entropy

Editorial

Physical-Layer Security, Quantum Key Distribution, and Post-Quantum Cryptography

Ivan B. Djordjevic

Department of Electrical and Computer Engineering, University of Arizona, 1230 E. Speedway Blvd., Tucson, AZ 85721, USA; ivan@email.arizona.edu; Tel.: +1-520-626-5119

Keywords: quantum information processing; physical-layer security; quantum key distribution (QKD), post-quantum cryptography, secure computation

Citation: Djordjevic, I.B. Physical-Layer Security, Quantum Key Distribution, and Post-Quantum Cryptography. *Entropy* **2022**, *24*, xyz. https://doi.org/…

Academic Editor: Ivan B. Djordjevic

Received: 27 June 2022
Accepted:
Published:

The growth of data driven technologies, 5G, and Internet pose enormous pressure on underlying information infrastructure. There exist numerous proposals on how to deal with the possible capacity crunch [1]. However, the security of both optical and wireless networks lags behind reliable and spectrally efficient transmission [2]. Significant achievements have been made recently in the quantum computing [3] and quantum communication [4, 5] arenas. Because most conventional cryptography systems rely on computational security, which guarantees the security against an efficient eavesdropper for a limited time, with the advancement in quantum computing this security can be compromised. To solve for these problems various schemes providing the perfect/unconditional security have been proposed including physical-layer security (PLS), quantum key distribution (QKD), and post-quantum cryptography. Unfortunately, it is still not clear how to integrate those different proposals with higher level cryptography schemes. So the purpose of this Special Issue was to integrate these various approaches and enable the next generation of cryptography systems whose security cannot be broken by the quantum computers.

The topics addressed in this Special Issue included: physical-layer security [2], quantum key distribution (QKD) [2], post-quantum cryptography [6], quantum enhanced cryptography [7], stealth communication [2], and covert communication [8]. There have been 14 papers published in this special issue, distributed as follows: one review paper, one perspective paper, and 12 articles.

In the review paper [9] authors apply the restricted Eve's concept to the satellite-to-satellite secret key distillation. In conventional QKD, it is assumed that Eve is the omnipotent, limited only by the laws of physics. This represents an unreasonable assumption for certain applications, where the presence of Eve is easy to detect such as free-space optical communications, in particular satellite-to-satellite communications. By introducing geometrical optics restricted model authors have shown that secret-key rate (SKR) can be significantly improved compared to the conventional QKD. Authors analyze SKRs from Bob's perspective through the exclusion zone approach and from Eve's perspective through dynamic positioning of the receiver aperture.

In the perspective paper [10], author discusses how to build a global quantum communication network (QCN) by interconnecting the disconnected terrestrial QCNs through LEO satellite QCN, based on the cluster state concept. This heterogenous global QCN will provide unprecedented security for future 5G+/6G wireless networks, Internet of Things (IoT), optical networks, and autonomous vehicles.

In the first article paper [11], authors discuss the underwater QKD. Authors apply measurement-device-independent (MDI) QKD with the zero-photon catalysis (ZPC) performed at the emitter of one side to improve the SKR and extend the transmission distance. Numerical results indicate that the proposed ZPC-based scheme outperforms the corresponding single photon subtraction-based scheme in the extreme asymmetric case.

In the second article paper [12], author describes how to build the multipartite QCN based on surface code (SC) concept. The key idea is to simultaneously entangle multiple nodes in an arbitrary topology based on SC approach. Author also describes how to extend the transmission distance between nodes to beyond 1000km using SCs.

In the third article paper [13], authors introduce an open-destination MDI QKD network that provides the security against untrusted relays and all detector side-channel attacks, in which all user users are capable of distributing keys with the help of other users.

In the fourth article paper [14], authors introduce a QKD protocol employing the mean multi-kings' problem in which a sender shares with receivers a bit sequence as a secret key. Authors study the relation between eavesdropper's information gain and disturbance introduced into legitimate users' information, which is for BB84 protocol known as the information disturbance theorem. Authors show that Eve's extracting information disturbs the quantum states and increases the error probability, as expected.

In the fifth article paper [15], authors introduce a QKD post-processing method raising cubically the SKR in the number of double matching detection events. In the proposed protocol, contrary to the conventional QKD protocols, the secret bits rely in the Bob's measurement basis selection rather than Alice's transmitted bits. Further, the proposed protocol combines the sifting, reconciliation, and amplification into a unique process, and as such requires a single round iteration with no redundancy bits being sent.

In the sixth article [16], authors study a recent proposal for quantum identity authentication from Zawadzki [17] and formally prove that the corresponding protocol is insecure.

In the seventh article [18], authors study the phase-matching QKD (PM-QKD) protocol employing discrete phase randomization and the phase post-compensation to improve the SKR quadratically. Unfortunately, according to authors the discrete phase randomization opens a security loophole. Authors introduce the unambiguous state discrimination measurement and the photon-number-splitting attack against PM-QKD with imperfect phase randomization and prove the rigorous security of decoy state PM-QKD with discrete phase randomization protocol.

In the eight article [19], authors introduce a nonclassical attack on QKD system and propose the corresponding countermeasure method. The proposed attack is based on the sync pulses attenuated to a photon level to determine the signaling interval. To solve for this attack authors propose to use of variable power synchronizing pulses at varying lengths, combined with the controlled signal attenuation.

In the nineth article paper [20], an entanglement-based QKD protocol is proposed that employs a modified symmetric version of the Bernstein-Vazirani algorithm to achieve secure and efficient key distribution, with two variants, fully symmetric and semi-symmetric, being presented.

In the 10th article paper [21], related to the physical-layer security, authors study the impact of injection and jamming attacks during the advantage distillation in a MIMO wireless system and show that the man-in-the-middle attack can be mounted as long as the attacker has one extra antenna with respect to the legitimate users. To solve for this problem authors propose to reduce the injection attack by using a particularly designed pilot randomization technique. Then by employing a game-theoretic approach authors evaluate the optimal strategies available to the legitimate users in the presence of reactive jammers.

In the 11th article [22], authors introduce a Bayesian probabilistic algorithm that incorporates all published information in qubit-based synchronization protocol to efficiently determine the clock offset without sacrificing any secure key. Given that the output of the algorithm is a probability, it can be used to quantify the synchronization confidence.

In the final article paper [23], related to the secure computation, authors present randomized versions of two known oblivious transfer protocols, one being quantum and the other being post-quantum with ring learning with an error assumption, and prove their security in the quantum universal composability framework, using a common reference string model.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Djordjevic, I.B. *Advanced Optical and Wireless Communications Systems, 2nd Ed.*; Springer Nature Switzerland AG: Cham, Switzerland, 2022.
2. Djordjevic, I.B. *Physical-Layer Security and Quantum Key Distribution*; Springer International Publishing AG: Cham, Switzerland; Heidelberg, Germany, 2019.

3. Djordjevic, I.B. *Quantum Information Processing, Quantum Computing, and Quantum Error Correction: An Engineering Approach*, 2nd ed.; Elsevier/Academic Press: London, UK; San Diego, CA, USA, 2021.
4. Cariolaro, G. *Quantum Communications*; Springer International Publishing AG: Cham, Switzerland; Heidelberg, Germany, 2015.
5. Djordjevic, I.B. *Quantum Communication, Quantum Networks, and Quantum Sensing*; Elsevier/Academic Press: London, UK, 2022.
6. Bernstein, D. J.; Buchmann, J.; Dahmen E. *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009.
7. Djordjevic, I. B. QKD-enhanced Cybersecurity Protocols. *IEEE Photonics Journal* **2021**, 13 (2), Article ID 7600208.
8. Bash B.A.; Goeckel D.; Towsley D. Limits of reliable communication with low probability of detection on AWGN channels. *IEEE Journal on Selected Areas in Communications* **2013**, 31, 1921-1930.
9. Pan, Z.; Djordjevic, I.B. Geometrical Optics Restricted Eavesdropping Analysis of Satellite-to-Satellite Secret Key Distillation. *Entropy* **2021**, *23*, 950.
10. Djordjevic, I.B. On Global Quantum Communication Networking. *Entropy* **2020**, *22*, 831.
11. Wang, Y.; Zou, S.; Mao, Y.; Guo, Y. Improving Underwater Continuous-Variable Measurement-Device-Independent Quantum Key Distribution via Zero-Photon Catalysis. *Entropy* **2020**, *22*, 571.
12. Djordjevic, I.B. Surface-Codes-Based Quantum Communication Networks. *Entropy* **2020**, *22*, 1059.
13. Cao, W.-F.; Zhen, Y.-Z.; Zheng, Y.-L.; Zhao, S.; Xu, F.; Li, L.; Chen, Z.-B.; Liu, N.-L.; Chen, K. Open-Destination Measurement-Device-Independent Quantum Key Distribution Network. *Entropy* **2020**, *22*, 1083.
14. Yoshida, M.; Nakayama, A.; Cheng, J. Distinguishability and Disturbance in the Quantum Key Distribution Protocol Using the Mean Multi-Kings' Problem. *Entropy* **2020**, *22*, 1275.
15. Lizama-Pérez, L.A.; López R., J.M.; Samperio, E.H. Beyond the Limits of Shannon's Information in Quantum Key Distribution. *Entropy* **2021**, *23*, 229.
16. González-Guillén, C.E.; González Vasco, M.I.; Johnson, F.; Pérez del Pozo, Á.L. An Attack on Zawadzki's Quantum Authentication Scheme. *Entropy* **2021**, *23*, 389.
17. Zawadzki, P. Quantum identity authentication without entanglement. Quantum Inf. Process. **2019**, 18, 7.
18. Zhang, X.; Wang, Y.; Jiang, M.; Lu, Y.; Li, H.; Zhou, C.; Bao, W. Phase-Matching Quantum Key Distribution with Discrete Phase Randomization. *Entropy* **2021**, *23*, 508.
19. Pljonkin, A.; Petrov, D.; Sabantina, L.; Dakhkilgova, K. Nonclassical Attack on a Quantum Key Distribution System. *Entropy* **2021**, *23*, 509.
20. Ampatzis, M.; Andronikos, T. QKD Based on Symmetric Entangled Bernstein-Vazirani. *Entropy* **2021**, *23*, 870.
21. Mitev, M.; Chorti, A.; Belmega, E.V.; Poor, H.V. Protecting Physical Layer Secret Key Generation from Active Attacks. *Entropy* **2021**, *23*, 960.
22. Cochran, R.D.; Gauthier, D.J. Qubit-Based Clock Synchronization for QKD Systems Using a Bayesian Approach. *Entropy* **2021**, *23*, 988.
23. Costa, B.; Branco, P.; Goulão, M.; Lemus, M.; Mateus, P. Randomized Oblivious Transfer for Secure Multiparty Computation in the Quantum Setting. *Entropy* **2021**, *23*, 1001.