QKD-enhanced Cybersecurity Protocols

Ivan B. Djordjevic, *Fellow, IEEE*

University of Arizona, Department of Electrical and Computer Engineering, 1230 E. Speedway Blvd., Tucson, AZ 85721, USA

Manuscript received February 17, 2021. This paper was supported in part by L3Harris Technologies Inc. and NSF.

Abstract: Security of QKD is guaranteed by the quantum mechanics laws rather than unproven assumptions employed in computational cryptography. Unfortunately, the secret-key rates are way too low and transmission distances are limited. The post-quantum cryptography (PQC) is proposed as an alternative to QKD. However, the PQC protocols are based on conjecture that there are no polynomial time algorithms to break the PQC protocols. To overcome key challenges of both post-quantum cryptography and QKD, we propose to use the QKD only in initialization stage to set-up corresponding cybersecurity protocols. The proposed concept is applied to both computational security and PQC protocols. The proposed QKD-enhanced cybersecurity protocols are tolerant to attacks initiated by quantum computers.

Index Terms: Physical-layer security, Quantum key distribution (QKD), Post-quantum cryptography, Information theoretic security, Computational security.

1. Introduction

The secure quantum communication (QuCom), also known as quantum key distribution (QKD), employs fundamental physics to guarantee security [1]-[5] rather than the unproven mathematical assumptions for computational security. While the first satellite-to-ground QKD demonstration [4] has given momentum to QuCom research, there remain several barriers to widespread applications. As an example, channel loss limits both the single-wavelength secret-key rate (SKR)/single-mode and achievable distance in a rate-loss tradeoff. To overcome such barriers, recently following two approaches have become popular: (i) the development of quantum relays [6] and (ii) the introduction of the trusted relays concept [7]. Unfortunately, the quantum relays require quantum memories of long-duration and high-fidelity entanglement, which are not commercially available. On the other hand, in practical applications it is difficult to verify the trust for the relay between any two nodes in an optical network. QKD can indeed be used to build the future secure networks. Unfortunately, the SKRs for current discrete variable (DV) QKD systems are very low so that the corresponding quantum key "pool" storing the secret and secure keys will often be empty, thus hampering the operation of these networks. Continuous variable (CV)-QKD systems do not exhibit the dead time problem and can be used to improve the SKRs, however as shown in [5], the achievable distance of CV-QKD schemes are significantly shorter compared to twin-field (TF) DV-QKD schemes [15]-[17]. As an illustration, the authors in [18] employed the multicore fiber with 37 cores to achieve the SKR of 105.7 Mb/s, but transmitted distance was only 7.9 km.

Post-quantum cryptography (PQC) is an advocated alternative to QKD [8]-[11]. Yet, similar to computational security, there is no evidence that PQC algorithms are unbreachable by sophisticated quantum algorithms. As an illustration, the lattice cryptography algorithms relay on conjecture that there is no polynomial time algorithm approximating lattice problems within polynomial factors [12]. Moreover, very often lattice cryptography is based on the collision resistance hash functions, such as: $\boldsymbol{u}=\mathbf{Ax}$, with $\boldsymbol{x}$ the Alice private vector, $\boldsymbol{u}$ the Alice public vector, and $\boldsymbol{A}$ the $m \times n$ public matrix describing the lattice, with columns the basis vectors of the lattice. Eve needs to perform an efficient quantum matrix inversion algorithm, similar to the Harrow-Hassidim-Lloyd (HHL) algorithm [13], to determine Alice's private vector by $\boldsymbol{u}=\boldsymbol{A}^{-1}\boldsymbol{x}$ and thus break the PQC protocol. The HHL algorithm is an exponential speedup over classical algorithms. To overcome the main problems of both QKD and PQC protocols, an option is to use joint QKD-PQC protocols [14]; however, even though the transmission distance of the phase-matching (PM)-TF-QKD protocol [16] can be doubled, the secret-key rate is orders of magnitude lower compared to data rates used in the state-of-the-art optical communication systems.

In this paper we propose to use a new strategy to overcome the above problems for QKD and PQC. Given the low raw key rates in QKD protocols, to get the common secure sequence we propose to use the traditional QKD schemes only in the initialization stage of the proposed protocols. Contrary to conventional QKD schemes, our common secure sequence will not be a symmetric key, but instead initialize the proposed cryptosystems. The key idea is to use the common secure sequence from QKD not as a secure key, but rather for: (i) a secure sequence of public keys; (ii) seeds for corresponding random "hash function" generators by Alice and Bob; (iii) parameters to initialize the protocols; *etc*. These secure sequences will be much shorter that the key length for one-time-pad encryption, hence the SKR of the corresponding QKD protocol is not a major concern. Even though we propose to use the QKD only for the initialization stage of our protocols, the limited distance of QKD is still a problem. To solve for this problem we discuss different strategies of using: (i) hybrid QKD-PQC concept, (ii) LEO satellites-based concept, (iii) restricted eavesdropping concept, and (iv) quantum error correction based repeaters. Given that in the proposed QKD-enhanced cybersecurity protocols, the low SKR of QKD subsystem used for initialization is not of major concern we do not perform the finite key analysis. Namely, the finite key length reduces the corresponding SKR, which is relevant for QKD only schemes.

The paper is organized as follows. In Sec. 2, we describe the proposed QKD-enhanced computational security protocols. In Sec. 3, we describe the how to modify PQC protocols to make them tolerant to any future quantum computer-initiated attack. Even though that QKD is used only in initialization stage so that low SKR is not of concern anymore, the limited distance is still an issue. In Sec. 4, we describe how to extend the transmission distance between network nodes employing QKD to initialize the cybersecurity protocols. Section 5 is devoted to concluding remarks.

2. QKD-enhanced Computational Security Protocols

The proposed concept is applicable to any computational security protocol, here we describe how to modify public key distribution, RSA, and secure regenerated keying (SRK) protocols to make them tolerant to quantum computers'-based attacks. We first describe the *quantum-enhanced public key* distribution. To initialize protocol, Alice and Bob run QKD to get a common sequence of large integers $\{g\}$ and common sequence of large prime numbers $\{n\}$ as well as the common seeds. In operational phase, Alice and Bob use the common seeds to randomly select the base g and prime number n, which are used only once and destroyed. Alice randomly selects a large integer x, calculates $X=g^{x}$ mod n, and sends X to Bob. Bob randomly selects a large integer y, calculates $Y=g^{y}$ mod n, and sends Y to Alice. Alice calculates the key K_A by: $K_A=Y^x$ mod n= g^{xy} mod n. Bob calculates the key K_B by: $K_B=X^y$ mod n= g^{xy} mod n. Clearly, both keys are identical, $K_A=K_B$. Since Alice and Bob use a randomly selected pair $\{g, n\}$ just for only one key Eve would need to use a brute force approach to break the protocol.

The original Rivest-Shamir-Adleman (RSA) encryption protocol is illustrated in Fig. 1(left). Bob randomly selects two primes p and q to get $N=pq$. He also selects e, which does not have a common divisor with $(p–1)(q–1)$, as a public key. He further calculates d as the inverse of e mod $(p–1)(q–1)$ and uses it as a private key. He further provides publicly $\{e, N\}$ to Alice. To send the message m to Bob Alice encrypts by m^e mod $N=c$ and send c to Bob. Bob decrypts the message as follows: c^d mod $N=m$. To break the protocol Eve needs to determine first the period r of the function $f(x)=m^x$ mod $N=f(x+r)$ $(r=0,1,\ldots,2^n–1)$. The period of function $f(x)$ can be found in one of the steps of the Shor's factorization algorithm, which requires $O(n^3)$ elementary operations $(2^n>N^2)$. Once the period r is determined, Eve is able to determine Bob's private key by calculating $d'=e^{-1}\bmod r$ and break the RSA protocol by determining the transmitted message m as follows:

$$c^{d'}\bmod N=\left(m^e\right)^{d'}\bmod N=m^{ed'}\bmod N\overset{ed'=1+kr,\ \exists k}{\overbrace{=}} m^{1+kr}\bmod=m\,\underbrace{m^{kr}}_{1\bmod n}\bmod N=m\bmod N, \qquad (1)$$

where we used that $ed'=1+kr\ \bmod N,\ \exists\ k$ and $m^{kr}=1\ \bmod N$.

We have to modify RSA protocol as shown in Fig. 1(right) so that it cannot be broken in polynomial time by a quantum computer. We propose to initialize the modified RSA protocol by running the QKD protocol to get a sequence of common primes $\{p\}$ and common primes $\{q\}$ as well as the common seeds. After initialization, Alice and Bob will use the common seed to randomly select p and q to get $N=pq$. This N will be used only once and be immediately destroyed. By using a different N for every new key, Eve cannot determine N by analyzing the cyphertext and needs to apply the brute force approach.

For the QKD-enhanced SRK protocol, the conventional SRK requires three types of IDs: (i) group (prime p and a quadratic residue mod p, denoted by g); (ii) personal; and (iii) partnership. These eliminate the need to store and transmit/expose vulnerable crypto information (encryption keys, passwords, etc.). The SRK employs the best available random number generator (in software or hardware) to create a truly random key, which then encrypts data and is immediately destroyed so that keys are never stored or transmitted. When the recipient processes the encrypted data, the SRK process recreates (regenerates) the original encryption key to decrypt the data. SRK also has the unique ability to encrypt data one time even for a large number of recipients. This approach requires the group IDs to be pre-installed, which might be impossible when end users are geographically separated. In the initialization stage, in SRK the participants exchange partnership IDs from the Diffie-Helman approach, e.g., $A = g^a \bmod p$ and $B = g^b \bmod p$. We propose to modify the SRK by exchanging all the parameters needed for the installation and initialization stages with the help of QKD. We describe this *modified SRK protocol* as follows. Device A uses a random number generator to create a new key, which encrypts the data sequence. The key, device A's personal ID, and device B's partnership ID produce a set of reference numbers by using secure bits from QKD, which are used for authentication purposes. To regenerate the decryption key, the receiver uses the reference numbers, device B's personal ID, and device A's partnership ID. By hiding relevant protocol parameters with the help of QKD, Eve will be unable to break the protocol even with a quantum computer.

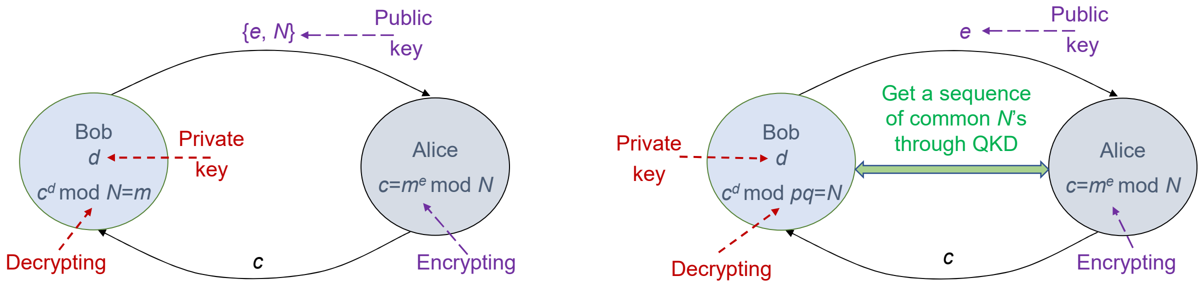


Fig. 1 Illustrating original and modified RSA: (left) original RSA protocol and (right) modified RSA protocol.

3. QKD-enhanced PQC Protocols

In this section we describe how to modify the PQC protocols so that they cannot be broken by any future advanced quantum computer-based attack. The popular PQC schemes include [9]: the code-based cryptography, lattice-based cryptography, hash-based cryptography, and multivariate cryptography. Here we concentrate on lattice-based cryptography. The lattice is generated by n linearly independent vectors $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n\in\mathcal{R}^m$ ($\mathcal{R}$-the set of real numbers) as follows: $\mathcal{L}(\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n)=\{x_i\boldsymbol{b}_i|\ x_i\in\mathcal{Z}\ \}$ ($\mathcal{Z}$-the set of complex numbers). By writing the basis vectors as columns we get the $m\times n$ matrix $\boldsymbol{A}$. In learning with errors (LWE)-based cryptography, we chose the elements of the basis vectors to be randomly selected from $\mathcal{Z}_q^n$, where $\mathcal{Z}_q$ is the set of integers per mod q. The matrix $\boldsymbol{A}$ and parameter q are made public. A simple LWE-based protocol can be described as follows. The Alice private vector $\boldsymbol{x}$ is related to the public vector $\boldsymbol{u}$ by $\boldsymbol{u}=\boldsymbol{Ax}$. Bob generates the private vector $\boldsymbol{s}$ and the error vector $\boldsymbol{e}$ and use them to generate the public vector $\boldsymbol{p}_1$ and scalar p_2 as follows: $\boldsymbol{p}_1=\boldsymbol{As}+\boldsymbol{e}$, $p_2=\boldsymbol{su}+e+bq/2$, where $b\in\{0,1\}$ is the bit to be encrypted. The error components e_i ($i=1,\ldots m$) and e are chosen randomly but need to be $<<q/4$. Alice decrypts by employing her private vector $\boldsymbol{x}$ as follows: $r=p_2-\boldsymbol{p}_1\boldsymbol{x}=e-\boldsymbol{ex}+bq/2$. Given that $e-\boldsymbol{ex}$ is small integer, when the result r is larger than $q/2$ Alice knows that transmitted bit was 1, otherwise the transmitted bit was 0. Clearly, to break this protocol Eve needs an efficient quantum matrix inversion to determine the Alice private vector by $\boldsymbol{x}=\boldsymbol{A}^{-1}\boldsymbol{u}$, similar to the HHL algorithm [13]. There exist more advanced versions of LWE-based cryptography protocols, but they can be broken in a similar fashion. To solve for this problem we propose to exchange the set of seeds to be used by Alice and Bob to generate the matrix $\boldsymbol{A}$ and the parameter q with the help of QKD. Now Alice and Bob generate the matrix $\boldsymbol{A}$ and q for every new key, by first randomly selecting the seed from the set of seeds exchanged by QKD and use it to generate $\boldsymbol{A}$ and q. Since such generated $\boldsymbol{A}$ and q are used only once Eve will not be able to break the protocol even with the most advanced quantum computer to be developed in future. The similar concept is applicable to other PQC protocols.

In both QKD-enhanced computational security and PQC protocols, the SKR used in corresponding QKD protocol does not need to be high since the QKD is used only to initialize the proposed protocols. However, the distance could represent the limitation, which is addressed in next section.

4. Improving the Distance for QKD-enhanced Protocols

Even though we propose to use QKD only for the initialization stage of our protocols, the limited distance of QKD is still a problem. In a standard QKD protocol, parity bits are transmitted over an authenticated noiseless channel to which Eve has access. By transmitting raw key over TF-QKD subsystem and parity bits over the PQC subsystem, we can significantly extend the achievable distance of TF-QKD as shown in [14].

When the ultra-low-loss fiber is used the transmission medium, the distance of 1238 km was reported in [14]. Let us now consider the free-space optical (FSO) link affected by the atmospheric turbulence. Based on theory described in [14] in Fig. 2 we report normalized SKRs vs. transmission distance, for horizontal path (the worst-case scenario), obtained by simulations, for different refractive structure parameters C_n^2 [5]. Clearly, the joint PM-TF-QKD-PQC is more tolerant to turbulence effects compared to PM-TF-QKD only [16]. For target normalized SKR of 0.004 the maximum distance for PM-TF-QKD is 35 km, while the corresponding distance of the joint scheme is 80 km. To extend transmission distance further, we can use the adaptive optics approaches [5].

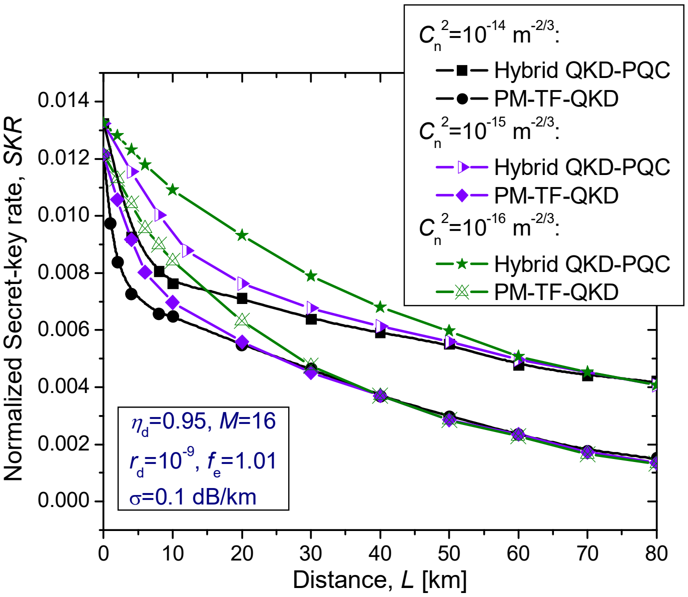


Fig. 2 Normalized SKR vs. distance (in the presence of turbulence) for joint PM-TF-QKD-PQC used in initialization stage of proposed QKD-enhanced protocols. The simulation parameters have been set as follows: single-photon detection efficiency of η_d=0.95, the dark count rate r_d of 10^{-9}, the error correction inefficiency to f_e=1.01, attenuation coefficient due to scattering effects σ=0.1 dB/km, and number of slices for PM-TF-QKD is M=16.

By placing the location of Charlie on LEO satellite distance between two quantum nodes can be significantly extended (see [19] for more details). This approach is applicable to both DV-QKD and CV-QKD schemes as demonstrated in [20]. Another approach would be to apply the limited eavesdropping concept, in which Eve is restricted in her information collection capabilities, allowing to significantly extend the transmission distance [21],[22].

The final approach would be to use the quantum error correction-based repeaters, with different strategies being summarized in [23]. In particular, the surface codes [24],[25] seem to be suitable for this application, given their simplicity. For completeness of presentation, we briefly describe an illustrative surface code, provided in Fig. 3.

The surface code is defined on a 2-D lattice with information (data) qubits denoted by solid circles. There are two types of stabilizers (quantum parity-check equations): (i) stabilizers containing all *Z* Pauli operators, denoted by white plaquettes, and (ii) stabilizers containing all *X* Pauli operators, denoted by shaded plaquettes. To illustrate, the plaquette stabilizer related to qubits 1 and 2 will be X_1X_2. On the other hand, the plaquette stabilizer related to qubits 1, 2, 4, and 5 will be $Z_1Z_2Z_4Z_5$. The minimum distance of the surface code will be the minimum side length, that is *d*=min(2,3)=2. The codeword length is determined as the product of side lengths, that is *n*=2×3=6. There are five stabilizers *n*–*k*=5, and therefore the number of information (data) qubits will be simply *n*–(*n*–*k*)=1.

Each node in a quantum network is equipped with the surface code. In scenario considered in this paper, in each intermediate node we perform simple syndrome-based decoding to identify the most probably error and correct it, with details being provided in ref. [25], and transmit the corrected codeword towards the next stage.

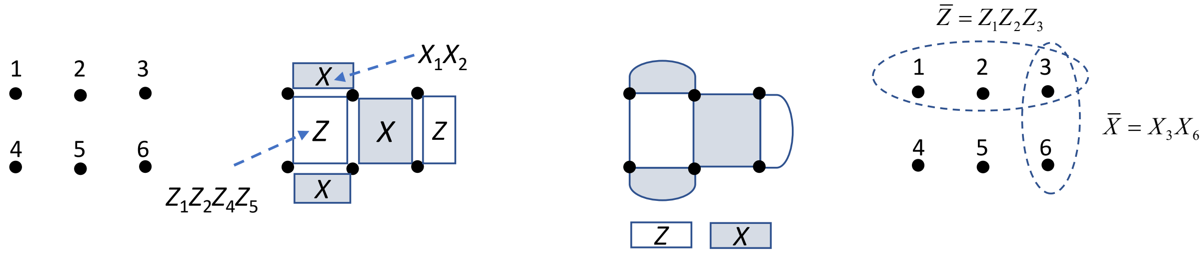
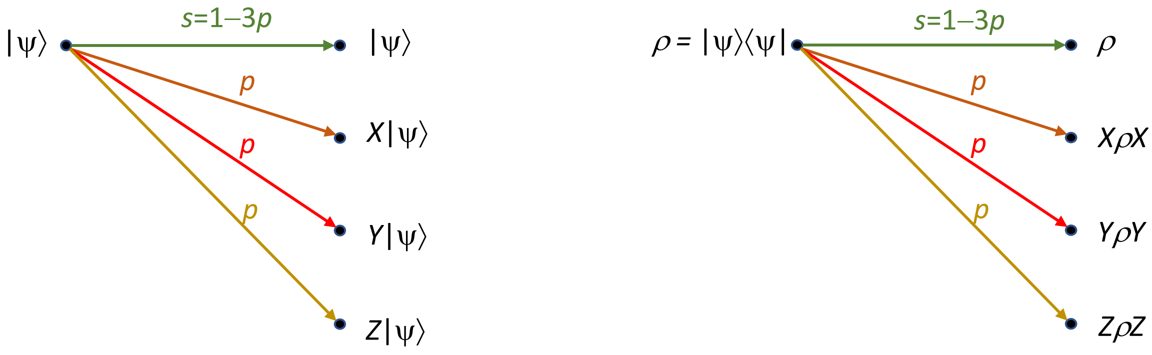


Fig. 3 Illustrating the surface code concept. The minimum distance of this code is *d*=min(2,3)=2 and the codeword length is *n*=2·3=6. The number of stabilizers (plaquettes) is *n*–*k*=5. Finally, the number of data (information) qubits is simply *n*–(*n*–*k*)=1.

Although the channel loss dominates the performance of quantum repeaters, given that quantum gates are imperfect there will be quantum errors associated with each stage, and we can use the depolarizing quantum channel model provided in Fig. 4, where *X*, Y, and *Z* quantum errors occurring with the same probability *p*, to represent errors introduced by both channel and imperfect gates. The corresponding Kraus representation is given by:

$$\rho_f = \xi(\rho) = (1-3p)\rho + pX\rho X + pY\rho Y + pZ\rho Z. \tag{2}$$



(a) (b)

Fig. 4 The depolarizing quantum channel model: (a) Pauli operator description and (b) density operator description.

For simplicity we consider simple BB84 protocol [5]. The normalized secret-key rate, *SKR*, after the *N* stages can be estimated by:

$$SKR = \left\{\left[1-P(E)\right]T\right\}^N \max\left(1 - f_e h(e_N^{(X)}) - h(e_N^{(Z)}), 0\right), \tag{3}$$

where we use f_e to denote the (in)efficiency of error correction ($f_e \geq 1$), $e_N^{(X)}$ $\left[e_N^{(Z)}\right]$ is the quantum bit-error rate (QBER) in the X-basis (*Z*-basis) after *N* stages, *T* is the transmissivity of single link, and *h*(*x*) denotes the binary entropy function, defined as $h(x)=-x\log_2(x)-(1-x)\log_2(1-x)$. The first subtraction term $f_e h(e_N^{(X)})$ is related to the amount of information leaked to the Eve during the error correction (also known as information reconciliation) phase. On the other hand, the second subtraction term $h(e_N^{(Z)})$ is Eve's information acquired during the raw-key transmission phase, which is typically removed from the final key through the privacy amplification phase.

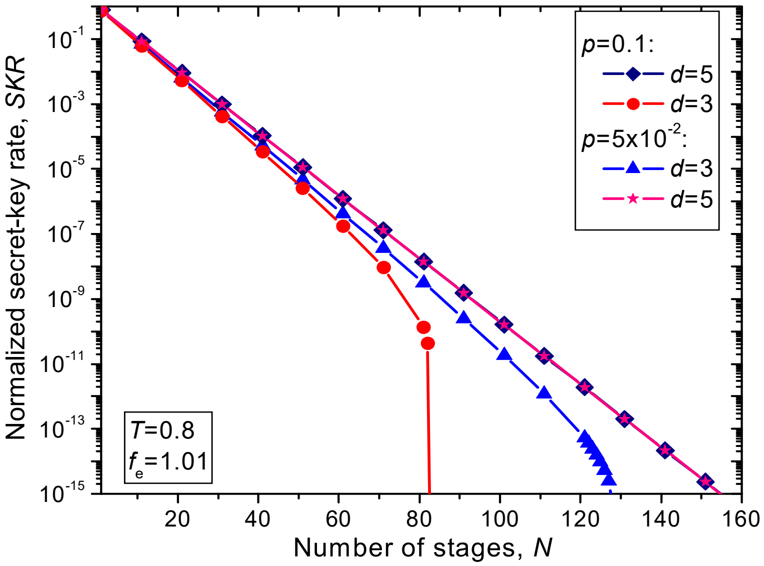


Fig. 5 Normalized SKR vs. number of stages, based on *d*×*d* surface codes, assuming that single-SMF link transmittance is *T*=0.8.

The overall QBER after *N* stages can be estimated by:

$$e_N = \frac{1-\left[1-3P(E)\right]^N}{3}, \tag{4}$$

where *P*(*E*) is the syndrome decoding error probability of each stage, and by using theory in [25] and [26], for surface code based on square lattice of side *d*, we obtain the following approximation for *P*(*E*):

$$P(E) \approx \sum_{j=0}^{d^2} 2^{k-d^2} \binom{d^2}{j} \sum_{k=0}^{\left\lfloor \frac{d^2-1}{2} \right\rfloor} \sum_{r=0}^{d^2} \binom{j}{k-r} \binom{d^2-j}{r} p^{j-k+r} (1-p)^{k-r} (1-s)^r s^{d^2-j-r}, \tag{5}$$

with $\lfloor \cdot \rfloor$ being the floor function. The multiplication term [1–*P*(*E*)]*T* in (3) is related to the single-stage success probability, while $\{[1-P(E)]T\}^N$ corresponds to the overall success probability (after *N* stages).

For depolarizing channel, for single-SMF link transmittance of *T*=0.8, in Fig. 5 we summarize normalized SKR performance assuming that BB84 protocol is used for two different *d*×*d* surface codes. The SKR is calculated by using equations (3)-(5). The total transmission distance can be estimated by $L_{\text{tot}}=NL_{\text{eff}}|\ln T|$, where L_{eff} is effective transmission distance, which for ultra-low-loss fiber described in [27] is 30.606 km. Given that in the proposed QKD-enhanced cybersecurity protocols the BB84 is to be used only in initialization stage, the low normalized SKR of 10^{-15} can be tolerated. The corresponding achievable transmission distance, for *d*=5 and *p*=0.1, will be then L_{tot}=1058.6 km. Therefore, even for short surface code and high transition probability, we can achieve the distance beyond 1000 km between any two quantum nodes.

5. Concluding Remarks

Despite appealing features of QKD, there remain fundamental and technical challenges to address prior to widespread applications. For instance, both the SKR and transmission distance for QKD are fundamentally limited by the channel loss. As an alternative to QKD, the PQC has been advocated. While PQC algorithms have been thought to be secure against attacks initiated by quantum computers, similar to computational security there is no evidence that these algorithms would be future proof against more sophisticated quantum algorithms. To overcome these key challenges for PQC and QKD, we have proposed to use QKD only in initialization stage to set-up corresponding cybersecurity protocols. We have described how to modify the computational security and PQC protocols to make them secure against any advanced quantum computer to be developed in future. Given that relevant parameters of the proposed QKD-enhanced cybersecurity protocols are hidden through the QKD used in initialization, the security of proposed schemes are comparable to that of QKD, while providing much higher secret key rates. We also have described how to extend the distance between nodes employing the QKD to initialize the proposed protocols. The proposed QKD-enhanced cybersecurity protocols will have the SKRs comparable to the data rates in the state-of-the-art optical communications.

References

[1] H.-K. Lo, X. Ma, K. Chen, “Decoy state quantum key distribution,” *Phys. Rev. Lett.*, vol. 94, p. 230504, 2005.

[2] H.-K. Lo, M. Curty, B. Qi, “Measurement-device-independent quantum key distribution,” *Physical Rev. Lett.*, vol. 108, no. 13, p. 130503, 2012.

[3] G. van Assche, *Quantum Cryptography and Secrete-Key Distillation*. Cambridge, UK: Cambridge University Press, 2006.

[4] S.-K. Liao, *et al*., “Satellite-to-ground quantum key distribution,” *Nature*, vol. 549, pp. 43–4, September 7, 2017.

[5] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution*. Cham, Switzerland: Springer Nature Switzerland AG, 2019.

[6] 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, 2001.

[7] J. Qiu, “Quantum communications leap out of the lab,” *Nature*, vol. 508, no. 7497, pp. 441−442, 2014.

[8] R. J. McEliece, “A public-key cryptosystem based on algebraic coding theory,” *DNS Progress Report*, pp. 114–116, Jet Propulsion Laboratory, CA, Pasadena, 1978.

[9] D. J. Bernstein, J. Buchmann, E. Dahmen, Berlin, Germany: *Post-Quantum Cryptography*. Springer, 2009.

[10] P. Branco, P. Mateus, C. Salema, A. Souto, “Using Low-Density Parity-Check codes to improve the McEliece cryptosystem,” *Information Sciences*, vol. 510, pp. 243-255, Feb. 2020.

[11] NIST, Post-quantum cryptography PQC, available at: https://csrc.nist.gov/projects/post-quantum-cryptography

[12] D. Micciancio O. Regev, “Lattice-based Cryptography,” in D.J. Bernstein, J. Buchmann, E. Dahmen (eds) *Post-Quantum Cryptography*, Springer, Berlin, Heidelberg, 2009.

[13] A. W. Harrow, A. Hassidim, S. Lloyd, “Quantum algorithm for solving linear systems of equations,” *Phys. Rev. Lett.*, vol. 103, p. 150502, 2009.

[14] I. B. Djordjevic, “Joint QKD-Post-Quantum Cryptosystems,” *IEEE Access*, vol. 8, pp. 154708−154712, 2020.

[15] M. Lucamarini, Z. L. Yuan, J. F. Dynes, A. J. Shields, “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” *Nature*, vol. 557, pp. 400–403, 2018.

[16] X. Ma, P. Zeng, H. Zhou, “Phase-matching quantum key distribution,” *Phys. Rev. X*, vol. 8, p. 031043, 2018.

[17] X.-T. Fang, P. Zeng, H. Liu, et al., “Implementation of quantum key distribution surpassing the linear rate-transmittance bound,” *Nat. Photonics*, vol. 14, pp. 422–425, 2020.

[18] D. Bacco, B. Da Lio, D. Cozzolino, *et al*., “Boosting the secret key rate in a shared quantum and classical fibre communication system,” *Commun. Phys.*, vol. 2, p. 140, 2019.

[19] I. B. Djordjevic, “On Global Quantum Communication Networking,” *Entropy*, vol. 22, no. 8, p. 831, 2020.

[20] T.-L. Wang, I. B. Djordjevic, J. Nagel, “Laser Beam Propagation Effects on Secure Key Rates for Satellite-to-Ground Discrete Modulation CV-QKD,” *Applied Optics*, vol. 58, no. 29, pp. 8061-8068, Oct. 2019.

[21] Z. Pan, *et al*., “Secret-key distillation across a quantum wiretap channel under restricted eavesdropping,” *Phys. Rev. Ap.*, vol. 14, p. 024044, 2020.

[22] Z. Pan, I. B. Djordjevic, “Secret key distillation over satellite-to-satellite free-space optics channel with a limited-sized aperture eavesdropper in the same plane of the legitimate receiver,” *Optics Express*, vol. 28, no. 25, pp. 37129-37148, 2020.

[23] R. V. Meter, *Quantum Networking*. London-Hoboken: ISTE Ltd. & John Wiley & Sons, Inc., 2014.

[24] A. Y. Kitaev, “Fault-tolerant quantum computation by anyons,” *Annals of Physics*, vol. 303, no. 1, pp. 2-30, 2003

[25] I. B. Djordjevic, *Quantum Information Processing, Quantum Computing, and Quantum Error Correction, 2nd Edition*. Elsevier/Academic Press, Feb. 2021.

[26] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*. Englewood Cliffs, NJ: Prentice Hall, 1995.

[27] Y. Tamura, *et al.*, “The First 0.14-dB/km loss optical fiber and its impact on submarine transmission,” *J. Lightw. Technol.*, vol. 36, pp. 44-49, 2018.