Hindawi
Security and Communication Networks
Volume 2024, Article ID 9870653, 1 page
https://doi.org/10.1155/2024/9870653

Retraction

Retracted: Cryptanalysis and Improvements on Quantum Key Agreement Protocol Based on Quantum Search Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] H. Abulkasim, E. Alabdulkreem, F. Karim et al., "Cryptanalysis and Improvements on Quantum Key Agreement Protocol Based on Quantum Search Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 3803621, 5 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 3803621, 5 pages
https://doi.org/10.1155/2022/3803621

Research Article

Cryptanalysis and Improvements on Quantum Key Agreement Protocol Based on Quantum Search Algorithm

Hussein Abulkasim,[1] **Eatedal Alabdulkreem**,[2] **Faten Karim**,[2] **Nada Ahmed**,[2] **Mona Jamjoom**,[2] **Myriam Hadjouni**,[2] **and Safia Abbas**[2]

[1]*Faculty of Science, New Valley University, El-Kharga 72511, Egypt*
[2]*Department of Computer Sciences, College of Computer and Information Science, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia*

Correspondence should be addressed to Hussein Abulkasim; hussein@scinv.au.edu.eg

Received 27 January 2022; Revised 9 February 2022; Accepted 24 February 2022; Published 17 March 2022

Academic Editor: Irshad Azeem

Recently, Huang et al. (2021) presented a quantum key agreement schemeto securely negotiate on a secret key employing the properties of a quantumsearch algorithm. First, the authors proposed the two-party quantum key agreement, and then they extended their work to the three-party case. Huang et al.'s protocol employs the unitary operation and single-particle measurements to negotiate on a secret key without using complex quantum technologies such as quantum memory or entangled quantum particles. The authors claimed that their protocol is secure and efficient. However, this work shows that Huang et al.'s protocol has a significant pitfall, where the private key of one user could be easily leaked to the attackers. Hence, the properties of security and fairness are not achieved. Accordingly, thetwo-party and three-party of Huang et al.'s protocol have been reviewed, and an improvementto address the shortcoming is suggested.

1. Introduction

Key agreement is a security protocol that aims to generate and exchange secure key encryption among two or more distant users. Due to its greatest significance, key agreement protocols have been employed to generate encryption keys in today's IT applications such as IoT applications [1], healthcare systems [2], vehicular communications [3], smart networks [4], satellite communications [5], cloud applications [6], and others. To resist quantum attacks, several security protocols have been proposed based on the principles of quantum physics for addressing various security problems [7–26]. The pioneering quantum-based key agreement (QKA) protocol was proposed in 2004 [27]. Subsequently, several QKA protocols have been introduced [11, 12, 16, 22]. Generally, there are different types of quantum key agreement protocols in terms of QKA's structure and efficiency [28]: (1) the tree-QKA protocols, in which each user sends their private data to all other users via a quantum channel; (2) the complete-graph-QKA protocol, in which each user sends his encoded private data as a sequence of particles to each user participated in the protocol; and (3) the circle-QKA protocol, which is the most adopted type, in which each user pra sequence of particles representing his private key and sends it to the next user in a circle to encode his private data until it is returned to the sender (the first user). The circle-QKA protocol is more efficient than the other QKA types and is better at achieving the characteristic of fairness. In contrast, the complete-graph-QKA is more secure than the other QKA types. Thus, designing a secure and efficient QKA protocol has become a challenging task and got more and more attention.

Recently, Huang et al. [29] presented a new QKA scheme based on Grover's algorithm []. Theirprotocol enables authorized users to negotiate on a shared secure key, and noneof the authorized users can fully get the final agreement key alone. Grover's search algorithm is used for accelerating the search process for the marked items. Their proposed protocol is feasible and does not use quantum memory or complex quantum devices. However, the Huang-QKA protocol cannot maintain the property of fairness since the level of security of the key agreement of users is not equal. A quick review of the Huang-QKA scheme is shown in Section 2. The security analysis of the Huang-QKA protocol and the suggested improvementsare presented in Section 3 and Section 4, respectively. The security analysis based on the modified steps is presented in Section 5. Section 6 concludes this work.

2. Review of Huang-QKA Protocol

Huang-QKA protocol employed the Grover quantum search algorithm (QSA) [30] to agree on a two-user QKA protocol. Basically, the Grover QSA is one of the most significant quantum computing algorithms which can be used to search for marked items in an unsorted database faster than all known classical search algorithms. For more clarification, assume that we we are searching for a target $\omega\omega \in \{00, 01, 10, 11\}$ in a two-qubit Grover QSA, and the targeted database is a two-qubit quantum system $|s = | + + = (|00, |01, |10, |11)/2$. Two unitary operations (U_ω, U_s) can be used to evolve the quantum system $|s$. The measurement $Z - \text{basis} = \{|0, |1\}$ can be used to measure $|s$. Wecan describe the two unitary operations as follows:

$$\begin{aligned} U_\omega &= (I - 2|\omega\omega|), \\ U_s &= (2|ss| - I), \end{aligned} \tag{1}$$

where I is identity operation, $\omega \in \{00, 01, 10, 11\}$, and the quantum system $s \in \{|{++}, |{+-}, |{-+}, |{--}\}$.

$|s_\omega$ can be defined as follows:

$$|s_\omega = \begin{cases} ++, & \text{where } \omega = 00, \\ -+, & \text{where } \omega = 01, \\ +-, & \text{where } \omega = 10, \\ ++, & \text{where } \omega = 11. \end{cases} \tag{2}$$

Two common properties of Grover QSA van be stated as follows.

Property 1 (see [31]). For $i = 1, 2, 3, 4$, let $\omega_i \in \{00, 01, 10, 11\}$. If we have $\omega_1 \oplus \omega_2 \oplus \omega_3 = \omega_4$, then we can say that $U_{\omega 1} U_{\omega 2} U_{\omega 2} |s_{11}\rangle = \pm U_{\omega 4} |s_{11}\rangle$.

Property 2 (see [32]). Assume that we have $v, \omega_1, \omega_2 \in \{00, 01, 10, 11\}$, and $\omega_1 \oplus v = \omega_2$. Then, we can say that $U_{s_{11}} U_{\omega 1} |s_v\rangle = \pm \omega_2$.

2.1. The Two-Party Huang-QKA Protocol. Assume that there are two remoteusers (e.g., Alice and Bob) who want to negotiate on an agreement key ($K = K_a \oplus K_b$). Aliceand Bob agree on generating two random $2n$ bit classical secret keys K_a and K_b, respectively.

$$\begin{aligned} K_a &= \left\{K_a^1, K_a^2, \ldots, K_a^m\right\}, \\ K_b &= \left\{K_b^1, K_b^2, \ldots, K_b^m\right\}, \end{aligned} \tag{3}$$

where $K_a^1, K_b^1 \in \{00, 01, 10, 11\}$ and $i \in \{1, 2, \ldots, m\}$.

By combining the idea of two-qubit Grover's QSA with the QKA protocol, Huang-QKA protocol has been proposed. The steps of Huang-QKA protocol can be described as follows (see also Figure 1).

(1) Alice generates an ordered sequence (S_a) of the two-qubit quantum state according to her private information K_a^i, that is, if Alice's two classical bits are 00, 01, 10, or 11, Alice generates the quantum state $|{++}\rangle$, $|{+-}\rangle$, $|{-+}\rangle$, or $|{--}\rangle$, respectively. Alice also employs the decoy qubit protocol to protect the quantum channel by preparing a sequence of $2m$ decoy qubit states randomly selected from the group states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The selected decoy qubits are inserted randomly into S_a obtaining new sequence (S_a') and Alice records their positions. Subsequently, Alice sends the evolved sequence (S_a') to Bob through a quantum channel.

(2) Upon getting the evolved sequence S_a', Bob publicly announces his secret key (K_b) through an authenticated classical channel.

(3) After receiving the secret key of Bob (K_b), Alice computes the expression $K = K_a \oplus K_b$ to get the final agreement key (K).

(4) Alice publicly announces the positions of the decoy qubits in S_a' and their measurement bases to Bob. Alice and Bob start evaluating the error rate ofmeasurement. If the computed error rate exceeds a preset threshold, the users should stop the protocol and restart from the first step. Otherwise, they proceed to the last step.

(5) Bob discards the measured decoy qubits and gets the ordered sequence S_a. Based on his private key K_b^i, Bob applies the two unitary operations $U_{K_b^i}$ and $U_{S_{11}}$ to S_a getting a new quantum sequence S_a. Bob measures the new sequence (S_a) using $Z - \text{basis} = \{|0\rangle, |1\}$. The measurement result that Bob gets is the final agreement key (K).

2.2. The Three-Party Huang-QKA Protocol. Assume that there are three remote users (e.g.,Alice, Bob, Charlie) who want to negotiate on an agreement key ($K_{abc} = K_a \oplus K_b \oplus K_c$). Alice, Bob, and Charlie agree on generating three random$2n$ bit classical secret keys K_a, K_b, and K_c, respectively.

$$\begin{aligned} K_a &= \left\{K_a^1, K_a^2, \ldots, K_a^m\right\}, \\ K_b &= \left\{K_b^1, K_b^2, \ldots, K_b^m\right\}, \\ K_c &= \left\{K_c^1, K_c^2, \ldots, K_c^m\right\}, \end{aligned} \tag{4}$$

where $K_a^1, K_b^1, K_b^1 \in \{00, 01, 10, 11\}$ and $i \in \{1, 2, \ldots, m\}$.

The steps of the three-party Huang-QKA protocol are as follows:

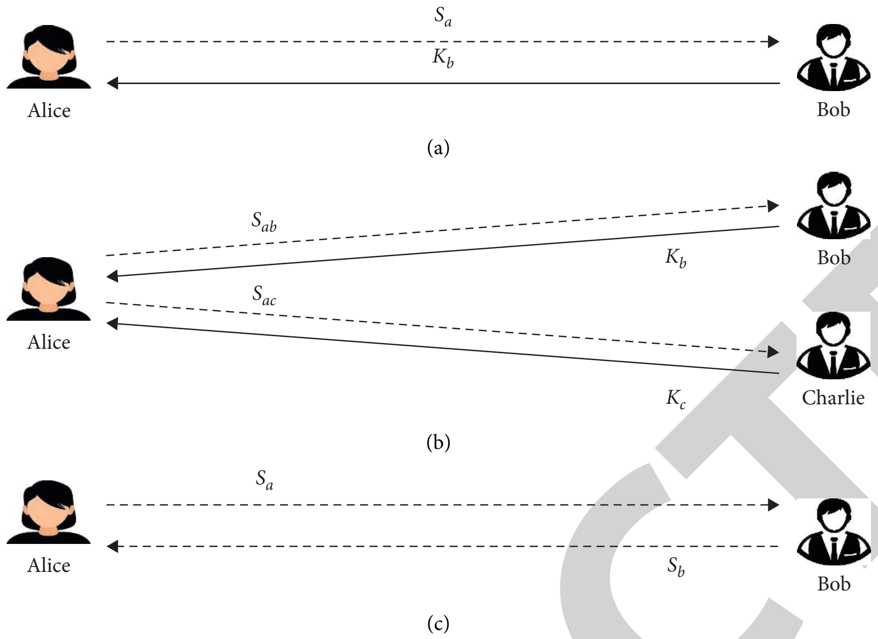

FIGURE 1: (a) represents the two-party Huang-QKA protocol; (b) represents the three-party Huang-QKA protocol; (c) represents the modified two-party Huang-QKA protocol. The dashed and solid lines represent the quantum and classical channels, respectively.

(1) Alice generates an ordered sequence (S_a) of the two-qubit quantum state according to her private information K_a^i, that is, if Alice's two classical bits are 00, 01, 10, or 11, Alice generates the quantum state $|{+}{+}\rangle$, $|{+}{-}\rangle$, $|{-}{+}\rangle$, or $|{-}{-}\rangle$, respectively. Alice also employs the decoy qubit protocol to protect the quantum channel by preparing a sequence of $4m$ decoy qubit states randomly selected from the group states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The selected decoy qubits are inserted randomly into S_{ab} and S_{ac} obtaining new sequences $S'_{ab}$and S'_{ac}. Subsequently, Alice sends the evolved sequences $S'_{ab}$and $S'_{ac}$to Bob and Charlie, respectively, through two quantum channels.

(2) Upon getting the evolved sequences $S'_{ab}(S'_{ab})$, Bob (Charlie) publicly announces his secret key $K_b\,(K_c)$ through an authenticated classical channel.

(3) After receiving the secret key of Bob (Charlie), Alice computes the expression $K_{abc} = K_a \oplus K_b \oplus K_c$ to get the final agreement key (K_{abc}).

(4) Alice publicly reveals positions of the decoy qubits in $S'_{ab}(S'_{ac})$ and their measurement bases to Bob (Charlie). Alice and Bob (Charlie) start evaluating the error rate ofmeasurement. If the computed error rate exceeds a preset threshold, the users should stop the protocol and restart from the first step. Otherwise, they proceed to the last step.

(5) Bob (Charlie) discards the measured decoy qubits and gets the ordered sequence $S_{ab}\,(S_{ac})$. Based on his private key $K_b^i\,(K_c^i)$, Bob (Charlie) applies the two unitary operations $U_{K_b^i}\,(U_{K_c^i})$ and $U_{S_{11}}$ to $S_{ab}\,(S_{ac})$ getting a new quantum sequence $S_b\,(S_c)$ Bob measures the new sequence $S_b\,(S_a)$ using $Z-\text{basis} = \{|0\rangle, |1\rangle\}$. The measurement result that Bob (Charlie) gets is the final agreement key (K_{abc}).

3. The Security Analysis of Huang-QKA Protocol

The quantum key agreement aims to agree on a secret key among two or more users fairly. There are three properties that should be guaranteed while designing a QKA protocol as follows.

Security. External eavesdroppers cannot obtain the final key or any useful information about it without being caught.

Correctness. Each legal user is guaranteed that the key agreement that it gets is correct.

Fairness. All involved users influence the final agreement key equally. One user receives her/his agreement key if and only if the other user receives their agreement key with the same level of security, power, and feasibility.

In the Huang-QKA protocol, there are two proposed protocols, the two-party QKA protocol and the extended three-party QKA protocol. Since the two proposed protocols are similar, we only here discuss the security of the two-party case of Huang-QKA protocol. In step (1), only Alice prepares a quantum sequence (S_a) based on her private key (K_a) through a quantum channel. In step (2), Bob sends his private key (K_b) though an authenticated classical channel. While in step (3), Alice can get the agreement key by computing $K_{ab} = K_a \oplus K_b$. If the used classical channel in step (2) is secure enough to share the private key of Bob, why do we not use a similar channel to share the private key of Alice? Of course, there is no need to employ quantum technology to achieve the key agreement if we do this. Also, this is against the aim of the Huang-QKA protocol. Obviously, there are shortcomings in the design of the Huang-QKA protocol, as eavesdroppers can clone the key transmitted over the classic channel if they have sufficient computing power or a quantum computer. Even if this shortcoming does not affect the security of the agreement key, at least it can lead to the leakage of Bob's private key. The attackers can easily clone the private key of Bob (K_b). Therefore, the Huang-QKA protocol cannot maintain the property of fairness based on the suggested strategy.

4. Improvement on Huang-QKA Protocol

To address the shortcoming of the Huang-QKA protocol, three steps of the Huang-QKA protocol should be modified and the remaining steps will remain unchanged as follows:

(1) Alice (Bob) generates an ordered sequence $S_a\,(S_b)$ of the two-qubit quantum state according to her private information $K_a^i\,(K_b^i)$, that is, if Alice's (Bob's) two classical bits are 00, 01, 10, or 11, Alice (Bob) generates the quantum state $|{+}{+}\rangle$, $|{+}{-}\rangle$, $|{-}{+}\rangle$, or $|{-}{-}\rangle$, respectively. Alice (Bob) also employs the decoy qubit protocol to protect the quantum channel by preparing a sequence of $2m$ decoy qubit states selected from the group states $\{\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ randomly. The selected decoy qubits are inserted into $S_a\,(S_b)$ obtaining new sequence $S_a'(S_b')$ and Alice (Bob) records their positions. Subsequently, Alice (Bob) sends the evolved sequence $S_a'(S_b')$ to Bob (Alice) through a quantum channel.

(2) Upon getting the evolved sequence $S_a'(S_b')$, Bob (Alice) publicly reveals positions of the decoy qubits in $S_a'(S_b')$ and their measurement bases to Bob (Alice). Alice and Bob start evaluating the error rate ofmeasurement. If the computed error rate exceeds a preset threshold, the users should stop the protocol and restart from the first step. Otherwise, they proceed to the last step.

(3) Bob (Alice) discards the measured decoy qubits and gets the ordered sequence $S_a\,(S_b)$. Based on his private key $K_a^i\,(K_b^i)$, Bob (Alice) applies the two unitary operations $U_{K_b^i}$ and $U_{S_{11}}$ to S_a ($U_{K_a^i}$ and $U_{S_{11}}$ to S_b) getting a new quantum sequence $S_a\,(S_b)$. Bob (Alice) measures the new sequence $S_a\,(S_b)$ using $Z - \text{basis} = \{|0\rangle, |1\rangle\}$. The measurement result that Bob (Alice) gets is the final key (K).

5. Security Analysis

In addition to the security analysis shown in the original protocol [29], this section shows how the modified steps overcome the security flaw in the Huang-QKA protocol (see Figure 1). In step (1) of the modified protocol, Alice and Bob send their private information (S_a (S_b)) through a quantum channel. Alice (Bob) uses the decoy photon protocol to check transmission security. If an eavesdropper tries to get useful information from the quantum channel, she/he must stop the traveled sequence and measure it; then, she/he must resend it to the receiver. The probability of selecting correct measurement bases is 50%, and the probability of choosing correct initial bases to regenerate the traveled photons is 50%. So, the probability of passing the security check is 50% × 50% = 25%. The probability of detecting the malicious behavior of the eavesdropper is close to one $(1 - (3/4)^{2m})$ when the decoy sequence ($2m$) is large enough. Thus, the modified protocol is secure against eavesdroppers and achieves the principle of fairness.

6. Conclusion

This work studies the security of the Huang-QKA schemeto securely negotiate on a secret key employing the properties of a quantumsearch algorithm. Their work uses the technique of decoy photons to secure thetransmission against external eavesdroppers. Besides, Grover's search algorithm is used for accelerating the search process for the marked items in an unsorted database. This work found that the Huang-QKA protocol cannot maintain the properties of security and fairness since the level of security of the key agreement of users is not equal. Finally, we suggested an improved version of the Huang-QKA protocol that achieves the properties of fairness and security.

Data Availability

All data generated or analyzed during this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R104), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

References

[1] T.-Y. Wu, T. Wang, Y.-Q. Lee, W. Zheng, S. Kumari, and S. Kumar, "Improved authenticated key agreement scheme for fog-driven IoT healthcare system," *Security and Communication Networks*, vol. 2021, Article ID 6658041, 16 pages, 2021.

[2] Y. Chen and J. Chen, "A secure three-factor-based authentication with key agreement protocol for e-Health clouds," *The Journal of Supercomputing*, vol. 77, no. 4, pp. 3359–3380, 2021.

[3] S. A. Eftekhari, M. Nikooghadam, and M. Rafighi, "Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications," *Vehicular Communications*, vol. 28, Article ID 100306, 2021.

[4] L. Deng and R. Gao, "Certificateless two-party authenticated key agreement scheme for smart grid," *Information Sciences*, vol. 543, pp. 143–156, 2021.

[5] I. Altaf, M. Arslan Akram, K. Mahmood, S. Kumari, H. Xiong, and M. Khurram Khan, "A novel authentication and key-agreement scheme for satellite communication network," *Transactions on Emerging Telecommunications Technologies*, vol. 32, Article ID e3894, 2021.

[6] I. Hayat, S. Chaudhry, and A. Irshad, "A symmetric cryptography based key agreement protocol for distributed cloud computing environment," *Researchpedia Journal of Computing*, vol. 2, pp. 117–126, 2021.

[7] A. Yin and T. Chen, "Authenticated semi-quantum secret sharing based on GHZ-type states," *International Journal of Theoretical Physics*, vol. 60, pp. 265–273, 2021.

[8] G. Gao, Y. Wang, D. Wang, and L. Ye, "Comment on 'authenticated quantum secret sharing with quantum dialogue based on bell states'," *Physica Scripta*, vol. 93, no. 2, Article ID 027002, 2018.

[9] Z. Liu and H. Chen, "Analyzing and improving the secure quantum dialogue protocol based on four-qubit cluster state," *International Journal of Theoretical Physics*, vol. 59, pp. 2120–2126, 2020.

[10] P. Zawadzki, "Quantum identity authentication without entanglement," *Quantum Information Processing*, vol. 18, no. 1, pp. 1–12, 2019.

[11] L. Wang and W. Ma, "Quantum key agreement protocols with single photon in both polarization and spatial-mode degrees of freedom," *Quantum Information Processing*, vol. 16, no. 5, p. 130, 2017.

[12] V. S. Naresh, M. M. Nasralla, S. Reddi, and I. García-Magariño, "Quantum d-hellman extended to dynamic quantum group key agreement for e-healthcare multi-agent systems in smart cities," *Sensors*, vol. 20, no. 14, p. 14, 2020.

[13] R. G. Zhou and Y. Huo, "Dynamic multiparty quantum secret sharing with a trusted party based on generalized GHZ state," *Ieee Access*, vol. 9, pp. 22986–22995, 2021.

[14] P. H. Lin, T. Hwang, and C. W. Tsai, "Efficient semi-quantum private comparison using single photons," *Quantum Information Processing*, vol. 18, pp. 1–14, 2019.

[15] S.-S. Wang, G.-B. Xu, X.-Q. Liang, and Y.-L. Wu, "Multiparty quantum key agreement with four-qubit symmetric W state," *International Journal of Theoretical Physics*, vol. 57, no. 12, pp. 3716–3726, 2018.

[16] H. Abulkasim and A. Alotaibi, "Improvement on 'multiparty quantum key agreement with four-qubit symmetric W state'," *International Journal of Theoretical Physics*, vol. 58, no. 12, pp. 4235–4240, 2019.

[17] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy, and A. Ghoneim, "Secure quantum steganography protocol for fog cloud internet of things," *IEEE access*, vol. 6, pp. 10332–10340, 2018.

[18] G.-l. Long, F.-g. Deng, C. Wang, X.-h. Li, K. Wen, and W.-y. Wang, "Quantum secure direct communication and deterministic secure quantum communication," *Frontiers of Physics in China*, vol. 2, no. 3, pp. 251–272, 2007.

[19] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," *Physical Review A*, vol. 71, Article ID 044305, 2005.

[20] J.-Y. Hu, B. Yu, M.-Y. Jing et al., "Experimental quantum secure direct communication with single photons," *Light: Science & Applications*, vol. 5, no. 9, e16144 pages, 2016.

[21] A. Elhadad, S. Abbas, H. Abulkasim, and S. Hamad, "Improving the security of multi-party quantum key agreement with five-qubit Brown states," *Computer Communications*, vol. 159, pp. 155–160, 2020.

[22] H. Abulkasim, A. Mashatan, and S. Ghose, "Secure multiparty quantum key agreement against collusive attacks," *Scientific Reports*, vol. 11, pp. 1–8, 2021.

[23] X.-Q. Cai, T.-Y. Wang, C.-Y. Wei, and F. Gao, "Cryptanalysis of multiparty quantum digital signatures," *Quantum Information Processing*, vol. 18, pp. 1–12, 2019.

[24] S. Singh, N. K. Rajput, V. K. Rathi, H. M. Pandey, A. K. Jaiswal, and P. Tiwari, "Securing blockchain transactions using quantum teleportation and quantum digital signature," *Neural Processing Letters*, pp. 1–16, 2020.

[25] C.-M. Zhang, Y. Zhu, J.-J. Chen, and Q. Wang, "Practical quantum digital signature with configurable decoy states," *Quantum Information Processing*, vol. 19, pp. 1–7, 2020.

[26] H. Abulkasim, A. Mashatan, and S. Ghose, "Security improvements for privacy-preserving quantum multiparty computation based on circular structure," *Quantum Information Processing*, vol. 21, pp. 1–12, 2022.

[27] N. Zhou, G. Zeng, and J. Xiong, "Quantum key agreement protocol," *Electronics Letters*, vol. 40, no. 18, pp. 1149-1150, 2004.

[28] B. Liu, D. Xiao, H.-Y. Jia, and R.-Z. Liu, "Collusive attacks to "circle-type" multi-party quantum key agreement protocols," *Quantum Information Processing*, vol. 15, no. 5, pp. 2113–2124, 2016.

[29] X. Huang, S.-B. Zhang, Y. Chang, C. Qiu, D.-M. Liu, and M. Hou, "Quantum key agreement protocol based on quantum search algorithm," *International Journal of Theoretical Physics*, vol. 60, no. 3, pp. 838–847, 2021.

[30] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Physical Review Letters*, vol. 79, no. 2, pp. 325–328, 1997.

[31] H.-Y. Tseng, C.-W. Tsai, and T. Hwang, "Controlled deterministic secure quantum communication based on quantum search algorithm," *International Journal of Theoretical Physics*, vol. 51, no. 8, pp. 2447–2454, 2012.

[32] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," 2020, https://arxiv.org/abs/2003.06557.