photons are lost during their transmission through an FSO channel or optical fibers [19]. By contrast, phase damping (or dephasing) models the contamination of quantum information without any loss of energy. This may occur, for example, due to the scattering of photons or due to the perturbation of electronic states induced by stray electrical charges. This combined amplitude-damping and phase-damping model of quantum decoherence may be further reduced to a so-called Pauli channel, which merely inflicts bit-flip and/or phase-flip errors upon the qubit. Specifically, a Pauli channel $\mathcal{N}_P$ may inflict a phase-flip (**Z**), a bit-flip (**X**), or a bit-and-phase-flip (**Y**) error with probabilities of p_z, p_x, and p_y, respectively, on a qubit having density matrix ρ, which may be formulated as [20]

$$\mathcal{N}_P(\rho) = (1 - p_z - p_x - p_y)\,\rho + p_z \mathbf{Z}\rho\mathbf{Z} + p_x \mathbf{X}\rho\mathbf{X} + p_y \mathbf{Y}\rho\mathbf{Y}. \tag{1}$$

The error probabilities p_z, p_x, and p_y depend on the qubit relaxation time T_1 and the qubit dephasing time T_2, as given in the following:

$$\begin{aligned} p_x = p_y &= \frac{1}{4}\left(1 - e^{-t/T_1}\right) \\ p_z &= \frac{1}{4}\left(1 + e^{-t/T_1} - 2e^{-t/T_2}\right). \end{aligned} \tag{2}$$

T_1 is the time it takes for the excited state to decay to the ground state, while T_2 is the time for which the superimposed quantum state is maintained. Both T_1 and T_2 times vary with the qubit implementation technology (e.g., superconducting, trapped ion, and quantum dot) because they depend on the properties of the material and the associated environmental interaction mechanisms.

This Pauli channel may also be viewed as the QD counterpart of a quaternary classical channel. The Pauli channel is also often represented as a pair of independent channels, namely, the bit-flip and phase-flip channels, inflicting errors with probabilities $(p_x + p_y)$ and $(p_z + p_y)$, respectively. These individual bit-flip and phase-flip channels are analogous to classical binary symmetric channels. Furthermore, a widely used class of Pauli channels—the so-called *depolarizing channel*—assumes that all three types of errors are equally likely, i.e., $(p_z = p_x = p_y)$.

Despite the existence of the abovementioned inherent isomorphism between the quantum and classical channels, the conception of quantum codes was deemed infeasible in the early quantum era. This was partly because of the so-called no-cloning theorem [21], which does not allow the qubits to be copied—they can only be processed by so-called unitary operations to avoid their collapse to the CD. Hence, it was hard to envision how redundancy attached to or imposed on the original information qubits by QEC coding (QECC) could be exploited by the QECC decoder for correcting QD errors caused by decoherence. More explicitly, since the qubits collapse to the CD upon their observation or measurement, QECC decoding poses a challenge. To elaborate, classical decoding processes rely on observing/measuring the received bits. Therefore, correcting qubits without perturbing their coherent superimposed state was considered an infeasible task. However, Shor [22] dispelled these notions in 1995 by conceiving his seminal 9-qubit QECC that is capable of correcting a single-qubit error. This 9-qubit QECC having a coding rate of 1/9 is reminiscent of the classical 1/3-rate 3-bit repetition code, as exemplified in Fig. 3, where one of the 1/3-rate codes is used for correcting a single bit-flip error and the other a phase-flip error.

Inspired by this significant contribution, Calderbank and Shor [24], as well as Steane [25], [26], separately developed a generalized framework for designing quantum codes from binary linear classical codes. This framework laid the foundation of the well-known family of CSS codes, which allows constructing an $[n, k_1 - k_2]$ CSS code from a pair of classical linear block codes $C_1(n, k_1)$ and $C_2(n, k_2)$, provided that $C_2 \subset C_1$. The code C_1 is exploited for bit-flip error correction, while the dual of code C_2, denoted as $C_2^{\perp}$, is used for phase-flip error correction. Hence, the resultant CSS code is capable of correcting t bit-flips and t phase-flips, if both C_1 and $C_2^{\perp}$ can correct t errors in the CD. Furthermore, a specific category of CSS codes known as *dual-containing* CSS codes was introduced, which originates from dual-containing binary codes. In essence, dual-containing CSS codes constitute a distinct subset of CSS codes, where $C_2 = C_1^{\perp}$. Following these principles, Steane [26] used the classical $(7, 4)$ Hamming code to design a single-error correcting $[[7, 1]]$ dual-containing CSS code.

Both dual-containing and nondual-containing CSS codes can be viewed as an amalgam of two independent quantum codes, one for bit-flip and the other for phase-flip correction. Since the bit-flip and phase-flip errors are corrected independently, CSS codes do not fully exploit the redundant qubits. This led to the development of non-CSS codes, such as the optimal 5-qubit quantum code by Laflamme et al. [27] and Bennett et al. [28], representing the shortest possible codeword required for single-qubit error correction.

As a further development, Gottesman [29] formalized the design of quantum codes from the known classical binary and quaternary codes during his Ph.D. by presenting QSCs [30]. Recall that an (n, k) classical linear block code uses an $(n-k)$ by n PCM for computing the error syndrome

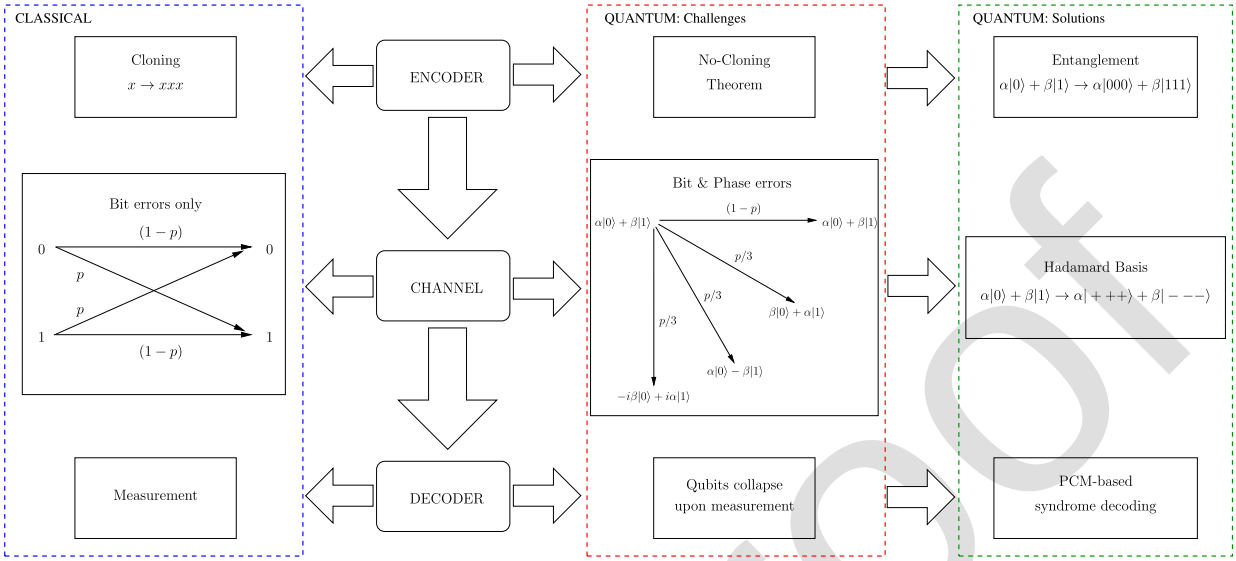

Fig. 3. ***Transition of error correction codes from the classical to the QD [23]. Encoder: Classical encoders replicate the information bits. Since qubits cannot be cloned, quantum encoders exploit entanglement to clone the information in the basis states. Channel: While classical channel incurs only bit errors, qubits may experience bit-flip as well as phase-flip errors. Hadamard basis {$|+\rangle, |-\rangle$} is used to protect against phase errors. Decoder: Classical decoders rely on measuring the received bits. Since qubits collapse upon measurement, quantum decoders invoke PCM-based syndrome decoding for estimating the channel errors without measuring the received qubits.***

of length $(n-k)$.[1] Similarly, an $[[n,k]]$ QSC invokes a set of $(n-k)$ *commuting* Pauli generators $g_i \in \mathcal{G}_n$,[2] called the stabilizers, for computing syndromes. The stabilizers can be linked to a classical PCM by mapping each constituent Pauli operator, i.e., **I**, **X**, **Y**, and **Z**, to a pair of classical bits as follows [31], [32]:

$$\mathbf{I} \rightarrow (0,0)\,,\ \mathbf{X} \rightarrow (0,1)\,,\ \mathbf{Y} \rightarrow (1,1)\,,\ \mathbf{Z} \rightarrow (1,0)\,. \quad (3)$$

Based on this Pauli-to-binary isomorphism, the $(n-k)$ stabilizers of an $[[n,k]]$ QSC can be mapped to an $(n-k)$ by $2n$ PCM $\mathbf{H}$, which consists of two concatenated $(n-k)\times n$ binary matrices $\mathbf{H}_z$ and $\mathbf{H}_x$, as given in the following:

$$\mathbf{H} = (\mathbf{H}_z|\mathbf{H}_x)\,. \quad (4)$$

The matrix $\mathbf{H}_z$ is used for bit-flip error correction, while the matrix $\mathbf{H}_x$ is used for phase-flip error correction. Furthermore, the commutative constraint of stabilizers is translated into the orthogonality of rows of $\mathbf{H}$ with respect to the symplectic product (or the twisted product), which is satisfied for all the rows of $\mathbf{H}$ if and only if we have

$$\mathbf{H}_z\mathbf{H}_x^{\mathrm{T}} + \mathbf{H}_x\mathbf{H}_z^{\mathrm{T}} = 0. \quad (5)$$

Hence, any classical PCM which meets the symplectic product criterion of (5) may be used for designing a QSC. It is pertinent to point out here that when the equivalent classical PCM assumes the following structure:

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}'_z & \mathbf{0} \\ \mathbf{0} & \mathbf{H}'_x \end{pmatrix} \quad (6)$$

where we have

$$\mathbf{H}_z = \begin{pmatrix} \mathbf{H}'_z \\ \mathbf{0} \end{pmatrix}, \quad \mathbf{H}_x = \begin{pmatrix} \mathbf{0} \\ \mathbf{H}'_x \end{pmatrix}$$

then it reduces to a CSS code.

The conception of the above stabilizer formalism marked a major breakthrough in the realm of QECCs, serving as a universal panacea for converting classical codes into their quantum counterparts. Research efforts have remained more focused on the conversion of algebraic codes in the initial years, aiming for maximizing the minimum Hamming distance of legitimate codewords by leveraging finite Galois-field arithmetic. This led to the development of qQBCH codes [33], [34], [35], [36], [37], [38], QRM codes [39], and QRS codes [40]. While leveraging the classical-to-quantum isomorphism has proven valuable in terms of importing classical codes into the

[1] Let $y = \overline{x} + e$ be the received codeword, $\overline{x}$ be the transmitted codeword, and e be the channel error. The classical syndrome of length $(n-k)$ is computed by using: $s = yH^{\mathrm{T}} = \overline{x}H^{\mathrm{T}} + eH^{\mathrm{T}} = eH^{\mathrm{T}}$. This syndrome is then harnessed for either detecting the expected codeword (codeword decoding) or the expected error pattern (error decoding).

[2] The Pauli group $\mathcal{G}_n$ is an n-fold tensor product of single-qubit Pauli operators, i.e., **I** (identity), **X** (bit-flip), **Y** (simultaneous bit-and-phase-flip), and **Z** (phase-flip).

QD, it also became clear that they require a high number of qubits, and thus, their practical employment will only become realistic in years to come.

This realization has inspired expedited research in the field of short-block QECCs, placing the design of QSCs based on the intricacies of quantum topology and homology in the limelight. This includes, for example, toric codes [41], [42], [43], surface codes [44], [45], color codes [46], cubic codes [47], hyperbolic codes [48], [49], and homological product codes [50].

While algebraic coding provides a powerful mechanism for designing codes having a high minimum distance, it does not guarantee a near-capacity design, which requires probabilistic codes. Explicitly, the probabilistic coding avenue is inspired by Shannon's [51] random coding theory and strives for striking a beneficial performance versus complexity tradeoff. The QD counterpart of the famous Shannon capacity is the so-called hashing bound [52], [53], [54], which sets a lower limit on the capacity of Pauli channels. More specifically, analogous to the Shannon capacity of classical binary symmetric channels, the hashing bound specifies the capacity of quantum channels based on the coherent information output of the channel. In the case of a depolarizing channel associated with the probability p, the hashing bound is given by [28], [55]

$$C_Q(p) = 1 - H_2(p) - p\log_2(3) \tag{7}$$

where $H_2(p)$ denotes the binary entropy function. It must be pointed out here that the actual quantum channel capacity is higher than the hashing bound due to the so-called quantum *degeneracy* [56], [57], [58]. This is a unique quantum phenomenon, which is inherently present in QSCs but does not exist in the classical world. To elaborate, quantum degeneracy implies that different channel errors may have the same impact on the encoded quantum state and thus can be corrected by the same error correction operation.[3] This, in turn, enhances the channel capacity.

In duality to the classical probabilistic coding theory, a random quantum code $\mathcal{C}$ having a sufficiently long codeword is expected to incur an arbitrarily low QBER at a depolarizing probability of p, provided that its coding rate is below the hashing limit $C_Q(p)$ of (7). Although having long codewords is not desirable in the QD due to stringent latency requirements arising from the short qubit relaxation and dephasing times, the urge to approach the capacity triggered interest in probabilistic code designs. This led to the development of QLDPC codes [32], [59], [60], [61], QCCs [62], [63], [64], [65], QTCs [66], [67], QIrCCs [23], QPCs [2], [68], and QURC [69]. The performance of some

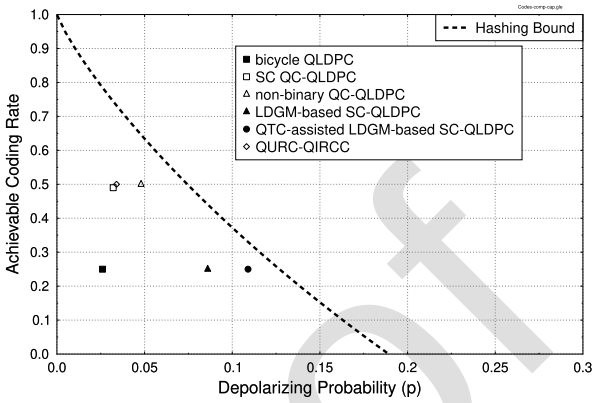

Fig. 4. *Achievable performance at a word error rate (or frame error rate) of 10^{-3} benchmarked against the hashing bound [1] for the "bicycle QLDPC" code ($R = 0.25$ and $n = 19\,014$) of [32], "SC QC-QLDPC" code ($R = 0.49$ and $n = 181\,000$) of [70], "nonbinary QC-QLDPC" code [$R = 0.5$, $n = 20\,560$, and GF(2^{10})] of [71] and [72], "LDGM-based SC-QLDPC" code ($R = 0.25$ and $n = 76\,800$) of [73], "QTC-assisted LDGM-based SC-QLDPC" code ($R = 0.25$ and $n = 821\,760$) of [74], and "QURC concatenated with QIrCC" ($R = 0.5$ and $n = 2000$) of [69].*

of these codes is benchmarked against the hashing bound in Fig. 4.

Recall that classical codes used for designing QSCs must satisfy the stringent symplectic product criterion. This symplectic criterion may sometimes lead to undesirable code properties, such as having short cycles in QLDPC codes, which degrade the decoding performance. Furthermore, not every classical code can be transformed into a quantum code due to the symplectic criterion. For example, there is no quantum counterpart for a family of recursive noncatastrophic convolutional codes used for QTCs. Hence, QTCs tend to exhibit a bounded minimum distance.[4] To circumvent the symplectic product criterion of QSCs, EA quantum codes [75], [76], [77], [78] were conceived, which rely on the availability of preshared entangled qubits. Since these preshared entangled qubits are generally assumed to be transmitted reliably before actual transmission, EA codes are capable of achieving a higher capacity. Fig. 5 shows the comparison of the hashing bound of the maximally entangled[5] EA codes to that of their unassisted counterparts.

An EA code can operate anywhere in the hashing region, which is bounded by the maximally entangled and the unassisted hashing limits. The notion of entanglement-assistance has been extended to nearly all quantum coding families, including EA-QLDPC codes [79], EA-QCCs [80], EA-QTCs [55], [81], and EA-QPCs [82], [83], [84].

[3]Let us consider a two-qubit state $|\psi\rangle = |00\rangle + |11\rangle$. The error patterns **IZ** as well as **ZI** yield the same corrupted state $(|00\rangle - |11\rangle)$, and thus are termed as degenerate errors. Similarly, the error pattern **ZZ** does not perturb the original state $|\psi\rangle$. Hence, the identity operation **II** and the error pattern **ZZ** also constitute a degenerate pair.

[4]If the minimum distance of a concatenated code with an interleaver increases almost linearly with the interleaver length, then it has an unbounded minimum distance.

[5]An EA code may have $0 \leq c \leq (n-k)$ preshared qubits. It reduces to an unassisted code when $c = 0$, while it is called a maximally entangled code when $c = n - k$.

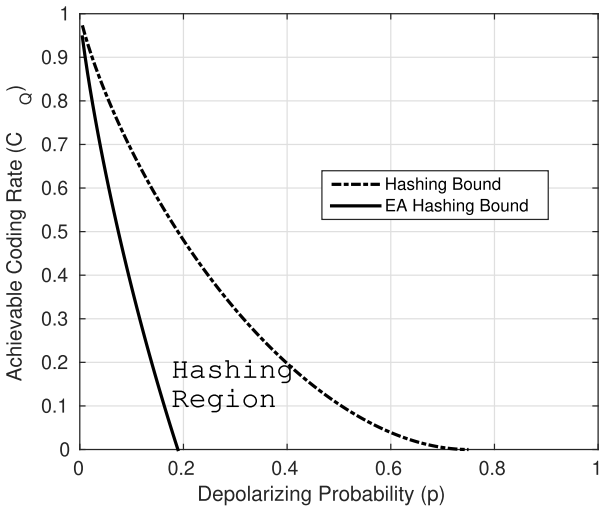

Fig. 5. ***Hashing bounds for the unassisted and maximally entangled quantum codes. The enclosed region, labeled the "hashing region," quantifies the capacity of EA codes with the varying number of preshared entangled qubits, i.e., $0 < c < (n - k)$ [1].***

To conclude this section, Fig. 6 depicts the taxonomy of QSCs based on their binary PCM representations, and Fig. 7 portrays the timeline of historical milestones in the field of QECC.

B. Knowledge Gaps and Challenges

The near-hashing-limit performance can be achieved by utilizing QSCs having a very long codeword. However, with state-of-the-art quantum technologies, the number of qubits that can be used to perform error correction is limited. Thus, finding a family of QSCs that exhibit excellent error-correction capability at short to moderate codeword length and are also efficiently decodable has become a more pivotal problem than ever. In contrast to the CD—where error correction can be implemented using error-free encoding and decoding circuits—the implementation of QSCs must contend with imperfect quantum gates for processing both the information and redundancy qubits. Quantum gates—the fundamental building blocks for quantum circuits—are not yet flawless, and their imperfections tend to introduce more errors during the encoding and decoding processes, potentially corrupting the information they are meant to safeguard. Therefore, the design and the implementation of QSCs have to correct qubit errors imposed both by external gates to be protected by the QECC and also by the gates used in the QECC encoding and decoding processes. This requires the employment of a so-called fault-tolerant approach to QSCs [101], where the encoding and decoding steps are intricately designed to limit the error proliferation within the quantum circuits.

To compound the issue further, qubits inherently suffer from short coherence times, which is the duration of maintaining their uncontaminated quantum state. This imposes a stringent time constraint during which all encoding and decoding algorithms must be completed. In light of this race against time, the fault-tolerant implementation of QSCs must operate within this limited coherence time frame to prevent the degradation of quantum information. If the qubits begin to decohere before the completion of the error correction cycle—encoding, stabilizer measurements, decoding—the information may become irretrievably lost, undermining the very purpose of quantum coding. This necessitates not only *good* QSC constructions for short to moderate codeword lengths, but also the development of reliable encoding and stabilizer measurements—a method to measure the syndrome values of QSCs without collapsing the encoded quantum state—as well as decoding algorithms. These decoders must be capable of high-fidelity operation even in the face of imperfect encoding and stabilizer measurements in order to make correct decoding decisions, thereby preserving the quantum states essential for reliable quantum communications.

Significant advances have been made in the field of code constructions, particularly in developing near-hashing-bound performances using only moderate codeword lengths. A notable development relies on harnessing a quantum-domain unity-rate code (QURC) in conjunction with QIrCCs to create near-hashing-limit QTCs. This approach, detailed in [69], achieves a remarkable error-correction performance without compromising the coding rate or the number of information qubits. A similar strategy that also achieves near-hashing-limit error correction performance is presented in [3] and [4] upon substituting the QIrCCs by QSBCs as the outer codes of this serially concatenated arrangement.

Impressive progress has also been observed in the field of QLDPC codes. For instance, QC QLDPC code constructions having outstanding error-correction performance were proposed in [96], while SC QLDPC codes were designed in [104]. Both these treatises demonstrate near-hashing-limit performance, despite using significantly shorter codewords than the earlier studies in [70], [73], and [105]. Efforts to develop unassisted QPCs began to unfold from [68], which were then formalized in [2]. However, these initial findings suggest

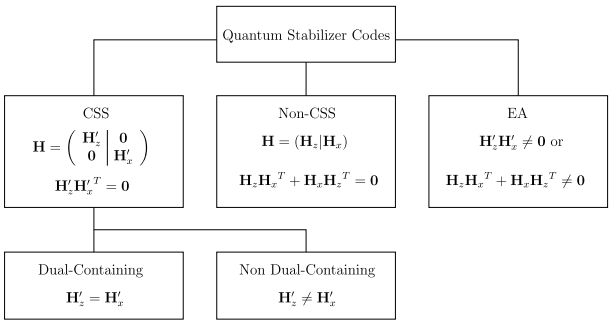

Fig. 6. ***Taxonomy of QSCs based on their binary PCM representations [85].***

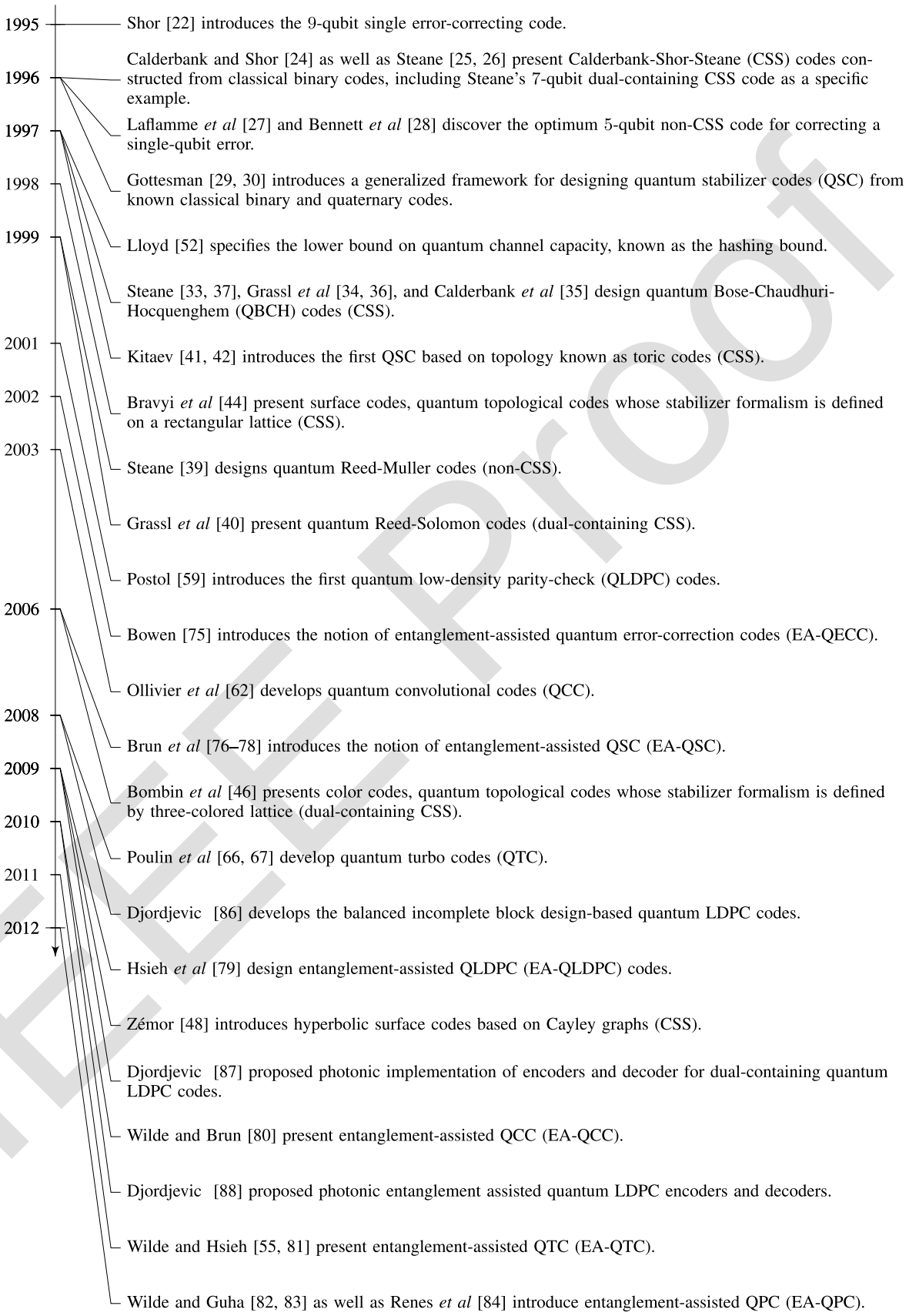

Fig. 7. ***Timeline of QEC codes milestones.***

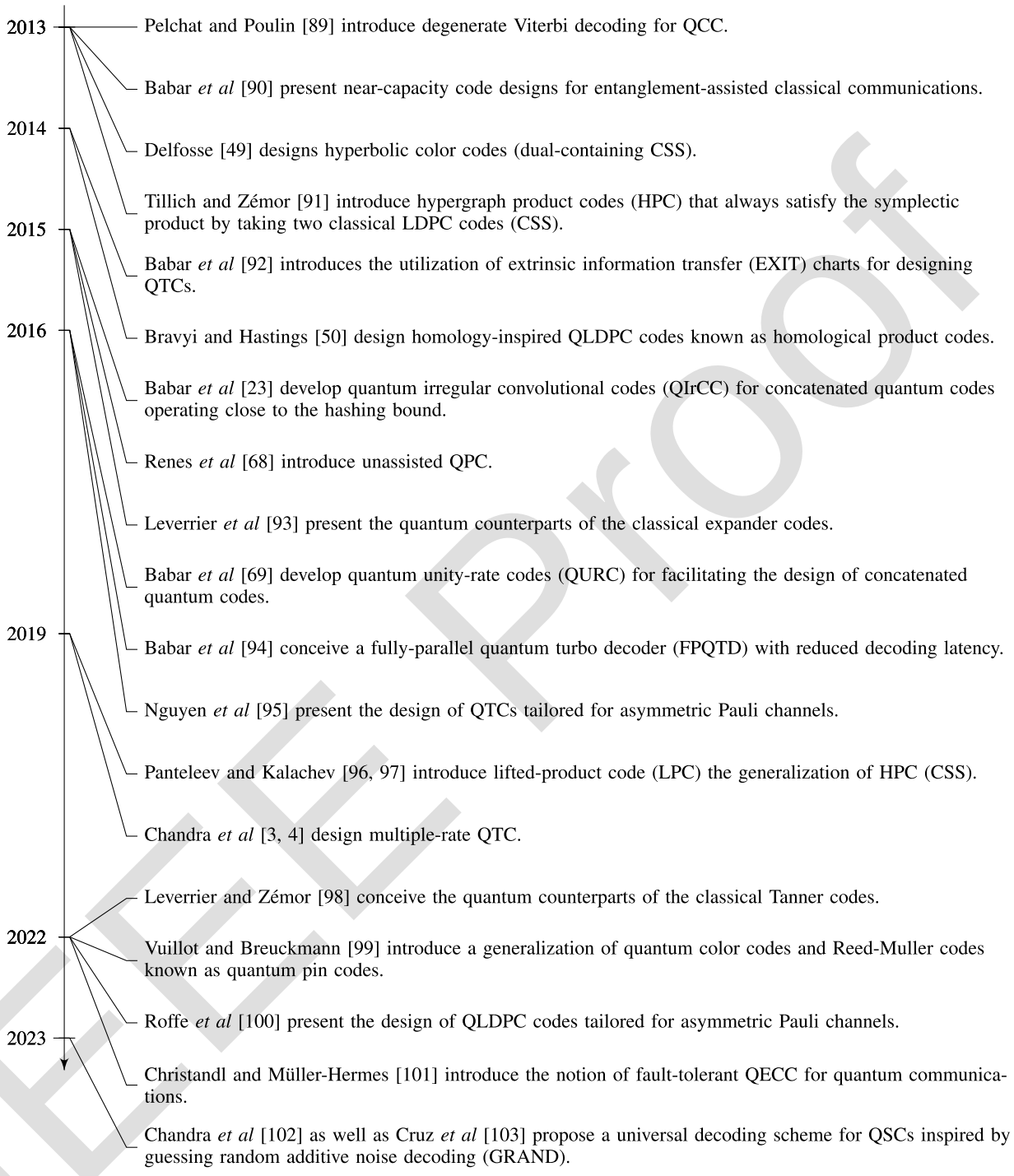

Fig. 7. ***(Continued.) Timeline of QEC codes milestones.***

AQ:10

that QPCs may not perform well for short to moderate codeword lengths [102], [106].

The standard encoding for QSCs as described in [107] and the more specific encoding rules proposed for dual-containing CSS codes and detailed in [32] are inherently not fault-tolerant. This means that a single quantum gate error in the encoder may proliferate the number of errors, in which the QSCs are unable to correct. A fault-tolerant approach to encode information qubits has been demonstrated for the family of QTECCs, which involves performing a round of stabilizer measurements to encode the information qubits, as seen in [108]. However, it remains to be investigated, whether the same approach can result in fault-tolerant encoding for the popular families of probabilistic codes, such as QTCs, QPCs, and QLDPC codes.

In the realm of stabilizer measurements, substantial efforts have been dedicated to designing circuits having inherent capabilities for error detection and, in some cases, error correction, as detailed in [109], [110], and [111]. However, these methods necessitate that the redundant qubits are *encoded*, which, in turn, introduces additional overhead for preparing these fault-tolerant redundant qubits. Consequently, significant efforts have been channeled into minimizing the overhead associated with redundant qubits, while preserving their error detection capabilities [112] or into striking a balance between the overhead and the error-correction/error-detection capabilities of the encoded redundant qubits [113].

Finally, since stabilizer measurements can provide additional error information, it is crucial for the decoder to integrate this information into making an informed correction decision. For QTECCs, the reliability of stabilizer measurements often requires multiple repetitions to enhance confidence in the measured syndrome values, as discussed in [114]. However, it has also been shown that some QLDPC codes inherently possess a *single-shot* property, as described in [115] and [116]. Notable results in QLDPC code construction and decoder pairs that exhibit high single-shot error-correction performance are highlighted in [117], [118], [119], [120], and [121].

C. Research Roadmap

The field of fault-tolerant quantum communications encompasses diverse active research areas, each addressing critical challenges to achieve reliable and scalable quantum communications. Key areas of ongoing research include practical quantum code constructions and real-time decoding.

Creating or discovering a specific set of QSC constructions that are guaranteed to deliver good error-correction performance for various codeword lengths and coding rates is of the essence. At the time of writing, only QTCs have been able to offer this assurance although promising methods of single-shot decoding remain largely unexplored. The preliminary findings pertain only to the application of single-shot decoding on QCCs [122]. Conversely, while some QLDPC codes possess single-shot error correction capabilities, efficient techniques of generating QLDPC codes that maintain good performance across various codeword lengths and coding rates are still unknown.

Another significant factor in the design of QSCs for quantum communications is the time-varying nature of quantum channels [123]. Given that the limited number of qubits in the state-of-the-art quantum technology must be frugally used, taking into account the noise levels or depolarizing probabilities of the quantum channels is crucial. Therefore, the development of adaptive QSCs, which allow their error correction capabilities to be adjusted in response to noise levels, may be expected to lead to more efficient exploitation of the valuable qubits. Preliminary studies indicate the feasibility of designing such adaptive codes within the realms of QTCs [3], [4] and QLDPC codes [124].

To meet the demand for a fast and reliable decoder, enhancements to the speed of cutting-edge decoders can be achieved through parallelization and intelligent scheduling within the state-of-the-art decoding algorithm [94], [125], [126]. Additionally, adopting relatively low-complexity decoding algorithms for short-to-moderate codeword lengths is another avenue that can be explored. This path has been recently considered in classical URLLC, as demonstrated in [127], by investigating the potential of OSD [128], [129] and GRAND [130]. In the QD, the use of OSD has been explored primarily as a postprocessing tool in [96], rather than as a standalone decoder. On the other hand, the first studies of GRAND as a standalone decoder have been disseminated in [102], [103], and [131]. GRAND is often referred to as a universal decoder because it may be readily harnessed for the entire family of the abovementioned CSS codes. Hence, GRAND decoders may be expected to gain popularity and attract further research.

QECCs may also be specifically designed for the amplitude-damping channel, which was investigated by harnessing the popular stabilizer formalism in [132], where improved error recovery operations were conceived as a function of the amplitude-damping probability.

Since the family of QECC schemes has to correct both bit-flips as well as phase-flips, its members tend to have a low coding rate due to requiring numerous redundant bits. An attractive design alternative is to harness sophisticated error mitigation techniques dispensing with QECCs, as detailed in Section III.

III. MITIGATION OF DECOHERENCE WITHOUT CODING

The Myth: The impressive hardware developments of recent years that led to quantum computers in excess of a hundred controllable qubits are already enabling useful applications.

The Reality: Unfortunately current devices are incapable of QEC and uncontrolled errors severely limit the practical applicability of early quantum hardware. Quantum error mitigation is a major enabler in utilizing noisy quantum devices but practical quantum advantage, i.e., the point at which a quantum computer solves a practical problem faster than any classical supercomputer, remains to be demonstrated.

The Future: Further theoretical as well as hardware developments are required but it is anticipated that some form of early practical quantum advantage may be achieved in the near term and the techniques we are about to describe will be absolutely instrumental in this endeavor.

Abstract: Quantum computers are becoming a reality at the time of writing. However, hardware imperfections still overwhelm these devices and fault-tolerant quantum devices relying on QEC codes require substantial hardware developments. Explicitly, a single *logical qubit* may have

to be encoded into a potentially large number of *physical qubits* and one has to harness additional complex measures such as *magic-state distillation* or the constant monitoring of stabilizers—which may be deemed prohibitive with the aid of existing and near-term technology.

The limited number of qubits available in the near term means that we cannot use powerful QECCs for cleaning up all qubit errors. Hence, it is an exciting challenge to find applications without full fault-tolerance using NISQ devices in the near term or early fault-tolerant devices further down the road. To circumvent the limitation of having a low number of qubits, we have to resort to QEM techniques. In this section, we highlight their basic concepts, historic evolution, and open research challenges.

A. State of the Art

1) Scope of QEM: QEM may be viewed as a lower complexity design alternative to the QECCs discussed in Section II, which does not require significant qubit overhead and thus can be implemented already at the time of writing relying on existing quantum devices. However, the significant difference is that, while QECCs spot errors and correct them on the fly to recover the pure quantum states, QEM is unable to correct errors in quantum states. Rather, QEM mitigates the effect of errors on average by measuring the associated expected values through many consecutive activations of a quantum circuit. In particular, in near-term applications, such as in certain QML applications discussed in Section III, one has to repeatedly activate a quantum circuit many times to obtain an accurate estimate of the particular CF, which is often chosen to be the expectation value $\mathrm{tr}[\rho O]$ of some observable O.

We can illustrate this through an example whereby we run a circuit once and measure a qubit which indeed yields an outcome of either $+1$ or -1. Then, the expected value of the Pauli operator $\langle Z\rangle = \mathrm{tr}[\rho_{\mathrm{id}} Z] = p_+ - p_-$ is estimated by repeated activations of the same circuit through the relative frequency $p_\pm$ of the ± 1 outcomes. Even with noise-free qubits, one obtains a distribution for $\langle Z\rangle_{\mathrm{id}}$ whose width is determined by the number of samples N_s as $N_s^{-1/2}$. In a realistic noisy quantum device, however, the center of the distribution is biased $\langle Z\rangle$ as illustrated in Fig. 7 (red arrow versus orange distribution). Again, QEM does not correct errors in the individual circuit runs but rather introduces a new distribution whose bias is reduced [see Fig. 7 (blue distribution)]. However, this comes at the cost that the width of the distribution following error mitigation is increased. Hence, one requires an increased number of samples to get a sufficiently accurate estimate of $\langle Z\rangle_{\mathrm{id}}$. As we discuss in the following, this overhead quantified in terms of the number of samples increases exponentially with the expected number of circuit errors. Nonetheless, this is a tradeoff that is worth making in many practical scenarios: error mitigation techniques may deliver accurate results at reasonable measurement overheads, provided that the expected number of errors in a quantum circuit is not significantly higher than 1.

Indeed the advantage of QEM is that at the current state of the art, it requires drastically reduced quantum resources compared to QECC. Due to the high complexity of QECC, experimental demonstrations have been limited to correcting a single logical qubit in a short codeword, whereas QEM techniques have already been routinely applied in experiments relying on hundred plus qubits. QEM may be viewed as a family of numerous diverse techniques and "tricks," and in the following, we review some of the most popular ones.

2) Zero-Noise Extrapolation: The seminal contributions [133], [134] made the observation that by artificially increasing the error burden on the qubits, one can learn how the QD noise affects the measured expected values and reduce the bias by extrapolating to zero error rates. These constitute the family of ZNE techniques. In particular, by denoting the average number of errors in each circuit run as λ, the output state will be denoted by the density matrix ρ_λ. One then aims for measuring a set of expected values $\langle O_k\rangle = \mathrm{Tr}[\rho_{\lambda_k} O]$ at increased error rates λ_k. Fitting a model—most typically a linear or exponential function [136], [148]—to the graph $\langle O_k\rangle$ versus $\{\lambda_k\}$ allows us to estimate the expected value $\mathrm{Tr}[\rho_{\lambda\to 0} O]$ at zero noise.

Several methods have been developed for artificially boosting the error rates in a controllable fashion. The first of such methods increases the pulse time used for implementing the gates in the circuit [134], which simultaneously exposes the qubits to the decoherence mechanisms for a longer period. This led to the first successful demonstration of QEM in an experiment that achieved accurate measurements of expected values in small-scale systems [140] using linear extrapolation model functions.

Further methods for boosting errors have also been explored, such as inserting sequences of gates and their inverses, which would ideally combine into identity operations, but introduce additional errors due to realistic imperfections [139]. Given that the ZNE techniques are very simple and they do not require any advanced pre- or postprocessing steps, ZNE has become one of the most widely used QEM techniques. In a recent experiment, ZNE was used for demonstrating that it is indeed possible to arrive at an accurate expectation values in a 127-qubit quantum computer, with an accuracy comparable to those of the most advanced classical approximate simulation methods [147].

3) Probabilistic Error Cancellation: Another family of error mitigation techniques relies on a sophisticated Monte Carlo scheme that probabilistically inserts additional gates into each activation of the quantum circuit, so that on average, these additional gates can cancel out the damage inflicted by the errors in the expectation values. These techniques belong to the family of PEC solutions.

This approach was originally introduced in [134]. We can consider the simple example of trying to prepare the ideal state ρ_0, but we end up with the noisy state

$\rho = \mathcal{N}_X(\rho_0) = (1-p)\rho_0 + pX\rho_0 X$, which was corrupted by the bit-flip channel introduced in Section II. We can also express the inverse of this noise process as

$$\rho_0 = \mathcal{N}_X^{-1}\rho = \gamma_1\rho + \gamma_2 X\rho X \tag{8}$$

where we have $\gamma_1 = (1 - p/1 - 2p)$ and $\gamma_2 = -(p/1 - 2p)$. While $\mathcal{N}_X^{-1}$ does not represent a channel that can be physically implemented, we are actually interested in the the expectation value of some observable O as

$$\mathrm{Tr}\left(O\rho_0\right) = \gamma_1 \mathrm{Tr}\left(O\rho\right) + \gamma_2 \mathrm{Tr}\left(OX\rho X\right).$$

The ideal expected value $\mathrm{Tr}(O\rho_0)$ is, thus, simply a linear combination of the expectation value measured in the noisy state ρ and the expectation value measured in the noisy state $X\rho X$ to which we apply an additional X gate.

The corresponding Monte Carlo sampling scheme may be formulated by rewriting the above linear combination as

$$\begin{aligned}\mathrm{Tr}\left(O\rho_0\right) = {} & p_1\left(|\gamma_1| + |\gamma_2|\right)\mathrm{sgn}\left(\gamma_1\right)\mathrm{Tr}\left(O\rho\right) \\ & + p_2\left(|\gamma_1| + |\gamma_2|\right)\mathrm{sgn}\left(\gamma_2\right)\mathrm{Tr}\left(OX\rho X\right).\end{aligned}$$

The above may be interpreted as obtaining the ideal expectation value by activating the original circuit with the probability of $p_1 = (|\gamma_1| / |\gamma_1| + |\gamma_2|)$ and modifying the output with the aid of both the sign $\mathrm{sgn}(\gamma_1)$ and the scaling factor $(|\gamma_1| + |\gamma_2|)$, while the circuit associated with the additional X gate is chosen with the probability of $p_2 = (|\gamma_2| / |\gamma_1| + |\gamma_2|)$ and its output is modified both by the sign $\mathrm{sgn}(\gamma_2)$ and the scaling factor $(|\gamma_1| + |\gamma_2|)$. Hence, we simulate the effect of $\mathcal{N}_X^{-1}$ by probabilistically applying an additional X gate to the circuit while also adjusting the sign of the output accordingly.

The above arguments may be readily extended beyond bit-flip impairments, and they still hold even if the additional gates applied are imperfect [136], provided that we have accurate knowledge of the nature of errors. However, PEC requires full knowledge of the specific form of the channel imposing qubit errors, which are classically intractable for circuits that are applied to a large number of qubits. Hence, in practice, PEC is often directly applied to individual gates in the circuit, whose noise models can be accurately characterized. Instead of completely removing all noise, this approach is only capable of mitigating the deleterious effects of noise contributions. This philosophy may be harnessed for obtaining data points of reduced noise for ZNE, which can be more effective than extrapolating with boosted noise levels [148].

Measurement error mitigation is closely connected to probabilistic error cancellation. At the measurement stage, both the ideal and the noisy output states are transformed into the corresponding noisy and ideal probabilistic distribution of bit strings, respectively, denoted as $\vec{p}_0$ and $\vec{p}_{\mathrm{noi}}$. Hence, the channel representing the impairments simply becomes a stochastic matrix (transition matrix) that transforms the ideal distribution $\vec{p}_0$ into the noisy distribution $\vec{p}_{\mathrm{noi}}$ [149] as

$$\vec{p}_{\mathrm{noi}} = A\vec{p}_0. \tag{9}$$

The effect of noise can, thus, be removed by inverting the transition matrix as $\vec{p}_0 = A^{-1}\vec{p}_{\mathrm{noi}}$ [150]. Similar to PEC, fully characterizing the noise matrix A becomes intractable, as the circuits are scaled up and thus one has to make assumptions concerning the noise model to simplify the form of A. For example, we can assume that the measurement noise corrupting the individual qubits is uncorrelated, which means that the global noise matrix A is simply a tensor product of single-qubit measurement noise matrices.

4) Purification-Based Error Mitigation: The QEM techniques we detailed so far were clearly distinct from QECCs in that they did not introduce any redundant qubits, but rather made use of noisy outputs that were linearly combined in a postprocessing stage. By contrast, purification-based techniques in a way share more similarities with QECCs since they also introduce redundancy—but as we will describe now, the approach only requires a handful of copies of the qubits as opposed to potentially thousands in the case of QECCs.

Recall that a noisy quantum state ρ, which we describe by a density matrix, can be diagonalised to obtain probabilities p_k as eigenvalues and pure states $|\psi_k\rangle$ as eigenvectors. Purification-based techniques commonly exploit that, somewhat surprisingly, the dominant eigenvector $|\psi_1\rangle$ of the density matrix is a good approximation of the noise-free quantum state [152]. Thus, one proceeds by preparing multiple copies of the state as $\rho^{\otimes n}$ [144], [145]. By performing a cyclic permutation operation, or more generally by creating a derangement operation [144], one can guarantee that only permutation-symmetric combinations such as $|\psi_k\rangle^{\otimes n}$ contribute to the measurement process, which happen with probabilities of $(p_k)^n$. Thus, low probabilities are exponentially suppressed. Hence, this technique acts similar to a high-pass filter that passes the dominant component $p_1 \gg p_k$ but drastically attenuates low-probability "error events" associated with $k > 1$ [153].

More specifically, this approach takes n independently prepared copies of the computational state and applies to it a derangement circuit that is controlled by an ancilla qubit, as illustrated in Fig. 9. Measuring the probability of the $|0\rangle$ outcome of the ancilla qubit allows one to formally estimate the expected value [153]

$$\frac{\mathrm{tr}\left[\rho^n\sigma\right]}{\mathrm{tr}\left[\rho^n\right]} = \frac{1}{\sum_{k=1}^{2^N}(p_k)^n}\sum_{k=1}^{2^N}(p_k)^n\langle\psi_k|\sigma|\psi_k\rangle$$

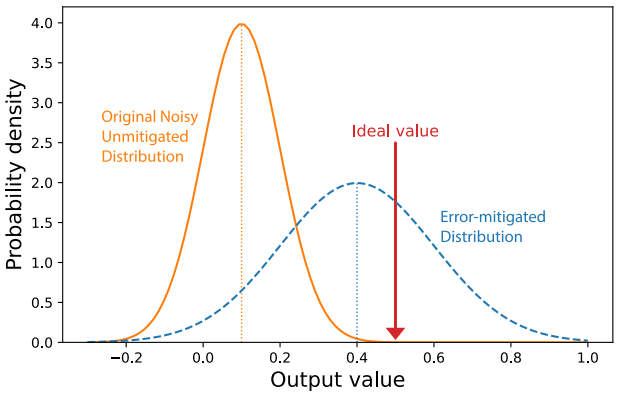

Fig. 8. ***QEM techniques require drastically fewer quantum resources than QEC but are limited to mitigating errors in expected value measurements: even with noise-free qubits, one needs to repeat a quantum circuit many times to obtain an accurate expected value of an observable (red arrow). (Orange distribution) Due to errors affecting the qubits, the expected-value measurement yields a biased distribution (shifted mean) while QEM techniques generally aim to mitigate the effect of errors on average by reducing the bias, i.e., the mean of blue distribution is closer to the ideal value. QEM techniques come at the cost of an increased measurement count, i.e., the width of the blue distribution is larger.***

which indeed gets exponentially close to the desired, "noise-free" expected value $\langle\psi_1|\sigma|\psi_1\rangle$ as we increase n.

This approach has the significant advantages that one does not have to know the noise model of the quantum device and that there are various different ways of physically implementing the derangement operations. As such, many variants have been proposed that explore various tradeoffs. First, the approach was demonstrated in an experiment whereby an array of qubits in Google's Sycamore quantum processor was divided into two halves [146]; the same noisy state preparation circuit was applied to both halves of the qubit array and finally the qubits were measured in the Bell basis—this variant only applies to $n = 2$ copies but forgoes the challenging controlled operations on an ancilla qubit. A similar approach—termed as EV—was also conceived, whereby one does not introduce any redundant qubits, but rather the redundancy is introduced in the time domain by consecutively activating the state preparation circuit and its inverse [146], [154]. Further generalizations have been explored whereby multiple copies are used both in the space and time domains [155].

It was also pointed out that bespoke architectures should be designed for optimally accommodating purification-based techniques [151]. Semiconductor-based qubit technology constitutes a promising platform for cost-effectively manufacturing a multitude of quantum cores on a single chip. Each of these quantum cores could then be used for implementing the same quantum circuits in parallel. One would then apply the derangement operator in a distributed mode through a linking of the separate quantum cores via quantum communication channels. Ion trap quantum computers are similarly promising and indeed entangling operations across the quantum cores have been demonstrated experimentally in [156]. For hardware platforms relying on semiconductor spins and trapped ions, one can also use the pipeline architecture of [157], which allows both for native parallel processing of multiple copies and for transversal operations between the copies, thus dispensing with the space–time overhead associated with the purification-based QEM.

5) Symmetry Verification: In many quantum algorithms, such as in QML applications of Section III, the problem considered exhibits inherent symmetries, which forces symmetry constraints on the target output state. We can exploit these symmetries by performing measurements that verify the symmetry of the output state and thus project the output state to the subspace of correct symmetry [137], [138], [158]. These techniques are quite powerful since they allow us to mitigate all noise sources that break the symmetry of the output state. A simple example is represented by the family of variational algorithms that are used for simulating physical systems. In this context, the Jordan–Wigner encoding simply states that the number of particles corresponds to the Hamming weight of bitstrings modulo a known constant shift. Exploiting this allows us to discard all measurement outcomes of incorrect Hamming weight, which mitigates the effect of quantum impairments.

In practice, Pauli symmetry operators are straightforward to implement, whereby the target output state $|\psi\rangle$ is in the $+1$ subspace of the symmetry operator S via the eigenvalue equation

$$S|\psi\rangle = |\psi\rangle.$$

Non-Pauli symmetry operators can often be transformed into a related Pauli symmetry. For example, instead of measuring the number of particles, we can measure the odd or even parity of this number, which indeed corresponds to the action of a Pauli operator. Then, by performing the measurement of the symmetry operator in a nondestructive way and postselecting the $+1$ outcome, one effectively projects the noisy output state to the subspace of correct symmetry as

$$\rho_{\text{sym}} = \frac{\Pi_S \rho \Pi_S}{\text{Tr}\,(\Pi_S \rho)} \tag{10}$$

where $\Pi_S = (1 + S/2)$ is the projector to the $+1$ subspace of S.

The symmetry operator S is often a global property of the state and thus may be challenging to measure since the measurements in quantum devices are typically related to single qubits. A potential workaround is to transform S into a single-qubit measurement through a basis change (global Clifford circuit) which, however, may be too costly

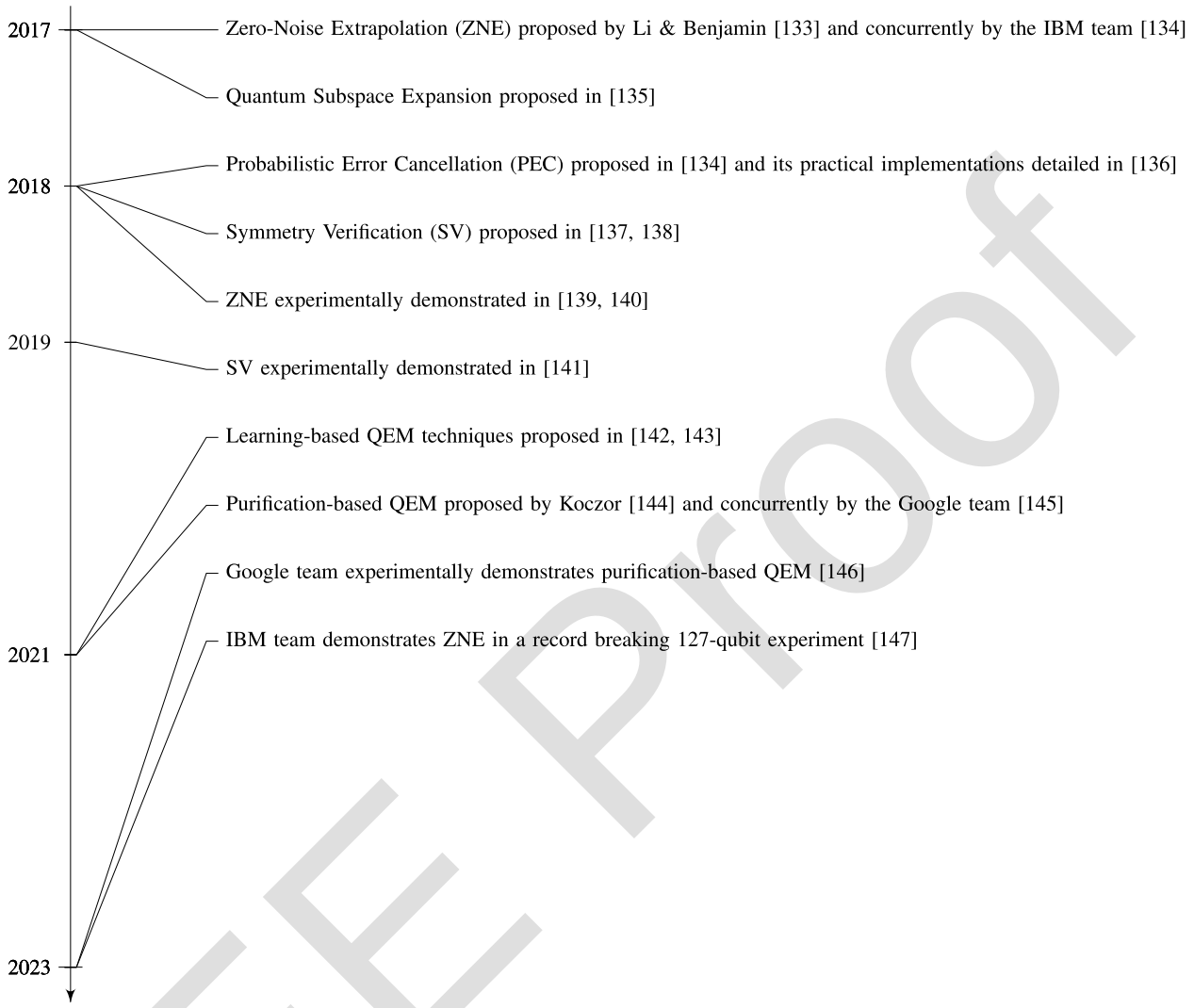

Fig. 9. ***Timeline of QEM milestones.***

to implement in near-term devices. Another design alternative exploits the fact that S is a tensor product of single-qubit Pauli operators $S = \bigotimes_{n=1}^{N} S_n$ that we can directly measure; one then multiplies the individual outcomes to obtain the desired output in postprocessing. Of course, the output state in the individual runs will differ from (10).

Furthermore, one often only cares about obtaining the expectation value of a Pauli observable $O = \bigotimes_{n=1}^{N} O_n$ with respect to the correct symmetries $\mathrm{Tr}(O\rho_{\mathrm{sym}})$, which allows us to further simplify the problem. If O commutes qubitwise with S for each qubit, i.e., we have $[S_n, O_n] = 0$ for all n, then we can simply measure O on the postselected state by measuring all of its constituent single-qubit Paulis $\{O_n\}$ and then multiply the individual outcomes together. As such, performing only local measurements to obtain S and O via postprocessing is effectively equivalent to postselecting the $+1$ outcome of S as long as S and O commute qubitwise and the aim is to estimate the expectation value $\mathrm{Tr}(O\rho_{\mathrm{sym}})$. Given that postselection implies that only a fraction $\mathrm{Tr}(\Pi_S\rho)$ of the circuit runs is retained, i.e., the "useful" circuit runs that pass the test, the sampling overhead of this method depends on $\mathrm{Tr}(\Pi_S\rho)^{-1}$.

On the other hand, if S and O do not commute qubitwise, we rewrite the "symmetrized" expectation value in (10) as

$$\mathrm{Tr}\left(O\rho_{\mathrm{sym}}\right) = \frac{\mathrm{Tr}\left(O\rho\right) + \mathrm{Tr}\left(SO\rho\right) + \mathrm{Tr}\left(OS\rho\right) + \mathrm{Tr}\left(SOS\rho\right)}{2 + 2\mathrm{Tr}\left(S\rho\right)}$$

which can be obtained by postprocessing the expectation values of O, S, SO, OS, and SOS. If both S and O are Pauli strings, then their products are Pauli strings too; thus, the desired expected values can be obtained through single-qubit Pauli measurements and postprocessing, as detailed above. The measurement overhead of this approach then depends on $\mathrm{Tr}(\Pi_S\rho)^{-2}$ [159], [160].

Beyond exploiting the inherent symmetries of the problem, one can similarly exploit symmetries that arise from

encoding particles, such as fermions into qubits [161], [162], [163], [164], or artificially constructed symmetries like parity checks in QECC [165].

6) Quantum Subspace Expansion: The most typical problem in QML—which was the subject of Section III—is to prepare the eigenvector $|\psi_0\rangle$ of a Hamiltonian H matrix of the smallest eigenvalue that is often termed as the ground state. Due to circuit-depth limitations, however, one can only prepare an approximation $|\phi_0\rangle$. In quantum subspace expansion [135], one proceeds by applying a set of operators $\{G_m\}$ to the approximate state. The resultant collection of vectors $\{G_m|\phi_0\rangle\}$ spans a subspace of the full Hilbert space and allows one to efficiently find an improved approximation within this subspace.

A general state within this subspace can be written as $|\psi_{\vec{w}}\rangle = \sum_{m=1}^{M} w_m G_m|\phi_0\rangle$ with the weights $\vec{w}$ chosen for ensuring that we have $\langle\psi_{\vec{w}}|\psi_{\vec{w}}\rangle = 1$. In this way, we can identify the optimal ground state within the subspace by solving

$$\vec{w}^* = \arg\min_{\vec{w}} \langle\psi_{\vec{w}}| H|\psi_{\vec{w}}\rangle \quad \text{s.t. } \langle\psi_{\vec{w}}|\psi_{\vec{w}}\rangle = 1. \tag{11}$$

The above optimization problem can be solved efficiently through defining the matrices

$$\overline{H}_{ij} = \langle\phi_i| H|\phi_j\rangle, \quad \overline{S}_{ij} = \langle\phi_i|\phi_j\rangle \tag{12}$$

and solving $\overline{H}W = \overline{S}WE$ which is often referred to as the generalized eigenvalue equation. The eigenvector in W that corresponds to the lowest eigenvalue in E is the optimal of coefficient vector $\vec{w}^*$ that solves the problem in (11). Given that the approximation prepared by the quantum device $|\phi_0\rangle$ is within the subspace, the optimal ground state $|\psi_{\vec{w}^*}\rangle$ is guaranteed to be an approximation no worse than $|\phi_0\rangle$.

In practice, one proceeds by preparing $|\phi_0\rangle$ with a quantum device and estimates the matrix entries

$$\begin{aligned}\overline{H}_{ij} &= \langle\phi_0| G_i^\dagger H G_j|\phi_0\rangle = \text{Tr}\left[G_i^\dagger H G_j \rho\right] \\ \overline{S}_{ij} &= \langle\phi_0| G_i^\dagger G_j|\phi_0\rangle = \text{Tr}\left[G_i^\dagger G_j \rho\right]\end{aligned} \tag{13}$$

for all i and j. The right-hand sides above define the matrix elements in terms of measurements applied to a density matrix $\rho = |\phi_0\rangle\langle\phi_0|$ and this allows us to generalize the approach to mixed states ρ since the subspace expansion technique may be applied to circuits undergoing stochastic noise [135], [141], [166], [167].

Alluding briefly to the context of quantum chemistry, a possible choice of the expansion operators $\{G_m\}$ is constituted by products of fermionic raising and lowering operators [135] in line with classical CI techniques. Improvements to the ground state can also be achieved by applying powers of H [168] or ρ [169] to the probe state. Furthermore, SV may actually be viewed as a specific instance of subspace expansion using symmetry operators [160], [165], and this can also be further linked to purification-based methods [160].

7) Learning-Based Error Mitigation: As we briefly alluded to in Section III, classical machine learning techniques may be employed for improving error mitigation techniques [142], [143]. In particular, one is typically interested in the expected value at the output $E(\mathbf{C}_0)$ of an ideal circuit $\mathbf{C}_0$, but only has access to the noisy circuit $\mathbf{C}_{\text{noi}}$ and its noisy output expectation $E(\mathbf{C}_{\text{noi}})$. Then, our aim is to estimate a more accurate expected value $f_{\vec{\alpha}}(\mathbf{C}_{\text{noi}})$ through an error mitigation strategy that results in reduced distance from the ideal value formulated as $|f_{\vec{\alpha}}(\mathbf{C}_{\text{noi}}) - E(\mathbf{C}_0)| < |\mathbf{C}_{\text{noi}} - E(\mathbf{C}_0)|$.

However, our model depends on a set of unknown parameters $\vec{\alpha}$, which we can find by training. Thus, one aims for constructing training circuits $\mathbf{T}_0$, which resemble to $\mathbf{C}_0$ in terms of their circuit structure, but can be efficiently simulated classically, i.e., we can readily calculate $E(\mathbf{T}_0)$. We, then, activate the circuit (and any of its variants) on the quantum machine—which individually result in noisy expected values—and feed them to our model. The model is then trained on these noisy expected values in order to find the optimal parameters $\vec{\alpha}^*$, which minimize the distance from the ideal output formulated as $|f_{\vec{\alpha}}(\mathbf{T}_{\text{noi}}) - E(\mathbf{T}_0)|$. Upon applying this optimized model to our circuit of interest, we obtain the desired error-mitigated estimates $f_{\vec{\alpha}^*}(\mathbf{C}_{\text{noi}})$.

The simplest such error-mitigation model employs a scaling and shifting of the noisy expectated value, which is expressed as $f_{\vec{\alpha}}(\mathbf{C}_{\text{noi}}) = \alpha_0 + \alpha_1 E(\mathbf{C}_{\text{noi}})$ [142], [170]. The potential training circuits to use include the family of Clifford gate variants of the original circuit [142], [143] and the so-called free fermion circuits of [171]. One can also introduce parametrized models into other QEM methods and apply learning-based techniques. This has been demonstrated for PEC in order to account for the presence of correlated quantum noise [143].

The historic evolution of QEM is depicted at a glance in Fig. 8, which assists us in identifying the knowledge gaps in Section III-B.

B. Knowledge Gaps and Challenges

We now continue by highlighting some of the open challenges and main limitations of the abovementioned QEM techniques, and we also identify a number of knowledge gaps.

1) Sampling Overhead: Let us now detail the main limitation of QEM, which is the increased variance of the expected values [148], [172], [173], [174], [175]. The average number of errors occurring in the quantum circuit λ—which may also be termed as the circuit fault rate—is roughly the sum of the error rates of all the gates in the circuit. For example, if we have a circuit constructed

from N gates and each gate has an error rate of p, then the circuit fault rate will be $\lambda = Np$. For stochastic errors, the number of errors in the circuit follows a Poisson distribution, for which the probability of ℓ errors occurring is $e^{-\lambda}\lambda^{\ell}/\ell!$. Hence, the fraction of circuit activations that are noiseless ($\ell = 0$) is $e^{-\lambda}$ [148], [172]. We may surmise from this simplified picture that to obtain the same amount of information that is contained in a single noise-free circuit activation, we need approximately $\sim e^{\lambda}$ noisy circuit executions. Clearly, this represents the sampling overhead associated with QEM. However, QEM techniques typically fail to remove all noise contributions; thus, the above argument only applies to the specific fraction of error contributions that we succeed in removing: with λ_{rm} representing the average number of removable errors in the circuit for a given QEM technique, the associated sampling overhead is $\sim e^{\lambda_{\text{rm}}}$, while the effective noise level of the resultant circuit becomes $\lambda - \lambda_{\text{rm}}$.

This illustrates that indeed, in general, *the sampling overhead imposed by QEM grows exponentially with the number of errors in the circuit that is removed by a given QEM technique*. These overheads are usually specified as upper bounds and thus account for worst-case scenarios. However, the actual overhead of some of the most potent error mitigation techniques can be lower [147]. On the other hand, given that the sampling overhead grows exponentially with the circuit size, in contrast to QECC, QEM is not scalable to arbitrary system sizes. Thus, in practice, QEM techniques are applicable in the regime, where the number of removable errors is on the order of $\lambda \approx 1$ or lower. This ensures that the associated sampling overhead remains reasonable.

2) QEM Architectures: Advanced QEM techniques, such as purification-based ones, require multiple copies of the quantum state. As we detailed above, these can be prepared either by splitting a large qubit array into multiple regions or by actually assigning the same quantum circuit to multiple, physically separate quantum processors that are interlinked in the QD [151], [156].

While fascinating progress has been made, improving the quantum communication channels—such as the depolarizing channel characterizing the circuit imperfections, rather than, for example, FSO satellite channels—is an immense engineering challenge. This may require, for example, Bell-pair purification synchronization across multiple quantum cores [151]. However, multicore architectures are likely to deliver value even beyond QEM and may be a substrate for the so-called SWAP test [151], which is an important subroutine for many of the QML algorithms mentioned in Section III. Furthermore, multicore architectures will enable noise-resilient implementations of advanced, gradient-based training algorithms for conceived for QML, such as the quantum natural gradient techniques of [176] and [177].

3) Learning and Controlling Noise Models: The above QEM techniques tend to rely on rather different amounts of knowledge concerning the particular noise contaminating the qubits. For example, PEC requires that one explicitly learns the noise model. By contrast, purification-based techniques are—at least to a first approximation—oblivious to the error model, albeit the efficacy of the derangement circuits depends on the particular noise statistics. This has motivated the community to conceive sophisticated techniques for accurately learning the noise models [178]—some of these techniques were touched upon above. However, as the experiments are scaled up in size and are improved in accuracy, the importance of efficiently, reliably, and accurately learning and controlling the error statistics is becoming ever more crucial. The same is true for the design of potent QECC techniques.

4) Classical Communication Bottleneck: QEM protocols often require extensive classical communication whereby the circuits are frequently recalibrated. For example, PEC requires a new circuit for each activation. As such, at the time of writing, classical communication is one of the main bottlenecks. For example, the actual circuit execution time on some platforms is on the order of microseconds, while updating the circuit description through classical communication requires orders of magnitude more time [147]. Particularly, relevant is the intrinsic drift in the error statistics over time, which necessitates occasional recalibration.

C. Research Roadmap

In this section, we identify a suite of promising future research directions that may be of interest to readers with a background in the broad field of signal processing and machine learning in support of improved quantum computing and communications.

1) Integration With Randomized Measurement Protocols: The above QEM techniques assumed that the expected values are directly measured and then used in classical postprocessing. In recent years, randomized measurement protocols, such as classical shadows, have become an area of active research [179]. Rather than directly estimating the expected values, these techniques apply random measurements to the qubits and store the individual outcomes classically. The collection of these individual measurement outcomes has the fond connotation of a classical shadow and can be used for simultaneously predicting the expected values of many observables in classical postprocessing. Promising early works have shown the benefit of combining these powerful randomized protocols both with QEM [180], [181] and QML [182] techniques.

2) Error-Resilient Algorithms and Protocols: QEM constitutes a pivotal subroutine in near-term quantum algorithms in terms of estimating accurate expected values. However, for certain applications, one can construct bespoke protocols that are by construction resilient to noise.

For example, "quantum supremacy" experiments [183] based on random-circuit sampling techniques are by

construction noise-resilient. The reason for this is that the deep random circuits employed result in local qubit noise reminiscent of white noise, which only trivially affects the expected value measurements. Although practical quantum circuits may exhibit noise characteristics that are significantly different from the global white noise [170], randomized compiling techniques have been shown to be effective in combination with the above linear, learning-based QEM techniques [142], [170].

Another example is shadow spectroscopy, whereby one aims for estimating eigenvalue differences in a Hamiltonian matrix by encoding the eigenvalue differences as periodic signals that are estimated as time-dependent excepted values $S(t) = \mathrm{tr}[O\rho(t)]$ [184]. One can then use established signal processing techniques for estimating the frequencies of the signals in a way that the approach is provably immune to stochastic noise occurring in the corresponding circuits.

3) Exploring Tradeoffs and Combinations of QEM/QECC Techniques: For some application areas, such as training variational circuits, it may be more beneficial to only remove a fraction of noise contributions using QEM in exchange for a reduced measurement overhead. Furthermore, it has been shown that the locality of the observable may crucially affect the measurement overhead [147]. It is, thus, an exciting challenge to further explore nontrivial techniques that might assist in reducing the measurement costs. QEM techniques constitute a suite of diverse "tricks of the trade" and each variant has its own pros and cons; thus, there is immense potential for further improvements by combining different techniques [148], [172], [185], [186].

Going beyond pure QEM, even when QECC can be successfully implemented in experiments, there will still be an extended period of time when the effects of quantum impairments cannot be sufficiently mitigated due to the limited number of qubits. This period is often referred to as the early fault-tolerant era. In this era, harnessing QEM techniques is still essential for mitigating the residual errors for demonstrating quantum advantage [187], [188]. There is also a range of ideas for combining QEM and QECC. These ideas tend to be centered around sufficiently mitigating the qubit error ratio by QECC techniques, so that the residual errors may be "cleaned up" by QECCs without encountering avalanche-like error proliferation, as intimated in [174]. In this context *near-hashing-bound multiple-rate QECCs* may be beneficial in terms of adjusting the coding rate of QECC based on the estimated error rate in liaison with QEM techniques [3]. Another attractive proposition is to harness the *universal decoding* concept, which allows the employment of the same decoder for different types of linear codes, such as polar codes and BCH codes used in combination with QEM techniques [102].

Having surveyed the family of error mitigation solutions operating both with and without the aid of QECCs, let us now focus our attention on the pros and cons of QML.

IV. MODELING AND COUNTERACTING UNCERTAINTY VIA QML

The Myth: Quantum computers can speed up machine learning on large-scale data by exploiting the exponentially large vector space of quantum states.

The Reality: The benefits of QML applied to classical data are practically limited by the need to map the data onto quantum states. While classical processing units excel at handling large volumes of data by following deterministic computational graphs, quantum computers may serve as co-processors for the implementation of probabilistic tasks, such as generating discrete data.

The Future: Fundamental research is required for developing theoretical insights into the potential benefits of QML for the processing of both CD and QD data. The algorithms conceived for training and inference are likely to be informed by different principles than those of the classical machine learning workflow based on over-parameterization and stochastic gradient descent.

Abstract: In the previous sections, we have considered the popular design paradigm of quantum algorithms, which is based on a handcrafted selection of quantum gates and routines implementing functionalities such as QEM and error correction. In practice, optimizing gate placement and the circuit architecture is a complex task, particularly in the NISQ computers relying on a limited number of qubits. For these, the efficient exploitation of quantum resources is essential. In this context, QML is emerging as a promising paradigm to program gate-based quantum computers using a methodology that borrows insights from classical machine learning [189]. Applications of QML to the design of improved quantum computing algorithms, such as quantum error correction and QEM, are under intense investigation [143], [191], [192], [194], along with a host of other bespoke applications. As illustrated in Fig. 10, such applications also include quantum simulation, quantum data analysis, and classical data analysis [195], [196], [197]. AQ:12

At a technical level, QML is potentially capable of addressing combinatorial optimization problems, implementing probabilistic generative models, and carrying out inference tasks such as classification as well as regression. They can be instantiated within actual quantum computers via cloud-based interfaces accessible through several software libraries—such as IBM's Qiskit, Google's Cirq, and Xanadu's PennyLane. In this section, we provide a short overview of QML, and we point to the potential of QML as a tool to quantify and represent uncertainty.

A. State of the Art

1) Introducing QML: As illustrated in Fig. 11(top), in classical machine learning, a parameterized function $f(x|\theta)$, e.g., a neural network, is optimized by adjusting the free parameters θ based on an available training dataset. This is typically done by comparing the model outputs $f(x|\theta)$ with desired outputs extracted from the training

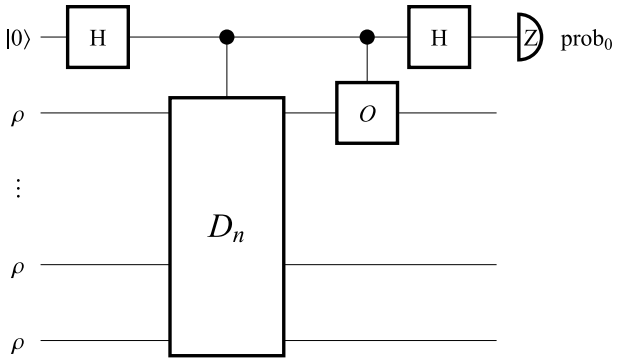

Fig. 10. *Purification-based techniques prepare n copies of a noisy quantum state ρ either by splitting an array of qubits into batches [146] or by using multiple quantum cores for state preparation [151]. A derangement D_n is a generalization of the SWAP gate, which applies a permutation to the qubits controlled on an ancilla qubit (topmost qubit). Estimating the probability of the $|0\rangle$ outcome allows one to suppress errors in the expected value measurement of the operator σ exponentially in n. Reproduced from [144] (CCBY 4.0).*

AQ:13

dataset, and making local adjustments to the free parameters θ to reduce the discrepancy between the two outputs.

As discussed in earlier sections, a quantum algorithm is specified by a quantum circuit operating on a set of n qubits. Furthermore, a quantum circuit consists of a sequence of quantum gates that are applied sequentially and in place to the n qubits, followed by measurements that convert the state of the n qubits into n classical bits. Quantum measurements are inherently *random*, producing a jointly distributed vector of n classical bits, and they cause the *collapse* of the quantum state.

As shown in Fig. 11(bottom), in QML, the gates of a quantum circuit depend on the free parameters θ, defining a *parameterized quantum circuit* (PQC) that implements a parameterized unitary matrix $U(\theta)$. PQCs are also known as *QNNs*. As we will see in this section, in a manner similar to classical machine learning, the parameters θ are tuned via classical optimization based on data and measurements of the outputs of the circuit. An important advantage of the QML framework is that, by keeping the quantum computer

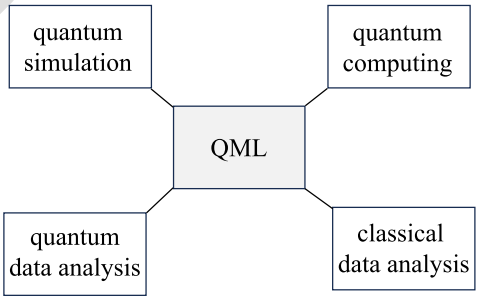

Fig. 11. *Possible applications of QML (adapted from [199]).*

Table 1 Taxonomy of QML Strategies ("C" Stands for Classical and "Q" Stands for Quantum)

		data C	processing Q
data generation	C	CC	CQ
	Q	QC	QQ

in the loop, the classical optimizer can account for the nonidealities and limitations of quantum operations on NISQ computers.

2) Taxonomy of QML Solutions: As illustrated in Table 1, data and processing can be generally of a quantum or classical nature. Quantum data refer to quantum states—which may be encoded by physical systems produced by quantum sensors [200]—while quantum processing refers to the use of quantum computers. Classical machine learning corresponds to the "CC" corner in Table 1, with classical data and processing. The other three cases, with data and/or processing being quantum, are the domain of QML.

While processing quantum data, e.g., chemistry and biology, is widely considered to be most promising in the long run, currently, the most common QML case is CQ: data are classical, while processing is quantum. The popularity of this setting is also due to the availability of many classical datasets. As shown in Fig. 12(top), in the CQ case, the measurement outputs from a PQC are compared to classical data within a classical computer, which then adjusts the local parameters θ to minimize the discrepancy between PQC outputs and targets. In principle, QC-based QML can implement any classical machine learning task. The largely open question at this stage is whether there are useful tasks for which QML can provide gains in terms of performance or efficiency.

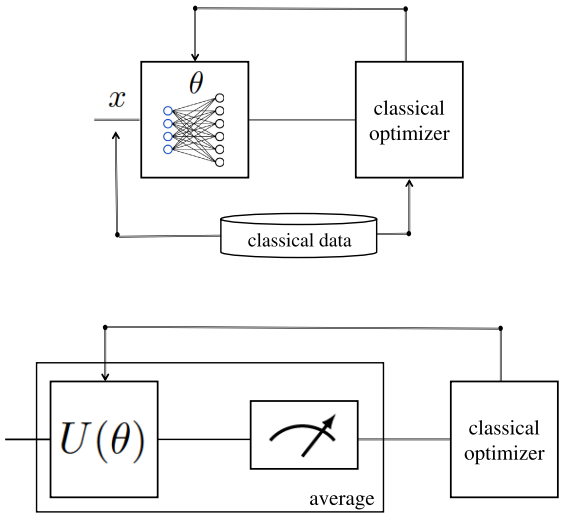

Fig. 12. *(Top) Classical machine learning versus (bottom) QML.*

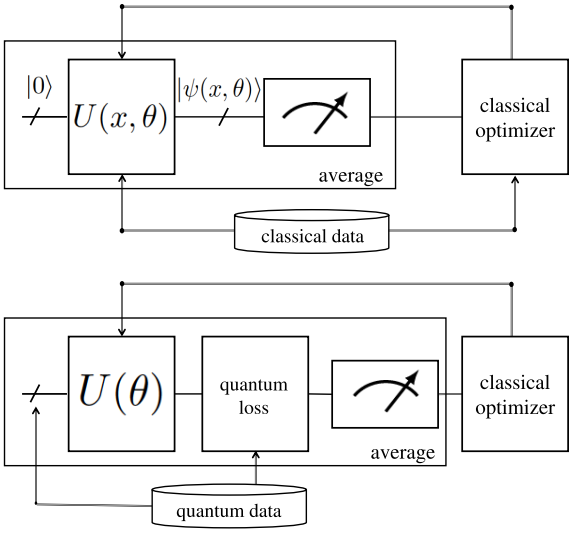

Fig. 13. *QML architectures for (top) classical data and quantum computing and (bottom) quantum data and quantum computing.*

As shown in Fig. 12(top), in the QQ case, the quantum state produced by the PQC is directly compared with a quantum data target to optimize θ. This comparison is done within the quantum computer, evaluating some loss metric that can then be measured by a classical optimizer for the update of parameters θ. Two examples of QQ models are quantum autoencoders [201] and QGANs [202].

Finally, in the QC case, there is no PQC, and the outputs of measurements of a quantum state are processed by a classical machine learning model. Examples include quantum tomography, in which the goal is that of estimating or representing an unknown quantum state [200].

3) Parameterized Quantum Circuits: As mentioned, a PQC is defined by a fixed sequence of quantum gates that can depend on a vector of classical parameters θ, defining a parameterized unitary matrix $U(\theta)$. The choice of the architecture of the PQC is akin to the selection of the model class in classical machine learning, which typically involves validating several different neural network architectures and hyperparameters. In QML, the architecture of the PQC $U(\theta)$ is referred to as the *ansatz* (from the German term for "approach" or "attempt"). As for the model class in machine learning, one should choose the ansatz, if possible, based on domain knowledge. For instance, in quantum chemistry, some ansatz can closely represent the physics of the system.

When lacking insights from the physics of the problem, one can select generic ansatzes, with the important constraint that they can be efficiently implementable on the given hardware. As shown in Fig. 13, the *hardware-efficient ansatz* applies layers of separate rotations on each qubit—which are typically available on all gate-based quantum computers—as well as fixed multiqubit entangling gates. The multiqubit entangling gate U_{ent} consists of a fixed cascade of two-qubit gates, whose connectivity structure abides by the locality properties of the architecture of the quantum computer.

The hardware-efficient ansatz is generic, and it is often viewed as playing a similar role to fully connected classical neural networks. In this regard, it is important to stress that a hardware-efficient ansatz does not have similar properties to fully connected classical neural networks in terms of dependence on model parameters. Notably, in fully connected classical neural networks, one has significant freedom in optimizing the connectivity among neurons by designing the individual synaptic weights as biases. By contrast, in the hardware-efficient ansatz, one can control only the rotations applied to each individual qubit, and the interdependencies among qubits are dictated by fixed entangling circuits.

It is finally noted that there are more complex alternatives to the hardware-aware ansatz, such as circuits that include parameterized two-qubit gates and ansatzes associated with increasing/decreasing number of qubits along the layers of the PQC [199].

4) Unsupervised Generative Learning: The most direct QML application with classical data is generative modeling—a key task in applications requiring the modeling of uncertainty. In particular, a *Born machine* is a generative model constructed for binary strings x that is implemented via a PQC [203]. In a Born machine, a measurement of the output of the PQC on n qubits, which produces a random n-bit string $x \sim p(x|\theta)$, is considered to be the generated data. The distribution $p(x|\theta)$ of the data generated by a Born machine can be controlled via the PQC parameters θ by Born's rule. Note that *shot noise*, i.e., the inherent randomness of quantum measurements, is the key feature leveraged by Born machines to produce random samples.

Many current claims of quantum supremacy/advantage rest on the capability of quantum circuits to generate samples from joint discrete distributions in a more efficient manner than classical devices although theoretical conclusions in this regard are conflicting [204], [205], [206]. It is an open question, in particular, whether Born machines can be efficiently learned [205], [206].

In practice, as illustrated in Fig. 14, training of a quantum generative model for discrete classical data is based on comparing the statistics of samples $x \sim p(x|\theta)$ generated by the model with the desired distribution inferred from training data. This is done by minimizing a specific measure of *divergence* between the target data distribution and $p(x|\theta)$. This estimate may entail evaluating the expected value of a cost observable or applying kernel-based divergence measures that directly depend on all samples in the dataset $\mathcal{D}$ and on measurements from the circuit, such as the MMD [207]. Note that, in contrast to sample generation, evaluating the loss requires repeating the measurement of the observable multiple times.

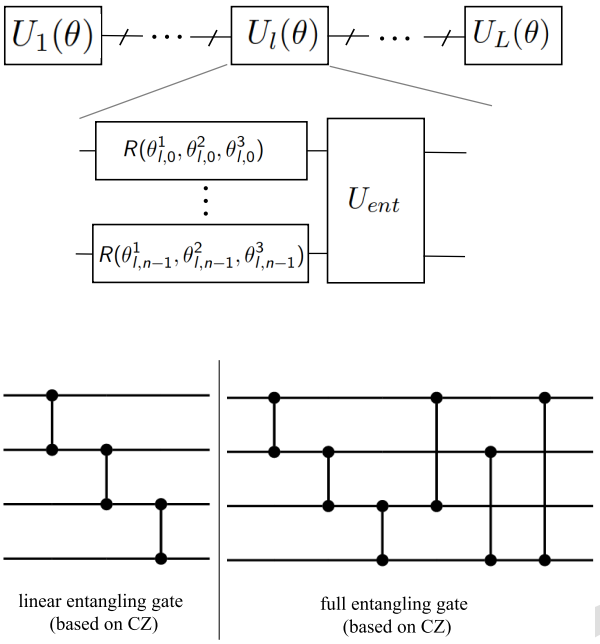

Fig. 14. *(Top) General form of a hardware-aware ansatz and (bottom) example of an entangling gate.*

Following standard practice in classical machine learning, optimization is typically carried out via gradient descent. However, in contrast to classical machine learning models, the backpropagation algorithm is not applicable since we do not have access to the internal operations of the PQC. Rather, the gradient is typically estimated via a perturbation-based, zeroth order method known as a *parameter shift rule* [190]. This entails a complexity that scales with the square of the number of parameters, rather than being a constant multiplicative factor of the complexity for the forward pass as is the case for classical models [208].

5) Supervised Learning: PQCs can also be used for supervised learning tasks with classical data. In this case, the classical input x is typically encoded in the operation of the PQC $U(x, \theta)$ in a manner similar to the model parameters θ, i.e., in the angle of single-qubit rotations. In the case of angle encoding, the PQC is obtained by alternating unitary operators dependent on x and dependent on θ. In this regard, it is advantageous to encode input x multiple times—a process known as *data reuploading*—to improve the expressiveness of the function encoded by the PQC. However, there are other ways of embedding classical information into a quantum state, such as amplitude encoding and basis encoding [189], [190].

Given a classical input x, probabilistic models obtain a randomized decision y through a single measurement of the PQC output. Given that the output is discrete, such models are suitable for classification. By contrast, deterministic models rely on a parametric function of the input x, which may be used for regression or classification. This is achieved by estimating the expectations of one or more observables. In contrast to probabilistic modes, shot noise averaging is required also for inference, not only for learning. Deterministic quantum models are akin to classical *kernel methods* in that they operate over a large feature space—the Hilbert space of dimension 2^n—via linear operations [189]. Supervised learning follows the same type of optimization strategies, as described above for unsupervised generative modeling.

Next, we embark on identifying the associated knowledge gaps in the light of the timeline seen in Fig. 15.

B. Knowledge Gaps and Challenges

We now briefly review a number of knowledge gaps and challenges in the QML field, which will be further addressed in this section. We divide the discussion into three main areas of research: architecture, optimization, and generalization theory.

1) Architecture: As discussed in Section IV-A, the state of the art tends to rely on generic ansatzes that are suitable for implementation on existing quantum computers in the absence of insights from the physics of the problem. Even using such ansatzes, one may ask whether there are useful tasks that may be addressed in ways that would be infeasible using classical means. Generative modeling provides a useful benchmark in this regard, and some initial studies have provided mixed conclusions [205], [206], [225]. Results about a possible separation between classical and quantum computers in their capacity to address special classes of learning problems are provided in [226].

Going beyond hardware-tailored ansatzes, it is important to identify alternative architectures satisfying the following requirements.

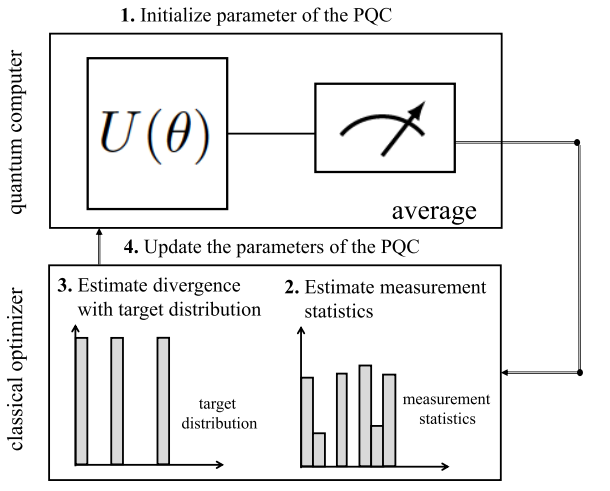

Fig. 15. *Illustration of the process of training a PQC.*

1) They are expressive enough to capture solutions to problems of interest for the analysis of classical or quantum data.
2) They can be efficiently implemented on hardware, being robust to impairments such as quantum noise, as well as to shot noise.
3) They can be efficiently learned using a limited amount of training data. In this regard, one is interested in assessing the scaling of the data requirements and of the time complexity with respect to the number of qubits, in the hope of finding solutions, whose complexity escalates slower than exponentially with the number of qubits.

Another interesting direction, espoused by the programs of companies like IBM, is the integration of QPUs with classical CPUs and graphics processing units (GPUs). We will return to this point below in the context of a research roadmap.

AQ:14 *2) Optimization:* At the core of QML lies the optimization of the free parameter θ via a classical computer. As covered in the previous subsection, QML cannot rely on the scaling efficiency of backpropagation, calling into question the adoption of gradient-based methods [208]. Furthermore, implementing gradient descent is practically made complicated by the fact that the loss landscape associated with generic ansatzes is not well behaved as the number of qubits increases [227].

In particular, the loss function for a randomly selected model parameter tends to have exponentially vanishing variance as the dimension of the circuit increases. This indicates that distinguishing different values of the loss functions requires an exponentially large number of measurements in order to overcome short noise. This behavior—known as *barren plateaus*—is verified under general conditions, which are exacerbated by the presence of entanglement noise and measurements that involve multiple qubits [227]. This points once more to the importance of choosing well-structured bespoke ansatzes [228].

3) Generalization Theory: The performance of both classical and QML must be quantified by applying the model to test data that were not used during training and validation. In other words, the goal of machine learning is generalization. Accordingly, the analysis of QML strategies calls for the development of theoretical tools that can correctly describe the dependence of the generalization performance on the amount of data and time required for the training of the QML model of interest. As in classical machine learning, several approaches exist for this purpose, from combinatorial arguments to information-theoretic methods [200], [224]. Open research questions concern aspects such as the impact of overfitting and quantum noise [229].

C. Research Roadmap

In this section, we point to several directions for future research in QML by concentrating on aspects that may be of particular interest to researchers with a background in signal processing, information theory, and communications.

1) Architecture: A principle way to identify useful ansatzes revolves around the idea of encoding the geometric properties of the data of interest into the architecture of a PQC. Geometric properties are defined by symmetries of the data. Classical examples include the translational invariance leveraged by convolutional neural networks and the permutation invariance encoded by graph neural networks [230]. The identification of relevant symmetries can lead to the design of efficient ansatzes that encapsulate useful domain knowledge about the problem, preserving invariance or equivariance to the transformations underlying the symmetry [231]. An example is given by the recent study [232], which introduced a class of quantum recurrent neural networks by encoding the specific property that the model class should be able to represent all classical time series that are related by a time-warping transformation.

Beyond purely quantum models, there is an interest, both commercial and academic, in finding effective and efficient ways of combining classical and QML models. As illustrated in Fig. 16 for the case of classical data, one may envision the combination of a classical model defined, e.g., by a neural network, and of a quantum model, implemented as a PQC. Such an architecture may benefit from the strengths of both classes of models. For instance, classical neural networks may be leveraged to process high-dimensional data, while quantum models could be tasked with generative modeling routines for discrete data.

For example, in [233], a Born machine is leveraged to encode the distribution over the binary weights of a classical Bayesian neural network (see also [234] for a related study). Bayesian neural networks maintain a distribution over the model parameters, which allows them to account for *epistemic uncertainty* via ensembling. Representing complex distributions in the model parameter space can enhance the capability of Bayesian neural networks to quantify and represent uncertainty, but this is a complex task for classical models, particularly in the case of discrete parameters. Therefore, adopting a PQC for the purpose of encoding model parameter uncertainty holds the promise of enhancing the reliability of classical machine learning models.

Parameterized quantum circuits can also be implemented in the form of *measurement-based quantum computation*, whereby the sequence of gates is encoded by the sequence of measurement settings applied to the qubits of a cluster state. This type of circuit has the additional source of uncertainty caused by the outcome of the intermediate measurements, which are typically compensated for in order to realize a deterministic unitary transformation [235]. Recent work [236] proposed to exploit this randomness for the purpose of improving generative modeling.

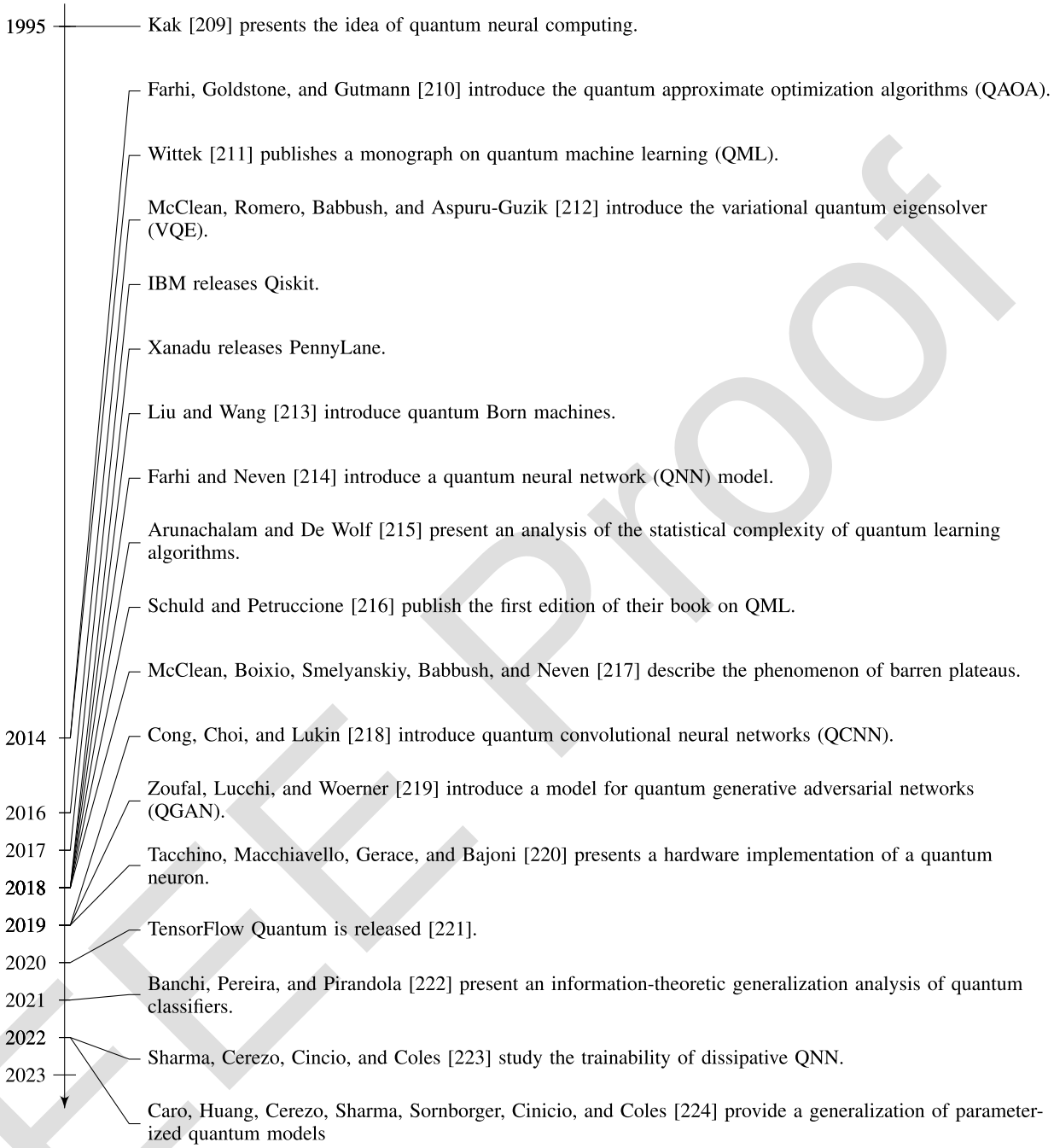

Fig. 16. ***Timeline of QML milestones (limiting the survey to variational quantum algorithms based on parameterized quantum circuits).***

2) Optimization: In the context of QML-aided optimization, the open questions include, but are not limited to: how to improve the performance of gradient descent in the presence of barren plateaus? and how to account for *quantum decoherence*?

With regards to the first question, in light of the limitations of gradient-based optimization, it may be desirable to use global optimization strategies. A well-established approach for global optimization is to leverage surrogate objective functions that extrapolate the value of the loss across different values of the model parameter vector θ. The surrogate function is typically updated sequentially based on previous measurements. One such method is *Bayesian optimization* [237].

As for the second question, it is important to evaluate the impact of quantum decoherence on optimization routines relying on QML. For example, quantum decoherence makes the gradients estimated from the measurements of a PQC biased. As seen earlier in this article, QEM trades chip area (qubits) against time, by running multiple noisy quantum circuits to emulate a noiseless one. QEM is capable of reducing the bias imposed by quantum gate

noise on the estimate of gradients, but it increases the variance. An analysis of the impact of QEM on gradient descent-based training of PQCs can be found in [238].

3) Theory: Generalization analysis formulates bounds—either average or probabilistic bounds—for the generalization error of QML algorithms, with the main goal of understanding the associated scaling laws with respect to the size of the dataset. So far, the focus has been almost exclusively on supervised learning, leaving the important task of unsupervised generative learning largely unexplored by the existing theory [200].

By its very nature, generalization analysis does not provide operational *error bounds* for the performance of quantum models, focusing instead on scaling laws. A recent piece of work [239] has initiated the investigation of statistical tools that can offer provable guarantees concerning the reliability of quantum models for test inputs. It is envisaged that this can be a fruitful direction for further research.

Following the above discourse on QML, let us now focus our attention on the radical frontier research of quantum radar systems.

V. QUANTUM RADARS

The Myth: With the aid of quantum radars, stealth aircrafts can be tracked up to several thousand of kilometers without being detected by the aircraft's radars.

The Reality: The microwave quantum radar demonstrations so far have provided only a marginal improvement over their classical counterpart within rather limited ranges.

The Future: Significant research efforts are required for developing high-fidelity entanglement generation sources and detectors at microwave frequencies. EA quantum radars operated at optical frequencies are more mature, but optical frequencies have limited propagation through both clouds as well as fog; hence, further research is needed to solve for this problem.

Abstract: Quantum radars offer alternatives to classical radars and are relevant in low-brightness and high-attenuation scenarios. The key promise of quantum radars is to outperform the quantum limit of classical sensors and thus improve the detection probability at very low SNRs. Even though some progress has been made in terms of quantum radars at microwave frequencies, further significant efforts are required for developing improved entangled sources and the corresponding detectors. In this section, we provide an overview of various quantum radar technologies, including both quantum interferometry and QI-based radars. The focus will be on a particular version of QI-based radars, namely, on EA radars. The EA radars operated in the C and L bands are much more mature than their microwave counterparts and lend themselves to supporting both monostatic and multistatic solutions, which are reminiscent of single- and multicell communications scenarios. The EA multistatic radar concept also offers the possibility of DFRC operation, which is also often referred to as ISAC.

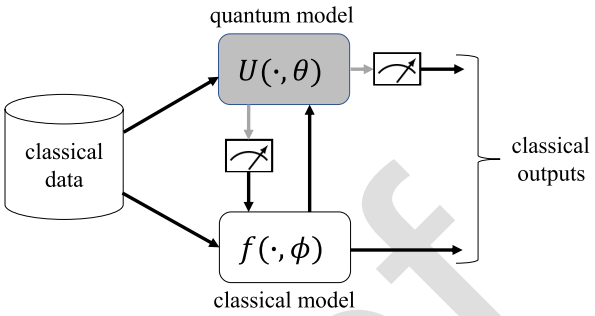

Fig. 17. ***General architecture of a hybrid classical-quantum model for QML.***

A. State of the Art

Quantum radar is a particular quantum sensing technique that exploits quantum-mechanical features of the electromagnetic fields to attain improvements in target detection compared to the classical scenario [240], [241], [242], [243], [244]. The key motivation behind the quantum radar studies is to outperform the quantum limit of classical sensors [240]. The potential advantages of quantum radars compared to the classical radars can be summarized as follows [240], [241], [242], [243], [244]: improved receiver sensitivity, enhanced target detection probability at low SNRs, improved penetration through clouds and fog when microwave photons are used, upgraded resilience to jamming, and improved synthetic aperture radar imaging quality. Furthermore, the quantum radar signals are harder to detect than their classical counterparts, and quantum radars have higher cross section (as shown in [240]), just to mention a few for their promises. However, unfortunately, they are significantly more challenging to implement, in particular at microwave frequencies. A pair of popular quantum radar designs are: 1) the quantum radar employing the QI sensing concept [240], [241], [242], [243], [244], [245], [246], [247], [248], [249], [250], [251], [252] and 2) interferometric quantum radar [240], [241], [253], [254], [255], [256] relying on a concept reminiscent of quantum interferometry. Depending on the specific underlying quantum phenomenon employed, the quantum sensors can be categorized into three types [240], [253].

Type 1: A quantum sensor transmits the quantum states of light that are not entangled with the receiver.

Type 2: The sensor transmits the classical states of lights but employs the quantum detectors for improving the performance.

Type 3: The quantum transmitter emits quantum states that are entangled with the reference states available at the receiver.

The monostatic single-photon radar, illustrated in Fig. 17, belongs to Type 1 quantum sensors, and its operating

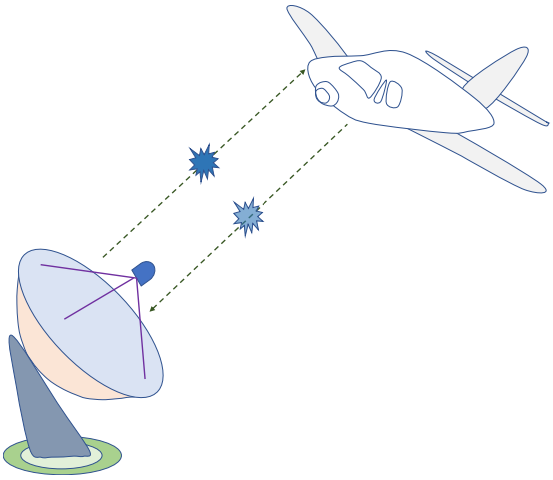

Fig. 18. ***Illustration of the single-photon monostatic quantum radar concept.***

principle is similar to that of the classical radars, but a single-photon pulse is used instead of an RF pulse. The single-photon quantum radar has larger radar cross section than classical radars [240], [257], but requires a large number of single-photon pulses to be transmitted.

The quantum LADAR solution belongs to Type-2 quantum sensors and employs principles similar to those of the light detection and ranging (LIDAR) technology [240], [253], [254], [255], [256]. Because the LADARs operate in the visible and near-infrared (IR) wavelength regions, the laser beam does not propagate well through clouds and fog, in particular in the VL band around 800 THz. Nevertheless, given that the operating wavelengths are much lower compared to the classical radars, the LADARs have much better spectral resolution.

EA radars belong to Type-3 quantum sensors, and the corresponding operational principle of the bistatic radar is illustrated in Fig. 18. The entanglement generation source orchestrates an entangled pair of photons, namely, the signal and idler photons. The idler photon is kept in the quantum memory of the receiver, but we hasten to add that at the time of writing, there is no quantum memory having a long retention duration. Nonetheless, for optical frequencies, this QM may rely on optical delay lines. By contrast, the signal photon is transmitted over a realistic noisy, lossy, and atmospheric turbulent channel toward the target. The reflected signal photon is detected by the radar, and the QD correlation between the signal and idler photons is exploited at the receiver side for improving both the receiver sensitivity and target detection probability.

In the next subsections, we describe interferometric quantum radars, QI-based radars, and EA radars.

1) Interferometric Quantum Radars: The interferometric quantum radars rely on the concept introduced in Fig. 19, where a single photon is present at the input port E_1 of the BBS1, while no photon is at the input E_2. The upper branch corresponds to the target branch, where the phase shift introduced by the presence of the target is denoted by ϕ. The expected value at the output port E4 in the absence of any background radiation is proportional to $R_t\cos^2(\phi/2)$, where R_t is the reflectivity of the target. If we repeat the target interrogation problem N times, the uncertainty of the phase estimate will become [240], [241] $N^{-1/2}$, which is commonly referred to as the standard quantum limit (SQL). If we apply entangled states at the input ports of the BBS1 in Fig. 19, that is, $|\psi>=2^{-1/2}(|N0>+|0N>)$, the uncertainty for the phase estimate will be $1/N$, which is known as the Heisenberg limit. Naturally, in practice, we have to take the realistic propagation effects of absorption, scattering, diffraction, and turbulence into account together with the background radiation into account, which may be modeled by a cascade of thermal Bosonic channels, as shown in Fig. 20. These are popularly harnessed for studying the efficiency of quantum radar techniques. The atmospheric turbulence [258], [259] is caused by the refractive index variations imposed on the beam propagation path by temperature and pressure fluctuations, introducing wavefront distortions. This indicates that the transmissivities T_i of different Bosonic stages of Fig. 20 are random variables. In the face of these hostile propagation effects, we can use the AO [260], [261], [262], [263] for enhancing the quantum radars sensitivity attained.

An AO system is composed of: 1) a wavefront sensor used for detecting atmospheric distortions; 2) a wavefront corrector harnessed for compensating the turbulence effects; and 3) a control processor employed for monitoring the wavefront sensor information and for updating the wavefront corrector [260], [261], [262], [263]. At the time of writing, the AO-based correction is capable of maintaining super-sensitivity over ranges of up to 5000 km [260]. The key idea behind Smith's [260] proposal is to introduce the phase shift ϕ_{AO} in the upper branch of Fig. 19 for interrogating the target, which is controlled by the radar operator. In the quantum radar scenario of

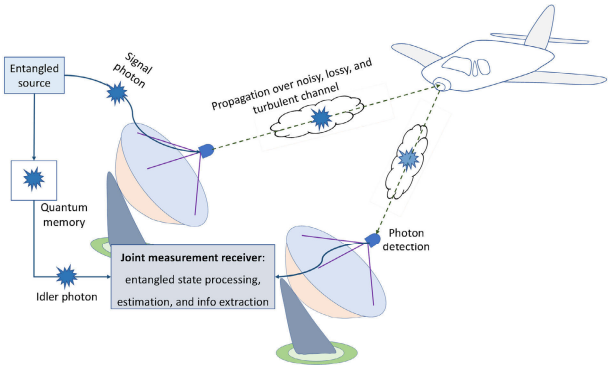

Fig. 19. ***Illustration of the entanglement-based bistatic quantum radar concept.***

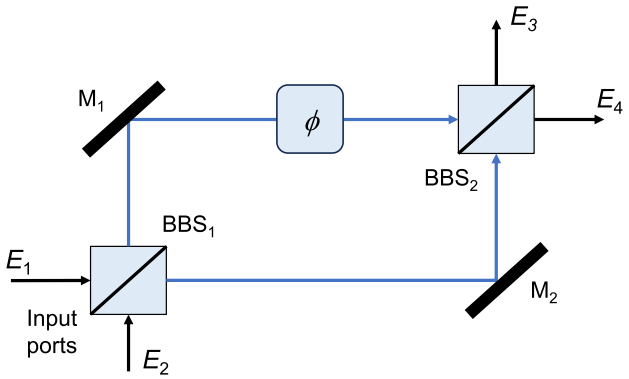

Fig. 20. *Illustration of the interferometric quantum radar concept. BBS: Balanced beam splitter. M: Mirror.*

Fig. 19, let us assume that the entangled source, generating the so-called NOON states,[6] is located at the transmitter side of the radar system. Hence, the distortions inflicted by turbulence and attenuation of the lower branch spanning from the transmitter side to the receiver side of the radar system can be neglected. When ϕ_{AO} is appropriately chosen, the corrected phase is also a function of the corrected transmissivity of the optical medium and thus it will never exactly reach the Heisenberg limit. Unfortunately, this method requires accurate knowledge of the target range. Alternatively, we can use the AO to compensate for the aberrations in the wavefront of a single photon imposed by turbulence to improve the transmissivity of the channel in a similar fashion to that in [262] and [263]. As a benefit, the latter approach does not require the knowledge of the target range.

2) QI-Based Radars: The QI technique proposed in [245] is capable of improving the sensitivity, when operating in a hostile noisy regime. Since it is not restricted to any specific wavelength, it may also be readily applied to both LADAR and microwave quantum radars. This approach does not require any Mach–Zehnder interferometer—simple photon counters are adequate for detection. They are also readily applicable to both entanglement-based and nonentangled quantum radars, and the corresponding principle was already highlighted in Fig. 18. Assuming that the target reflectivity is R_t and the average number of background photons is N_b, when entangled photons are used and the system dimensionality is D, the corresponding SNR will be [240], [241]

$$\text{SNR}_{\text{ent}} = \frac{R_t + (1 - R_t)\frac{N_b}{D}}{\frac{N_b}{D}} \tag{14}$$

[6]In quantum information science, NOON states typically refer to quantum states where a certain number of particles are in one state and the rest are in another, usually entangled in a specific way. These states have beneficial properties for precision measurements.

and the improvement in the SNR when entangled photons are used over nonentangled case, assuming that the target reflectivity is close to 1 will be

$$\frac{\text{SNR}_{\text{ent}}}{\text{SNR}} = \frac{1 - R_t + \frac{R_t D}{N_b}}{1 - R_t + \frac{R_t}{N_b}} \approx D. \tag{15}$$

Clearly, for a typical system dimensionality of $D = 2$, the improvement in the SNR originating from entanglement is up to 3 dB. Tan et al. [264] proposed to use an SPDC source as an entanglement generation source, but the corresponding detector has not been proposed. Audenaert et al. [265] used the quantum Chernoff bound under the assumption that the target is present with a probability of 0.5 and that the system is operated in a hostile noisy scenario in order to obtain the following bound for the asymptotic error probability:

$$P_e^{(\text{QCB})} \sim 0.5e^{-\text{MTN}_s/N_b} \tag{16}$$

where T is the overall transmissivity, M is the number of signal–idler photon pairs being utilized, and the mean photon count of the background radiation noise is given by $Nb/(1 - T)$. This bound is the same as the quantum Bhattacharyya bound, and it has been shown in [242] to be valid only for high SNR values. The corresponding classical counterpart relying on a coherent state at the transmitter side and on homodyne detection at the receiver side has the following bound [264]:

$$P_e^{(\text{CB})} \sim 0.5e^{-\text{MTN}_s/(c_f N_b)} \tag{17}$$

where $c_f = 4$ for the upper bound and $c_f = 2$ for the lower bound. Therefore, the expected entanglement advantage based on [264] is between 3 and 6 dB.

To perform the joint measurement required, we can arrange for the interaction of the radar return probe and of the stored idler by harnessing an OPA, as illustrated in Fig. 21 [241]. The bottom output port's annihilation operator $\hat{a}(\varphi)$ is related to the radar return probe $\hat{a}_{\text{probe}}(\varphi)$, where ϕ is the phase shift introduced by the target. The associated idler annihilation operator is denoted by $\hat{a}_{\text{idler}}$. The variable G in Fig. 21 denotes the OPA's gain,

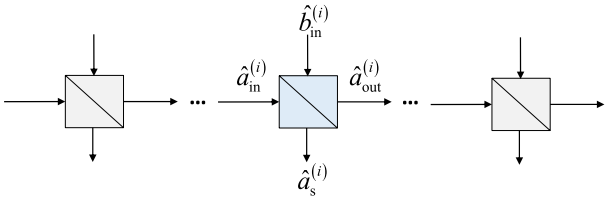

Fig. 21. *Light beam attenuation effects can be modeled by a cascade of lossy thermal Bosonic channel models.*

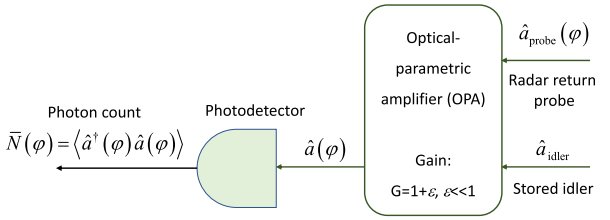

Fig. 22. ***OPA-based receiver.***

which is in this case chosen to be low, namely, $G = 1 + \varepsilon, \varepsilon << 1$. The concatenated transmitter–target–radar receiver channel is modeled as a lossy thermal Bosonic channel according to Fig. 20. It has been shown in [266] that the maximum possible SNR improvement is 3 dB, which is consistent with (15). However, once all realistic experimental imperfections have been included, the quantum illumination outperforms the classical limit by only about 1 dB [266]. This experiment carried out at optical frequencies was performed in a hostile noisy environment. Nevertheless, a quantum advantage was demonstrated, as an explicit benefit of entanglement. To improve the performance of the joint measurement-based detection scheme, Zhuang et al. [267] proposed the employment of sum-frequency generation, but the complexity of this detection scheme was found excessive.

3) EA Radars: Now, we shift our focus to the particular version of the quantum illumination relying on entangled sources. We describe several EA radar schemes: 1) EA monostatic [243] (depicted in Fig. 22) and 2) EA joint monostatic–bistatic [243] and EA multistatic [244] radar schemes. The EA bistatic scheme [242] was already described in Fig. 18. All of these schemes employ the Gaussian states generated through the continuous-wave SPDC process. The SPDC-based entangled source represents a broadband source having $M = T_m W$ independent identically distributed (i.i.d.) signal–idler photon pairs, where T_m is the measurement interval and W is the phase-matching SPDC bandwidth. Each signal–idler photons pair, which are represented by blue photons in Fig. 22, is, in fact, a TMSV state [241]. The signal–idler entanglement is characterized by the PSCC coefficient, defined as $C_{si} = \langle \hat{a}_s \hat{a}_i \rangle = (N_s(N_s + 1))^{1/2}$, which can be considered as the quantum limit. Clearly, in the low-brightness regime of $N_s << 1$, the PSCC is $(N_s)^{1/2}$ and it is much larger than the corresponding classical limit N_s. By going back to Fig. 22, an entangled source is used at the transmitter side to generate a quantum-correlated signal photon (probe) and an idler photon, where the latter serves as a local reference. The signal photon is transmitted over noisy, lossy, and atmospheric turbulent channels toward the target with the aid of an expanding telescope. The reflected photon representing the radar return is then collected by the compressing telescope and detected by the radar's receiver. In this context, the quantum correlation between the radar return and retained reference represented by the idler photon is exploited at receiver side for improving the receiver's sensitivity. The interaction between the probe (signal) photon and the target can be described by a beam splitter of transmissivity $T^{(r)}$. Therefore, we can model the concatenated transmitter–target–receiver (directly reflected mode) link (direct return channel) as a lossy thermal Bosonic channel, similar to Fig. 20, where the target is assumed to introduce the phase shift.

The operational principle of the EA joint monostatic–bistatic quantum radar detection scheme proposed in [243] is portrayed in Fig. 23. The wideband entangled source generates two entangled photon pairs, where each pair contains a signal photon and an idler photon. The idler photons are stored in the QMs of the receivers. Both signal photons are then transmitted with the aid of the corresponding expanding telescopes over noisy, lossy, and atmospheric turbulent channels to the target. The directly reflected photon is collected by the compressing telescope and is detected by the first radar receiver, while the forward scattered photon is collected by the second compressing telescope and is detected by the second radar receiver. The quantum correlation is, then, exploited at the receiver sides for improving the overall target detection probability. The inherent spatial diversity is also exploited for improving the overall SNR.

The operational principle of the EA multistatic quantum radar detection technique of [244] is depicted in Fig. 24. Compared to the joint monostatic–bistatic scheme from Fig. 23, the EA multistatic radar scheme has slightly higher complexity, but much better performance and improved flexibility. The multistatic radar scheme employs multiple entangled transmitters and multiple coherent detection-based receivers, as shown in Fig. 24, while the previous scheme only relied on a single transmitter and monostatic as well as bistatic receivers. In this scheme, the phase-sensitive quantum correlation is exploited at the receivers' sides with the objective of improving the overall detection probability of the target. Moreover, to increase the overall SNR, the spatial MIMO concept is harnessed. Compared to

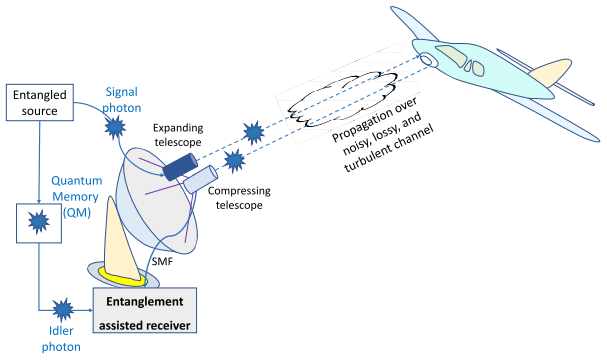

Fig. 23. ***EA monostatic quantum radar (modified from [243]).***

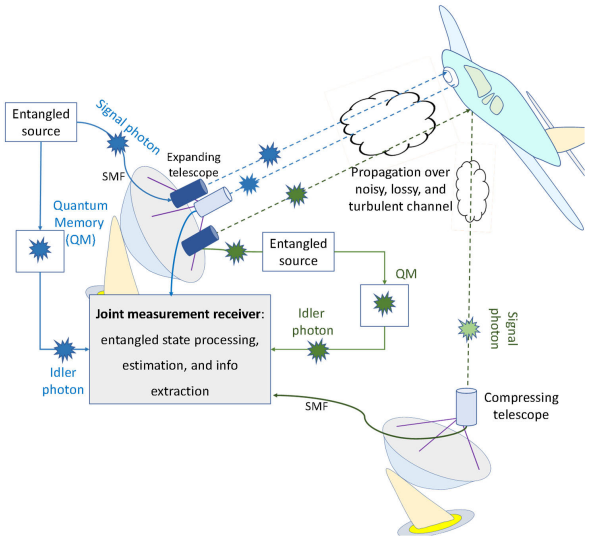

Fig. 24. *EA joint monostatic–bistatic quantum radar scheme (modified from [243]).*

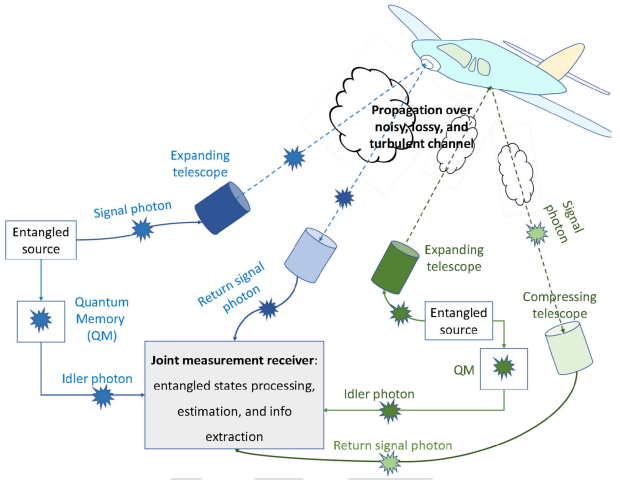

Fig. 25. *2 × 2 EA multistatic (MIMO) quantum radar scheme (modified from [244]).*

the reflected and forward scattered components available in joint monostatic and bistatic radars, which are correlated and as such do not provide full spatial diversity, by using multiple transmitters that are sufficiently far apart in space, we can ensure statistical independence of different optical paths, thus achieving the maximum attainable diversity order of the multistatic radar concept. This leads to improvements both in terms of the diversity order and the array gain compared to joint bistatic–monostatic schemes. An alternative terminology for this scheme is the EA MIMO radar concept [268].

To simplify the transceivers' design and reduce the system's cost, the transmitter sides' OPC—which is required before the detection takes place—has been performed at the transmitter side so that classical balanced coherent detectors can be utilized as the EA detectors [244]. Furthermore, the employment of a single broadband entangled source combined with a WDM demultiplexer has been proposed as the common source for all transmitters, which is illustrated in Fig. 25. First, a PPLN waveguide serves as the SPDC source, which generates a large number of signal-photon pairs, where only the mth signal-photon pair is illustrated in Fig. 25. The signal and idler photons become separated by an appropriately designed Y-junction. The idler photons become further separated by the WDM demultiplexer, whose outputs are directed toward the QMs of the corresponding EA receivers. On the other hand, all signal photons get simultaneously modulated by a training sequence known to all EA receivers, imposed by a Q-ary phase-shift keying (PSK) modulator. This sequence is then used for estimating the phase shift introduced by the target and the channel. The common sequence is also used for determining the target's range more precisely by harnessing the cross-correlation method. The second PPLN waveguide is then used for carrying out the OPC by employing the popular DFG process, in which the mth signal photon at angular frequency $\omega_{s,m}$ interacts with the pump photon ω_p to get the PC photon at the radial frequency $\omega_p - \omega_{s,m}$. We then use the WDM demultiplexer for demultiplexing the signal photons to be used in the multistatic transmitters, as depicted in Fig. 25.

Given that the OPC is carried out at the transmitter, we do not have to use OPC-based EA receivers—instead, commercially available classical balanced coherent detectors may be used as the EA receivers, such as the one shown in Fig. 26. This substantially reduces the overall system cost and complexity. For the associated simulation-based results, interested readers might like to refer to [244]. For experimental characterization of the EA radar concept in the context of realistic turbulent FSO channels, motivated readers might like to consult [263].

B. Knowledge Gaps and Challenges

As a step toward QI-based radar operating at microwave frequencies, Barzanjeh et al. [249] proposed an optical–microwave transduction scheme for generating the

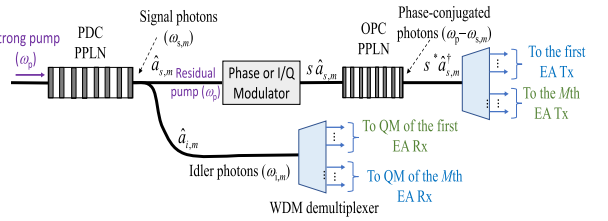

Fig. 26. *Integrated multistatic (MIMO) EA transmitter with transmitter-side OPC. We use s to denote a phase (or I/Q) modulator-induced signal constellation point. QM: quantum memory, PPLN: periodically poled LiNbO3 waveguide, PDC: parametric downconversion, OPC: optical phase conjugation, and WDM: wavelength-division multiplexing. (Modified from [244].)*

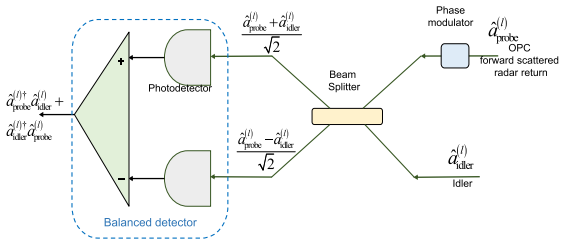

Fig. 27. ***EA receiver corresponding to the lth forward scattered component. The receiver-side phase modulator is used to select either in-phase or quadrature component of the corresponding PC signal. The photodiode responsivity is set to 1 A/W. (Modified from [244].)***

entangled microwave and optical idler photons. The microwave photon return probe is converted by the same type of device into the optical domain so that the joint measurement can be carried out in the optical domain. For example, the OPA-based detection scheme of Fig. 21 may be harnessed in this context. Unfortunately, the current optical–microwave transduction devices [269], [270] still have a low transduction efficiency to be of practical importance. The Josephson parametric converter—which serves a similar role to the SPDC device—has been used in [250] for generating the entangled microwave photons. However, the quantum advantage of the experimental demonstration remained rather limited. In a recent experiment [271], the Josephson ring modulator has been employed for coupling a pair of microwave resonators and thus for producing the entangled microwave photons. This experiment employed the OPA-based receiver and succeeded in achieving an approximately 20% advantage over its corresponding classical counterpart.

The first experimental demonstration of QI based on entangled photons at optical frequencies over an FSO link length of 750 m was documented in [263] in the face of strong atmospheric turbulence. The system applied the OPC to the idler photons before the balanced homodyne detector by relying on the concept introduced in [262]. In order to improve the tolerance to turbulence effects, AO was used.

The devices facilitating QI-based radar services at microwave frequencies are summarized in Fig. 27. One of the important issues for QI is the need for quantum memory, which will store the idler photons until they are needed for balanced detection. In experimental demonstration [263], an optical delay line is used instead of real QM. For quantum radar applications, variable delay lines can be used. However, the commercially available ones are bulky, slow, and expensive. The research of QM having improved retention duration is currently ongoing [272], [273], [274], [275], [276], [277], [278], [279]. However, these solutions are still far from commercialization. Another challenging open problem is the design of detectors having near-unity quantum efficiency [280], [281], [282]. As a further advance, for the OPA-based receiver of Fig. 21, photon-number-resolving detectors are required [283], [284]. As for microwave radar illumination, efficient quantum transducers should be developed [270], [285], [286]. Furthermore, new types of receivers suitable for QI should be developed [287], [288]. Finally, for quantum multistatic radars associated with numerous transmitters, large-scale entanglement sources are needed [289], [290], [291].

C. Research Road Map

The quantum radar relies on a relatively new concept compared to its classical counterparts. In Fig. 28, we provide the timeline describing the quantum radar research activities. The quantum illumination radars appear to be more practical than the quantum interferometry-based radars. Among various QI radar schemes, EA radars have received the most attention at the time of writing.

For QI at microwave frequencies, the quantum advantage over classical radar has remained limited so far [250], [271]. A substantial community effort is required for developing improved entangled sources and detectors operating at microwave frequencies. Again, the optical–microwave transduction devices have limited efficiency [269], [270], [292], [293], and significant research efforts have to be invested in this field as well.

The QI based on entangled states at optical frequencies [241], [242], [243], [244] appears to be much more mature compared to its microwave counterparts. There are some relevant EA quantum demonstrations at these frequencies [263], [266], but this field is very much in its infancy and it may be expected to attract scientists looking for exciting open challenges. Clearly, the EA radars operating at optical frequencies suffer from substantial performance erosion in the face of clouds and fog; hence, additional research efforts are likely to be invested in this field as well.

Another research area along this evolutionary quantum radar research path is related to the covert sensing concept, with the first experimental demonstration reported in [296]. The quantum covert radar concept can be considered as a specific QI scheme, in which the transmission of the probe is controlled by an agent, who tries to perceive the presence of any sensing. By ensuring that the probe is partially masked by the background noise, this agent

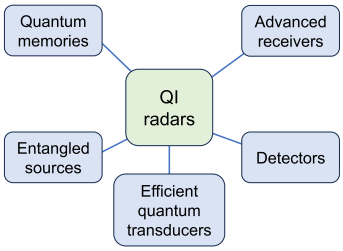

Fig. 28. ***QI-based radar enabling devices.***

will not be able to detect the sensing attempt due to the statistical fluctuations in his measurement attempts. The QI concept has also become relevant for LIDAR applications [297], [298], and it may be expected to attract substantial research attention.

As part of the roadmap, it is necessary to develop the quantum illumination radars operating at microwave frequencies closer to the commercialization, which requires the development of new type of receivers and devices [299], [300]. As for implementations at optical frequencies, the photonic integration research is making progress [241], [242], [243], [244], while on theoretical side, tighter bounds are expected to be developed for QI [301].

Another interesting, but hitherto largely unexplored area in the QI literature will be to combine quantum radars and communications. This research problem is known in the classical RF and optical wireless communication literature as DFRC [302], [303], [304], [305]. To elaborate briefly, the integrated multistatic entanglement source of Fig. 25 is also suitable for simultaneous radar and communication services. Briefly, similar to EA communications [262], we organize the data to be transmitted into packets, with the packet-header known to the receiver. The data sequence may be protected by a variety of error correction codes, such as an LDPC code, and mapped to the payload. In both radar and communication applications, we use the packet-header to determine the beginning of the packet by the popular cross-correlation method. In radar systems, we only need the header for estimating the target detection probability and the target range, while in the EA communication system, we further process the payload and carry out LDPC decoding for recovering the transmitted sequence.

The original QI concept was conceived for target detection. In this context, it is also relevant to demonstrate quantum advantage in terms of the range [241], [242], [243], [244], [306], angle, and speed of the target, which is an active research topic. Harnessing QI at microwave frequencies is very challenging because the background radiation noise is significantly higher than at optical frequencies. Hence, significant research efforts are needed to make efficient QI at microwave frequencies a reality.

While the quantum radar systems of this section are still very much in their infancy, the QKD systems of Section VI are now commercially available. However, there is a pressing need for further research to architect the global Qinternet relying on large-scale multiprotocol relay-aided networking solutions providing end-to-end security, as discussed in Section VI.

VI. QKD NETWORKS

The Myth: There is no need for QKD; postquantum cryptography (PQC) would eliminate all security risks that future quantum computers may cause.

The Reality: PQC could certainly be part of the solution for providing data security in future telecommunications networks, but it could still be susceptible to the "harvest now, decrypt later" type of attacks. QKD solutions are already an off-the-shelf reality and they constitute the most reliable solution that offers long-term security, provided that it is implemented appropriately with the aid of high-quality devices avoiding information leakage.

The Future: Having said that, the economy of scale has to reduce the cost to make it commercially viable for private subscribers *and* to offer end-to-end security for all relevant applications. A seven-step evolutionary pathway was constructed in [307] for outlining the associated roadmap. This would require further advances in both the relevant quantum and classical technologies, and a global research effort is required for integrating quantum and classical communications networks.

Abstract: QKD has been one of the most successful applications of quantum technologies, which crucially addresses some security gaps in our current communications systems [15], [308], [309]. In particular, the threat of quantum computers becoming able to crack some of the widely employed public-key cryptosystems has required developing new methodologies for sharing secret cryptographic keys among legitimate users. QKD offers a solution, based on the previously discussed laws of quantum mechanics, which offers confidentiality even for the future when large-scale quantum computers become available. Examples of such scenarios include the exchange of medical records over the Internet, which, for privacy reasons, may have to remain confidential during the lifetime of an individual and even beyond that. For such personal applications, it is vital that we expand our communications network infrastructure in such a way that it accommodates QKD deployment.

The key objective of a QKD protocol is to exchange, in a secure way, a secret cryptographic key between a pair of authenticated network users, historically referred to as Alice and Bob. In the so-called *prepare-and-measure schemes*, Alice generates a random key on her side, and then maps the corresponding bits to quantum states and sends them to Bob according to a certain protocol. Bob would then observe or measure the potentially error-infested received signals, and by exchanging some classical information with Alice via an authenticated channel, they attempt to agree about the specific choice of an identical secret key with each other. The level of security is typically characterized by a security parameter, which specifies the distance between an ideal randomly generated secret key and the one that can be obtained by the QKD protocol, accounting for the fact that Alice and Bob have the option to abort the protocol if the estimated error rate is higher than a certain threshold, because it is deemed to be tampered with by the Eve [310]. Indeed, one could argue AQ:15 that if E attempts to observe the confidential QD signal, it collapses back into the CD.

A unique property of QKD is that we can detect eavesdropping attempts, which is not possible in the CD. This allows us to limit the amount of information leakage

concerning the secret key to a third party in a point-to-point system. In order for QKD to be accessible to a wide range of customers, it is essential to cover long distances, in conjunction with a variety of classical services that NG wireless systems aim to offer. However, the challenge is that given a 0.2-dB/km fiber attenuation, at a distance of 100 km, the quantum signal is attenuated by 20 dB, i.e., to 1% of its original power and it cannot be amplified without first observing/measuring the signal, which returns it to the CD. Therefore, it is plausible that the achievable rate is a direct function of the SNR in dB, which is, in turn, determined by the distance. This physically tangible relationship results in the formulation of the salient QKD performance metric, namely, the *key rate versus distance relationship*. Hence, sophisticated terrestrial relaying techniques are required for longer distances and there is also a clear *tradeoff between the key rate versus the number of relays*, when covering a fixed distance. More explicitly, the key rate may be increased by shortening the distance of relays, but at the current state of the art, the so-called *trusted relays* must be hosted in secure customer premises for preventing tampering by Eve. For example, the Eurasian QKD link spanning from Vladivostok to Helsinke has a length in excess of 15 000 km and relies on numerous expensive relays. As a design alternative, FSO satellite links have to be harnessed for long-haul transmission. Furthermore, as alluded to above, QKD systems also require a classical channel in support of the key negotiations between Alice and Bob, which may be accommodated by the same fiber as the quantum channel by using WDM. However, utter care must be exercised to avoid that the weak quantum signal is overwhelmed by the out-of-band interference of the high-power classical signal.

We continue with a brief critical appraisal of the state of the art in Section VI-A, followed by challenges we are facing, when aiming for providing end-to-end security in networking scenarios, as detailed in Section VI-B. We conclude with a vision for the roll-out of a long-distance QKD network in Section VI-C.

A. State of the Art

1) Key Principles: The basic idea behind the original QKD protocol, known as BB84 after its inventors Bennett and Brassard [311], can be explained using the experiments shown in Fig. 29. Assume that we have a source that can generate a single photon. Let this photon propagate through a 50:50 mirror, known as a *BBS*. Then, the question arises—which one of the two ideal energy meters in Fig. 29(a) would click? Because quantum mechanics only allows discrete energy levels for each mode of light, this single photon cannot be split into a pair of smaller packets of energy. Hence, only one of the single-photon detectors would click—each with a probability of 1/2.

The second experiment in Fig. 29(b) uses two BBSs, which jointly constitute an interferometer. We know from classical optics that for a laser source at the input, the two output ports of the second beam splitter exhibit constructive and destructive interference, respectively, thus resulting in only one of the detectors registering some energy. Interestingly, the same thing happens at the quantum mechanical level for the single-photon input. This is due to the superposition principle where, after the first beam splitter, the state of the system is characterized by the single photon being in the superposition of the upper and lower arms of the interferometer. Finally, let us assume that a curious third-party observer measures which arm the photon in Fig. 29(b) has actually taken. Given this knowledge, the experiment in Fig. 29(c) becomes identical to that of Fig. 29(a), where—in contrast to the setup of Fig. 29(b)—either of the detectors may actually click.

By appropriately combining the above ideas, one can design a simple QKD protocol as follows. In this protocol, Alice uses two types of encoding, chosen at random, for transmitting her key bits to Bob. In the first type, used for key generation, she uses a dual rail system, as shown in Fig. 30(a). To send a bit 1 (0), she sends a single photon via the upper (lower) channel. In the second encoding type seen at the bottom of Fig. 30(a), Alice generates a superimposed state from the photon in the upper and lower arms, as shown in Fig. 30(b). Let us assume that at the receiver, Bob happens to opt for the matching decoder. Naturally, in a real experiment, Bob does not know which encoder Alice has used. However, he can randomly choose one of his two decoders and later check with Alice via their authenticated classical channel, whether the encoder and decoder match for a particular bit interval. In the absence of eavesdropping attempts—an ideal scenario—we would expect that the decoder of Fig. 30(a) can register clicks on either of the detectors, whereas the decoder in Fig. 30(b) should observe clicks in only one of the detectors. In this setting, if an Eve attempts to check, which channel the photon is traveling through, she would then perturb the statistics of the test rounds, which results in an increased bit error rate. For this scenario, it is possible to formulate bounds for quantifying, how much information might have been leaked to Eve. In practical QKD protocols, so-called *reconciliation* schemes relying on sophisticated classical error correction codes may be used for mitigating the error rate experienced. Finally, some of the secret key bits generated may be dropped by relying on the technique of *privacy amplification* for further confusing Eve. By contrast, if the error rate is excessive, the legitimate users may decide to abort the protocol and recommence the key-negotiation process.

To elaborate a little further on Bennett and Brassard [311] protocol, we briefly refer to Table 2 abridged from [14], where further details may be found.

1) A random binary key is generated by Alice in the classical domain, which is referred to as the raw key.
2) Then, she randomly selects either a rectilinear or diagonal polarization basis represented by a + and ×

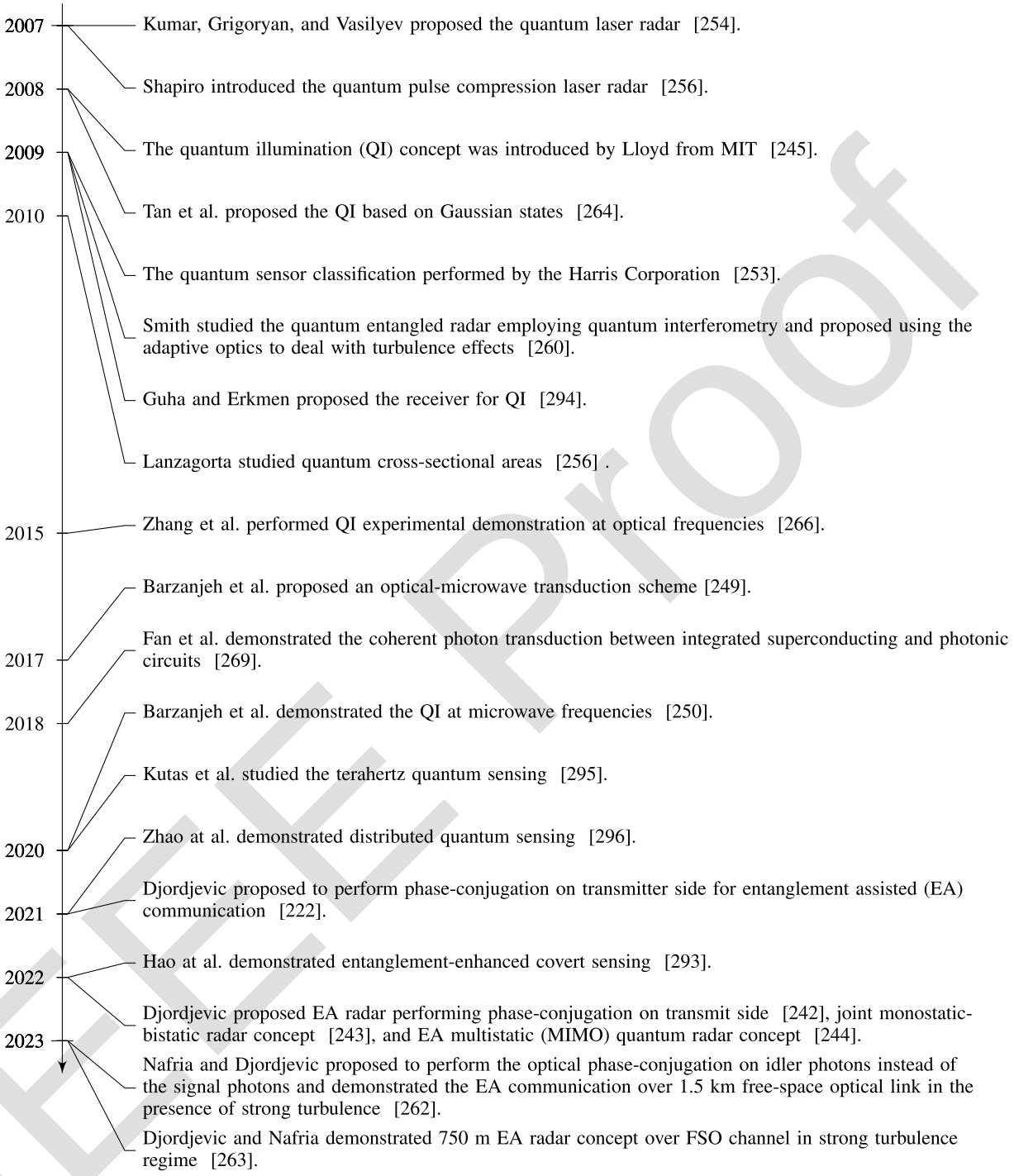

Fig. 29. ***Timeline describing the quantum radar research activities.***

character in order to convey the 0/1 bits of the raw key; this is the so-called preparation basis.

3) As shown in Table 2, the quantum state is prepared by mapping the binary key of Step (1) according to the specific polarizations of Step (2), as indicated by the arrows.
4) As for Bob, he randomly selects a so-called measurement basis and the instances where the preparation as well as measurement bases match are marked in green in Table 2.
5) The received quantum states are then measured by Bob using the random measurement basis coined in Step (4), where nothing is output, where the measurement and preparation bases are different.
6) At this stage, Bob's detected states are mapped onto 1/0 classical bits. The instances where the detected

Table 2 Prepare-and-Measure DV BB84 QKD Example (in the Absence of Eve and Noise) (©IEEE Hosseinidehaj et al. [14])

Alice													
1	Raw key	1	0	0	1	1	1	0	1	0	0	0	1
2	Preparation (or encoding) basis	+	+	×	×	+	×	+	+	×	×	+	×
3	Quantum state preparation	→	↑	↗	↘	→	↘	↑	→	↗	↗	↑	↘
Bob													
4	Measurement basis	+	×	×	+	×	×	+	×	×	+	+	+
5	Quantum state detected	→	↘	↗	→	↗	↘	↑	↘	↗	→	↑	→
6	Detected key	1	1	0	1	0	1	0	1	0	1	0	1
Classical post-processing													
7	Sifted key	1		0			1	0		0		0	
8	Parameter (or error) estimation												
9	Information reconciliation												
10	Privacy amplification												

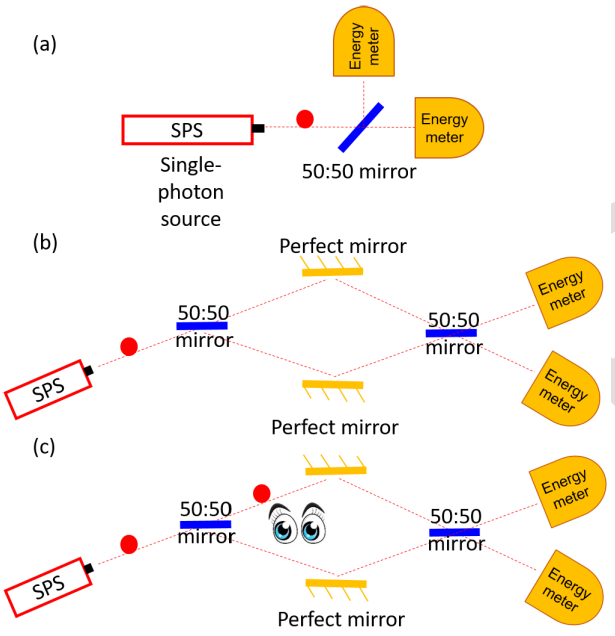

Fig. 30. ***Three experiments at the heart of BB84: (a) single photon does not split, but randomly chooses a path; (b) interference holds even at the single-photon level; and (c) making observations can change the superposition state.***

and raw key bits differ are marked in red in Table 2; these classical bits are then postprocessed as follows.

7) Only those bits are retained, which have the same preparation and measurement basis, resulting in the *sifted key*.
8) The error rate is estimated for detecting the presence/absence of Eve.
9) The information reconciliation scheme corrects errors in the shifted key.
10) Finally, the *reconciled key* is shortened by the *privacy amplification* scheme, thus reducing Eve's chances of guessing the agreed key.

2) Evolution of QKD Protocols: Historically, the BB84 protocol was inspired by some of the ideas in an earlier article by Wiesner [312], but in recent years, the field of QKD has evolved quite rapidly in different directions. Some developments have focused on simplifying the hardware requirements, while others have been related to security proofs that support these new or modified protocols. They belong to the family of DV and CV QKD protocols, which are detailed in [14] and [15].

In both cases, the security level attained effectively boils down to being able to exploit the correlation between Alice and Bob in terms of an entangled state. In the DV case, for instance, it can be shown that if Alice and Bob share a maximally entangled state, they can readily agree upon a shared secret key by measuring their share of the entangled state. In fact, the second major QKD protocol following the BB84—which was proposed by Ekert [313]— relied on verifying Bell inequality violations for a shared entangled state between Alice and Bob. Then, in 1992, a simplified entanglement-based QKD protocol was conceived by Bennett et al. [314], which is termed as the BBM92 protocol. This required similar measurement actions to those in the BB84 protocol. Since then, a large number of QKD protocols have been devised and Fig. 31 captures these evolutionary developments.

To expound a little further, the first decade of the new millennium witnessed the development of rigorous security proofs for QKD protocols. Shor and Preskill [318] offered a simple security proof for ideal BB84 based

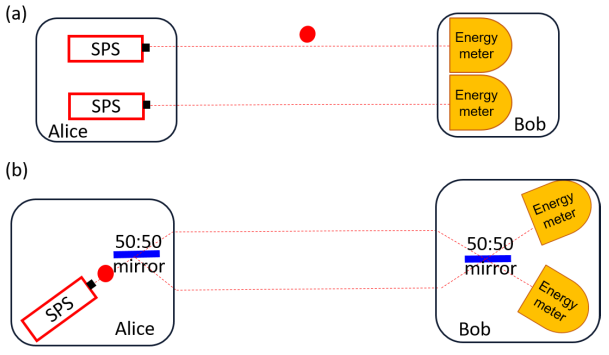

Fig. 31. ***Conjugate encodings used in our toy model QKD protocol. (a) In key transmission rounds, Alice sends a single photon on the upper (lower) arm to encode bit 1 (0). (b) In test rounds, Alice sends a superposition state to Bob.***

on entanglement distillation. Later in 2004, the security proofs were extended to the case of using weak coherent pulses (WCPs) generated by lasers, instead of the ideal single photons. The Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) framework [341] predicted that the key rate would not scale desirably versus the distance when we consider the extra photons that can exist in a coherent state. This problem was fixed by the development of the decoy-state idea [321], [322], [324], where having multiple intensities of light would facilitate for her and Bob to better estimate the key bits generated by true single-photon states. New or improved security proofs were introduced by Renner [325] and Koashi [342], which have been the basis for many later protocols conceived in the next decade.

Still referring to Fig. 31, the decade of 2010–2020 started with the conception of several experimental attacks on some QKD system implementations [343]. Interestingly, most of these attacks capitalized on some imperfections of the measurement devices in the QKD systems. As a remedy, MDI QKD systems [329], [330] emerged as a practical solution against this type of attack. Naturally, both Alice and Bob have a transmitter, but all the measurements can be carried by an untrusted party somewhere in the middle of the link. This idea led to numerous breakthroughs in the ensuing era, resulting in protocols capable of improving the key rate versus distance scaling. These are exemplified by the twin-field [338], [345] and the mode-pairing [339] QKD protocols, and to a range of others that lend themselves to integration into future generations of quantum communications networks [347].

B. Knowledge Gaps and Challenges

1) Issue of Distance: Again, due to the transmission of weak signals, point-to-point QKD suffers from a channel attenuation of about 0.2 dB/km in fiber and from hostile atmospheric propagation phenomena in FSO satellite scenarios. This may result in complete loss of signal in DV-QKD, or in an excessively low SNR in CV-QKD. As a result, the total distance over which we can exchange a secret key without using repeater or relay nodes is limited. Current terrestrial records are at around 1000 km [348], albeit at very low secret key generation rates. In Section VI-C, we will hypothesize about the roadmap of extending the reach of QKD networks to arbitrarily long distances. In our formulation, we will show how we can achieve end-to-end security in QKD networks. This may require scientific advances in several technical areas, including quantum devices, e.g., QMs, and even our quantum processing capabilities.

2) Cost and Network-Wide Deployment: For QKD to become ubiquitously available as a technology, we have to reduce the cost of deployment by sharing it among many users. This includes the cost of individual devices that have to be produced on a commercial scale as well as the infrastructure costs of running quantum applications. There are a number of promising directions to be pursued for facilitating wide-scale deployment. This includes using photonic integrated circuits to design QKD transmitter and receiver modules [334], [335]. This is particularly important for the transmitter side, which is expected to be the main terminal that all the end users would need. In terms of the infrastructure, it is very important to use the existing fiber-optic networks laid out across the globe for both quantum and classical applications. A lot of efforts have, therefore, been directed at integrating QKD links with WDM channels. Again, the key challenge that we face when sending quantum and classical signals over the same optical fiber is that the crosstalk generated by the high-power classical channels may overwhelm the weak signals traveling through the quantum channels. Sophisticated filtering techniques have been used to make this possible, and several demonstrations have confirmed the feasibility of this [328], [350], [352], [353], [355]. Resource allocation in such networks is another challenging issue, requiring the holistic optimization of the overall performance [356], [358]. A further largely unexplored area is the development of the network stack for quantum applications [359], [360], and ensuring its compatibility with the evolving classical communications solutions, such as software-defined networking [361].

3) QKD in Wireless Terrestrial and Satellite Settings: Another important issue, especially with regard to compatibility with emerging 6G technologies, is the adaptability of QKD to wireless solutions. This has been of interest from early on, and in 2006, a group of scientists at Bristol University, Bristol, U.K., along with their collaborators at HP Labs developed the first demonstration of a handheld QKD device exchanging a key with an ATM-like receiver [326]. This was further enhanced recently and demonstrated in indoor settings [327]. The next step along this line is to enable wireless access to QKD networks (see Fig. 32). The related theoretical analysis suggests that this is within reach even with the aid of off-the-shelf technology in benign indoor settings under mild lighting conditions [363], [365] although extending it to outdoor applications is still an open challenge [366].

On a completely different distance scales, wireless settings are capable of substantially improving the reach of QKD systems by employing satellite-based quantum communications techniques. The key advantage of relying on satellites is that the attenuation in free space scales with the square of the distance, rather than attenuating it exponentially as in optical fibers. Hence, the total path loss in the satellite-to-ground link of a LEO satellite may be as low as 30–40 dB, when the satellite passes over a ground station. This allows us to connect nodes on different continents of the world via orbiting satellites [337], and eventually via a constellation of such satellites. Early demonstrations by the in-orbit Chinese satellite referred to as Micius have already paved the way in this regard [336]. A lot of global investment has been allocated to further this line of technology since it is envisaged that a satellite-based

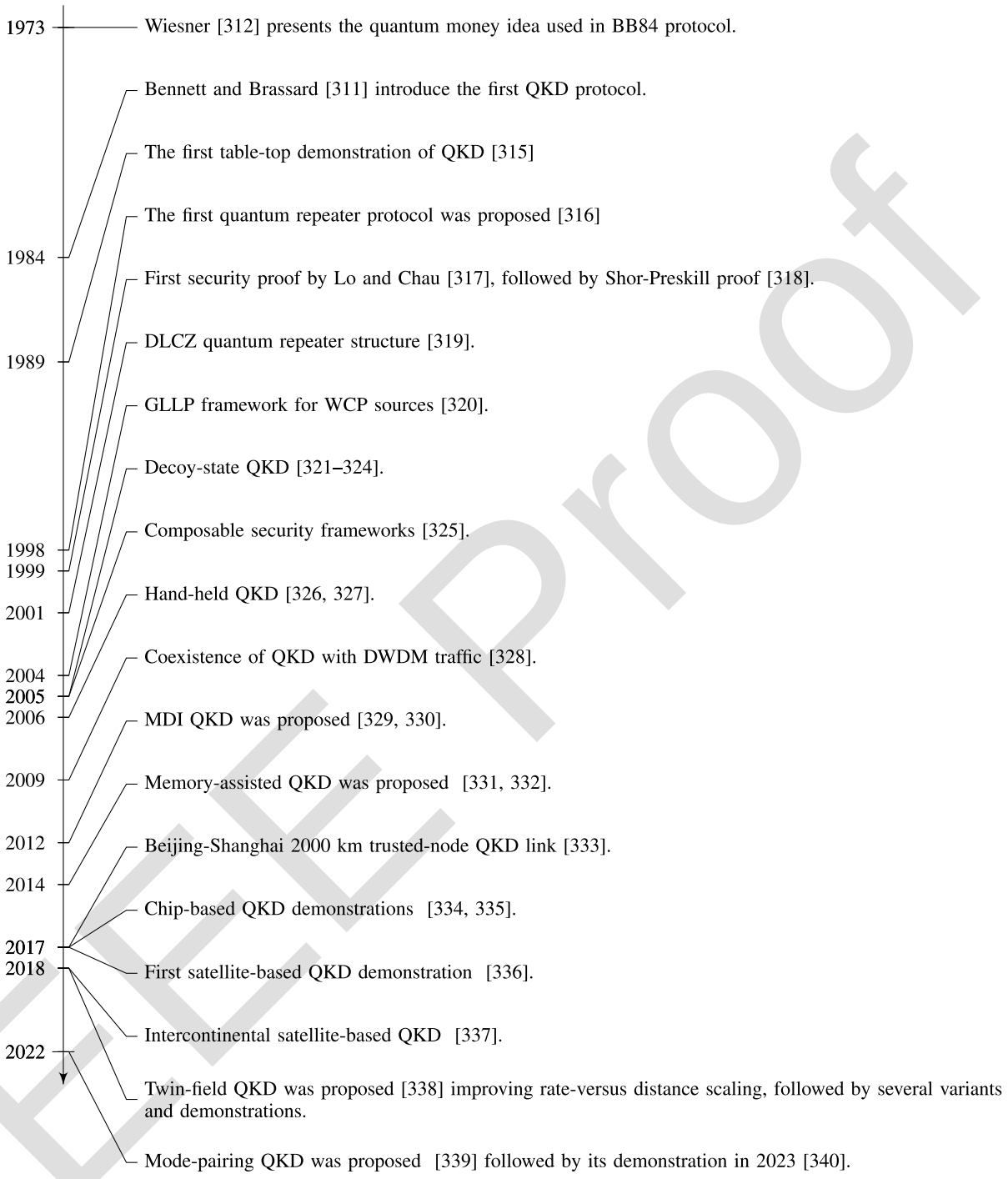

Fig. 32. ***Timeline of QKD milestones.***

infrastructure could be part of our future generations of quantum networks [368].

Satellite-based QKD may also allow for new security frameworks, where some of the assumptions concerning the Eves are relaxed [369], [370], [372]. This is primarily because it is hard for Eve to intercept an optical line-of-sight satellite link without being visually detected [372].

Another interesting matter when it comes to wireless QKD systems is the range of frequencies over which QKD can operate. Conventionally, QKD has only been demonstrated in the optical regime. The key advantage of the optical band over the RF bands is that the effect of QD noise is less dramatic than in the RF band. This is because there is only a negligible amount of thermally generated optical noise compared to the optical shot noise. By cooling down our detectors, QKD can operate in a shot-noise-limited regime, with the thermal noise effects imposed by the dark current being orders of magnitude

lower. However, this balance would gradually shift, as we move to lower and lower frequencies, and once we reach the THz regime, we should deal with the inherent thermal noise in our devices and channels [373]. That said, theoretically, it might be possible to reduce the frequency even down to 0.1 THz, and be able to exchange a secret key over a few meters in indoor QKD scenarios. At larger distances, THz could be an option in intersatellite quantum communications, where the free-space channel has low temperature [374]. Finally, regardless of whether considering the THz or the optical regime, wireless QKD systems would substantially benefit from sophisticated MIMO techniques, especially in hostile channel conditions [375], [376], [377].

4) Implementation Security: As QKD becomes more and more practical, it is important to appropriately adjust the corresponding security proofs to match the reality of the system implemented. For instance, in a typical QKD protocol, we may have to generate certain states for the protocol to rely on. However, once we implement the protocol, the states generated by the devices employed may deviate from the required one. Implementation-oriented security deals with such issues [378] and aims to offer rigorous security proofs that can be used in commercial settings. Other issues that become relevant in such settings are the use of a finite number of data points to bound the amount of information leaked to Eve, as discussed in [379], [380], and [381] for example. The assumptions we make about the probability of certain attacks constitute another area of QKD research. For instance, in the so-called Trojan horse attack, an Eve can shed strong light on Alice's transmitter in order to glean information about the settings employed. In the field of implementation security, we account for possible leakage of information under practical constraints and derive the achievable secret key rate [382].

Another important factor in the deployment of QKD is the need for characterizing the devices employed. Different QKD protocols set different requirements in this regard and as expected, typically the best performers require detailed knowledge of the transmitter and receiver specifications, while others such as MDI-QKD and device independent QKD [383] aim for alleviating this requirement. Naturally, it might be very challenging for an end-user to engage with the characterization process. To circumvent this issue, standardization bodies are putting together certification processes that enable the QKD industry and customers to do business with each other in a convenient and reliable way. The entire list of QKD-oriented standards formulated across the globe can be found in [15].

C. Research Roadmap

The prospect of deploying wide-scale quantum communications networks has received a considerable boost over the past decade. This is partly driven by several scientific breakthroughs facilitated by substantial funding from governmental and industrial bodies. As seen at a glance in Fig. 33 to be detailed later in this section, different countries across the globe—including the U.K., Germany, The Netherlands, and France, among others in Europe, as well as China, Japan, and the USA—have invested on the order of several billion dollars overall. European Union has also initiated an EU-wide 10-year flagship program of the same scale to lead the second quantum revolution.

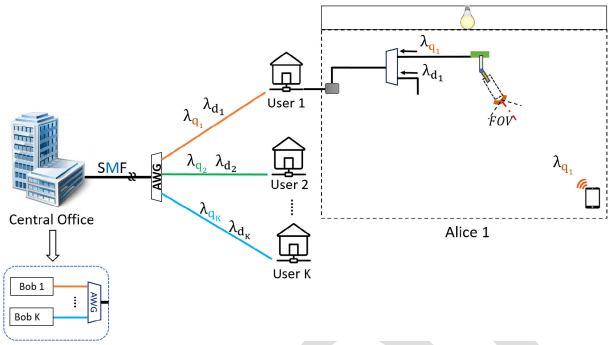

Fig. 33. *Schematic view of exchanging secret keys between an indoor wireless user, Alice, and the central office (CO) within a DWDM passive optical network. SMF: Single-mode fiber and AWG: arrayed waveguide grating.*

In the context of the above developments, it is important to have a a realistic view of how quantum technologies will evolve in the future, and in which fields we as a community have to invest research efforts. The research roadmap envisioned in this section is going to address this subject from the perspective of deploying QKD systems across our communications networks. There have been several other recent roadmap documents that approach the question of "quantum futures" from different angles. Notably, Wehner et al. [384] adopted an application-centric approach for predicting the future evolution of the Qinternet relying on six milestones along their predicted roadmap. By contrast, Awschalom et al. [293] focused more on the hardware required. As a further advance, Long et al. [307] added an extra stage to the six-stage roadmap of [384] for the development of the Qinternet by introducing the concept of *secure repeater networks (SRNs)*, which is compatible with the existing classical Internet and relies on the popular philosophy of requiring excessively complex operations for breaking security. However, their SRN concept relying on the QSDC concept of Section VII-G [385]—rather than QKD—incorporates eavesdropping detection, which is a valuable extra feature.

Again, at this stage, we use [360, Fig. 35] for connecting the state-of-the-art Section VI-A, the knowledge-gap Section VI-B, and the future roadmap Section VI-C. Observe in the figure that the architecture of all existing QKD networks is rather simple. Furthermore, for covering large distances by optical fiber requires numerous repeaters, where the quantum signal is observed and the resultant classical signal is amplified before preparing the quantum states for transmission to the next relay. A similar

procedure has to be applied also for relaying-aided FSO-based satellite systems, but naturally, they are capable of covering larger distances. Observe, furthermore, in the figure that these networks tend to rely on rather diverse QKD protocols. The acronyms identifying the protocols are listed in the caption of the figure, and their specific features are detailed in [15] for readers, who would like to probe further. Suffice to say that the key performance metric of QKD networks is the secret key rate versus distance. This is because the quantum signal must not be amplified and thus it is gradually attenuated throughout its propagation. The resultant attenuated signal can only support a reduced key rate.

Observe, for example, at the bottom right corner of Fig. 33 that the Beijing–Shanghai link using the BB84 protocol has 31 hops between the source and destination and it relies on so-called *trusted relays*, which must be hosted in secure premises to avoid eavesdropping on the classical signal to be amplified. By contrast, some of these networks rely on so-called *untrusted relays*, which rely on more secure protocols than their trusted counterparts. They may also be referred to *trust-free relays/nodes*, which are capable of resisting eavesdropping due to their sophisticated entanglement-based protocol design. Hence, they do not have to be in secure premises. Clearly, a wide variety of protocols having different levels of security have been harnessed across the globe, and the issues of *trusted versus trust-free* relay nodes will be further detailed as part of our evolutionary roadmap of Phase I–Phase III. Suffice to say that for constructing the global Qinternet of the future, QKD protocol converters are required, as detailed in [360]. This also underlines the importance of global standardization for connecting the network segments relying on different protocols, as discussed in [15] for readers, who might like to explore further.

We believe that the roadmap envisioned here complements the above efforts and altogether offers a tangible serve-oriented perspective on how quantum communications technologies may evolve.

Our solution envisaged for long-distance QKD evolves through multiple developmental phases, which would naturally define relevant milestones in our roadmap seen in Table 3. Below, we highlight what might be delivered in each developmental phase, and what would be required to achieve it, with speculative timescales for the relevant milestones.

1) Phase I: Trusted Node QKD Networks: The first phase of deployment, which is already in service, relies on trusted node-based QKD. Briefly, in trusted node QKD, secret key exchange between parties A and B is carried out via multiple intermediate nodes located at sufficiently short distances from each other. Hence, efficient point-to-point QKD is feasible between the adjacent nodes without excessively reducing the key rate, as illustrated in Fig. 34. If these intermediate relay nodes can be trusted by parties A and B, then the *local key* exchanged between the adjacent nodes can be readily used for relaying an *end-to-end key* between A and B. If multiple independent paths exist between A and B, then the requirement on trusting the middle nodes can be alleviated [386].

From a technology development perspective, trusted node-based QKD would certainly serve as a significant stepping stone toward future phases of deployment. This is why at the time of writing trusted node QKD research is at the core of almost all network demonstrations. This includes the Chinese backbone network, the EU OpenQKD networks, and the U.K. Quantum network, *inter alia*. This structure is expected to have certain niche markets among high-security sectors, including military and government bases as well as the financial and health sectors. While the assumption of all nodes being trusted may be acceptable in certain use cases, this is not necessarily acceptable in high-security scenarios. Gazing into the future, the community has to construct chip-based QKD [387], efficient detectors, and reliable sources. Radical frontier research is required also on how to manage the resources of a hybrid communications network that supports both quantum and classical applications.

Hence, we recognize that the expansion of trusted node-based QKD constitutes an essential part of the roadmap leading to large-scale QKD networks. We might speculate that the next decade will be dedicated to improving the performance of all different components, as well as expanding the market within its relevant target sectors.

2) Phase II: Partially Trusted QKD Networks: The next evolutionary phase following a trusted node QKD network is an upgraded network, in which the trust requirement on relay nodes in the middle has been reduced, so that a larger group of customers may opt for harnessing QKD services. There are several promising technologies that facilitate this transition.

1) *MDI QKD:* MDI QKD allows a pair of users to exchange a secret key via an untrusted node. This may only sound like a small adjustment to the trust issue, but in practice, this will allow a larger number of enterprises to use the service since they can use the service provider nodes to connect two of their trusted nodes, as shown in Fig. 35. This way the need for having a fully private network would be alleviated. Moreover, with the advent of the new twin-field QKD protocols [338], [388], [389], the MDI structure can be used for improving the rate-versus-distance scaling as well. MDI protocols have been around for a while, but have not been widely used in commercial settings. They pave the way for future phases of deployment.
2) *Memory-assisted QKD:* An alternative technique of improving the rate versus distance scaling is to harness QMs in the MDI setup [331], [332]. This will constitute a rudimentary repeater system that relies on quantum memories and will be the stepping stone to the solutions that have to be developed in the third phase. The first demonstrations of such systems have

QKD Family	Protocols	Features	Environments	Advantages	Limitations
SPM	BB84, GG02, DPS, SARG04, COW, etc.	QTx-QRx	Optical fiber Free space	High key rates High maturity	Relatively low security level Relatively low scalability
EB	E91, BBM92, etc.	QRx-QTx-QRx	Optical fiber Free space	High scalability High security level	Relatively low key rates Relatively low maturity
MDI	Original MDI, TF, etc.	QTx-QRx-QTx	Optical fiber Free space	Long distance High security level	Relatively low robustness Relatively low maturity

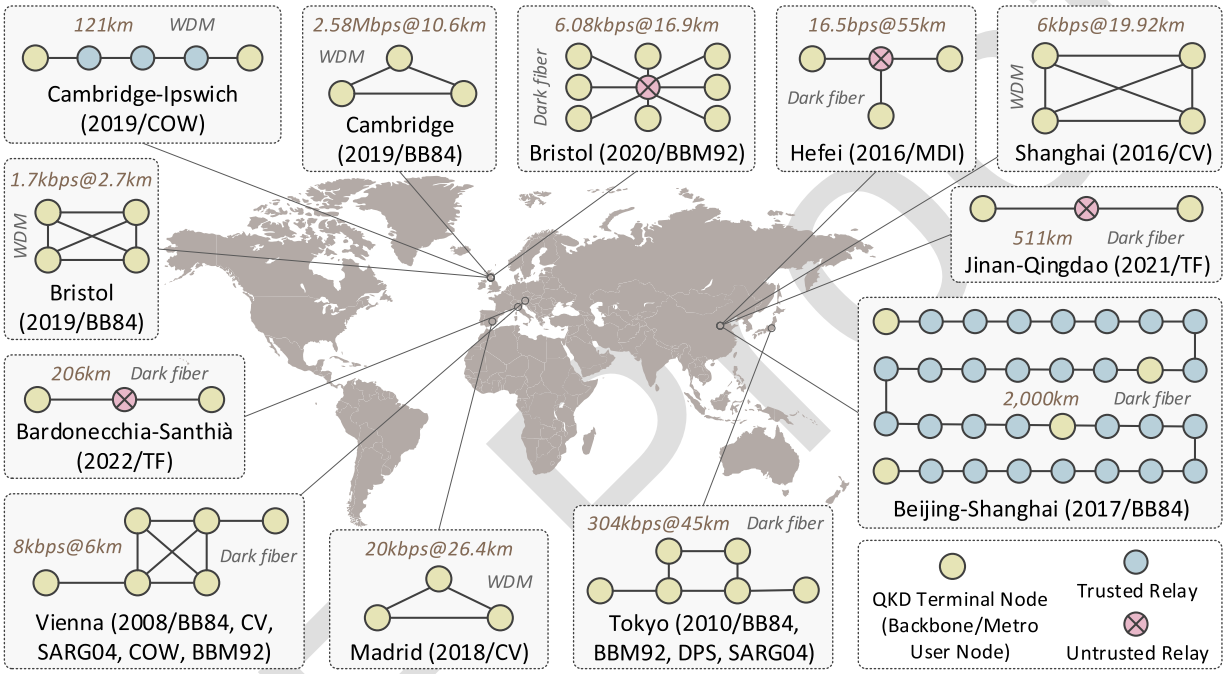

Fig. 34. *Diverse families of QKDPs and typical field trials of quantum networks around the world. SPM: Single-prepare-and-measure; EB: entanglement-based; MDI: measurement-device-independent; QTx: QKD transmitter; QRx: QKD receiver; BB84: Bennett–Brassard-1984; GG02: Grosshans–Grangier-2002; DPS: differential phase shift; SARG04: Scarani–Acín–Ribordy–Gisin-2004; COW: coherent-one-way; E91: Ekert-91; BBM92: Bennett–Brassard–Mermin-1992; CV: continuous-variable; and TF: twin-field (©IEEE Cao et al. [360]).*

just been reported in the literature [390], paving the way for their introduction into realistic/commercial settings.

3) *Satellite-based QKD:* One of the emerging routes to long-distance quantum communications is via satellites, possibly in different orbits. They may be harnessed as intermediate relay nodes between two ground stations. Prototype experiments of this nature have already been carried out using the Micius satellite, for example, for exchanging a secret key between China and Austria by only trusting the satellite node [337]. This structure can also be expanded by using a constellation of satellites to serve a large number of users [368]. It can also be employed in the near future for further expanding quantum communications networks during the developmental phase III to the space domain [368].

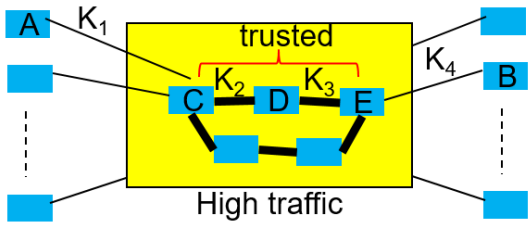

Fig. 35. *Schematic of a trusted node QKD network. For users A and B to exchange a secret key, we need to create a secret key between any two adjacent nodes that connect A to B (e.g., C–E). Then, we can use these keys to securely relay a key from A to B. If there are multiple paths between A and B, we can generate separate keys using each path and then combine them in the end.*

It is envisaged that the above technologies can make substantial advances in the next decade or so, and will prepare us for the final phase of deployment when no trust concerning the intermediate relay nodes of the network is needed.

3) Phase III: Trust-Free QKD Networks: The key enabling idea behind trust-free QKD networks is to distribute entanglement between a pair of remote nodes in an efficient

Table 3 Possible Roadmap, With Speculative Timelines, for Deploying QKD Technologies in Our Existing and Developing Infrastructures. The Deployment Can Take Place in Three Phases, Where in Each Phase, by Employing More Advanced Technologies, the Trust Requirement on the Service Provider Nodes Is Reduced

Stage of Development	Major milestones, services, or functionalities	Timeline (years)
Phase I: Trusted Node QKD Networks	Reliable chip-based QKD modules	0-5
	QKD standardisation for deployment on existing infrastructure	0-5
	Early demonstrations of additional satellite QKD links	0-5
	Adding QKD functionalities/modules to telecom networks	0-10
	Offering QKD services to private networks	0-10
	Offering QKD services via wireless optical links	0-10
Phase II: Partially Trusted QKD Networks	Upgrading telecom networks to support MDI protocols	5-10
	Upgrading telecom networks to support memory-enhanced protocols	5-10+
	Expanding satellite-based QKD and linking it to ground networks	5-10+
Phase III: Trust Free QKD Networks	Lab-based demonstrations of simple quantum repeater chains with no distillation	0-5
	Lab-based demonstrations of advanced quantum repeater chains with QEC-based distillation	5-10
	Field demonstrations of simple quantum repeater chains with no distillation	5-10
	Field demonstration of advanced quantum repeater chains with QEC-based distillation	10-15
	Adding repeater nodes in space	10-15+
	Upgrading telecom networks to support repeater nodes	10-15+

way. The users can then run an entanglement-based QKD protocol [314] to share a secret key while still being able to limit the amount of information that might become leaked to any potential Eve. In effect, how the network provides the users with the entangled state does not matter from a security-assurance perspective. Hence, no trust is required concerning intermediate relay nodes. An entanglement-based network can also accommodate many other quantum applications, such as distributed quantum computing since reliable quantum data transfer can be achieved via quantum teleportation [384].

The creation of long-distance entanglement distribution requires fully fledged quantum repeaters [316], [319], [393], [394]. Quantum repeaters extend the single-hop entanglement over a short distance to longer distances by employing certain joint measurements, while relying on QMs. The entangled state generated in this way may have to be distilled for obtaining a higher quality entangled state. Based on the specific stage of development, the joint measurement and/or entanglement distillation process may be carried out either in a probabilistic [319], [395] or deterministic [392] manner. The probabilistic solutions often offer lower key rates and require longer storage times. By contrast, the deterministic solutions require reliable quantum processing capabilities. Depending on the quality of quantum processing operations carried out in the quantum repeater, we can specify what security level may be expected from our repeater-based network. In the long run, when high-performing quantum computers are available, we can in principle use quantum repeaters that do not require long storage times, but, rather they map the QD data to large clusters of photons and send them from one node to another, where each node can mitigate the errors along the way and regenerate the encoded state [393].

The exact timing of commercial quantum repeaters may be hard to predict, but we envisage their appearance in 15+ years, as indicated by the early demonstrations relying on probabilistic measurements [396], [397]. Quantum repeaters that rely on the QEM techniques of Section III and on the QEC codes [398] similar to those discussed in Section II are expected to speed up this evolutionary process by eliminating the propagation of errors across consecutive hops. But again, advances are also required in the field of QM units and their interaction with light [400].

VII. NG QUANTUM-AIDED WIRELESS ROADMAP

A. Holistic Roadmap

In this system-oriented section, we further develop the initial vision of the fiber-oriented Qinternet highlighted in Fig. 1 and extend it to the even broader quantum-native NG wireless roadmap of Fig. 36 relying on a physical-, network-, and application-layer vision. These holistic system-oriented aspects are detailed in great depth by Zhou et al. [401].

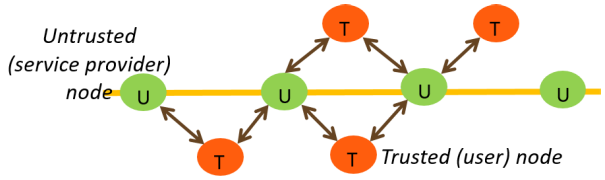

Fig. 36. *Schematic of a partially trusted QKD network. We exchange a key, using, e.g., MDI techniques, between two adjacent trusted (T) nodes via the untrusted (U) node that connects them together. The key exchange between the two trusted nodes not directly linked via an untrusted node can then be done similarly to that of Fig. 34.*

As seen at the bottom of Fig. 36, a diverse variety of industrial robots, autonomous vehicles, virtual/augmented reality (VR/AR) services, industrial process controllers, and even future smartphones and tablets are expected to benefit.

Recall from Section II that *the impairments imposed by quantum circuits are typically modeled by the depolarizing channel of Fig. 3*. In this context, one could draw a parallel with the classical AWGN channel, which models the Brownian motion of electrons. *By contrast, when considering quantum communications over quantum channels, the physical properties of the FSO quantum transmission medium or of the fiber have to be considered.*

In this practical transmission context, much of the quantum communications research has been based on either optical fiber or FSO-based satellite communications. For a detailed discourse on satellite-based QKD channels, please refer to [14]. Indeed, NTN based on satellites constitutes one of the most topical subjects in the 3GPP study schedule, as shown in [402, Fig. 6], which is a study item in Release 19 of the 5G/6G standardization. This subject area is pictured in the center of Fig. 36 and it is expected to attract continued research atteantion. The network layer echoes the architecture of Fig. 1 and the terminals portrayed at the bottom of Fig. 36 support the services of the application layer seen at the top of the figure. *In the rest of this section, we will hypothesize as to what if any lessons of classical wireless communications may be relied upon in the design of future quantum communications systems.*

B. Spectrum Harmonization in the PHz Band

In [403], the concept of spectrum harmonization was conceived, which relies on a sophisticated cognitive spectrum sensing scheme capable of identifying the most suitable wavelength or frequency domains for supporting a specific service. Briefly, the authors aim to unify the existing IR, VL, and ultraviolet (UV) subbands while also exploring the potential of the petahertz (PHz) band to support secure bandwidth-thirsty telepresence/VR-style applications. A hitherto scarcely used unlicensed spectral band is the PHz band, which is defined as the frequency range spanning from 0.01 to 100 PHz, where 1 PHz $= 10^{15}$ Hz. The corresponding optical wireless wavelength domain stretches from 30 μm to 3 nm, as shown in Fig. 37, which encompasses the THz, the IR, the VL, and the UV subbands. Their propagation properties are detailed by Xu et al. [403], but these bands deserve further exploration in the context of quantum communications. The most mature solutions can be found in the realms of VL communications. Xu et al. [403] also survey their modulation schemes, system performance, multiple access techniques, and networking. They conclude with a range of PetaCom challenges and open research issues.

C. Quantum Communications in the THz Band

The feasibility of short-range quantum communication in the THz band has been critically appraised by Ottaviani et al. [373]. In this context, Liu et al. [404] conceived a continuous-valued satellite-to-satellite secret sharing scheme [405] and a CV-QKD arrangement relying on THz-band multicarrier transmissions [406]. A range of THz-band hardware aspects were discussed in recent years in [373], [407], [408], [409], and [410], with special attention dedicated to the conception of sensitive detectors [411], [412], [413], [414], [415], [416], [417], [418]. The next few years may be expected to unveil further advances in the THz band, which may be able to usher in an era of RF-based quantum communications.

D. MIMO Techniques for Quantum Communications

The field of classical wireless systems has been revolutionalized by the conception of MIMO techniques, which rely on a combination of multiple antennas and sophisticated signal processing, as detailed in [419]. The four basic MIMO types routinely used in the CD are [420] STCs, SM schemes, spatial division multiple access (SDMA) arrangements, and beamformers (BFs) [420]. Laser-based narrow beams naturally lend themselves to angularly selective quantum communications, but a whole suite of other MIMO solutions have been conceived either for improving the reception quality or for increasing the throughput attained [375], [377], [421], [422], [423], [424]. As a representative result, Zhou et al. [424] benchmarked the performance of an MU-MIMO scheme against that of a classical scheme relying on an $N \times M = 4 \times$ 16-D array, which attained a substantial gain for transmission over a Gamma–Gamma fading link.

E. Multiple Access for Quantum Communications

In order to support multiple quantum communications users, multiple access methods are required. Hence, the cardinal question arises, as to which of the numerous classical multiple access techniques might lend themselves to amalgamation with quantum communications. In this context, a CDMA-based multiuser system was designed by Razavi [425], Rezai and Salehi [426], and Sharma and Banerjee [427], where unique user-specific spreading

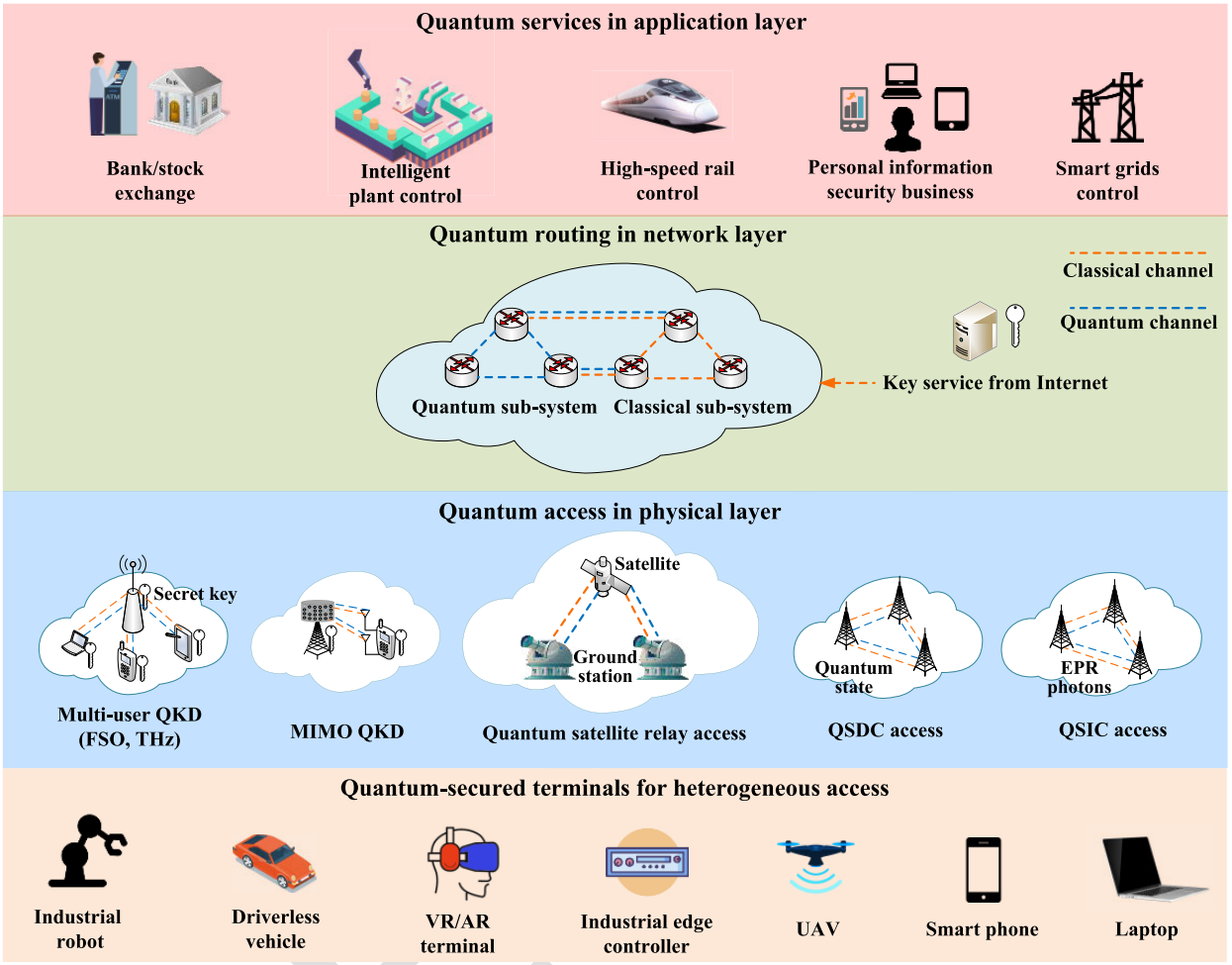

Fig. 37. *NG quantum-secured wireless system vision. The integration of QECC of Section II, QEM of Section III, QML of Section IV, quantum radar of Section V, and QKD of Section VI under the NG wireless vision will be a long-term development process. In the future, quantum-secured terminals are expected to appear in support of heterogeneous access. Quantum-secured technologies, such as QKD and QSDC, may be harnessed for quantum access in the physical layer. In the network layer, QML and quantum computing may be employed for quantum routing, and at the application layer, compelling quantum-secured services will become available, which also facilitate eavesdropping detection (©Zhou et al. [401]).*

codes were employed for distinguishing the users. By contrast, optical OFDM was employed in [428] and [429] for QKD transmission.

F. Network Coding for Quantum Communications

In the simplest form of CD network coding, the intermediate relay nodes between a pair of communicating parties use a modulo-two gate for combining the data streams received from both destination. This allows us to detect both the identical and different bit positions. This capability can be exploited for reducing the teletraffic of the network. Hence, network coding is capable of increasing the overall throughput, despite reducing the amount of energy required per packet as well as the latency of packets [430].

Due to the inherent nature of quantum communications—namely, that copying of quantum information is precluded by the no-cloning theorem—the question arises again as to whether the QD counterpart of classical network coding might be created. This dilemma was raised in [431] and [432]. However, provided that preshared entanglement may be made available [433], [434], [435], [436], [437], [438], [439], [440] or a high-rate classical channel may be harnessed [432], [441], [442], [443], QNC is indeed realizable [12].

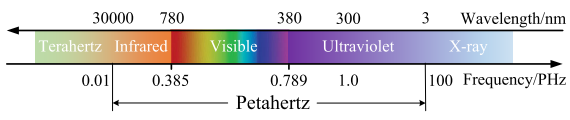

Fig. 38. *PHz band (©Xu et al. [403]).*

G. Quantum-Secured Direct Communications

Recall from Section VI that QKD solutions carry out key negotiation in the QD, but the associated encryption

process is reminiscent of its classical counterpart. By contrast, QSDC constitutes a complete QD communications solution [385]. However, the original QSDC protocol of Long and Liu [444] relies on a block-based communications philosophy, which necessitates the employment of QM. However, QM having an adequate retention duration is unavailable at the time of writing. This impediment has then been remedied in [444] and sophisticated solutions circumventing this problem were proposed in [445]. At the time of writing, QSDC is developing in strides, to a great extent, thanks to the pioneering frontier research at Tsinghua University, as detailed in [307], [446], [447], [448], [449], and [450].

H. Quantum-Search-Aided Solution of Large-Scale Classical Wireless Search Problems

When large-scale quantum computing becomes a commercial reality, numerous demanding search problems routinely found in science and engineering may be solved more efficiently than by harnessing classical search algorithms. The field of wireless communications also has numerous large-scale search problems, as exemplified by the following nonexhaustive list [8], [451].

1) *MUD [5], [6]:* The complexity of classical maximum-likelihood MUD in the uplink increases exponentially with the number of users, and thus is not practical with classical algorithms, specifically for large-dimensional systems.
2) *Noncoherent multiple symbol differential detection in high-Doppler wireless systems [7]:* Differential modulation relying on noncoherent detection over multiple symbols is an attractive alternative for coherent detection and provided performance gains over conventional noncoherent detection. However, it is computationally intensive.
3) *Large-scale beam-alignment problems of mm-wave systems:* Beamforming for large-scale MU-MIMO systems is another computationally intensive search problem whose complexity increases with the number of users and antenna dimensions.
4) *Joint channel estimation and data detection [452]:* Joint channel estimation and MUD are imperative for improving the performance of iterative receivers. However, such joint processing incurs high complexity, especially for high-dimensional wireless systems.
5) *MUT [453]:* Optimizing MUT on the downlink is another computationally intensive search problem, particularly for rank deficient systems with limited channel state feedback from the users.
6) *COMP:* COMP is being used in LTE and 5G for enhancing network coverage and capacity. Resource allocation for COMP is another challenging search problem, as it requires joint optimization of data rate, interference, and network capacity.
7) *Localization problems [11]:* High localization accuracy and infrastructure/scenario constraints increase the computational complexity of optimal full-search-based localization problems.
8) *Multiobjective system optimization [9], [10]:* Wireless systems also have other multiobjective optimization functions, for example, joint delay, energy, and load optimization for routing in multihop networks having a large number of nodes.
9) Recall that the quantum signal must not be amplified because it would collapse back to the CD; relaying plays a pivotal role in extending the length of quantum networks, as detailed in [15]. As a design alternative, LEO satellites may be employed for covering large distances [454] via the satellite-to-ground downlink and the ground-to-satellite uplink. Since the dimensions of the satellite are severely limited, its receiver aperture is typically much smaller than that of the ground station. Hence, the uplink reception at the satellite requires substantial further research, as detailed in [454].

Valued colleague, join this community effort, which is dedicated to solving the suite of open problems touched upon in this treatise! ■ AQ:16

REFERENCES

[1] 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.
[2] Z. Babar et al., "Polar codes and their quantum-domain counterparts," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 123–155, 1st Quart., 2019.
[3] 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.
[4] D. Chandra, S. X. Ng, and L. Hanzo, "EXIT-chart aided design of irregular multiple-rate quantum turbo block codes," *IEEE Access*, vol. 11, pp. 96177–96195, 2023.
[5] P. Botsinis, S. X. Ng, and L. Hanzo, "Fixed-complexity quantum-assisted multi-user detection for CDMA and SDMA," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 990–1000, Mar. 2014.
[6] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Iterative quantum-assisted multi-user detection for multi-carrier interleave division multiple access systems," *IEEE Trans. Commun.*, vol. 63, no. 10, pp. 3713–3727, Oct. 2015.
[7] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Noncoherent quantum multiple symbol differential detection for wireless systems," *IEEE Access*, vol. 3, pp. 569–598, 2015.
[8] P. Botsinis et al., "Quantum search algorithms for wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1209–1242, 2nd Quart., 2019.
[9] D. Alanis, P. Botsinis, Z. Babar, S. X. Ng, and L. Hanzo, "Non-dominated quantum iterative routing optimization for wireless multihop networks," *IEEE Access*, vol. 3, pp. 1704–1728, 2015.
[10] D. Alanis, J. Hu, P. Botsinis, Z. Babar, S. X. Ng, and L. Hanzo, "Quantum-assisted joint multi-objective routing and load balancing for socially-aware networks," *IEEE Access*, vol. 4, pp. 9993–10028, 2016.
[11] P. Botsinis et al., "Quantum-assisted indoor localization for uplink mm-wave and downlink visible light communication systems," *IEEE Access*, vol. 5, pp. 23327–23351, 2017.
[12] 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.
[13] D. Chandra, P. Botsinis, D. Alanis, Z. Babar, S.-X. Ng, and L. Hanzo, "On the road to quantum communications," *Infocommunications J.*, vol. 14, no. 3, pp. 2–8, 2022.
[14] 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.
[15] 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. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, 2nd Quart., 2022.
[16] 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, Jun. 2020.
[17] R. Van Meter and S. J. Devitt, "The path to scalable distributed quantum computing," *Computer*, vol. 49, no. 9, pp. 31–42, Sep. 2016.
[18] J. F. Fitzsimons, "Private quantum computation: An introduction to blind quantum computing and related protocols," *NPJ Quantum Inf.*, vol. 3, no. 1, pp. 1–11, Jun. 2017.
[19] I. L. Chuang, D. W. Leung, and Y. Yamamoto, "Bosonic quantum codes for amplitude damping," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 2, pp. 1114–1125, Aug. 1997.
[20] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler, "Asymmetric quantum codes: Constructions, bounds and performance," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 465, no. 2105, pp. 1645–1672, May 2009.
[21] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.
[22] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, pp. 2493–2496, Oct. 1995.
[23] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "The road from classical to quantum codes: A hashing bound approaching design procedure," *IEEE Access*, vol. 3, pp. 146–176, 2015.
[24] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996.
[25] A. Steane, "Multiple-particle interference and quantum error correction," *Proc. Royal Soc. London A, Math., Phys. Eng. Sci.*, vol. 452, no. 1954, pp. 2551–2577, 1996.
[26] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, pp. 793–797, Jul. 1996.
[27] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, no. 1, pp. 198–201, Jul. 1996.
[28] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 5, pp. 3824–3851, Nov. 1996.
[29] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Inst. Technol., Pasadena, CA, USA, 1997.
[30] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 3, pp. 1862–1868, Sep. 1996.
[31] R. Cleve, "Quantum stabilizer codes and classical linear codes," *Phys. Rev. A, Gen. Phys.*, vol. 55, no. 6, pp. 4054–4059, Jun. 1997.
[32] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2315–2330, Oct. 2004.
[33] A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 6, pp. 4741–4751, Dec. 1996.
[34] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 1, pp. 33–38, Jul. 1997.
[35] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.
[36] M. Grassl and T. Beth, "Quantum bch codes," in *Proc. 10th Int. Symp. Theor. Electr. Eng. (ISTET)*, 1999, pp. 207–212.
[37] A. M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2492–2495, Nov. 1999.
[38] L. Xiaoyan, "Quantum cyclic and constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 547–549, Mar. 2004.
[39] A. M. Steane, "Quantum Reed–Müller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1701–1703, Jul. 1999.
[40] M. Grassl, W. Geiselmann, and T. Beth, "Quantum Reed–Solomon codes," in *Proc. 13th Int. Symp. Appl. Algebra, Algebr. Algorithms Error-Correcting Codes (AAECC)*. Cham, Switzerland: Springer, 1999, pp. 231–244.
[41] A. Y. Kitaev, "Quantum computations: Algorithms and error correction," *Russian Math. Surv.*, vol. 52, no. 6, pp. 1191–1249, Dec. 1997.
[42] A. Y. Kitaev, "Fault-tolerant quantum computation by anyons," *Ann. Phys.*, vol. 303, no. 1, pp. 2–30, Jan. 2003.
[43] K. Fujii, *Quantum Computation With Topological Codes: From Qubit To Topological Fault-Tolerance*, vol. 8. Cham, Switzerland: Springer, 2015.
[44] S. B. Bravyi and A. Yu. Kitaev, "Quantum codes on a lattice with boundary," 1998, *arXiv:quant-ph/9811052*.
[45] D. Horsman, A. G. Fowler, S. Devitt, and R. V. Meter, "Surface code quantum computing by lattice surgery," *New J. Phys.*, vol. 14, no. 12, Dec. 2012, Art. no. 123011.
[46] H. Bombin and M. A. Martin-Delgado, "Topological quantum distillation," *Phys. Rev. Lett.*, vol. 97, no. 18, Oct. 2006, Art. no. 180501.
[47] J. Haah, "Local stabilizer codes in three dimensions without string logical operators," *Phys. Rev. A, Gen. Phys.*, vol. 83, no. 4, Apr. 2011, Art. no. 042330.
[48] G. Zémor, "On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction," in *Proc. Int. Conf. Coding Cryptol.* Cham, Switzerland: Springer, 2009, pp. 259–273.
[49] N. Delfosse, "Tradeoffs for reliable quantum information storage in surface codes and color codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 917–921.
[50] S. Bravyi and M. B. Hastings, "Homological product codes," in *Proc. 46th Annu. ACM Symp. Theory Comput.*, May 2014, pp. 273–282.
[51] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, 1948.
[52] S. Lloyd, "Capacity of the noisy quantum channel," *Phys. Rev. A, Gen. Phys.*, vol. 55, no. 3, pp. 1613–1622, Mar. 1997.
[53] P. W. Shor, "Capacities of quantum channels and how to find them," *Math. Program.*, vol. 97, no. 1, pp. 311–335, Jul. 2003.
[54] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, Jan. 2005.
[55] M. M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1203–1222, Feb. 2014.
[56] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, "Quantum-channel capacity of very noisy channels," *Phys. Rev. A, Gen. Phys.*, vol. 57, no. 2, pp. 830–839, Feb. 1998.
[57] G. Smith and J. A. Smolin, "Degenerate quantum codes for Pauli channels," *Phys. Rev. Lett.*, vol. 98, no. 3, Jan. 2007, Art. no. 030501.
[58] P. Fuentes, J. E. Martinez, P. M. Crespo, and J. Garcia-Frías, "Degeneracy and its impact on the decoding of sparse quantum codes," *IEEE Access*, vol. 9, pp. 89093–89119, 2021.
[59] M. S. Postol, "A proposed quantum low density parity check code," 2001, *arXiv:quant-ph/0108131*.
[60] T. Camara, H. Ollivier, and J.-P. Tillich, "Constructions and performance of classes of quantum LDPC codes," 2005, *arXiv:quant-ph/0502086*.
[61] T. Camara, H. Ollivier, and J.-P. Tillich, "A class of quantum LDPC codes: Construction and performances under iterative decoding," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 811–815.
[62] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, no. 17, Oct. 2003, Art. no. 177902.
[63] H. Ollivier and J.-P. Tillich, "Quantum convolutional codes: Fundamentals," 2004, *arXiv:quant-ph/0401134*.
[64] G. D. Forney and S. Guha, "Simple rate-1/3 convolutional and tail-biting quantum error-correcting codes," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Sep. 2005, pp. 1028–1032.
[65] G. D. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 865–880, Mar. 2007.
[66] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo-codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 310–314.
[67] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2776–2798, May 2009.
[68] J. M. Renes, D. Sutter, F. Dupuis, and R. Renner, "Efficient quantum polar codes requiring no preshared entanglement," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6395–6414, Nov. 2015.
[69] Z. Babar et al., "Serially concatenated unity-rate codes improve quantum codes without coding-rate reduction," *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 1916–1919, Oct. 2016.
[70] M. Hagiwara, K. Kasai, H. Imai, and K. Sakaniwa, "Spatially coupled quasi-cyclic quantum LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2011, pp. 638–642.
[71] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Non-binary quasi-cyclic quantum LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2011, pp. 653–657.
[72] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Quantum error correction beyond the bounded distance decoding limit," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1223–1230, Feb. 2012.
[73] I. Andriyanova, D. Maurice, and J.-P. Tillich, "Spatially coupled quantum LDPC codes," in *Proc. IEEE Inf. Theory Workshop*, Sep. 2012, pp. 327–331.
[74] D. Maurice, J.-P. Tillich, and I. Andriyanova, "A family of quantum codes with performances close to the hashing bound under iterative decoding," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 907–911.
[75] G. Bowen, "Entanglement required in achieving entanglement-assisted channel capacities," *Phys. Rev. A, Gen. Phys.*, vol. 66, no. 5, Nov. 2002, Art. no. 052313.
[76] T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, Oct. 2006.
[77] T. A. Brun, I. Devetak, and M.-H. Hsieh, "General entanglement-assisted quantum error-correcting codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2101–2105.
[78] M.-H. Hsieh, I. Devetak, and T. Brun, "General entanglement-assisted quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 76, no. 6, Dec. 2007, Art. no. 062313.
[79] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Phys. Rev. A, Gen. Phys.*, vol. 79, no. 3, Mar. 2009, Art. no. 032340.
[80] M. M. Wilde and T. A. Brun, "Entanglement-assisted quantum convolutional coding," *Phys. Rev. A, Gen. Phys.*, vol. 81, no. 4, Apr. 2010, Art. no. 042333.
[81] M. M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2011, pp. 445–449.
[82] M. M. Wilde and S. Guha, "Polar codes for classical-quantum channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1175–1187, Feb. 2013.
[83] M. M. Wilde and S. Guha, "Polar codes for degradable quantum channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4718–4729, Jul. 2013.
[84] J. M. Renes, F. Dupuis, and R. Renner, "Efficient polar coding of quantum information," *Phys. Rev. Lett.*, vol. 109, no. 5, Aug. 2012, Art. no. 050504.
[85] D. Chandra et al., "Quantum coding bounds and a

closed-form approximation of the minimum distance versus quantum coding rate," *IEEE Access*, vol. 5, pp. 11557–11581, 2017.
[86] I. Djordjevic, "Quantum LDPC codes from balanced incomplete block designs," *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 389–391, May 2008.
[87] I. B. Djordjevic, "Photonic quantum dual-containing LDPC encoders and decoders," *IEEE Photon. Technol. Lett.*, vol. 21, no. 13, pp. 842–844, Jul. 1, 2009.
[88] I. B. Djordjevic, "Photonic entanglement-assisted quantum low-density parity-check encoders and decoders," *Opt. Lett.*, vol. 35, no. 9, pp. 1464–1466, May 2010.
[89] E. Pelchat and D. Poulin, "Degenerate Viterbi decoding," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3915–3921, Jun. 2013.
[90] Z. Babar, S. X. Ng, and L. Hanzo, "Near-capacity code design for entanglement-assisted classical communication over quantum depolarizing channels," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4801–4807, Dec. 2013.
[91] J.-P Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1193–1202, Feb. 2014.
[92] Z. Babar, S. X. Ng, and L. Hanzo, "EXIT-chart-aided near-capacity quantum turbo code design," *IEEE Trans. Veh. Technol.*, vol. 64, no. 3, pp. 866–875, Mar. 2015.
[93] A. Leverrier, J.-P. Tillich, and G. Zemor, "Quantum expander codes," in *Proc. IEEE 56th Annu. Symp. Found. Comput. Sci.*, Oct. 2015, pp. 810–824.
[94] Z. Babar et al., "Fully-parallel quantum turbo decoder," *IEEE Access*, vol. 4, pp. 6073–6085, 2016.
[95] H. V. Nguyen et al., "EXIT-chart aided quantum code design improves the normalised throughput of realistic quantum devices," *IEEE Access*, vol. 4, pp. 10194–10209, 2016.
[96] P. Panteleev and G. Kalachev, "Degenerate quantum LDPC codes with good finite length performance," *Quantum*, vol. 5, p. 585, Nov. 2021.
[97] P. Panteleev and G. Kalachev, "Quantum LDPC codes with almost linear minimum distance," *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 213–229, Jan. 2022.
[98] A. Leverrier and G. Zemor, "Quantum Tanner codes," in *Proc. IEEE 63rd Annu. Symp. Found. Comput. Sci. (FOCS)*, Denver, CO, USA, Oct. 2022, pp. 872–883.
[99] C. Vuillot and N. P. Breuckmann, "Quantum pin codes," *IEEE Trans. Inf. Theory*, vol. 68, no. 9, pp. 5955–5974, Sep. 2022.
[100] J. Roffe, L. Z. Cohen, A. O. Quintavalle, D. Chandra, and E. T. Campbell, "Bias-tailored quantum LDPC codes," *Quantum*, vol. 7, p. 1005, May 2023.
[101] M. Christandl and A. Müller-Hermes, "Fault-tolerant coding for quantum communication," *IEEE Trans. Inf. Theory*, vol. 70, no. 1, pp. 282–317, Jan. 2024.
[102] D. Chandra, Z. B. K. Egilmez, Y. Xiong, S. X. Ng, R. G. Maunder, and L. Hanzo, "Universal decoding of quantum stabilizer codes via classical guesswork," *IEEE Access*, vol. 11, pp. 19059–19072, 2023.
[103] D. Cruz, F. A. Monteiro, and B. C. Coutinho, "Quantum error correction via noise guessing decoding," *IEEE Access*, vol. 11, pp. 119446–119461, 2023.
[104] S. Yang and R. Calderbank, "Spatially-coupled QDLPC codes," 2023, *arXiv:2305.00137*.
[105] M. Hagiwara and H. Imai, "Quantum quasi-cyclic LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 806–810.
[106] Z. Yi, Z. Liang, Y. Wu, and X. Wang, "Quantum polar stabilizer codes based on polarization of pure quantum channel don't work for quantum computing," 2022, *arXiv:2204.11655*.
[107] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 1, pp. 76–82, Jul. 1997.
[108] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation," *Phys. Rev. A, Gen. Phys.*, vol. 86, no. 3, Sep. 2012, Art. no. 032324.
[109] P. Shor, "Fault-tolerant quantum computation," in *Proc. 37th Conf. Found. Comput. Sci.*, Oct. 1996, pp. 56–65.3.
[110] A. M. Steane, "Active stabilization, quantum computation, and quantum state synthesis," *Phys. Rev. Lett.*, vol. 78, no. 11, pp. 2252–2255, Mar. 1997.
[111] A. M. Steane, "Fast fault-tolerant filtering of quantum codewords," 2002, *arXiv:quant-ph/0202036*.
[112] R. Chao and B. W. Reichardt, "Quantum error correction with only two extra qubits," *Phys. Rev. Lett.*, vol. 121, no. 5, Aug. 2018, Art. no. 050502.
[113] S. Huang and K. R. Brown, "Between Shor and Steane: A unifying construction for measuring error syndromes," *Phys. Rev. Lett.*, vol. 127, no. 9, Aug. 2021, Art. no. 090505.
[114] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, "Topological quantum memory," *J. Math. Phys.*, vol. 43, no. 9, pp. 4452–4505, Sep. 2002.
[115] H. Bombín, "Single-shot fault-tolerant quantum error correction," *Phys. Rev. X*, vol. 5, no. 3, Sep. 2015, Art. no. 031043.
[116] E. T. Campbell, "A theory of single-shot error correction for adversarial noise," *Quantum Sci. Technol.*, vol. 4, no. 2, Feb. 2019, Art. no. 025006.
[117] N. P. Breuckmann and V. Londe, "Single-shot decoding of linear rate LDPC quantum codes with high performance," *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 272–286, Jan. 2022.
[118] A. O. Quintavalle, M. Vasmer, J. Roffe, and E. T. Campbell, "Single-shot error correction of three-dimensional homological product codes," *PRX Quantum*, vol. 2, no. 2, Jun. 2021, Art. no. 020340.
[119] A. Grospellier, L. Grouès, A. Krishna, and A. Leverrier, "Combining hard and soft decoders for hypergraph product codes," *Quantum*, vol. 5, p. 432, Apr. 2021.
[120] O. Higgott and N. P. Breuckmann, "Improved single-shot decoding of higher-dimensional hypergraph-product codes," *PRX Quantum*, vol. 4, no. 2, May 2023, Art. no. 020332.
[121] S. Gu, E. Tang, L. Caha, S. H. Choe, Z. He, and A. Kubica, "Single-shot decoding of good quantum LDPC codes," 2023, *arXiv:2306.12470*.
[122] W. Zeng, A. Ashikhmin, M. Woolls, and L. P. Pryadko, "Quantum convolutional data-syndrome codes," in *Proc. IEEE 20th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jul. 2019, pp. 1–5.
[123] J. E. Martinez, P. Fuentes, P. Crespo, and J. Garcia-Frias, "Time-varying quantum channel models for superconducting qubits," *npj Quantum Inf.*, vol. 7, no. 1, p. 115, Jul. 2021.
[124] Y.-J. Wang, Z.-Y. Xiao, Y. Zhang, X.-Y. Xiong, and S. Shi, "Construction of multiple-rate quantum LDPC codes sharing one scalable stabilizer circuit," *IEEE Trans. Commun.*, vol. 71, no. 2, pp. 1071–1082, Feb. 2023.
[125] L. Skoric, D. E. Browne, K. M. Barnes, N. I. Gillespie, and E. T. Campbell, "Parallel window decoding enables scalable fault tolerant quantum computation," *Nature Commun.*, vol. 14, no. 1, p. 7040, Nov. 2023.
[126] F. Battistel et al., "Real-time decoding for fault-tolerant quantum computing: Progress, challenges and outlook," *Nano Futures*, vol. 7, no. 3, Sep. 2023, Art. no. 032003.
[127] C. Yue, V. Miloslavskaya, M. Shirvanimoghaddam, B. Vucetic, and Y. Li, "Efficient decoders for short block length codes in 6G URLLC," *IEEE Commun. Mag.*, vol. 61, no. 4, pp. 84–90, Apr. 2023.
[128] M. P. C. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inf. Theory*, vol. 41, no. 5, pp. 1379–1396, Sep. 1995.
[129] C. Yue, M. Shirvanimoghaddam, G. Park, O.-S. Park, B. Vucetic, and Y. Li, "Probability-based ordered-statistics decoding for short block codes," *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1791–1795, Jun. 2021.
[130] K. R. Duffy, J. Li, and M. Médard, "Capacity-achieving guessing random additive noise decoding," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4023–4040, Jul. 2019.
[131] A. Roque, D. Cruz, F. A. Monteiro, and B. C. Coutinho, "Efficient entanglement purification based on noise guessing decoding," 2023, *arXiv:2310.19914*.
[132] 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.
[133] Y. Li and S. C. Benjamin, "Efficient variational quantum simulator incorporating active error minimization," *Phys. Rev. X*, vol. 7, no. 2, Jun. 2017, Art. no. 021050.
[134] K. Temme, S. Bravyi, and J. M. Gambetta, "Error mitigation for short-depth quantum circuits," *Phys. Rev. Lett.*, vol. 119, no. 18, Nov. 2017, Art. no. 180509.
[135] J. R. McClean, M. E. Kimchi-Schwartz, J. Carter, and W. A. de Jong, "Hybrid quantum-classical hierarchy for mitigation of decoherence and determination of excited states," *Phys. Rev. A, Gen. Phys.*, vol. 95, no. 4, Apr. 2017, Art. no. 042308.
[136] S. Endo, S. C. Benjamin, and Y. Li, "Practical quantum error mitigation for near-future applications," *Phys. Rev. X*, vol. 8, no. 3, Jul. 2018, Art. no. 031027.
[137] S. McArdle, X. Yuan, and S. Benjamin, "Error-mitigated digital quantum simulation," *Phys. Rev. Lett.*, vol. 122, no. 18, May 2019, Art. no. 180501.
[138] X. Bonet-Monroig, R. Sagastizabal, M. Singh, and T. E. O'Brien, "Low-cost error mitigation by symmetry verification," *Phys. Rev. A, Gen. Phys.*, vol. 98, no. 6, Dec. 2018, Art. no. 062339.
[139] E. F. Dumitrescu et al., "Cloud quantum computing of an atomic nucleus," *Phys. Rev. Lett.*, vol. 120, no. 21, May 2018, Art. no. 210501.
[140] A. Kandala, K. Temme, A. D. Córcoles, A. Mezzacapo, J. M. Chow, and J. M. Gambetta, "Error mitigation extends the computational reach of a noisy quantum processor," *Nature*, vol. 567, no. 7749, pp. 491–495, Mar. 2019.
[141] R. Sagastizabal et al., "Experimental error mitigation via symmetry verification in a variational quantum eigensolver," *Phys. Rev. A, Gen. Phys.*, vol. 100, no. 1, Jul. 2019, Art. no. 010302.
[142] A. T. Arrasmith, P. J. Czarnik, P. J. Coles, and L. Cincio, "Error mitigation with Clifford quantum-circuit data," *Quantum*, vol. 5, p. 592, Nov. 2021.
[143] A. Strikis, D. Qin, Y. Chen, S. C. Benjamin, and Y. Li, "Learning-based quantum error mitigation," *PRX Quantum*, vol. 2, no. 4, Nov. 2021, Art. no. 040330.
[144] B. Koczor, "Exponential error suppression for near-term quantum devices," *Phys. Rev. X*, vol. 11, no. 3, Sep. 2021, Art. no. 031057.
[145] W. J. Huggins et al., "Virtual distillation for quantum error mitigation," *Phys. Rev. X*, vol. 11, no. 4, Nov. 2021, Art. no. 041036.
[146] T. E. O'Brien et al., "Purification-based quantum error mitigation o pair-correlated electron simulations," *Nature Phys.*, vol. 19, no. 12, pp. 1787–1792, Oct. 2023.
[147] Y. Kim et al., "Evidence for the utility of quantum computing before fault tolerance," *Nature*, vol. 618, no. 7965, pp. 500–505, Jun. 2023.
[148] Z. Cai, "Multi-exponential error extrapolation and combining error mitigation techniques for NISQ applications," *npj Quantum Inf.*, vol. 7, no. 1, p. 80, May 2021.
[149] J. M. Chow et al., "Detecting highly entangled states with a joint qubit readout," *Phys. Rev. A, Gen. Phys.*, vol. 81, no. 6, Jun. 2010, Art. no. 062325.
[150] A. Kandala et al., "Hardware-efficient variational

quantum eigensolver for small molecules and quantum magnets," *Nature*, vol. 549, no. 7671, pp. 242–246, Sep. 2017.
[151] H. Jnane, B. Undseth, Z. Cai, S. C. Benjamin, and B. Koczor, "Multicore quantum computing," *Phys. Rev. Appl.*, vol. 18, no. 4, Oct. 2022, Art. no. 044064, doi: 10.1103/physrevapplied.18.044064.
[152] B. Koczor, "The dominant eigenvector of a noisy quantum state," *New J. Phys.*, vol. 23, no. 12, Dec. 2021, Art. no. 123047.
[153] Y. Xiong, S. X. Ng, and L. Hanzo, "Quantum error mitigation relying on permutation filtering," *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1927–1942, Mar. 2022.
[154] M. Huo and Y. Li, "Dual-state purification for practical quantum error mitigation," *Phys. Rev. A, Gen. Phys.*, vol. 105, no. 2, Feb. 2022, Art. no. 022427.
[155] Z. Cai, "Resource-efficient purification-based quantum error mitigation," 2021, *arXiv:2107.07279*.
[156] L. J. Stephenson et al., "High-rate, high-fidelity entanglement of qubits across an elementary quantum network," *Phys. Rev. Lett.*, vol. 124, no. 11, Mar. 2020, Art. no. 110501, doi: 10.1103/physrevlett.124.110501.
[157] Z. Cai, A. Siegel, and S. Benjamin, "Looped pipelines enabling effective 3D qubit lattices in a strictly 2D device," *PRX Quantum*, vol. 4, no. 2, Jun. 2023, Art. no. 020345.
[158] Y. Xiong, D. Chandra, S. X. Ng, and L. Hanzo, "Circuit symmetry verification mitigates quantum-domain impairments," *IEEE Trans. Signal Process.*, vol. 71, pp. 477–493, 2023.
[159] W. J. Huggins et al., "Efficient and noise resilient measurements for quantum chemistry on near-term quantum computers," *npj Quantum Inf.*, vol. 7, no. 1, p. 23, Feb. 2021.
[160] Z. Cai, "Quantum error mitigation using symmetry expansion," *Quantum*, vol. 5, p. 548, Sep. 2021.
[161] S. B. Bravyi and A. Y. Kitaev, "Fermionic quantum computation," *Ann. Phys.*, vol. 298, no. 1, pp. 210–226, May 2002.
[162] K. Setia and J. D. Whitfield, "Bravyi–Kitaev superfast simulation of electronic structure on a quantum computer," *J. Chem. Phys.*, vol. 148, no. 16, Apr. 2018, Art. no. 164104.
[163] C. Derby, J. Klassen, J. Bausch, and T. Cubitt, "Compact fermion to qubit mappings," *Phys. Rev. B, Condens. Matter*, vol. 104, no. 3, Jul. 2021, Art. no. 035118.
[164] Z. Jiang, J. McClean, R. Babbush, and H. Neven, "Majorana loop stabilizer codes for error mitigation in fermionic quantum simulations," *Phys. Rev. Appl.*, vol. 12, no. 6, Dec. 2019, Art. no. 064041.
[165] J. R. McClean, Z. Jiang, N. C. Rubin, R. Babbush, and H. Neven, "Decoding quantum errors with subspace expansions," *Nature Commun.*, vol. 11, no. 1, p. 636, Jan. 2020.
[166] J. I. Colless et al., "Computation of molecular spectra on a quantum processor with an error-resilient algorithm," *Phys. Rev. X*, vol. 8, no. 1, Feb. 2018, Art. no. 011021.
[167] M. Urbanek, D. Camps, R. Van Beeumen, and W. A. de Jong, "Chemistry on quantum computers with virtual quantum subspace expansion," *J. Chem. Theory Comput.*, vol. 16, no. 9, pp. 5425–5431, Sep. 2020.
[168] M. Motta et al., "Determining eigenstates and thermal states on a quantum computer using quantum imaginary time evolution," *Nature Phys.*, vol. 16, no. 2, pp. 205–210, Feb. 2020.
[169] N. Yoshioka, H. Hakoshima, Y. Matsuzaki, Y. Tokunaga, Y. Suzuki, and S. Endo, "Generalized quantum subspace expansion," *Phys. Rev. Lett.*, vol. 129, no. 2, Jul. 2022, Art. no. 020502.
[170] J. Foldager and B. Koczor, "Can shallow quantum circuits scramble local noise into global white noise?" *J. Phys. A, Math. Theor.*, vol. 57, no. 1, Jan. 2024, Art. no. 015306.
[171] A. Montanaro and S. Stanisic, "Error mitigation by training with fermionic linear optics," 2021, *arXiv:2102.02120*.
[172] Z. Cai, "A practical framework for quantum error mitigation," 2021, *arXiv:2110.05389*.
[173] Y. Quek, D. S. França, S. Khatri, J. J. Meyer, and J. Eisert, "Exponentially tighter bounds on limitations of quantum error mitigation," 2022, *arXiv:2210.11505*.
[174] Y. Xiong, D. Chandra, S. X. Ng, and L. Hanzo, "Sampling overhead analysis of quantum error mitigation: Uncoded vs. Coded systems," *IEEE Access*, vol. 8, pp. 228967–228991, 2020.
[175] Y. Xiong, S. X. Ng, and L. Hanzo, "The accuracy vs. sampling overhead trade-off in quantum error mitigation using Monte Carlo-based channel inversion," *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1943–1956, Mar. 2022.
[176] B. Koczor and S. C. Benjamin, "Quantum natural gradient generalized to noisy and nonunitary circuits," *Phys. Rev. A, Gen. Phys.*, vol. 106, no. 6, Dec. 2022, Art. no. 062416.
[177] J. Stokes, J. Izaac, N. Killoran, and G. Carleo, "Quantum natural gradient," *Quantum*, vol. 4, p. 269, May 2020.
[178] E. Van Den Berg, Z. K. Minev, A. Kandala, and K. Temme, "Probabilistic error cancellation with sparse Pauli–Lindblad models on noisy quantum processors," *Nature Phys.*, vol. 19, no. 8, pp. 1116–1121, 2023.
[179] A. Elben et al., "The randomized measurement toolbox," *Nature Rev. Phys.*, vol. 5, no. 1, pp. 9–24, Dec. 2022.
[180] H. Jnane, J. Steinberg, Z. Cai, H. C. Nguyen, and B. Koczor, "Quantum error mitigated classical shadows," 2023, *arXiv:2305.04956*.
[181] A. Seif, Z.-P. Cian, S. Zhou, S. Chen, and L. Jiang, "Shadow distillation: Quantum error mitigation with classical shadows for near-term quantum processors," *PRX Quantum*, vol. 4, no. 1, Jan. 2023, Art. no. 010303.
[182] G. Boyd and B. Koczor, "Training variational quantum circuits with CoVaR: Covariance root finding with classical shadows," *Phys. Rev. X*, vol. 12, no. 4, Nov. 2022, Art. no. 041022, doi: 10.1103/physrevx.12.041022.
[183] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.
[184] H. H. S. Chan, R. Meister, M. L. Goh, and B. Koczor, "Algorithmic shadow spectroscopy," 2022, *arXiv:2212.11036*.
[185] A. Lowe, M. H. Gordon, P. Czarnik, A. Arrasmith, P. J. Coles, and L. Cincio, "Unified approach to data-driven quantum error mitigation," *Phys. Rev. Res.*, vol. 3, no. 3, Jul. 2021, Art. no. 033098.
[186] D. Bultrini et al., "Unifying and benchmarking state-of-the-art quantum error mitigation techniques," *Quantum*, vol. 7, p. 1034, Jun. 2023.
[187] Y. Suzuki, S. Endo, K. Fujii, and Y. Tokunaga, "Quantum error mitigation as a universal error reduction technique: Applications from the NISQ to the fault-tolerant quantum computing eras," *PRX Quantum*, vol. 3, no. 1, Mar. 2022, Art. no. 010345.
[188] C. Piveteau, D. Sutter, S. Bravyi, J. M. Gambetta, and K. Temme, "Error mitigation for universal gates on encoded qubits," *Phys. Rev. Lett.*, vol. 127, no. 20, Nov. 2021, Art. no. 200505.
[189] M. Schuld and F. Petruccione, *Machine Learning With Quantum Computers*. Cham, Switzerland: Springer, 2021.
[190] O. Simeone, "An introduction to quantum machine learning for engineers," *Found. Trends Signal Process.*, vol. 16, nos. 1–2, pp. 1–223, 2022.
[191] A. Valenti, E. van Nieuwenburg, S. Huber, and E. Greplova, "Hamiltonian learning for quantum error correction," *Phys. Rev. Res.*, vol. 1, no. 3, Nov. 2019, Art. no. 033092.
[192] H. P. Nautrup, N. Delfosse, V. Dunjko, H. J. Briegel, and N. Friis, "Optimizing quantum error correction codes with reinforcement learning," *Quantum*, vol. 3, p. 215, Dec. 2019.
[193] C. Kim, K. D. Park, and J.-K. Rhee, "Quantum error mitigation with artificial neural network," *IEEE Access*, vol. 8, pp. 188853–188860, 2020.
[194] D. F. Locher, L. Cardarelli, and M. Müller, "Quantum error correction with quantum autoencoders," *Quantum*, vol. 7, p. 942, Mar. 2023.
[195] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019.
[196] Z. I. Tabi, A. Marosits, Z. Kallus, P. Vaderna, I. Godor, and Z. Zimboras, "Evaluation of quantum annealer performance via the massive MIMO problem," *IEEE Access*, vol. 9, pp. 131658–131671, 2021.
[197] J. Cui, Y. Xiong, S. X. Ng, and L. Hanzo, "Quantum approximate optimization algorithm based maximum likelihood detection," *IEEE Trans. Commun.*, vol. 70, no. 8, pp. 5386–5400, Aug. 2022.
[198] H. H. S. Chittoor and O. Simeone, "Quantum machine learning for distributed quantum protocols with local operations and noisy classical communications," *Entropy*, vol. 25, no. 2, p. 352, Feb. 2023.
[199] M. Cerezo, G. Verdon, H.-Y. Huang, L. Cincio, and P. J. Coles, "Challenges and opportunities in quantum machine learning," *Nature Comput. Sci.*, vol. 2, no. 9, pp. 567–576, Sep. 2022.
[200] L. Banchi, J. L. Pereira, S. T. Jose, and O. Simeone, "Statistical complexity of quantum learning," 2023, *arXiv:2309.11617*.
[201] J. Romero, J. P. Olson, and A. Aspuru-Guzik, "Quantum autoencoders for efficient compression of quantum data," *Quantum Sci. Technol.*, vol. 2, no. 4, Dec. 2017, Art. no. 045001.
[202] P.-L. Dallaire-Demers and N. Killoran, "Quantum generative adversarial networks," *Phys. Rev. A, Gen. Phys.*, vol. 98, no. 1, 2018, Art. no. 012324.
[203] B. Coyle, D. Mills, V. Danos, and E. Kashefi, "The born supremacy: Quantum advantage and training of an Ising born machine," *npj Quantum Inf.*, vol. 6, no. 1, p. 60, Jul. 2020.
[204] X. Gao, E. R. Anschuetz, S.-T. Wang, J. I. Cirac, and M. D. Lukin, "Enhancing generative models via quantum correlations," *Phys. Rev. X*, vol. 12, no. 2, May 2022, Art. no. 021037.
[205] N. Pirnay, R. Sweke, J. Eisert, and J.-P. Seifert, "Superpolynomial quantum-classical separation for density modeling," *Phys. Rev. A, Gen. Phys.*, vol. 107, no. 4, Apr. 2023, Art. no. 042416.
[206] M. Hinsche et al., "One t gate makes distribution learning hard," *Phys. Rev. Lett.*, vol. 130, no. 24, Jun. 2023, Art. no. 240602.
[207] Y. Du, Z. Tu, B. Wu, X. Yuan, and D. Tao, "Power of quantum generative learning," 2022, *arXiv:2205.04730*.
[208] A. Abbas et al., "On quantum backpropagation, information reuse, and cheating measurement collapse," 2023, *arXiv:2305.13362*.
[209] S. C. Kak, "Quantum neural computing," *Adv. Imag. Electron Phys.*, vol. 94, pp. 259–313, Sep. 1995.
[210] E. Farhi, J. Goldstone, and S. Gutmann, "A quantum approximate optimization algorithm," 2014, *arXiv:1411.4028*.
[211] P. Wittek, *Quantum Machine Learning: What Quantum Computing Means to Data Mining*. New York, NY, USA: Academic, 2014.
[212] J. R. McClean, J. Romero, R. Babbush, and A. Aspuru-Guzik, "The theory of variational hybrid quantum-classical algorithms," *New J. Phys.*, vol. 18, no. 2, Feb. 2016, Art. no. 023023.
[213] J.-G. Liu and L. Wang, "Differentiable learning of quantum circuit born machines," *Phys. Rev. A, Gen. Phys.*, vol. 98, no. 6, Dec. 2018, Art. no. 062324.
[214] E. Farhi and H. Neven, "Classification with quantum neural networks on near term processors," 2018, *arXiv:1802.06002*.
[215] S. Arunachalam and R. de Wolf, "Optimal quantum sample complexity of learning algorithms," *J. Mach. Learn. Res.*, vol. 19, no. 1, pp. 2878–2879, Jan. 2018.
[216] M. Schuld and F. Petruccione, *Supervised Learning With Quantum Computers*, vol. 17. Cham, Switzerland: Springer, 2018.
[217] J. R. McClean, S. Boixo, V. N. Smelyanskiy,

R. Babbush, and H. Neven, "Barren plateaus in quantum neural network training landscapes," *Nat. Commun.*, vol. 9, no. 1, p. 4812, 2018.
[218] I. Cong, S. Choi, and M. D. Lukin, "Quantum convolutional neural networks," *Nature Phys.*, vol. 15, no. 12, pp. 1273–1278, 2019.
[219] C. Zoufal, A. Lucchi, and S. Woerner, "Quantum generative adversarial networks for learning and loading random distributions," *NPJ Quant. Inf.*, vol. 5, p. 103, Nov. 2019.
[220] F. Tacchino, C. Macchiavello, D. Gerace, and D. Bajoni, "An artificial neuron implemented on an actual quantum processor," *NPJ Quantum Inf.*, vol. 5, no. 1, p. 26, Mar. 2019.
[221] M. Broughton et al., "TensorFlow quantum: A software framework for quantum machine learning," 2020, *arXiv:2003.02989*.
[222] L. Banchi, J. Pereira, and S. Pirandola, "Generalization in quantum machine learning: A quantum information standpoint," *PRX Quantum*, vol. 2, no. 4, Nov. 2021, Art. no. 040321.
[223] K. Sharma, M. Cerezo, L. Cincio, and P. J. Coles, "Trainability of dissipative perceptron-based quantum neural networks," *Phys. Rev. Lett.*, vol. 128, no. 18, May 2022, Art. no. 180505.
[224] M. C. Caro et al., "Generalization in quantum machine learning from few training data," *Nature Commun.*, vol. 13, no. 1, p. 4919, Aug. 2022.
[225] A. Nietner et al., "On the average-case complexity of learning output distributions of quantum circuits," 2023, *arXiv:2305.05765*.
[226] Y. Liu, S. Arunachalam, and K. Temme, "A rigorous and robust quantum speed-up in supervised machine learning," *Nature Phys.*, vol. 17, no. 9, pp. 1013–1017, Sep. 2021.
[227] M. Ragone et al., "A lie algebraic theory of barren plateaus for deep parameterized quantum circuits," 2023, *arXiv:2309.09342*.
[228] A. Pesah, M. Cerezo, S. Wang, T. Volkoff, A. T. Sornborger, and P. J. Coles, "Absence of barren plateaus in quantum convolutional neural networks," *Phys. Rev. X*, vol. 11, no. 4, Oct. 2021, Art. no. 041011.
[229] E. Peters and M. Schuld, "Generalization despite overfitting in quantum machine learning models," 2022, *arXiv:2209.05523*.
[230] M. M. Bronstein, J. Bruna, T. Cohen, and P. Veličković, "Geometric deep learning: Grids, groups, graphs, geodesics, and gauges," 2021, *arXiv:2104.13478*.
[231] E. Perrier, D. Tao, and C. Ferrie, "Quantum geometric machine learning for quantum circuits and control," *New J. Phys.*, vol. 22, no. 10, Oct. 2020, Art. no. 103056.
[232] I. Nikoloska, O. Simeone, L. Banchi, and P. Veličković, "Time-warping invariant quantum recurrent neural networks via quantum-classical adaptive gating," *Mach. Learning: Sci. Technol.*, vol. 4, no. 4, Dec. 2023, Art. no. 045038.
[233] I. Nikoloska and O. Simeone, "Quantum-aided meta-learning for Bayesian binary neural networks via born machines," in *Proc. IEEE 32nd Int. Workshop Mach. Learn. Signal Process. (MLSP)*, Aug. 2022, pp. 1–6.
[234] J. Carrasquilla et al., "Quantum HyperNetworks: Training binary neural networks in quantum superposition," 2023, *arXiv:2301.08292*.
[235] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," *Phys. Rev. A, Gen. Phys.*, vol. 68, no. 2, Aug. 2003, Art. no. 022312.
[236] A. Majumder, M. Krumm, T. Radkohl, H. P. Nautrup, S. Jerbi, and H. J. Briegel, "Variational measurement-based quantum computation for generative modeling," 2023, *arXiv:2310.13524*.
[237] S. Tibaldi, D. Vodola, E. Tignone, and E. Ercolessi, "Bayesian optimization for QAOA," *IEEE Trans. Quantum Eng.*, vol. 4, pp. 1–11, 2023.
[238] S. T. Jose and O. Simeone, "Error-mitigation-aided optimization of parameterized quantum circuits: Convergence analysis," *IEEE Trans. Quantum Eng.*, vol. 3, pp. 1–19, 2022.
[239] S. Park and O. Simeone, "Quantum conformal prediction for reliable uncertainty quantification in quantum machine learning," 2023, *arXiv:2304.03398*.
[240] M. Lanzagorta, *Quantum Radar*. San Rafael, CA, USA: Morgan & Claypool, 2012.
[241] I. B. Djordjevic, *Quantum Communication, Quantum Networks, and Quantum Sensing*. Amsterdam, The Netherlands: Elsevier, 2022.
[242] I. B. Djordjevic, "Entanglement assisted radars with transmitter side optical phase conjugation and classical coherent detection," *IEEE Access*, vol. 10, pp. 49095–49100, 2022.
[243] I. B. Djordjevic, "Entanglement-assisted joint monostatic-bistatic radars," *Entropy*, vol. 24, no. 6, p. 756, May 2022.
[244] I. B. Djordjevic, "On entanglement-assisted multistatic radar techniques," *Entropy*, vol. 24, no. 7, p. 990, Jul. 2022.
[245] S. Lloyd, "Enhanced sensitivity of photodetection via quantum illumination," *Science*, vol. 321, no. 5895, pp. 1463–1465, Sep. 2008.
[246] J. H. Shapiro, "The quantum illumination story," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 35, no. 4, pp. 8–20, Apr. 2020.
[247] R. G. Torromé, N. Ben Bekhti-Winkel, and P. Knott, "Introduction to quantum radar," 2020, *arXiv:2006.14238*.
[248] A. Karsa, G. Spedalieri, Q. Zhuang, and S. Pirandola, "Quantum illumination with a generic Gaussian source," *Phys. Rev. Res.*, vol. 2, no. 2, Jun. 2020, Art. no. 023414.
[249] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, "Microwave quantum illumination," *Phys. Rev. Lett.*, vol. 114, no. 8, Feb. 2015, Art. no. 080503.
[250] S. Barzanjeh, S. Pirandola, D. Vitali, and J. M. Fink, "Microwave quantum illumination using a digital receiver," *Sci. Adv.*, vol. 6, no. 19, May 2020, Art. no. eabb0451.
[251] G. Sorelli, N. Treps, F. Grosshans, and F. Boust, "Detecting a target with quantum entanglement," 2020, *arXiv:2005.07116*.
[252] C. Noh, C. Lee, and S.-Y. Lee, "Quantum illumination with definite photon-number entangled states," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 39, no. 5, p. 1316, 2022.
[253] H. Corporation, "Quantum sensors program," Tech. Rep. AFRL-RI-RS-TR-2009-208, 2009.
[254] P. Kumar, V. Grigoryan, and M. Vasilyev, "Noise-free amplification: Towards quantum laser radar," in *Proc. 14th Coherent Laser Radar Conf.*, Jul. 2007, pp. 1–12.
[255] Z. Dutton, J. H. Shapiro, and S. Guha, "LADAR resolution improvement using receivers enhanced with squeezed-vacuum injection and phase-sensitive amplification," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 27, no. 6, p. 63, 2010.
[256] J. Shapiro, "Quantum pulse compression laser radar," *Proc. SPIE*, vol. 6603, pp. 31–38, Jun. 2007.
[257] M. Lanzagorta, "Quantum radar cross sections," *Proc. SPIE*, vol. 7727, Apr. 2010, Art. no. 77270K.
[258] L. C. Andrews and R. L. Philips, *Laser Beam Propagation Through Random Media*. Bellingham, WA, USA: SPIE Press, 2005.
[259] I. B. Djordjevic, *Advanced Optical and Wireless Communications Systems*, 2nd ed., Cham, Switzerland: Springer, 2022.
[260] J. F. Smith, "Quantum entangled radar theory and a correction method for the effects of the atmosphere on entanglement," *Proc. SPIE*, vol. 7342, pp. 76–87, Apr. 2009.
[261] R. K. Tyson, *Principles of Adaptive Optics*. Boca Raton, FL, USA: CRC Press, 2015.
[262] V. Nafria and I. B. Djordjevic, "Entanglement assisted communication over the free-space optical link with azimuthal phase correction for atmospheric turbulence by adaptive optics," *Opt. Exp.*, vol. 31, no. 24, p. 39906, 2023.
[263] I. B. Djordjevic and V. Nafria, "Entanglement assisted quantum radar demonstration over turbulent free-space optical channels," in *Proc. Asia Commun. Photon. Conf./Int. Photon. Optoelectronics Meetings (ACP/POEM)*, Nov. 2023, pp. 1–4.
[264] S.-H. Tan et al., "Quantum illumination with Gaussian states," *Phys. Rev. Lett.*, vol. 101, no. 25, Dec. 2008, Art. no. 253601.
[265] K. M. R. Audenaert et al., "Discriminating states: The quantum Chernoff bound," *Phys. Rev. Lett.*, vol. 98, no. 16, Apr. 2007, Art. no. 160501.
[266] Z. Zhang, S. Mouradian, F. N. C. Wong, and J. H. Shapiro, "Entanglement-enhanced sensing in a lossy and noisy environment," *Phys. Rev. Lett.*, vol. 114, no. 11, Mar. 2015, Art. no. 110506.
[267] Q. Zhuang, Z. Zhang, and J. H. Shapiro, "Optimum mixed-state discrimination for noisy entanglement-enhanced sensing," *Phys. Rev. Lett.*, vol. 118, no. 4, Jan. 2017, Art. no. 040801.
[268] I. B. Djordjevic, "Entanglement assisted MIMO quantum radars," in *Proc. 23rd Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2023, pp. 1–4.
[269] L. Fan et al., "Superconducting cavity electro-optics: A platform for coherent photon conversion between superconducting and photonic circuits," *Sci. Adv.*, vol. 4, no. 8, Aug. 2018, Art. no. eaar4994.
[270] X. Han, W. Fu, C.-L. Zou, L. Jiang, and H. X. Tang, "Microwave-optical quantum frequency conversion," *Optica*, vol. 8, no. 8, p. 1050, 2021.
[271] R. Assouly, R. Dassonneville, T. Peronnin, A. Bienfait, and B. Huard, "Quantum advantage in microwave quantum radar," *Nature Phys.*, vol. 19, no. 10, pp. 1418–1422, Oct. 2023.
[272] A. I. Lvovsky, B. C. Sanders, and W. Tittel, "Optical quantum memory," *Nature Photon.*, vol. 3, no. 12, pp. 706–714, Dec. 2009.
[273] D. D. Sukachev et al., "Silicon-vacancy spin qubit in diamond: A quantum memory exceeding 10 ms with single-shot state readout," *Phys. Rev. Lett.*, vol. 119, no. 22, Nov. 2017, Art. no. 223602.
[274] S. Sun, H. Kim, Z. Luo, G. S. Solomon, and E. Waks, "A single-photon switch and transistor enabled by a solid-state quantum memory," *Science*, vol. 361, no. 6397, pp. 57–60, Jul. 2018.
[275] Y. Wang et al., "Efficient quantum memory for single-photon polarization qubits," *Nat. Photon.*, vol. 13, no. 5, pp. 346–351, May 2019.
[276] A. Wallucks, I. Marinković, B. Hensen, R. Stockill, and S. Gröblacher, "A quantum memory at telecom wavelengths," *Nature Phys.*, vol. 16, no. 7, pp. 772–777, Jul. 2020.
[277] X. Liu et al., "Heralded entanglement distribution between two absorptive quantum memories," *Nature*, vol. 594, no. 7861, pp. 41–45, 2021.
[278] P.-J. Stas et al., "Robust multi-qubit quantum network node with integrated error detection," *Science*, vol. 378, no. 6619, pp. 557–560, 2022.
[279] J.-M. Mol et al., "Quantum memories for fundamental science in space," *Quantum Sci. Technol.*, vol. 8, no. 2, Apr. 2023, Art. no. 024006.
[280] D. V. Reddy et al., "Superconducting nanowire single-photon detectors with 98% system detection efficiency at 1550 nm," *Optica*, vol. 7, no. 12, pp. 1649–1653, 2020.
[281] G.-Z. Xu et al., "Superconducting microstrip single-photon detector with system detection efficiency over 90% at 1550 nm," *Photon. Res.*, vol. 9, no. 6, pp. 958–967, 2021.
[282] Y. Pan et al., "Mid-infrared $Nb4N_3$-based superconducting nanowire single photon detectors for wavelengths up to 10 μm," *Opt. Exp.*, vol. 30, pp. 40044–40052, Jan. 2022.
[283] M. Eaton et al., "Resolution of 100 photons and quantum generation of unbiased random numbers," *Nature Photon.*, vol. 17, no. 1, pp. 106–111, Jan. 2023.
[284] R. Cheng, Y. Zhou, S. Wang, M. Shen, T. Taher, and H. X. Tang, "A 100-pixel photon-number-resolving detector unveiling photon statistics," *Nature Photon.*, vol. 17, no. 1, pp. 112–119, Jan. 2023.
[285] M. Forsch et al., "Microwave-to-optics conversion using a mechanical oscillator in its quantum ground state," *Nature Phys.*, vol. 16, no. 1, pp. 69–74, Jan. 2020.
[286] W. Jiang et al., "Efficient bidirectional piezo-optomechanical transduction between microwave and optical frequency," *Nature Commun.*, vol. 11, no. 1, p. 1166, Mar. 2020.
[287] K. Tsujino et al., "Quantum receiver beyond the

standard quantum limit of coherent optical communication," *Phys. Rev. Lett.*, vol. 106, no. 25, Jun. 2011, Art. no. 250503.
[288] S. Izumi, J. S. Neergaard-Nielsen, S. Miki, H. Terai, and U. L. Andersen, "Experimental demonstration of a quantum receiver beating the standard quantum limit at telecom wavelength," *Phys. Rev. Appl.*, vol. 13, no. 5, May 2020, Art. no. 054015.
[289] C. Reimer et al., "Generation of multiphoton entangled quantum states by means of integrated frequency combs," *Science*, vol. 351, no. 6278, pp. 1176–1180, Mar. 2016.
[290] M. Kues et al., "Quantum optical microcombs," *Nature Photon.*, vol. 13, no. 3, pp. 170–179, Mar. 2019.
[291] Z. Yang et al., "A squeezed quantum microcomb on a chip," *Nature Commun.*, vol. 12, no. 1, p. 4781, Aug. 2021.
[292] N. Lauk et al., "Perspectives on quantum transduction," *Quantum Sci. Technol.*, vol. 5, no. 2, Mar. 2020, Art. no. 020501.
[293] D. Awschalom et al., "Development of quantum interconnects (QuICs) for next-generation information technologies," *PRX Quantum*, vol. 2, no. 1, Feb. 2021, Art. no. 017002.
[294] S.-R. Zhao et al., "Field demonstration of distributed quantum sensing without post-selection," *Phys. Rev. X*, vol. 11, no. 3, Jul. 2021, Art. no. 031009.
[295] I. B. Djordjevic, "On entanglement assisted classical optical communication with transmitter side optical phase-conjugation," *IEEE Access*, vol. 9, pp. 168930–168936, 2021.
[296] S. Hao et al., "Demonstration of entanglement-enhanced covert sensing," *Phys. Rev. Lett.*, vol. 129, no. 1, Jun. 2022, Art. no. 010501.
[297] G. G. Taylor, D. Morozov, N. R. Gemmell, K. Erotokritou, and R. H. Hadfield, "2.3μm wavelength single photon LiDAR with superconducting nanowire detectors," in *Proc. Conf. Lasers Electro-Opt.*, 2019, pp. 1–12.
[298] T. Staffas, M. Brunzell, S. Gyger, L. Schweickert, S. Steinhauer, and V. Zwiller, "3D scanning quantum LiDAR," in *Proc. Conf. Lasers Electro-Optics (CLEO)*, May 2022, pp. 1–2.
[299] M. Reichert, Q. Zhuang, J. H. Shapiro, and R. Di Candia, "Quantum illumination with a hetero-homodyne receiver and sequential detection," *Phys. Rev. Appl.*, vol. 20, no. 1, Jul. 2023, Art. no. 014030.
[300] F. Kronowetter et al., "Quantum microwave parametric interferometer," *Phys. Rev. Appl.*, vol. 20, no. 2, Aug. 2023, Art. no. 024049.
[301] S.-Y. Lee, D. H. Kim, Y. Jo, T. Jeong, Z. Kim, and D. Y. Kim, "Bound for Gaussian-state quantum illumination using a direct photon measurement," *Opt. Exp.*, vol. 31, no. 23, p. 38977, 2023.
[302] Z. Xue, S. Li, X. Xue, X. Zheng, and B. Zhou, "Photonics-assisted joint radar and communication system based on an optoelectronic oscillator," *Opt. Exp.*, vol. 29, no. 14, pp. 22442–22454, Jul. 2021.
[303] T. Huang, X. Xu, Y. Liu, N. Shlezinger, and Y. C. Eldar, "A dual-function radar communication system using index modulation," in *Proc. IEEE 20th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jul. 2019, pp. 1–5.
[304] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths, and L. Hanzo, "Joint radar and communication design: Applications, state-of-the-art, and the road ahead," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3834–3862, Jun. 2020.
[305] J. Wang, N. Varshney, C. Gentile, S. Blandino, J. Chuang, and N. Golmie, "Integrated sensing and communication: Enabling techniques, applications, tools and data sets, standardization, and future directions," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 23416–23440, Dec. 2022.
[306] Q. Zhuang and J. H. Shapiro, "Ultimate accuracy limit of quantum pulse-compression ranging," *Phys. Rev. Lett.*, vol. 128, no. 1, Jan. 2022, Art. no. 010501.
[307] G.-L. Long, D. Pan, Y.-B. Sheng, Q. Xue, J. Lu, and L. Hanzo, "An evolutionary pathway for the quantum internet relying on secure classical repeaters," *IEEE Netw.*, vol. 36, no. 3, pp. 82–88, May 2022.
[308] S. Pirandola et al., "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020. [Online]. Available: http://aop.osa.org/abstract.cfm?URI=aop-12-4-1012
[309] M. Razavi, *An Introduction to Quantum Communications Networks*. San Rafael, CA, USA: Morgan & Claypool, 2018, doi: 10.1088/978-1-6817-4653-1.
[310] R. Renner and R. König, "Universally composable privacy amplification against quantum adversaries," in *Theory of Cryptography*, J. Kilian, Ed., Berlin, Germany: Springer, 2005, pp. 407–425.
[311] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Bangalore, India, Dec. 1984, pp. 175–179.
[312] S. Wiesner, "Conjugate coding," *ACM SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983, doi: 10.1145/1008908.1008920.
[313] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.
[314] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, Feb. 1992.
[315] C. H. Bennett and G. Brassard, "Experimental quantum cryptography: The dawn of a new era for quantum cryptography: The experimental prototype is working," *ACM SIGACT News*, vol. 20, no. 4, pp. 78–80, Nov. 1989, doi: 10.1145/74074.74087.
[316] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, p. 5932, Dec. 1998.
[317] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999, doi: 10.1126/science.283.5410.2050.
[318] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, p. 441, 2000.
[319] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, no. 6862, pp. 413–418, Nov. 2001.
[320] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *Proc. Int. Symp. Inf. Theory*, Sep. 2004, p. 136.
[321] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, Aug. 2003, Art. no. 057901.
[322] X.-B. Wang, "Beating the PNS attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, Jun. 2005, Art. no. 230503.
[323] X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," *Phys. Rev. A, Gen. Phys.*, vol. 72, no. 1, Jul. 2005, Art. no. 012322.
[324] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 72, no. 1, Jul. 2005, Art. no. 012326.
[325] R. Renner, "Security of quantum key distribution," Ph.D. dissertation, Swiss Federal Inst. Technol., Zurich, Switzerland, 2005.
[326] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, "Low cost and compact quantum key distribution," *New J. Phys.*, vol. 8, no. 10, p. 249, Oct. 2006.
[327] H. Chun et al., "Handheld free space quantum key distribution with dynamic motion compensation," *Opt. Exp.*, vol. 25, no. 6, p. 6784, 2017.
[328] N. A. Peters et al., "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," *New J. Phys.*, vol. 11, no. 4, Apr. 2009, Art. no. 045012.
[329] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar. 2012.
[330] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130502.
[331] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," *New J. Phys.*, vol. 16, no. 4, Apr. 2014, Art. no. 043005.
[332] S. Abruzzo, H. Kampermann, and D. Bruß, "Measurement-device-independent quantum key distribution with quantum memories," *Phys. Rev. A, Gen. Phys.*, vol. 89, no. 1, Jan. 2014, Art. no. 012301, doi: 10.1103/physreva.89.012301.
[333] Y.-A. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021, doi: 10.1038/s41586-020-03093-8.
[334] P. Sibson et al., "Chip-based quantum key distribution," *Nature Commun.*, vol. 8, no. 1, p. 13984, Feb. 2017, doi: 10.1038/ncomms13984.
[335] L.-C. Kwek et al., "Chip-based quantum key distribution," *AAPPS Bull.*, vol. 31, no. 1, p. 15, Jun. 2021, doi: 10.1007/s43673-021-00017-0.
[336] S.-K. Liao et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Sep. 2017, doi: 10.1038/nature23655.
[337] S.-K. Liao et al., "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, Jan. 2018, Art. no. 030501, doi: 10.1103/physrevlett.120.030501.
[338] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, May 2018, doi: 10.1038/s41586-018-0066-6.
[339] P. Zeng, H. Zhou, W. Wu, and X. Ma, "Mode-pairing quantum key distribution," *Nature Commun.*, vol. 13, no. 1, p. 3903, Jul. 2022, doi: 10.1038/s41467-022-31534-7.
[340] L. Zhou et al., "Experimental quantum communication overcomes the rate-loss limit without global phase tracking," *Phys. Rev. Lett.*, vol. 130, no. 25, Jun. 2023, Art. no. 250801, doi: 10.1103/physrevlett.130.250801.
[341] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quant. Inf. Comput.*, vol. 4, no. 5, p. 325, 2004.
[342] M. Koashi, "Simple security proof of quantum key distribution based on complementarity," *New J. Phys.*, vol. 11, no. 4, Apr. 2009, Art. no. 045018.
[343] C. Wiechers et al., "After-gate attack on a quantum cryptosystem," *New J. Phys.*, vol. 13, no. 1, Jan. 2011, Art. no. 013043.
[344] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors," *New J. Phys.*, vol. 13, no. 7, Jul. 2011, Art. no. 073024.
[345] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," *Phys. Rev. A, Gen. Phys.*, vol. 98, no. 6, Dec. 2018, Art. no. 062323, doi: 10.1103/physreva.98.062323.
[346] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Phys. Rev. X*, vol. 8, no. 3, Aug. 2018, Art. no. 031043, doi: 10.1103/physrevx.8.031043.
[347] N. L. Piparo and M. Razavi, "Long-distance trust-free quantum key distribution," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 123–130, May 2015.
[348] Y. Liu et al., "Experimental twin-field quantum key

distribution over 1000 km fiber distance," *Phys. Rev. Lett.*, vol. 130, no. 21, May 2023, Art. no. 210801, doi: 10.1103/physrevlett.130.210801.

[349] J. A. Dolphin, T. K. Paraïso, H. Du, R. I. Woodward, D. G. Marangon, and A. J. Shields, "A hybrid integrated quantum key distribution transceiver chip," *npj Quantum Inf.*, vol. 9, no. 1, p. 84, Sep. 2023, doi: 10.1038/s41534-023-00751-3.

[350] T. E. Chapuran et al., "Optical networking for quantum key distribution and quantum communications," *New J. Phys.*, vol. 11, Oct. 2009, Art. no. 105001.

[351] I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," *New J. Phys.*, vol. 13, no. 6, Jun. 2011, Art. no. 063039.

[352] K. A. Patel et al., "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Phys. Rev. X*, vol. 2, no. 4, Nov. 2012, Art. no. 041010.

[353] K. A. Patel et al., "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.*, vol. 104, no. 5, Feb. 2014, Art. no. 051123.

[354] R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable QKD with intense DWDM classical channels," *New J. Phys.*, vol. 17, no. 4, Apr. 2015, Art. no. 043027.

[355] M. Pistoia et al., "Paving the way toward 800 gbps quantum-secured optical channel deployment in mission-critical environments," *Quantum Sci. Technol.*, vol. 8, no. 3, May 2023, Art. no. 035015, doi: 10.1088/2058-9565/acd1a8.

[356] S. Bahrani, M. Razavi, and J. A. Salehi, "Crosstalk reduction in hybrid quantum-classical networks," *Scientia Iranica*, vol. 23, no. 6, pp. 2898–2907, Oct. 2016.

[357] S. Bahrani, M. Razavi, and J. A. Salehi, "Wavelength assignment in hybrid quantum-classical networks," *Sci. Rep.*, vol. 8, no. 1, p. 3456, Feb. 2018, doi: 10.1038/s41598-018-21418-6.

[358] S. Bahrani, O. Elmabrok, G. Currás Lorenzo, and M. Razavi, "Wavelength assignment in quantum access networks with hybrid wireless-fiber links," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 36, no. 3, p. 99, Mar. 2019. [Online]. Available: https://opg.optica.org/josab/abstract.cfm?URI=josab-36-3-B99

[359] P. K. Tysowski, X. Ling, N. Lütkenhaus, and M. Mosca, "The engineering of a scalable multi-site communications system utilizing quantum key distribution (QKD)," *Quantum Sci. Technol.*, vol. 3, Nov. 2017, Art. no. 024001, doi: 10.1088/2058-9565/aa9a5d.

[360] Y. Cao, Y. Zhao, J. Zhang, Q. Wang, D. Niyato, and L. Hanzo, "From single-protocol to large-scale multi-protocol quantum networks," *IEEE Netw.*, vol. 36, no. 5, pp. 14–22, Nov. 2022.

[361] A. Aguado et al., "The engineering of software-defined quantum key distribution networks," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 20–26, Jul. 2019.

[362] D. Lowndes, S. Frick, A. Hart, and J. Rarity, "A low cost, short range quantum key distribution system," *EPJ Quantum Technol.*, vol. 8, no. 1, p. 15, May 2021, doi: 10.1140/epjqt/s40507-021-00101-2.

[363] O. Elmabrok and M. Razavi, "Wireless quantum key distribution in indoor environments," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 35, no. 2, pp. 197–207, Feb. 2018.

[364] O. Elmabrok, M. Ghalaii, and M. Razavi, "Quantum-classical access networks with embedded optical wireless links," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 35, no. 3, p. 487, 2018.

[365] S. Bahrani, O. Elmabrok, G. C. Lorenzo, and M. Razavi, "Finite-key effects in quantum access networks with wireless links," in *Proc. IEEE Globecom Workshops*, Dec. 2018, pp. 1–5.

[366] S.-K. Liao et al., "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nature Photon.*, vol. 11, no. 8, pp. 509–513, Aug. 2017, doi: 10.1038/nphoton.2017.116.

[367] J.-G. Ren et al., "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, no. 7670, pp. 70–73, Sep. 2017, doi: 10.1038/nature23675.

[368] C. Liorni, H. Kampermann, and D. Bruss, "Quantum repeaters in space," *New J. Phys.*, vol. 23, no. 5, 2020, Art. no. 053021.

[369] T. Vergoossen, R. Bedington, J. A. Grieve, and A. Ling, "Satellite quantum communications when man-in-the-middle attacks are excluded," *Entropy*, vol. 21, no. 4, p. 387, Apr. 2019. [Online]. Available: https://www.mdpi.com/1099-4300/21/4/387

[370] Z. Pan et al., "Secret-key distillation across a quantum wiretap channel under restricted eavesdropping," *Phys. Rev. Appl.*, vol. 14, no. 2, Aug. 2020, Art. no. 024044, doi: 10.1103/physrevapplied.14.024044.

[371] A. Vázquez-Castro, D. Rusca, and H. Zbinden, "Quantum keyless private communication versus quantum key distribution for space links," *Phys. Rev. Appl.*, vol. 16, no. 1, Jul. 2021, Art. no. 014006, doi: 10.1103/physrevapplied.16.014006.

[372] M. Ghalaii et al., "Satellite-based quantum key distribution in the presence of bypass channels," *PRX Quantum*, vol. 4, no. 4, Nov. 2023, Art. no. 040320, doi: 10.1103/prxquantum.4.040320.

[373] C. Ottaviani et al., "Terahertz quantum cryptography," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 483–495, Mar. 2020.

[374] Z. Wang, R. Malaney, and J. Green, "Inter-satellite quantum key distribution at terahertz frequencies," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–7.

[375] 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, Oct. 2021.

[376] S. Sahu, A. Lawey, and M. Razavi, "Continuous variable quantum key distribution in multiple-input multiple-output settings," 2023, *arXiv:2308.11320*.

[377] N. K. Kundu, M. R. McKay, A. Conti, R. K. Mallik, and M. Z. Win, "MIMO terahertz quantum key distribution under restricted eavesdropping," *IEEE Trans. Quantum Eng.*, vol. 4, pp. 1–15, 2023.

[378] M. Pereira, M. Curty, and K. Tamaki, "Quantum key distribution with flawed and leaky sources," *npj Quantum Inf.*, vol. 5, no. 1, p. 62, Jul. 2019, doi: 10.1038/s41534-019-0180-9.

[379] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Phys. Rev. A, Gen. Phys.*, vol. 95, no. 1, Jan. 2017, Art. no. 012333.

[380] D. Bunandar, L. C. G. Govia, H. Krovi, and D. Englund, "Numerical finite-key analysis of quantum key distribution," *npj Quantum Inf.*, vol. 6, no. 1, p. 104, Dec. 2020, doi: 10.1038/s41534-020-00322-w.

[381] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, "Tight finite-key security for twin-field quantum key distribution," *npj Quantum Inf.*, vol. 7, no. 1, p. 22, Feb. 2021, doi: 10.1038/s41534-020-00345-3.

[382] Á. Navarrete and M. Curty, "Improved finite-key security analysis of quantum key distribution against trojan-horse attacks," *Quantum Sci. Technol.*, vol. 7, no. 3, Jun. 2022, Art. no. 035021, doi: 10.1088/2058-9565/ac74dc.

[383] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," *Nature Commun.*, vol. 9, no. 1, p. 459, Jan. 2018, doi: 10.1038/s41467-017-02307-4.

[384] 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. [Online]. Available: https://science.sciencemag.org/content/362/6412/eaam9288

[385] 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.

[386] T. R. Beals and B. C. Sanders, "Distributed relay protocol for probabilistic information-theoretic security in a randomly-compromised network," in *Information Theoretic Security*, R. Safavi-Naini, Ed., Berlin, Germany: Springer, 2008, pp. 29–39.

[387] T. K. Paraïso et al., "A modulator-free quantum key distribution transmitter chip," *npj Quantum Inf.*, vol. 5, no. 1, p. 42, May 2019, doi: 10.1038/s41534-019-0158-7.

[388] J.-P. Chen et al., "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Phys. Rev. Lett.*, vol. 124, no. 7, Feb. 2020, Art. no. 070501, doi: 10.1103/physrevlett.124.070501.

[389] M. Pittaluga et al., "600-km repeater-like quantum communications with dual-band stabilization," *Nature Photon.*, vol. 15, no. 7, pp. 530–535, Jul. 2021, doi: 10.1038/s41566-021-00811-0.

[390] M. K. Bhaskar et al., "Experimental demonstration of memory-enhanced quantum communication," *Nature*, vol. 580, no. 7801, pp. 60–64, Apr. 2020, doi: 10.1038/s41586-020-2103-5.

[391] S. Langenfeld, P. Thomas, O. Morin, and G. Rempe, "Quantum repeater node demonstrating unconditionally secure key distribution," *Phys. Rev. Lett.*, vol. 126, no. 23, Jun. 2021, Art. no. 230506, doi: 10.1103/physrevlett.126.230506.

[392] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, "Quantum repeater with encoding," *Phys. Rev. A, Gen. Phys.*, vol. 79, no. 3, Mar. 2009, Art. no. 032325.

[393] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, "Quantum communication without the necessity of quantum memories," *Nature Photon.*, vol. 6, no. 11, pp. 777–781, Nov. 2012.

[394] M. Razavi, *Fiber-Based Quantum Repeaters*. Hoboken, NJ, USA: Wiley, 2023, ch. 24, pp. 675–691, doi: 10.1002/9783527837427.ch24.

[395] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Phys. Rev. A, Gen. Phys.*, vol. 59, no. 1, pp. 169–181, Jan. 1999.

[396] Y. Yu et al., "Entanglement of two quantum memories via fibres over dozens of kilometres," *Nature*, vol. 578, no. 7794, pp. 240–245, 2020.

[397] M. Pompili et al., "Realization of a multinode quantum network of remote solid-state qubits," *Science*, vol. 372, no. 6539, pp. 259–264, 2021. [Online]. Available: https://science.sciencemag.org/content/372/6539/259

[398] Y. Jing, D. Alsina, and M. Razavi, "Quantum key distribution over quantum repeaters with encoding: Using error detection as an effective postselection tool," *Phys. Rev. Appl.*, vol. 14, no. 6, Dec. 2020, Art. no. 064037.

[399] Y. Jing and M. Razavi, "Simple efficient decoders for quantum key distribution over quantum repeaters with encoding," *Phys. Rev. Appl.*, vol. 15, no. 4, Apr. 2021, Art. no. 044027.

[400] A. Ortu et al., "Simultaneous coherence enhancement of optical and microwave transitions in solid-state electronic spins," *Nature Mater.*, vol. 17, no. 8, pp. 671–675, Aug. 2018, doi: 10.1038/s41563-018-0138-x.

[401] X. Zhou et al., "Towards quantum-native communication systems: New developments, trends, and challenges," 2023, *arXiv:2311.05239*.

[402] L.-H. Shen, K.-T. Feng, and L. Hanzo, "Five facets of 6G: Research challenges and opportunities," *ACM Compt. Surv.*, vol. 55, no. 11, pp. 1–39, 2023.

[403] Z. Xu, W. Liu, Z. Wang, and L. Hanzo, "Petahertz communication: Harmonizing optical spectra for wireless communications," *Digit. Commun. Netw.*, vol. 7, no. 4, pp. 605–614, Nov. 2021.

[404] C. Liu, C. Zhu, Z. Li, M. Nie, H. Yang, and C. Pei, "Continuous-variable quantum secret sharing based on thermal terahertz sources in inter-satellite wireless links," *Entropy*, vol. 23,

no. 9, p. 1223, Sep. 2021.
[405] K. Senthoor and P. K. Sarvepalli, "Theory of communication efficient quantum secret sharing," *IEEE Trans. Inf. Theory*, vol. 68, no. 5, pp. 3164–3186, May 2022.
[406] 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, Aug. 2021.
[407] I. B. Djordjevic, "Integrated optics modules based proposal for quantum information processing, teleportation, QKD, and quantum error correction employing photon angular momentum," *IEEE Photon. J.*, vol. 8, no. 1, pp. 1–12, Feb. 1, 2016.
[408] X. Cai, "Photonic integrated devices for exploiting the orbital angular momentum of light in optical communications," in *Proc. Prog. Electromagn. Res. Symp. (PIERS)*, Aug. 2016, p. 3164.
[409] Z. S. Lin et al., "Characterization of orbital angular momentum applying single-sensor compressive imaging based on a microwave spatial wave modulator," *IEEE Trans. Antennas Propag.*, vol. 69, no. 10, pp. 6870–6880, Oct. 2021.
[410] Z. Wang, Q. Tan, Y. Liang, X. Zhou, W. Zhou, and X. Huang, "Active manipulation of the spin and orbital angular momentums in a terahertz graphene-based hybrid plasmonic waveguide," *Nanomaterials*, vol. 10, no. 12, p. 2436, Dec. 2020.
[411] L. Viti, D. G. Purdie, A. Lombardo, A. C. Ferrari, and M. S. Vitiello, "HBN-encapsulated, graphene-based, room-temperature terahertz receivers, with high speed and low noise," *Nano Lett.*, vol. 20, no. 5, pp. 3169–3177, May 2020.
[412] M. Asgari et al., "Highly sensitive photodetectors at 0.6 THz based on quantum dot single electron transistors," in *Proc. 46th Int. Conf. Infr., Millim. THz Waves (IRMMW-THz)*, Aug. 2021, pp. 1–2.
[413] M. Asgari et al., "Quantum-dot single-electron transistors as thermoelectric quantum detectors at terahertz frequencies," *Nano Lett.*, vol. 21, no. 20, pp. 8587–8594, Oct. 2021.
[414] T. Liu, Y. Huang, Q. Wei, K. Liu, X. Duan, and X. Ren, "Optimized uni-traveling carrier photodiode and mushroom-mesa structure for high-power and sub-terahertz bandwidth under zero- and low-bias operation," *J. Phys. Commun.*, vol. 3, no. 9, Sep. 2019, Art. no. 095004.
[415] A. E. Yachmenev, R. A. Khabibullin, and D. S. Ponomarev, "Recent advances in THz detectors based on semiconductor structures with quantum confinement: A review," *J. Phys. D, Appl. Phys.*, vol. 55, no. 19, May 2022, Art. no. 193001.
[416] Z. Zhang, Z. Fu, C. Wang, and J. Cao, "Research on Terahertz quantum well photodetector," *J. Infr. Millim. Waves*, vol. 41, no. 1, pp. 103–109, 2022.
[417] D. Shao et al., "Research progress on terahertz quantum-well photodetector and its application," *Frontiers Phys.*, vol. 9, p. 581, Nov. 2021.
[418] L. Viti et al., "Thermoelectric graphene photodetectors with sub-nanosecond response times at terahertz frequencies," *Nanophotonics*, vol. 10, no. 1, pp. 89–98, Jul. 2020.
[419] L. Hanzo, M. El-Hajjar, and O. Alamri, "Near-capacity wireless transceivers and cooperative communications in the MIMO era: Evolution of standards, waveform design, and future perspectives," *Proc. IEEE*, vol. 99, no. 8, pp. 1343–1385, Aug. 2011.
[420] S. Sugiura, S. Chen, and L. Hanzo, "MIMO-aided near-capacity turbo transceivers: Taxonomy and performance versus complexity," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 421–442, 2nd Quart., 2012.
[421] R. Yuan and J. Cheng, "Free-space optical quantum communications in turbulent channels with receiver diversity," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5706–5717, Sep. 2020.
[422] N. K. Kundu, S. P. Dash, M. R. Mckay, and R. K. Mallik, "Channel estimation and secret key rate analysis of MIMO terahertz quantum key distribution," *IEEE Trans. Commun.*, vol. 70, no. 5, pp. 3350–3363, May 2022.
[423] M. Gabay and S. Arnon, "Quantum key distribution by a free-space MIMO system," *J. Lightw. Technol.*, vol. 24, no. 8, pp. 3114–3120, Aug. 15, 2006.
[424] X. Zhou, C. Wei, D. Shen, C. Xu, L. Wang, and X. Yu, "A shot noise limited quantum iterative massive MIMO system over Poisson atmospheric channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.
[425] M. Razavi, "Multiple-access quantum key distribution networks," *IEEE Trans. Commun.*, vol. 60, no. 10, pp. 3071–3079, Oct. 2012.
[426] M. Rezai and J. A. Salehi, "Quantum CDMA communication systems," *IEEE Trans. Inf. Theory*, vol. 67, no. 8, pp. 5526–5547, Aug. 2021.
[427] V. Sharma and S. Banerjee, "Quantum communication using code division multiple access network," *Opt. Quantum Electron.*, vol. 52, no. 8, pp. 1–22, Aug. 2020.
[428] M. Anandan, S. Choudhary, and K. P. Kumar, "OFDM for frequency coded quantum key distribution," in *Proc. Int. Conf. Fiber Opt. Photon. (PHOTONICS)*, Dec. 2012, pp. 1–3.
[429] S. Bahrani, M. Razavi, and J. A. Salehi, "Orthogonal frequency-division multiplexed quantum key distribution," *J. Lightw. Technol.*, vol. 33, no. 23, pp. 4687–4698, Dec. 2015.
[430] C. Fragouli and E. Soljanin, "Network coding fundamentals," *Found. Trends Netw.*, vol. 2, no. 1, pp. 1–133, 2007.
[431] M. Hayashi, K. Wama, H. Nishimura, R. Raymond, and S. Yamashita, *Quantum Network Coding* (Lecture Notes in Computer Science), vol. 4393. Berlin, Germany: Springer-Verlag, 2007, pp. 610–621. [Online]. Available: <Go to ISI>://WOS:000245503800052
[432] 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. [Online]. Available: http://ieeexplore.ieee.org/ielx5/18/5484964/05485004.pdf?tp=&arnumber=5485004&isnumber=5484964
[433] 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.
[434] 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. [Online]. Available: http://ieeexplore.ieee.org/ielx7/4234/7033064/06980095.pdf?tp=&arnumber=6980095&isnumber=7033064
[435] 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, doi: 10.1103/physreva.93.032302.
[436] 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. [Online]. Available: http://ieeexplore.ieee.org/ielx7/4234/6818356/06784159.pdf?tp=&arnumber=6784159&isnumber=6818356
[437] 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, doi: 10.1103/physreva.86.032331.
[438] A. Jain, M. Franceschetti, and D. A. Meyer, "On quantum network coding," *J. Math. Phys.*, vol. 52, no. 3, p. 610, 2011. [Online]. Available: http://scitation.aip.org/docserver/fulltext/aip/journal/jmp/52/3/1.3555801.pdfexpires=1447779606&id=id&accname=2103930&checksum=932D2C468D049497975E80ED33E678FD
[439] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, "From quantum multiplexing to high-performance quantum networking," *Nat. Photon.*, vol. 4, no. 11, pp. 792–796, Nov. 2010. [Online]. Available: http://www.nature.com/nphoton/journal/v4/n11/pdf/nphoton.2010.213.pdf
[440] 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. [Online]. Available: <Go to ISI>://WOS:000250619700001
[441] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rötteler, "Constructing quantum network coding schemes from classical nonlinear protocols," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2011, pp. 109–113. [Online]. Available: http://ieeexplore.ieee.org/ielx5/6026198/6033677/06033701.pdf?tp=&arnumber=6033701&isnumber=6033677
[442] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rötteler, "Perfect quantum network communication protocol based on classical network coding," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2686–2690.
[443] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Roetteler, *General Scheme for Perfect Quantum Network Coding With Free Classical Communication* (Lecture Notes in Computer Science), vol. 5555. Berlin, Germany: Springer, 2009, pp. 622–633. [Online]. Available: <Go to ISI>://WOS:000270963700051
[444] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 3, Feb. 2002, Art. no. 032302.
[445] Z. Sun et al., "Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5778–5792, Sep. 2020.
[446] X.-J. Li, D. Pan, G.-L. Long, and L. Hanzo, "Single-photon-memory measurement-device-independent quantum secure direct communication—Part I: Its fundamentals and evolution," *IEEE Commun. Lett.*, vol. 27, no. 4, pp. 1055–1059, Apr. 2023.
[447] X.-J. Li, D. Pan, G.-L. Long, and L. Hanzo, "Single-photon-memory measurement-device-independent quantum secure direct communication—Part II: A practical protocol and its secrecy capacity," *IEEE Commun. Lett.*, vol. 27, no. 4, pp. 1060–1064, Apr. 2023.
[448] F. Li et al., "Demonstration of fully-connected quantum communication network exploiting entangled sideband modes," *Frontiers Phys.*, vol. 18, no. 4, Aug. 2023, Art. no. 42303.
[449] Z.-Z. Sun, D. Pan, D. Ruan, and G.-L. Long, "One-sided measurement-device-independent practical quantum secure direct communication," *J. Lightw. Technol.*, vol. 41, no. 14, pp. 4680–4690, Feb. 15, 2023.
[450] D. Pan et al., "The evolution of quantum secure direct communication: On the road to the qinternet," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 3, pp. 1898–1949, 3rd Quart., 2024.
[451] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design," *IEEE Access*, vol. 1, pp. 94–122, 2013.
[452] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Joint quantum-assisted channel estimation and data detection," *IEEE Access*, vol. 4, pp. 7658–7681, 2016.
[453] P. Botsinis et al., "Quantum-aided multi-user transmission in non-orthogonal multiple access systems," *IEEE Access*, vol. 4, pp. 7402–7424, 2016.
[454] E. Villaseñor, M. He, Z. Wang, R. Malaney, and M. Z. Win, "Enhanced uplink quantum communication with satellites via downlink channels," *IEEE Trans. Quant. Eng.*, vol. 2, pp. 1–18, 2021.

ABOUT THE AUTHORS

Lajos Hanzo (Life Fellow, IEEE) received the degree from the Technical University of Budapest, in 2009, and the degree from Edinburgh University, in 2015.

Dr. Hanzo was a recipient of the IEEE Eric Sumner Technical Field Award. He is a Foreign Member of the Hungarian Science Academy and a fellow of the Royal Academy of Engineering (FREng), IET, and EURASIP.

Zunaira Babar (Senior Member, IEEE) received the B.Eng. degree from the National University of Science and Technology (NUST), Pakistan, in 2008, and the M.Sc. (honors) and Ph.D. degrees from the University of Southampton, Southampton, U.K., in 2011 and 2015, respectively.

She is currently a Staff Research Scientist with the VIAVI Marconi Labs and also an Adjunct Fellow with the University of Southampton. She has authored about 40 journal articles on quantum communications.

Zhenyu Cai received the B.A. and M.Sc. degrees from the University of Cambridge, Cambridge, U.K., in 2017, and the Ph.D. degree in quantum technologies from the University of Oxford, Oxford, U.K., in 2020.

Since then, he has been a Junior Research Fellow of physics with St John's College, University of Oxford. His current research interests center around quantum error correction, quantum error mitigation, and their practical implementations in actual quantum hardware.

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, Southampton, U.K., in 2020.

He is currently a Quantum Error Correction Researcher with Photonic Inc., Canada, and also a Visiting Research Fellow with the University of Southampton. He has authored about 30 journal articles on quantum communications.

Ivan B. Djordjevic (Fellow, IEEE) received the Ph.D. degree from the Faculty of Electronic Engineering, University of Nis, Yugoslavia, in 1999.

He held appointments at the University of Bristol, Bristol, U.K., and the University of the West of England, Bristol, Tyco Telecommunications, USA, National Technical University of Athens, Greece, and State Telecommunication Company, Nis, Yugoslavia. He is currently a Professor of ECE and optical sciences with The University of Arizona, Tucson, AZ, USA, where he also serves as the Director for the Optical Communications Systems Laboratory (OCSL) and the Quantum Communications (QuCom) Laboratory. He has authored or coauthored 11 books, 13 book chapters, and more than 590 journal and conference publications, and holds 56 U.S. patents. His current research interests are quantum communications, networking, and sensing.

Dr. Djordjevic is an Optica (formerly OSA) Fellow. He is serving as an Editor for IEEE TRANSACTIONS ON COMMUNICATIONS, *Optical and Quantum Electronics*, and *Frequenz*. He has served as an Associate Editor for *Journal of Optical Communications and Networking* from 2019 to 2023. He has served as an Area Editor/a Senior Editor/an Editor for IEEE COMMUNICATIONS LETTERS from 2012 to 2021. He has served as an Associate Editor/an Editorial Board Member for *Journal of Optics* (IOP) and *Physical Communication Journal* (Elsevier) from 2016 to 2021.

Balint Koczor received the Ph.D. degree from the Technical University of Munich, Munich, Germany, where he worked on fundamental quantum theory and mathematical physics.

He then joined the Group of Prof. Simon Benjamin, Oxford, U.K., to work on the theory of early quantum computers and held a Glasstone Research Fellowship. He is internationally recognized for his research on quantum error mitigation and near-term quantum computing. He works part-time as a Lead Quantum Theorist with Quantum Motion Company. He is currently an Associate Professor of quantum information theory and a Future Leaders Fellow with the Mathematical Institute, Oxford. He has authored widely on quantum science and engineering.

Soon Xin Ng (Senior Member, IEEE) received the B.Eng. degree (First Class) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively.

From 2003 to 2006, he was a Postdoctoral Research Fellow working on collaborative European research projects known as SCOUT, NEWCOM, and PHOENIX. Since August 2006, he has been an Academic Staff Member with the School of Electronics and Computer Science, University of Southampton. He is involved in the OPTIMIX and CONCERTO European projects as well as the IU-ATC and UC4G projects. He is currently a Full Professor of telecommunications with the University of Southampton. He has published widely in quantum communications. His research interests include adaptive coded modulation, coded modulation, channel coding, space–time coding, joint source and channel coding, iterative detection, orthogonal frequency-division multiplexing (OFDM), multiple-input multiple-output (MIMO), cooperative communications, distributed coding, quantum error correction codes, and joint wireless-and-optical-fiber communications. He has authored over 200 articles and co-authored two John Wiley/IEEE Press books in this field.

Dr. Ng is a Chartered Engineer and a fellow of the Higher Education Academy, U.K. He is one of the four members of the IEEE Quantum Communications and Information Technology (QCIT), emerging Technical Committee's Leadership Team.

Mohsen Razavi received the B.Sc. and M.Sc. degrees in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 1998 and 2000, respectively, and the Ph.D. degree from MIT, in 2006.

He was a Postdoctoral Fellow with the Institute for Quantum Computing, University of Waterloo, Waterloo, ON, Canada, until September 2009. Then, he joined the School of Electronic and Electrical Engineering, University of Leeds, Leeds, U.K., where he is currently a Professor of quantum communications. He has authored a book *Quantum Communications Networks* in IOP Concise Physics Series. His research interests include a variety of topics in quantum optical communications, quantum optics, and quantum communications networks.

Dr. Razavi was a recipient of the Marie-Curie International Reintegration Grant. He organized the first International Workshop on Quantum Communication Networks in 2014. He was a Coordinator of the European Innovative Training Network, QCALL, which aimed at providing quantum communications services to all users.

Osvaldo Simeone (Fellow, IEEE) received the M.Sc. (honors) and Ph.D. degrees in information engineering from the Politecnico di Milano, Milan, Italy, in 2001 and 2005, respectively.

From 2006 to 2017, he was a Faculty Member with the Electrical and Computer Engineering (ECE) Department, New Jersey Institute of Technology (NJIT), Newark, NJ, USA, where he was affiliated with the Center for Wireless Information Processing (CWiP). He is currently a Professor of information engineering with the Centre for Telecommunications Research, Department of Engineering, King's College London, London, U.K., where he directs the King's Communications, Learning and Information Processing Laboratory. He has authored the textbook "Machine Learning for Engineers" (Cambridge University Press), four monographs, including "An Introduction to Quantum Machine Learning" on the Foundations and Trends in Signal Processing, and more than 180 research journal and magazine articles. His research interests include information theory, machine learning, wireless communications, neuromorphic computing, and quantum machine learning.

Dr. Simeone was a co-recipient of the 2022 IEEE Communications Society Outstanding Paper Award, the 2021 IEEE Vehicular Technology Society Jack Neubauer Memorial Award, the 2019 IEEE Communication Society Best Tutorial Paper Award, the 2018 IEEE Signal Processing Best Paper Award, the 2017 JCN Best Paper Award, the 2015 IEEE Communication Society Best Tutorial Paper Award, and the best paper awards of IEEE SPAWC 2007 and IEEE WRECOM 2007. He was awarded the Open Fellowship by the EPSRC in 2022 and the Consolidator Grant by the European Research Council (ERC) in 2016. He is a fellow of IET and EPSRC. His research has also been supported by the U.S. National Science Foundation, the European Commission, ERC, Vienna Science and Technology Fund, and the European Space Agency, as well as by a number of industrial collaborations including with Intel Labs and InterDigital. He is the Chair of the Signal Processing for Communications and Networking Technical Committee of the IEEE Signal Processing Society and the U.K. and Ireland Chapter of the IEEE Information Theory Society. He is currently a Distinguished Lecturer of the IEEE Communications Society. He was a Distinguished Lecturer of the IEEE Information Theory Society from 2017 to 2018.