Development of a Hybrid Quantum Key Distribution Concept for Multi-User Networks

Begimbayeva Y[1], Zhaxalykov T[2]*, Makarov M[3], Ussatova O[4], Tynymbayev S[5], Temirbekova Zh[6]
KazNRTU Named after K. I. Satbayev, Almaty, Kazakhstan[1, 2, 3, 4]
Kazakh British Technical University, Almaty, Kazakhstan[1, 2, 3]
Department of Cybersecurity, Energo University, Almaty, Kazakhstan[1, 4]
Faculty Information Technology, Kazakh National University Named After Al-Farabi (KazNU), Almaty, Kazakhstan[5]
Faculty of Computer Technology and Cybersecurity, International IT University (IITU), Almaty, Kazakhstan[6]

***Abstract*—This paper investigates the increasing concerns related to the vulnerability of contemporary security solutions in the face of quantum-based attacks, which pose significant challenges to existing cryptographic methods. Most current Quantum Key Distribution (QKD) protocols are designed with a focus on point-to-point communication, limiting their application in broader network environments where multiple users need to exchange information securely. To address this limitation, a thorough analysis of twin-field-based algorithms is conducted, emphasizing their distinct characteristics and evaluating their performance in practical scenarios in Sections II, III, and IV. By synthesizing insights from these analyses, integrating cutting-edge advancements in Quantum Communication technologies, and drawing on proven methodologies from established point-to-point protocols, this study introduces a novel concept for a Hybrid Twin-Field QKD protocol in Section IV. This network-oriented approach is designed to facilitate secure communication in networks involving multiple users, offering a practical and scalable solution. The proposed protocol aims to reduce resource consumption while maintaining high-security standards, thereby making it a viable option for real-world quantum communication networks. This work contributes to the development of more resilient and efficient quantum networks capable of withstanding future quantum-based threats.**

Keywords*—Quantum key distribution; quantum communication; multi-user networks; network security; quantum-based attacks; cryptography; point-to-point protocols; resource efficiency; cryptography; information security

I. Introduction

The increasing concern regarding the physical vulnerability of fiber networks has become a significant issue, as traditional security mechanisms are increasingly bypassed by sophisticated attackers. This escalating threat underscores the necessity for the development of innovative quantum-based security solutions. Notably, the global metric for the 'Estimated Cost of Cybercrime' within the cybersecurity sector is projected to rise steadily from 2023 to 2028, with an anticipated increase of 5.7 trillion U.S. dollars, representing a 69.94% growth. By 2028, after eleven consecutive years of growth, this figure is expected to reach a new high of 13.82 trillion U.S. dollars [1], emphasizing the urgent need for advanced cybersecurity measures. Furthermore, the ongoing advancements and strategic roadmaps of technology leaders, such as IBM [2], suggest rapid developments in the computational power of quantum computers, posing significant threats to existing secure communication protocols like RSA [3] and AES [4]. The widespread reliance on these algorithms, particularly among critical businesses essential to the functioning of foundational societal ecosystems, exacerbates the risk posed by emerging quantum threats.

Recent years have seen significant progress in the field of cryptography, with researchers exploring new mathematical foundations and encryption techniques to enhance security [5] [6] [7] [8] [9] [10].

To mitigate these risks, the implementation of quantum cryptography offers a promising solution. Quantum cryptography provides secure communication channels that are resilient to both classical and quantum attacks, leveraging two fundamental principles of quantum mechanics: Quantum Entanglement, which enables the encoding and sharing of information across vast distances while monitoring for any unauthorized interference, and the No-Cloning Theorem, which ensures protection against potential eavesdroppers attempting to replicate unique quantum states. One effective method for achieving such security is through Quantum Key Distribution (QKD) protocols, which facilitate the secure generation and distribution of secret keys among communication participants.

However, the majority of existing QKD protocols are limited to point-to-point applications or are heavily reliant on specific infrastructures, leaving much of the global network infrastructure vulnerable. This paper seeks to address this challenge by proposing a novel concept for a network-oriented QKD protocol.

- Research problem: Currently available protocols are only suitable in a point-to-point scenario.
- Research questions: a) Is it possible to construct a different protocol that would be able to support network communication? b) Is it possible to make it applicable to the current network infrastructure?
- Research objectives: a) to review the related literature b) to find suitable protocols for the optic fiber-based network communication c) explain the proposed approach mathematically.

- Research significance and contribution: a novel QKD network-oriented approach applicable to the current optic fiber infrastructure.

II. Literature Review

A. Historical Origins and the Emergence of First QKDs

The early 1970s began with the initial development of Quantum Key Distribution (QKD) protocols. By 1984, the scientific community was introduced to the novel polarization-based algorithm for key distribution [11] developed by C. H. Bennett and G. Brassard, marking a significant milestone. In this work, Bennett and Brassard proposed a key distribution protocol based on the polarization property of a quantum state as well as a change of measurement bases. Although its protocol as-is can be utilized over the current infrastructure, it seriously lacks in terms of security against such attacks [12] as IRUD attacks, Beam-Splitting attacks, Denial of Service attacks, Man-In-The-Middle, IRA attacks, etc. Therefore, making it not a standalone QKD solution but a potential building block for a bigger picture.

B. Entanglement-based QKDs

This discovery was closely followed by another, in 1992, with the presentation of the first entanglement-based algorithm [13] developed by A. K. Ekert. In this work, Ekert utilized the property of entanglement in order to address the possibility of an eavesdropping attack. However, this protocol as-is also quite vulnerable [12] to IRUD attacks, Beam-Splitting attacks, and Denial of Service attacks. Overall, these innovative algorithms utilized fundamental concepts of quantum physics such as the Entanglement Effect, Quantum Teleportation, Polarization, etc. These foundational algorithms have paved the way for all subsequent research in the field.

C. Review of Measurement Device Independent QKDs

The next logical step in the development of this branch was the new protocols that further advanced the complexity of security-assuring physical phenomena, such as BBM92 [14], SARG04 [15] [16], KMB09 [15], AK15 [16], etc. As well as continuous testing and improvement of already existing ones. For instance, since the emergence of E91 as a theoretical concept, there have been many tests that piece-by-piece proved the concept [17] [18] [19] [20], yet still failed to prove its applicability in field test or real-world applications due to poor unstable key-generation rates, relying on a theoretical piece of equipment such as quantum repeaters, limited duration of CHSH violation, or poor handling of noise. The same was done, albeit more successfully, for BB84 [21][22][23]. Although, BB84 is still suffers from the weak coherence of quantum states during transmission, which is limiting its operational range significantly. It also suffers from a limited key generation rate as-is, though there is a possibility for improvement. However, while E91 has hardly ever seen practical field applications, BB84 has already been tested in real-world applications [24] [25] and is already commercially available. After that, the next big step in the development of QKD protocols was Measurement-Independent QKD (MI-QKD) that are removing all detector side-channel attacks as well as Device-Independent QKD (DI-QKD), which security does not rely on trusting that the quantum devices used are truthful. Ultimately, these two sub-branches merged into one (MDI-QKD).

D. Twin-Field-based MDI-QKDs

One representative of this sub-branch is a Twin-Field group of QKD protocols [26] that provide a much higher key rate and greater distance compared to previous strategies (such as adding extra loss or not using any compensation). [27]. Some examples of Twin-Field QKD Protocols are include but not limited to: Sending-Not-Sending (SNS) [28], CAL19 [29], or Phase-Matching Protocol [30], which demonstrates the potential to overcome the key-rate limit and achieves a quadratic improvement over phase-encoding MDI-QKD [30]. For instance, the SNS protocol claimed to reach a distance limit of up to 800 km without misalignment error, while authors of CAL19 managed to find a solution to the key-rate drop issue of the original TF-QKD by Lucamarini et al. [26] and improve the key-rate by an order of magnitude. All of these protocols not only provided ways of robust security against common threats but also addressed some of the crucial issues on the way toward actually functioning Quantum Network [27].

E. Authentication

While all of these algorithms and approaches can be effective to various degrees and the question of a central node becoming trusted is still standing, one has to consider an approach for another big question that could render previously mentioned algorithms useless – the authentication phase. Currently, few quantum authentication algorithms would apply to this setup. Firstly, one should focus on those algorithms that do not utilize entanglement or use it in a limited capacity, since a system that requires necessary equipment for entanglement would be considerably expensive.

A good example is the work of Kanamori et al. [31]. Instead of solely relying on entanglement or a trusted center, authors chose to capitalize on the superposition. One big advantage is that this particular algorithm can re-use the TFQKD (1 phase) for the initial authentication. Another advantage is that it can be utilized even without a classical channel of communication, which provides additional security due to the dispersed approach. However, it would be cumbersome to re-use this algorithm due to the need for the generation of new keys. Another great example is the work of Zhang et al. [32]. This approach shares many advantages with the previous one, but it has one that might tip the scales to its side - it can be re-used later without the re-generation of the key.

Although the algorithms that require devices related to entanglement can make the whole system considerably expensive, it is still required to review those that fit the design of this setup. For instance, the work of Lin et al. [33] could be utilized because it does not require a trusted center. Additionally, a lot of the crucial mechanisms that are necessary are also pretty straightforward, such as - a combination of CNOT gates, different measurement bases, etc. This approach also does not rely on a classical communication channel, which is a plus.

Despite the abundance of available algorithms, further security analysis is required.

III. Similar Works

While the idea of Lucamarini et al. [26] is still - comparatively - fresh, there are many teams worldwide already

who share the same excitement and the desire for a more secure, far- reaching, multi-node QKD protocol. For example, the workof Cao et al. [34] [35] attempts to improve on the protocol provided by Lucamarini et al. by providing it with additional layers of randomization and detection. However, it is still a standalone protocol that does not cover all of the inherent security concerns of multi-node communication. One such example could be the insider attack, both from a compromised center and/or nodes. As for the work of Metwaly et al. [36], while it does have an all-encompassing approach to ensure the security of the network as well as providing a way of scaling this approach for a network of networks, it is still very theoretical and lacks concrete examples of how certain stages can be achieved, if at all. A good example of the same idea but with better authentication ingrained would be the work of Sellami et al. [37]. In this work, a fairly straightforward approach to authentication was described. Still, the question of a trusted center stands.

IV. METHODS

A. Twin-Field Quantum Key Distribution

Twin-Field Quantum Key Distribution - is a protocol that is one of many protocols (more specifically MDI-QKD protocols) that sup- ports the delivery or distribution of secret key fragments or complete secret keys between certain parties via the utilizationof laws of quantum mechanics. More specifically, the classicalversion of this protocol [26] utilizes the notion of wave-particle interference between two parties Alice and Bob who utilize a remote measuring device, which is called Charlie or Eve. Eachof the participants utilizes what is called Weak Coherent State [38] in the X basis as well as Decoy State [39] in the Z basis both have assigned randomized phases and intensities.

Twin-Field Quantum Key Distribution (TF-QKD) is a protocol within the broader category of Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) protocols, designed to facilitate the secure delivery or distribution of secret key fragments or complete secret keys between parties using the principles of quantum mechanics. The classical version of this protocol [26] (General Scheme is shown in Fig. 1.) employs the concept of wave-particle interference between two parties, commonly referred to as Alice and Bob, who interact through a remote measurement device, often termed Charlie or Eve. Each participant utilizes a Weak Coherent State [38] in the X basis and a Decoy State [39] in the Z basis, both of which are characterized by randomized phases and intensities.

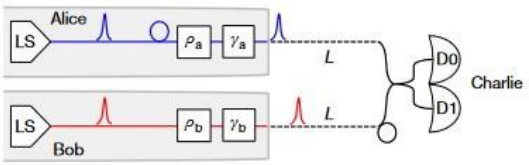

Fig. 1. Twin field QKD general scheme [26].

After the randomization of phases and intensities, each participant transmits respective Weak Coherent States (WCS) to Eve or Charlie, who performs the measurement and subsequently announces the acquired result. The announcement indicates whether the measurement detected photons with matching logical values (00 and 11) or differing values (10 and 01). Despite Eve being the entity that conducts the measurement and reports the results, Eve remains unaware of the actual key values (whether the bits are 1 and 1 or 0 and 0); Eve only knows the parity of the results. This particular QKD protocol ensures the centralized delivery of the "network portion" of the key to all hosts while providing robust security against external threats such as eavesdropping and Man-in-the-Middle (MITM) attacks.

B. KMB09

KMB09 is a protocol that, despite some skepticism, is considered part of the broader category of Measurement-Device-Independent Quantum Key Distribution (MI-QKD) protocols. The protocol relies on the mechanism of encoding a qubit into at least four different states (for simplicity, N=2 is considered) for Alice using two bases, E and F, as shown in Fig. 2. In the initial step, Alice randomly selects a basis and an index for encoding a photon and transmits the encoded photon through a quantum channel to Bob. Bob then measures the incoming photons using a randomly chosen basis. For Bob's measurement to be meaningful, Alice must disclose some information about the chosen bases publicly through a classical communication channel, such as fiber-optic. Specifically, Alice needs to reveal the selected index, either 1 or 2. However, this disclosure does not allow Eve or any other malicious party to gain knowledge about the key, as even with knowledge of the index, Eve cannot determine which basis Alice chose.

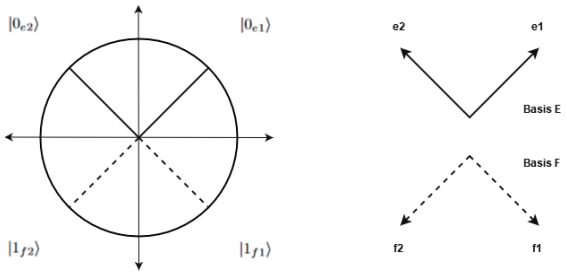

Fig. 2. KMB09 bases.

For example, if basis E is used to encode 0 and basis F is used to encode 1, the outcome of Bob's measurement, in conjunction with the non-parity of indices chosen by both Alice and Bob, determines whether the result is 1 or 0. If the indices match, a "no signal" message is announced to enhance the security of the transmission. This step ensures that the transmission remains secure even in the presence of potential eavesdropping.

As a result, and in alignment with findings from the original research article [40] and a recent overview paper [15], this protocol ensures the secure exchange of user or node-specific key portions between network participants, effectively mitigating the risk of intercept-resend attacks and similar types of security threats.

C. Proposed Method

This section details the functioning of the proposed hybrid concept within a network infrastructure that accommodates multiple users. The core objective of this concept is to secure communication among a verified number of nodes or clients within a centralized, untrusted network, as illustrated in Fig. 3.

To accomplish this, the approach combines the strengths of Measurement-Device-Independent Quantum Key Distribution (MDI-QKD), Measurement-Independent Quantum Key Distribution (MI-QKD), Continuous Variable QKD (CV-QKD), and Discrete Variable QKD (DV-QKD).

In this configuration, the untrusted center and the primary measuring device can be represented by entities such as Charlie or Eve, as the specific identity is inconsequential. The current iteration of this hybrid protocol is designed for integration with classical infrastructure. Consequently, the quantum channels utilized are standard fiber-optic cables.

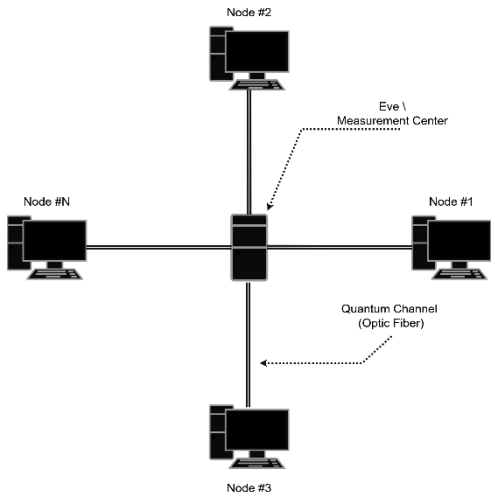

Fig. 3. General setup.

First, it is essential to verify the identities of all nodes within the network and eliminate any impostors. This can be achieved by employing a Quantum Digital Signature (QDS) protocol, such as the one described in study [41]. Once this verification process is complete, the first phase of the protocol can begin.

In the first phase, the Twin-Field QKD protocol is employed, wherein Weak Coherent States (WCSs) are transmitted from each authenticated node to the untrusted central node, Eve. Eve then measures the combined interference of all the sent states. The resulting values are not strictly 1 or 0 but rather a fluctuation between them. These fluctuations can be resolved using the Sigmoid Function, with the results publicly announced. By following this process, all nodes within a specific timeframe will obtain the "network portion" of the key.

In this step, each node transmits its respective randomized Weak Coherent States to initiate the creation of the "network portion" of the key at the measuring device, Eve (Fig. 4). This process should be repeated K times until a sufficient number of bits is accumulated within the "network portion" of the key.

In detail, each authenticated node U_i generates weak coherent states $|a_i\rangle$, where a_i represents the amplitude of the coherent state. The coherent state $|a_i\rangle$ can be expressed by following Eq. (1):

$$a_i = e^{\frac{\left(-|a_i|^2\right)}{2}} \sum_n^{\infty} \frac{a_i^n}{\sqrt{n!}} |n\rangle \quad (1)$$

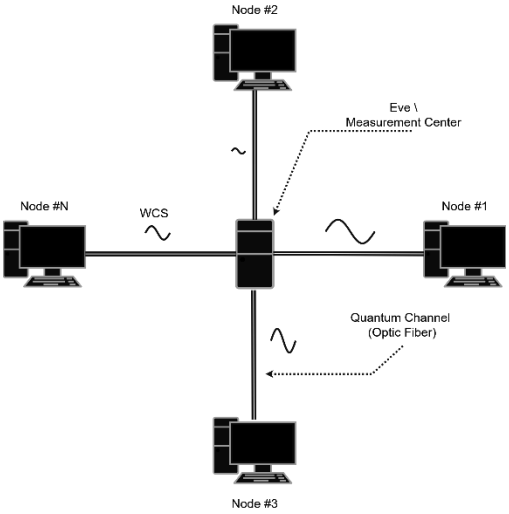

Fig. 4. Simplified stage 1.

where $|n\rangle$ represents the state with n photons. These states are sent to the central node E (Eve). The central node E measures the interference of all coherent states $|a_i\rangle$ sent by the different nodes. The total state at the central node can be described by a superposition of coherent states, refer to the Eq. (2):

$$|\phi\rangle = \sum_j |a_i\rangle \quad (2)$$

where $|a_i\rangle$ is the coherent state sent by the node U_j. The measured interference values I will fluctuate between 0 and 1. To convert these fluctuations into a more convenient format, the sigmoid function is applied. For the example refere to the Eq. (3):

$$\sigma(x) = \frac{1}{1+e^{-x}} \quad (3)$$

where x is the measured interference value. The result of $\sigma(1)$ provides a probabilistic estimate, which is then publicly announced to all nodes.

Once the measurement results are announced, each node can utilize this data to generate the "network portion" of the key. Let the measured values for node U_i and the central node E be denoted as K_i and K_E, respectively. Then, the key fragment for node U_i can be described as the following function (4):

$$U_i = f(\sigma(I), metadata) \quad (4)$$

where f is a function that defines how the measured data is transformed into key values.

Following the distribution of the "network portion" (NP), the next phase involves the generation and organization of "pair portions" (PP). This phase requires the application of the KMB09 protocol for individual pairing and key exchange. Each node or client must initiate a pairing process with every other node in the network, resulting in a total of $n-1$ pairings per node. Consequently, the total number of unique keys generated will be $(n*(n-1))/2$. The uniqueness of these pairwise keys is critical for ensuring security, as it provides protection not only against external threats but also from potential internal eavesdroppers.

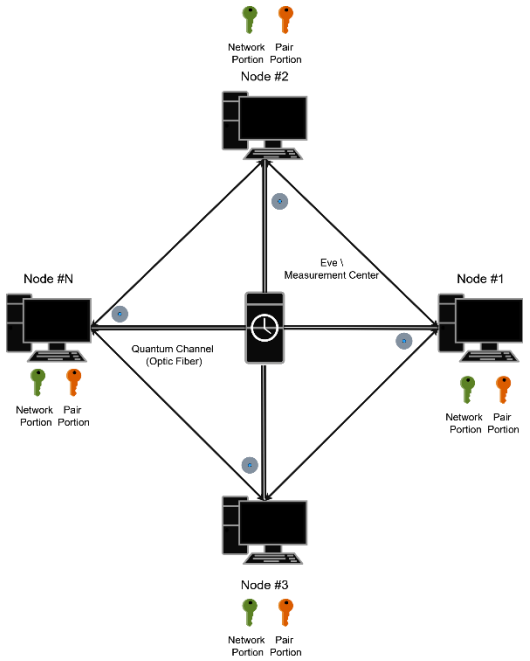

Fig. 5. Simplified stage 2.

In this setup (Fig. 5), each node transmits its randomly base-encoded photons to other nodes via a central untrusted measuring device, Eve. In this scenario, Eve acts purely as an intermediary, directing the photons to the appropriate quantum channels between the nodes intended for pairing. As a result, Eve does not obtain any information about the pair key, even if Eve attempts to intercept and resend a photon.

Thus, both the "network portion" and the "pair portion" have been successfully established. These keys can now be combined to generate a pair-unique master key, which facilitates the initiation of encrypted communication between selected nodes. To further elucidate the second part of the protocol, a mathematical analysis will be provided.

Consider a network consisting of n nodes. Each node U_i must establish a secure connection with each of the other nodes U_j, where $i \neq j$. For each node U_j, it is necessary to establish pairwise connections with the remaining $n-1$ nodes. As a result, there will be $\frac{n(n-1)}{n}$ unique pairwise keys. This quantity is determined by the formula for the number of combinations provided below (5):

$$\binom{n}{k} = \frac{n(n-1)}{2} \tag{5}$$

The KMB09 protocol is employed to generate and exchange pairwise keys between nodes. This protocol is grounded in quantum mechanics and includes the following steps:

- Initialization: Nodes U_i and U_j initiate the process by exchanging quantum states ϕ_i and ϕ_j, respectively.

- Measurement: Each node conducts measurements on the quantum state received from the other node.

- Key Extraction: Based on the measurements obtained, each node derives the key information K_{ij} corresponding to the secure communication between nodes U_i and U_j.

Let the key generated between nodes U_i and U_j be denoted as K_{ij}. Mathematically, this can be expressed as a key generation function provided below (6):

$$K_{ij} = f\left(|\phi_i\rangle, |\phi_j\rangle\right) \tag{6}$$

where f is a function that defines the algorithm for deriving a key based on the exchange of quantum states. After generating the pairwise keys K_{ij} for each pair of nodes, each node possesses:

- The network portion of the key $K_{network}$, which was generated during the first phase.

- The paired portion of the key K_{ij}, which was generated during the second phase for each node U_j.

To generate a unique master key for a pair of nodes U_i and U_j, it is necessary to combine their respective key components. Let $K_{master,ij}$ denote the master key for nodes U_i and U_j as in the example provided below (7):

$$K_{master,ij} = g\left(K_{master}, K_{ij}\right) \tag{7}$$

where g is a function that defines the method for combining the network portion and the pair portion of the keys.

Typically, this process involves applying an XOR operation or another concatenation function (8):

$$K_{master,ij} = K_{master} \oplus K_{ij} \tag{8}$$

where $\oplus$ represents the bitwise XOR operation.

To evaluate the scalability of the protocol, a graphical representation of the network is employed (Fig. 5). In a network consisting of *N* nodes, each node can exchange keys with every other node. This configuration can be visually depicted as a complete graph, where the nodes are represented as vertices and the connections between them are illustrated as edges.

V. Results and Discussion

In this paper, after careful comparison and analysis of existing methods, algorithms, and protocols a novel approach was proposed. This Hybrid Twin-Field QKD approach presents an opportunity to securely generate and share a secret key, communicate between specific nodes secured from internal eavesdroppers by the KMB09 protocol, and communicate within a network secured from outside interferences and eavesdroppers by Twin-Field QKD.

While the proposed hybrid QKD protocol is theoretically feasible, its practical implementation is currently limited, as only the individual components have been demonstrated to be achievable in real-world settings. Moreover, although Twin-Field QKD theoretically supports communication distances of up to 600 km or even 800 km, the protocol's overall range is constrained by the shortest distance supported by KMB09. This limitation highlights an important objective for future work:

extending the effective communication range of the hybrid protocol.

Additionally, there is a need for a more comprehensive analysis of the internal and external security aspects of the proposed concept, including metrics such as Quantum Bit Error Rate (QBER) [42]. Further research is also necessary in related areas, including Quantum Digital Signature (QDS) protocols, quantum authentication protocols in general, and improvements to the performance of KMB09. These avenues of investigation are crucial for enhancing the robustness and practicality of the hybrid QKD protocol.

VI. Conclusion

In conclusion, this paper has introduced and thoroughly analyzed a hybrid Twin-Field Quantum Key Distribution (QKD) protocol tailored for multi-user quantum networks. The proposed protocol addresses the increasing need for secure communication within untrusted, centralized networks, leveraging the strengths of both classical and quantum cryptographic techniques. By combining elements from various Quantum Key Distribution Protocols (QKDPs), the hybrid approach enhances the scalability and security of key distribution among multiple nodes.

The paper has provided a detailed examination of the global security landscape, highlighting the evolving challenges posed by quantum computing and the limitations of traditional cryptographic methods. Through a historical overview of QKDPs, the research identified key areas for improvement and integrated these insights into the proposed protocol.

The hybrid Twin-Field QKD protocol offers a robust solution for secure key distribution in complex network environments, ensuring protection against both external and internal threats. As quantum technologies continue to advance, this protocol represents a significant step toward realizing secure, scalable quantum communication networks. Future work may focus on further optimizing the protocol's efficiency and exploring its practical implementation in real-world quantum networks.

Acknowledgment

Research work was carried out within the framework of the project AP19675961 “Development and research of keys distribution protocols based on quantum properties”, which is being implemented at the Non-profit joint-stock company "Kazakh National Research Technical University named after K.I. Satbayev".

References

[1] Estimated cost of cybercrime worldwide 2018-2029. [Online]. Available: https://www.statista.com/forecasts/1280009/ cost-cybercrime-worldwide.

[2] The future of computing is quantum-centric. [Online]. Available: https://www.ibm.com/roadmaps/quantum/.

[3] V. Bhatia and K. Ramkumar, “An efficient quantum computing technique for cracking rsa using shor’s algorithm,” in 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), 2020, pp. 89–94.

[4] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, “Implementing grover oracles for quantum key search on aes and lowmc,” in Advances in Cryptology – EUROCRYPT 2020, A. Canteaut and Y. Ishai, Eds. Cham: Springer International Publishing, 2020, pp. 280–310.

[5] Biyashev, R.G., Kalimoldayev M.N., Nyssanbayeva, S.E., Kapalova N.A., Dyusenbayev, D.S., Algazy K.T., Development and analysis of the encryption algorithm in nonpositional polynomial notations // Eurasian Journal of Mathematical and Computer Applications. – 2018. - № 6(2). - P.19-33. DOI: 10.32523/2306-6172-2018-6-2-19-33.

[6] R.G. Biyashev, N.A. Kapalova, D.S. Duysenbayev, K.T. Algazy, Waldemar Wojcik, Andrzej Smolarz Development and Analysis of Symmetric Encryption Algorithm Qamal Based on a Substitution-permutation Network, International journal of electronics and telecommunications, № 1, 2021, P. 127-132 DOI: 10.24425/ijet.2021.135954.

[7] R. G. Biyashev, S. E. Nyssanbayeva, and Ye. Y. Begimbayeva Development of the model of protected cross-border information interaction // Open Engineering. – 2016. – № 6. – P. 199 – 205, DOI: https://doi.org/10.1515/eng-2016-0025.

[8] Maksat N. Kalimoldayev, Rustem G. Biyashev, Saule E. Nyssanbayeva, Yenlik Ye. Begimbayeva Modification of the digital signature, developed on the nonpositional polynomial notations // Eurasian Journal of Mathematical and Computer Applications. – 2016. – Vol. 4, Is. 2. – P. 33 – 38, DOI: 10.32523/2306-6172-2016-4-2-33-38.

[9] Y. Begimbayeva, T. Zhaxalykov and O. Ussatova, "Investigation of Strength of E91 Quantum Key Distribution Protocol," 2023 19th International Asian School-Seminar on Optimization Problems of Complex Systems (OPCS), Novosibirsk, Moscow, Russian Federation, 2023, pp. 10-13, doi: 10.1109/OPCS59592.2023.10275771.

[10] Ussatova, O., Makilenov, S., Mukaddas, A., Amanzholova, S., Begimbayeva, Y., & Ussatov, N. (2023). Enhancing healthcare data security: a two-step authentication scheme with cloud technology and blockchain. Eastern-European Journal of Enterprise Technologies, 6(2 (126), 6–16. https://doi.org/10.15587/1729-4061.2023.289325.

[11] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Mar 2020. [Online]. Available: https://arxiv.org/abs/2003.06557v1

[12] A. Abushgra and K. Elleithy, “Qkdp’s comparison based upon quantum cryptography rules,” in 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2016, pp. 1–5.

[13] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” Phys. Rev. Lett., vol. 67, pp. 661–663, Aug 1991. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.67.661

[14] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without bell’s theorem,” Phys. Rev. Lett., vol. 68, pp. 557–559, Feb 1992. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.68.557

[15] M. Lopes and N. Sarwade, “On the performance of quantum cryptographic protocols sarg04 and kmb09,” in 2015 International Conference on Communication, Information Computing Technology (ICCICT), 2015, pp. 1–6.

[16] A. A. Abushgra, “Sarg04 and ak15 protocols based on the run-time execution and qber,” in 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), 2021, pp. 176–180.

[17] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. O¨ mer, M. Fu¨rst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, “Entanglement-based quantum communication over 144km,” Nature Physics, vol. 3, no. 7, p. 481–486, Jun 2007. [Online]. Available: http://dx.doi.org/10.1038/nphys629

[18] A. Ling, M. P. Peloso, I. Marcikic, V. Scarani, A. Lamas-Linares, and C. Kurtsiefer, “Experimental quantum key distribution based on a bell test,” Physical Review A, vol. 78, p. 020301, 8 2008. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.78.020301

[19] M. Fujiwara, K. ichiro Yoshino, Y. Nambu, T. Yamashita, S. Miki, H. Terai, Z. Wang, M. Toyoshima, A. Tomita, and M. Sasaki, “Modified e91 protocol demonstration with hybrid entanglement photon source,” Optics Express, vol. 22, p. 13616, 6 2014. [Online]. Available: https://opg.optica.org/oe/abstract.cfm?uri=oe-22-11-13616

[20] J. Yin, Y. Cao, and et al., “Satellite-based entanglement distribution over 1200 kilometers,” Science, vol. 356, no. 6343, p. 1140–1144, Jun 2017. [Online]. Available: http://dx.doi.org/10.1126/science.aan3211

[21] B. Kebapci, V. E. Levent, S. Ergin, G. Mutlu, I. Baglica, A. Tosun, P. Paglierani, K. Pelekanakis, R. Petroccia, J. Alves, and M. Uysal, "Fpga-based implementation of an underwater quantum key distribution system with bb84 protocol," IEEE Photonics Journal, vol. 15, no. 4, pp. 1–10, 2023.

[22] C. Lee, I. Sohn, and W. Lee, "Eavesdropping detection in bb84 quantum key distribution protocols," IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2689–2701, 2022.

[23] M. Stipc˘evic´, "Enhancing the security of the bb84 quantum key distribution protocol against detector-blinding attacks via the use of an active quantum entropy source in the receiving station," Entropy, vol. 25, no. 11, 2023. [Online]. Available: https://www.mdpi.com/ 1099-4300/25/11/1518

[24] J. F. Dynes, A. Wonfor, and et al., "Cambridge quantum network," npj Quantum Information, vol. 5, no. 1, Nov 2019. [Online]. Available: http://dx.doi.org/10.1038/s41534-019-0221-4

[25] M. Sasaki, M. Fujiwara, and et al., "Field test of quantum key distribution in the tokyo qkd network," Mar 2011. [Online]. Available: https://arxiv.org/abs/1103.3566v1

[26] 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, p. 400–403, May 2018. [Online]. Available: http://dx.doi.org/10.1038/s41586-018-0066-6

[27] X. Zhong, W. Wang, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses," npj Quantum Information, vol. 7, no. 1, Jan 2021. [Online]. Available: http://dx.doi.org/10.1038/ s41534-020-00343-5

[28] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, "Sending-or- not-sending twin-field quantum key distribution in practice," Scientific Reports, vol. 9, no. 1, p. 3080, Feb 2019. [Online]. Available: https://doi.org/10.1038/s41598-019-39225-y

[29] M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," npj Quantum Information, vol. 5, no. 1, Jul 2019. [Online]. Available: http: //dx.doi.org/10.1038/s41534-019-0175-6

[30] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," Phys. Rev. X, vol. 8, p. 031043, Aug 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevX.8.031043

[31] Y. Kanamori, S.-M. Yoo, D. A. Gregory, and F. T. Sheldon, "Authentication protocol using quantum superposition states," International Journal of Network Security, vol. 9, no. 2, p. 101–108, Jan. 2009. [Online]. Available: http: //ijns.jalaxy.com.tw/contents/ijns-v9-n2/ijns-2009-v9-n2-p101-108.pdf

[32] D. Zhang and X. Li, "Quantum authentication using orthogonal product states," in Third International Conference on Natural Computation (ICNC 2007), vol. 4, 2007, pp. 608–612.

[33] T.-S. Lin, I.-M. Tsai, H.-W. Wang, and S.-Y. Kuo, "Quantum authentication and secure communication protocols," in 2006 Sixth IEEE Conference on Nanotechnology, vol. 2, 2006, pp. 863–866.

[34] X.-Y. Cao, Y.-S. Lu, Z. Li, J. Gu, H.-L. Yin, and Z.-B. Chen, "High key rate quantum conference key agreement with unconditional security," IEEE Access, vol. 9, p. 128870–128876, Jan. 2021. [Online]. Available: https://doi.org/10.1109/access.2021.3113939

[35] X.-Y. Cao, J. Gu, Y.-S. Lu, H.-L. Yin, and Z.-B. Chen, "Coherent one-way quantum conference key agreement based on twin field," New Journal of Physics, vol. 23, no. 4, p. 043002, Apr. 2021. [Online]. Available: https://doi.org/10.1088/1367-2630/abef98

[36] A. Metwaly, M. Z. Rashad, F. A. Omara, and A. A. Megahed, "Architecture of point to multipoint qkd communication systems (qkdp2mp)," in 2012 8th International Conference on Informatics and Systems (INFOS), 2012, pp. NW–25–NW–31.

[37] S. Ali, O. Mahmoud, and A. A. Hasan, "Multicast network security using quantum key distribution (qkd)," Jul. 2012. [Online]. Available: https://doi.org/10.1109/iccce.2012.6271355

[38] T. F. da Silva, G. C. do Amaral, D. Vitoreti, G. P. T. ao, and J. P. von der Weid, "Spectral characterization of weak coherent state sources based on two-photon interference," J. Opt. Soc. Am. B, vol. 32, no. 4, pp. 545–549, Apr 2015. [Online]. Available: https://opg.optica.org/josab/abstract.cfm?URI=josab-32-4-545

[39] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett., vol. 91, p. 057901, Aug 2003. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett. 91.057901

[40] M. M. Khan, M. Murphy, and A. Beige, "High error-rate quantum key distribution for long-distance communication," New Journal of Physics, vol. 11, no. 6, p. 063043, jun 2009. [Online]. Available: https://dx.doi.org/10.1088/1367-2630/11/6/063043

[41] C.-H. Zhang, X. Zhou, C.-M. Zhang, J. Li, and Q. Wang, "Twin-field quantum digital signatures," Opt. Lett., vol. 46, no. 15, pp. 3757–3760, Aug 2021. [Online]. Available: https://opg.optica.org/ol/abstract.cfm?URI=ol-46-15-3757

[42] M. Niemiec and A. R. Pach, "The measure of security in quantum cryptography," Dec. 2012. [Online]. Available: https://doi.org/10.1109/glocom.2012.6503238.