

Joint QKD-Post-Quantum Cryptosystems

IVAN B. DJORDJEVIC¹, (Fellow, IEEE)

Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721, USA

e-mail: ivan@email.arizona.edu

ABSTRACT To extend the transmission distance and/or improve secret-key rate of QKD protocols, we propose to employ the joint QKD-post-quantum cryptosystems in which QKD is used for raw-key transmission while the post-quantum cryptography (PQC) subsystem to transmit parity bits for information reconciliation. We also describe a run-time configurable spatially coupled (SC)-LDPC code, derived from template quasi-cyclic (QC)-LDPC, suitable for use in both information reconciliation and McEliece crypto-subsystem. For twin-field (TF)-QKD subsystem, the proposed joint cryptosystem, which takes the complexity of algorithm used to break the PQC subsystem into account, is able to achieve record distance of 1238 km over ultra-low-loss fiber.

INDEX TERMS Quantum communication, quantum key distribution (QKD), discrete variable (DV)-QKD, post-quantum cryptography, information reconciliation, McEliece cryptosystem, secret-key rate (SKR).

I. INTRODUCTION

Quantum communication (QuCom) employs the quantum information theory concepts to realize the distribution of keys with verifiable security, commonly referred to as quantum key distribution (QKD) [1], [2]. The theorems on no-cloning and indistinguishability of non-orthogonal quantum states give rise to QKD, where security is ensured by fundamental laws of physics as opposed to unproven mathematical assumptions employed in computational security-based cryptography. Despite the appealing features of QuCom, there are some fundamental and technical challenges that need to be addressed prior to its widespread applications. For instance, both rate and distance of QuCom are fundamentally limited by the channel loss, which is specified by the rate-loss trade-off. To overcome the rate-distance limit of discrete variable (DV)-QKD protocols, two approaches have been pursued recently: (i) development of quantum relays [3] and (ii) the employment of the trusted relays [4]. Unfortunately, the quantum relays require the use of long-duration quantum memories and high-fidelity entanglement distillation, which are still out of reach with current technology. On the other hand, the trusted-relay methodology assumes that the relay between two users can be trusted; unfortunately, this assumption is difficult to verify in practice. The measurement device independent (MDI)-QKD approach [5], was able to close the detection loopholes and extend the transmission distance, however, its secret-key rate (SKR) is still bounded by $O(T)$ -dependence of the upper limit (with T being transmissivity). Recently, the twin-field (TF) QKD has been proposed to

overcome the rate-distance limit [6]. The authors in [6] have shown that TF-QKD upper limit scales with the square-root of transmittance, that is $r \sim O(\sqrt{T})$, which represents a promising approach to extend the transmission distance. However, given that TF-QKD, similar to MDI-QKD, relies on partial Bell state measurements by Charlie (Eve), the Bell states $|\phi^\pm\rangle = 2^{-1/2}(|00\rangle + |11\rangle)$ cannot be distinguished resulting in low overall SKRs at extended distances.

To overcome these key challenges for DV-QKD, we propose a different strategy. To increase the generation rate of the secret key and to extend the transmission distance we propose to limit the information revealed during the error reconciliation phase by transmitting the parity bits by using the post-quantum cryptography (PQC) algorithms [7]. The PQC is typically referred to various cryptographic algorithms that are thought to be secure against any quantum computer-based attack. Unfortunately, the PQC is also based on unproven assumptions and some of the QPC algorithms might be broken in future by developing more sophisticated quantum algorithms. For instance lattice-based cryptography algorithms often rely on so called collision resistance hash functions, such as $\mathbf{u} = \mathbf{A}\mathbf{x}$, where \mathbf{x} is Alice private vector and \mathbf{u} is the public vector, with \mathbf{A} being $m \times n$ public matrix with columns representing the lattice basis vectors. To determine the Alice's private vector \mathbf{x} Eve will need to do matrix inversion to get $\mathbf{x} = \mathbf{A}^{-1}\mathbf{u}$. By using the quantum computer designed to perform Harrow-Hassidim-Lloyd (HHL)-like algorithm [8], Eve can get the exponential speed-up compared to corresponding classical algorithm, and the security of lattice-based cryptography cannot be guaranteed anymore. This is the reason why we propose here to use the PQC algorithms only in information reconciliation phase to limit the leakage due to transmission

The associate editor coordinating the review of this manuscript and approving it for publication was Sukhdev Roy.

of parity bits over an authenticated classical channel (in conventional QKD). Even though the best quantum algorithms can provide the exponential speed-up over corresponding classical algorithms, the complexity of quantum algorithms cannot be ignored, and it can be still expressed in terms of number of quantum gates required. So the number of security bits is still proportional to the $\log_2(L)$, where L is the number of operations needed for an attack to be successful [9]. When quantum algorithm is used to break-up the PQC protocol the number of security bits $\log_2(L)$ is typically not sufficient for perfect security algorithms, such as one-time pad. However, when an (N, K) LDPC code of high rate is used in information reconciliation, with the number of parity bits $N - K \ll n$ (the codeword length used in PQC subsystem), the QPC security is sufficient to eliminate the leakage during the error correction stage. In related paper [10], we proposed to use the covert channel for information reconciliation; however, the corresponding rigorous security proof has not been derived yet. In conventional QKD, it is commonly assumed that Eve is an all-powerful eavesdropper and the complexity of quantum algorithms used to break the classical cryptography algorithms is ignored. Unfortunately, this omnipotent assumption is often too restrictive and not realistic in practical applications. The proposed joint QKD-cryptosystem scheme belongs to the class of realistic cryptography schemes when Eve is not omnipotent in the sense that it assumes that algorithms used to break the protocols have complexity that cannot be ignored. Moreover, the proposed joint QKD-PQC scheme exploits the complexity of corresponding quantum algorithms. The security of this scheme is wholly dependent on still unproven security of its weakest link, namely the protection of the parity bits transmitted over PQC channel. As such, this scheme cannot claim the security consistent with full-scale QKD, but rather it represents an alternative to both full-scale QKD and PQC.

The paper is organized as follows. The proposed joint QKD-post-quantum cryptosystems are described in Section II. In Section III, the proposed joint TF-QKD-McEliece cryptosystem is described in detail. The illustrative secret-key rate results are provided in Sec. IV. Concluding remarks are provided in Sec. V.

II. JOINT QKD-POST-QUANTUM CRYPTOSYSTEMS

The proposed joint QKD-post-quantum encryption concept is applicable to any QKD scheme. Let us describe the joint cryptosystem for DV-QKD subsystem, in which reverse reconciliation is employed. The QKD subsystem is used for raw key transmission. After the sifting procedure and quantum bit-error rate (QBER) estimation, as shown in Fig. 1, Bob employs an (N, K) LDPC code with parity-check matrix H of size $(N - K) \times N$ to create the syndrome vector $\mathbf{p} = \mathbf{x}\mathbf{H}^T$, where \mathbf{x} is the Bob's vector after the sifting procedure. In conventional information reconciliation, Bob would transmit the syndrome vector over an (error-free) authenticated public channel to which Eve has access. In our proposed joint encryption scheme, we will encrypt the syndrome vector

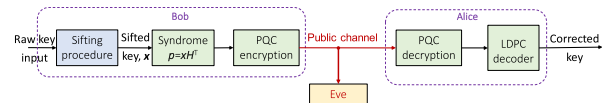


FIGURE 1. Illustrating the PQC-based information reconciliation.

by employing a properly chosen post-quantum cryptography algorithm. The popular PQC schemes include [7]: the code-based cryptography, lattice-based cryptography, hash-based cryptography, and multivariate cryptography. This work has gained greater attention from academics and industry through the PQCrypto conference series since 2006. In particular, the McEliece cryptosystem [12] based on quasi cyclic (QC) LDPC coding [13] is straightforward to implement. In this version, the adaptive LDPC code can be used for both information reconciliation and PQC-based encryption. Unfortunately, as mentioned in introduction already, similarly to computational cryptography, the PQC is based on unproven assumptions. Namely, some of the QPC algorithms might be broken in future by developing more advanced quantum algorithms. Further, the complexity of decryption algorithm in PQC dictates the number of secure bits, which is insufficient for perfect security, such as one-time pad. By using the PQC algorithms only to protect the transmission of syndrome vector of length $N - K$, which for high-rate LDPC codes is much shorter than the codeword length n used in PQC, we can achieve the perfect security. So the key idea of our proposal is to reduce leakage of information during error correction. On the other hand, by employing the QKD subsystem for raw-key transmission, we can identify the presence of the Eve. By limiting information leakage due to information reconciliation we can significantly extend the transmission distance, as shown in Section IV. As an illustration, the secret fraction r for decoy-state-BB84 protocol can be represented as follows [2], [11]:

$$r = q_1^{(Z)} \left[1 - h_2 \left(e^{(X)} \right) \right] - q_\mu^{(Z)} f_e h_2 \left(e_\mu^{(Z)} \right), \quad (1)$$

where we used the subscript 1 to denote the single-photon pulses and μ to denote the pulse with the mean photon number μ . In (1) $q^{(Z)}$ denotes the probability of declaring a successful result (“the gain”) when Alice sent a single-photon and Bob detected it in the Z-basis, f_e denotes the error correction inefficiency ($f_e \geq 1$), $e^{(X)}$ [$e^{(Z)}$] denotes the QBER in the X-basis (Z-basis), and $h_2(x)$ is the binary entropy function. The second term $q^{(Z)} h_2[e^{(X)}]$ corresponds to the amount of information Eve was able to learn during the raw key transmission. The third term $q^{(Z)} f_e h_2[e^{(Z)}]$ denotes the amount of information revealed during the information reconciliation stage, typically related to the parity-bits transmitted over an authenticated (noiseless) public channel. Now by transmitting the parity bits using the PQC, with number of parity bits lower than the number of security bits in PQC, the last term can be eliminated, which results in significant improvement in transmission distance (see Section IV). This is particularly true when the second term is close to the first term [see Eqn. (1)], which corresponds to the high attenuation regime.

The quantum algorithms to be developed (not yet known), capable of breaking the PQC algorithms will have certain complexity expressed in terms of number of operations L . By ensuring that the number of parity bits $N - K$ is shorter than the number of secure PQC bits $\log_2 L$, the proposed cryptographic scheme will be secure. Evidently, the proposed cryptographic scheme exploits the complexity of corresponding quantum algorithms used to break the PQC protocols. On the other hand, the conventional QKD algorithms assume that Eve is all-powerful and ignore the complexity of different quantum attacks. Therefore, the proposed cryptographic scheme belongs to the class of cryptographic schemes in which Eve is not omnipotent.

In incoming section we describe, the joint TF-QKD-McEliece cryptosystem with more details. In the rest of this section, we describe an adaptive LDPC coding scheme to be used in both information reconciliation and McEliece crypto subsystem. The starting point is the QC-LDPC code with the template parity-check matrix:

$$H_{QC} = \begin{bmatrix} I & I & I & \dots & I \\ p^{S[0]} & p^{S[1]} & p^{S[2]} & \dots & p^{S[c-1]} \\ p^{2S[0]} & p^{2S[1]} & p^{2S[2]} & \dots & p^{2S[c-1]} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p^{(r-1)S[0]} & p^{(r-1)S[1]} & p^{(r-1)S[2]} & \dots & p^{(r-1)S[c-1]} \end{bmatrix}, \quad (2)$$

where I and P are identity and permutation matrices of size $b \times b$, and integers $S[i] \in \{0, 1, \dots, b-1\}$ ($i = 0, 1, \dots, r-1$; $r < b$) are properly chosen to satisfy the girth (the largest cycle in corresponding bipartite graph representation of H_{QC}) constrains, as described in [14]. We can incorporate many QC-LDPC codes using this design. As an illustration, the column-weight-3 code of girth-10 can be designed to be a subcode of girth-8, column weight-4 code. Lower-rate code of the same girth should be a subcode of higher-rate code. This architecture allows run-time reconfiguration on codeword-by-codeword basis. Its operation has been demonstrated over a free-space optical channel in the presence of time-varying atmospheric turbulence in our recent paper [15]. Finer granulation in code rate adaptation can be implemented by shortening. For application of QC-LDPC code design in McEliece cryptosystem, we propose to generate many sets of integers $\{S[i]\}$ satisfying run-time configurability conditions and select them at random. By using this QC-LDPC code as a template design, we create a spatially coupled (SC)-LDPC code as illustrated in Fig. 2(left). The codeword length of this SC-LDPC code will be $b \times (l \times c - m \times (l - 1))$, where l is the number of coupled template QC-LDPC codes and m is the coupling length expressed in terms of number of blocks. Because there are $r \times c \times l$ non-empty submatrices in the parity-check matrix of the SC-LDPC code, we can introduce the layer index (l.i.) and reduce the memory requirements as illustrated in Fig. 2(right). In such a way we do not need to memorize the all-zeros submatrices. For full-rank parity-check matrix of the template QC-LDPC code,

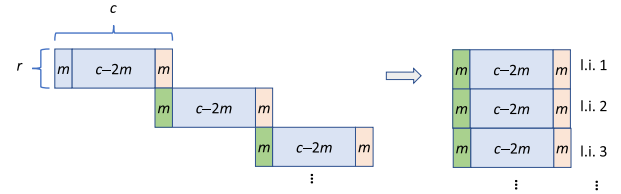


FIGURE 2. Illustrating the SC-LDPC code design derived from the template QC-LDPC code.

the code rate of SC-LDPC code will be simply:

$$R = 1 - \frac{rl}{lc - m(l - 1)}. \quad (3)$$

Therefore, for fixed l , by increasing the coupling length m we can reduce the code rate and thus improve the error-correction capability of the code. For FPGA implementation of decoders for SC-LDPC codes an interested reader is referred to our previous paper [16]. To adjust for error correction strength, depending on time-varying channel conditions, we can adapt both the template QC-LDPC code and parameters of corresponding SC-LDPC code. For application in McEliece crypto-subsystem, we propose to randomly select parameters of both QC- and SC-LDPC designs.

III. JOINT TF-QKD-McEliece CRYPTOSYSTEM

The proposed TF-QKD scheme with information reconciliation based on McEliece cryptosystem is provided in Fig. 3. The stabilized CW lasers of low linewidth are used on Alice and Bob sides to generate the global phase stabilized optical pulses with the help of amplitude modulator. Alice and Bob choose the random phases $\phi_A \in [0, 2\pi]$ and $\phi_B \in [0, 2\pi]$, respectively, with corresponding phase modulators. The random phase difference between Alice and Bob are discretized so that:

$$\phi_{A,B} \in \Delta\phi_{k_{A,B}} = \left[\frac{2\pi}{M} k_{A,B}, \frac{2\pi}{M} (k_{A,B} + 1) \right), \quad (4)$$

wherein the phase-bin $\Delta\phi_k$ is discretized by $k_{A,B} \in \{0, 1, \dots, M - 1\}$. Alice (Bob) then randomly select whether to use Z-basis or X-basis. When Z-basis is selected, the phase-randomized coherent state is sent with intensity either μ or 0. When X basis encoding is selected, Alice and Bob employ corresponding phase and amplitude modulators to randomly select 0 ($\pi/2$) and π ($3\pi/2$) representing logic bits 0 and 1, and such phase-encoded pulses are sent with randomly selected intensities. The corresponding quantum states, generated by Alice and Bob, are sent towards Charlie over the ultra-low-loss fiber link. The polarization

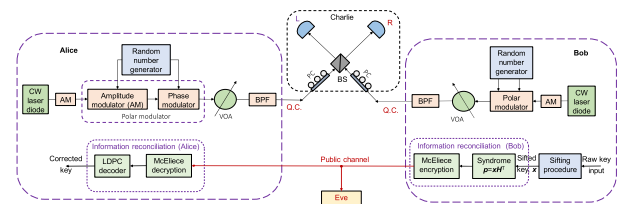


FIGURE 3. The proposed TF-QKD scheme with information reconciliation based on McEliece encryption. BS: beam splitter, PC: polarization controller, BPF: bandpass filter, VOA: variable optical attenuator.

controllers (PCs) ensure that Alice and Bob's pulses have the same polarization. Charlie performs the Bell state measurements (BSMs) and announces the results. Alice and Bob then disclose their phase information, that is $k_{A,B}$ and intensities, and these are used for parameter estimation. They keep the information related to Z-basis confidential to Charlie, and these data are used for raw key. Alice and Bob then perform McEliece encryption-based information reconciliation described below, followed by the privacy amplification, to get the common secure key.

Given that the McEliece cryptosystem [12] based on quasi cyclic (QC)-LDPC coding is straightforward to implement as shown in [13], while the corresponding LDPC encoders and decoders have been already implemented in FPGAs [15], it represents an excellent candidate to use for transmission of parity bits in TF-QKD scheme. In particular, rate-adaptive spatially coupled LDPC code derived from an QC-LDPC code, introduced in Fig. 2, is very flexible for use in both information reconciliation and McEliece cryptosystem to encrypt the parity bits. In reverse reconciliation, based on channel conditions Bob selects the block-columns in template QC-LDPC code, coupling length for spatial LDPC coding design, and the number of spatially coupling blocks and provides to Alice the details of the spatially coupling (N, K) LDPC code design. Bob further encodes the information bits \mathbf{u} obtained during sifting procedure by employing the selected spatially coupling LDPC code to get the parity bits (syndrome) \mathbf{p} .

Regarding the McEliece encryption subsystem, Alice randomly chooses the number of block-columns in template parity-check matrix of corresponding QC-LDPC code as well as the coupling length m and number of template QC-LDPC codes l to be used in McEliece encryption scheme. She generates the generator matrix \mathbf{G} based on [15], [16] and publishes the public key \mathbf{G}' determined by $\mathbf{G}' = \mathbf{S}^{-1}\mathbf{G}\mathbf{P}^{-1}$, where \mathbf{S} is the non-singular scrambling matrix and \mathbf{P} is the permutation matrix, different from \mathbf{P} in Eqn. (2). Bob will then encode the parity bits (syndrome vector) \mathbf{p} as follows $\mathbf{r} = \mathbf{p}\mathbf{G}' + \mathbf{e}$, where \mathbf{e} is the error pattern (vector) of low weight. Upon receiving \mathbf{r} Alice will perform the transformation $\mathbf{r}' = \mathbf{r}\mathbf{P}' = \mathbf{p}\mathbf{S}^{-1}\mathbf{G} + \mathbf{e}\mathbf{P}'$, followed by decoding based on the parity-check matrix to obtain $\mathbf{p}' = \mathbf{p}\mathbf{S}^{-1}$, and will recover \mathbf{p} by multiplication of \mathbf{p}' by \mathbf{S} . Alice will further use this parity bits \mathbf{p} to perform the error reconciliation and get \mathbf{u} .

The privacy amplification is further performed to distill from the corrected key a smaller set of bits whose correlation with Eve's string falls below the desired threshold, through the use of the universal hash functions. Assuming that Eve employs the quantum information set decoding (QISD) attack [9], the number of parity bits $N - K$ to be encrypted by (n, k) LDPC coding based McEliece encryption scheme is upper bounded by:

$$N - K \leq \log_2 \left[n^2 \sqrt{\binom{n}{k} / \left(0.29 \binom{n-t}{k} \right)} \right], \quad (5)$$

where t is the maximum number of errors that can be corrected by the LDPC code used in McEliece encryption subsystem. For high-rate QC- and spatially coupled LDPC codes used in information reconciliation this condition is much less stringent compared to using McEliece encryption to protect the information sequence instead.

IV. ILLUSTRATIVE SKR RESULTS

In Figure 4 we provide comparisons of the proposed joint TF-QKD-McEliece encryption scheme against the corresponding QKD subsystems employing phase-matching (PM) TF-QKD protocol introduced in [17], the MDI-QKD protocol [18], and decoy-state-based BB84 protocol [11]. The system parameters are selected as follows: the detector efficiency $\eta_d = 0.25$, reconciliation inefficiency $f_e = 1.15$, the dark count rate $p_d = 8 \times 10^{-8}$, misalignment error $e_d = 1.5\%$, and the number of phase slices for PM TF-QKD is set to $M = 16$. Regarding the transmission medium, it is assumed that recently reported ultra-low-loss fiber of attenuation 0.1419 dB/km (at 1560 nm) is used [19]. Both PM TF-QKD and joint TF-QKD-McEliece encryption schemes outperform the decoy-state BB84 protocol for distances larger than 162 km, while simultaneously outperforming MDI-QKD protocol for all distances. The PM TF-QKD protocol can achieve the maximum distance of 623 km. The proposed joint TF-QKD-McEliece encryption scheme, under QISD attack, is able to achieve the distance of even 1127 km thus significantly outperforming all other schemes. As expected, the improvement at higher normalized SKRs, such as 10^{-8} , is moderate (122 km). To improve the SKR further we propose to employ parallel joint TF-QKD-McEliece encryption systems by employing multiple photon degrees of freedom including polarization, wavelength, OAM, and spatial modes, and similar fashion as it was done in [20].

To determine what is the maximum possible transmission distance using this scheme, in Fig. 5 we study SKR vs. transmission distance of joint MP-TF-QKD-McEliece cryptosystem, under QISD attack, for different detector efficiencies, assuming $M = 16$, $f_e = 1.05$, and $p_d = 10^{-8}$. Clearly, for detector efficiency 0.5 the transmission distance can be

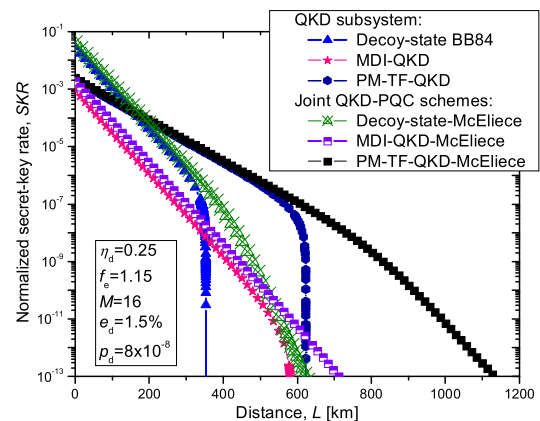


FIGURE 4. Proposed joint QKD-McEliece encryption schemes under QISD attack against decoy-state, MDI-QKD, and PM-TF-QKD in terms of SKR vs. distance.

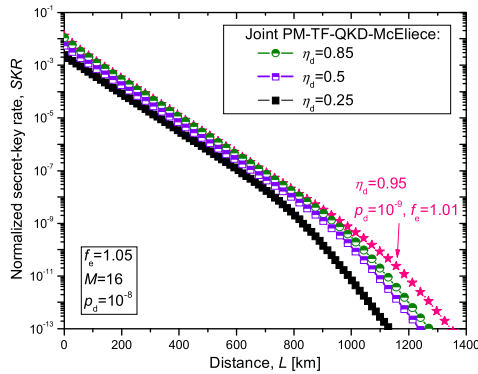


FIGURE 5. SKR vs. distance of proposed joint QKD-McEliece cryptosystem under QISD attack for different detector efficiencies.

extended to 1238 km. For almost ideal system parameters ($\eta_d = 0.95$, $f_e = 1.01$, and $p_d = 10^{-9}$), the maximum possible transmission distance for normalized SKR of 10^{-13} is 1355 km.

V. CONCLUDING REMARKS

The DV-QKD protocols are fundamentally limited by the channel loss, which is specified by the rate-loss tradeoff. To solve for this problem, we have proposed to employ the joint QKD-post-quantum cryptosystems in which QKD has been used for raw-key transmission, while the post-quantum cryptography subsystem has been used to transmit parity bits needed in information reconciliation. The proposed scheme is applicable to the realistic scenarios when Eve is not an omnipotent eavesdropper ignoring the complexity of algorithms used to break the protocol. We also have described a run-time configurable spatially coupled-LDPC code, derived from template quasi cyclic-LDPC code, suitable for use in McEliece-based information reconciliation. We have demonstrated by simulations that the joint twin-field-QKD-McEliece cryptosystem, under QISD attack, is able to achieve record distance over ultra-low-loss fiber of 1238 km.

The proposed scheme represents an alternative to both full-scale QKD and PQC. The extension of QKD range can also be achieved by relaxing security assumptions, such as the restricted eavesdropping scenario introduced in [21].

ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers for the comments that provided an improvement to the manuscript.

REFERENCES

- [1] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, Sep. 2017.
- [2] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution*. Cham, Switzerland: Springer, 2019.
- [3] 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.
- [4] J. Qiu, "Quantum communications leap out of the lab," *Nature*, vol. 508, no. 7497, pp. 441–442, Apr. 2014.
- [5] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-Device-Independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, Nov. 2016, Art. no. 190501.

- [6] 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.
- [7] D. J. Bernstein, J. Buchmann, E. Dahmen, *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009.
- [8] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for solving linear systems of equations," *Phys. Rev. Lett.*, vol. 103, Mar. 2009, Art. no. 150502.
- [9] D. J. Bernstein, "Grover vs. McEliece," in *Post-Quantum Cryptography—PQCrypto* (Lecture Notes in Computer Science), vol. 6061, N. Sendrier, Eds. Berlin, Germany: Springer, 2010.
- [10] J. Gariano and I. B. Djordjevic, "Employing covert communications-based information reconciliation and multiple spatial modes to polarization entanglement QKD," *Opt. Lett.*, vol. 44, no. 3, pp. 687–690, Feb. 1, 2019.
- [11] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, Jun. 2005, Art. no. 230504.
- [12] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DNS Prog. Rep., Jet Propuls. Lab., Pasadena, CA, USA, Tech. Rep. 42-44, 1978, pp. 114–116.
- [13] M. Baldi, F. Chiaraluce, and M. Bianchi, "Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes," *IET Inf. Secur.*, vol. 7, no. 3, pp. 212–220, Sep. 2013.
- [14] I. B. Djordjevic, L. Xu, T. Wang, and M. Cvijetic, "Large girth low-density parity-check codes for long-haul high-speed optical communications," in *Proc. OFC/NFOEC*, San Diego, CA, USA, 2008, Paper JWA53, pp. 1–3.
- [15] X. Sun, D. Zou, Z. Qu, and I. B. Djordjevic, "Run-time reconfigurable adaptive LDPC coding for optical channels," *Opt. Express*, vol. 26, no. 22, pp. 29319–29329, Oct. 29, 2018.
- [16] X. Sun and I. B. Djordjevic, "FPGA implementation of rate-adaptive spatially-coupled LDPC codes suitable for optical communications," *Opt. Express*, vol. 27, no. 3, pp. 3422–3428, Feb. 4, 2019.
- [17] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Phys. Rev. X*, vol. 8, no. 3, Aug. 2018, Art. no. 031043.
- [18] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503.
- [19] Y. Tamura, H. Sakuma, K. Morita, M. Suzuki, Y. Yamamoto, K. Shimada, Y. Honma, K. Sohma, T. Fujii, and T. Hasegawa, "The first 0.14-dB/km loss optical fiber and its impact on submarine transmission," *J. Lightw. Technol.*, vol. 36, no. 1, pp. 44–49, Jan. 1, 2018.
- [20] Z. Qu and I. B. Djordjevic, "Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels," *IEEE Photon. J.*, vol. 9, no. 6, Dec. 2017, Art. no. 7600408.
- [21] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, and S. Guha, "Secret-key distillation across a quantum wiretap channel under restricted eavesdropping," *Phys. Rev. A, Gen. Phys.*, vol. 14, no. 2, Aug. 2020, Art. no. 024044.



IVAN B. DJORDJEVIC (Fellow, IEEE) received the Ph.D. degree from the University of Nis, Yugoslavia, in 1999.

He is a Professor of electrical and computer engineering and optical sciences with The University of Arizona, the Director of the Optical Communications Systems Laboratory (OCSL) and the Quantum Communications (QuCom) Laboratory, and the Co-Director of the Signal Processing and Coding Laboratory. Prior to joining The University

of Arizona, he held appointments at the University of Bristol, the University of the West of England, U.K., Tyco Telecommunications, USA, the National Technical University of Athens, Greece, and State Telecommunication Company, Yugoslavia. He has authored or coauthored eight books, and more than 530 journal and conference publications, and holds 53 U.S. patents.

Dr. Djordjevic is an OSA Fellow. He serves as an Area Editor/Associate Editor/member of the Editorial Board for the following journals such as the IEEE COMMUNICATIONS LETTERS, the OSA/IEEE JOURNAL OF OPTICAL COMMUNICATIONS AND NETWORKING, the *Journal of Optics* (IOP), *Physical Communication* journal (Elsevier), *Optical and Quantum Electronics*, and *Frequenz*.

• • •