The object of this research is the security of communication networks, particularly in decentralized, multi-user environments where robust data protection and integrity are critical. The issue under discussion is the rising vulnerability of conventional cryptography systems resulting from ever complex cyberattacks and the expected risks presented by quantum computing possibilities. The development of a QKD protocol employing quantum superposition to improve data security and resilience against both present and future quantum-based cyber-attacks is demonstrated by the achieved results of this work. Achieving scalability and autonomous eavesdropping detection, this protocol lets several communication nodes securely exchange randomly produced keys without centralized management. A quick analysis of the results reveals that main elements influencing the great durability, security, and adaptability of the protocol are quantum superposition and its distributed character. Without centralized authority, the characteristics of the obtained results – especially the use of optical components, detectors, and quantum sources in conjunction with classical communication channels – solve the problem of ensuring data confidentiality and integrity in a multi-user environment. This protocol's practical reach covers safe communication applications in both public and private sectors, therefore addressing situations calling for strong data protection against modern cyberattacks. Conditions for practical application include settings like government, financial, or health-related interactions when safe information flow is crucial. This QKD system offers a future-ready security solution for high-stakes environments and represents notable advancement toward protecting data from quantum and conventional attacks

Keywords: quantum cryptography, quantum key distribution, quantum mechanics, qubit, decentralized protocols

UDC 004.056.5
DOI: 10.15587/1729-4061.2024.318588

DEVELOPMENT OF SUPERPOSITION-BASED QUANTUM KEY DISTRIBUTION PROTOCOL IN DECENTRALIZED FULL MESH NETWORKS

Yenlik Begimbayeva**
PhD, Senior Researcher*
Olga Ussatova
PhD, Senior Researcher**
Satbayev University*
Temirlan Zhaxalykov***
Corresponding author
Master of Technical Sciences, Scientific Researcher*
E-mail: zhaxalykov8@gmail.com
Amir Akhtanov***
Engineer*
School of Information Technology and Engineering***
Ruslan Pashkevich
Engineer*
School of Information Technology and Engineering***
Mukaddas Arshidinova
PhD, Scientific Researcher*
*Satbayev University
Satbayev str., 22, Almaty, Republic of Kazakhstan, 050013
**Institute of Information and Computational Technologies
Shevchenko str., 28, Almaty, Republic of Kazakhstan, 050010
***Kazakh-British Technical University
Tole bi str., 59, Almaty, Republic of Kazakhstan, 050000

Received 07.10.2024
Received in revised form 25.11.2024
Accepted 09.12.2024
Published 27.12.2024

How to Cite: *Begimbayeva, Y., Ussatova, O., Zhaxalykov, T., Akhtanov, A., Pashkevich, R., Arshidinova, M. (2024). Development of superposition-based quantum key distribution protocol in decentralized full mesh networks. Eastern-European Journal of Enterprise Technologies, 6 (9 (132)), 39–46. https://doi.org/10.15587/1729-4061.2024.318588*

1. Introduction

Data security issues are becoming more critical in modern society since digital technologies have permeated every part of our life. The incidence of cyber-attacks, particularly those employing cutting-edge technologies, rises daily. According to [1] cyberattacks are expected to keep increasing in 2024, and in the first months of the year, many data leaks have impacted thousands of companies globally. This demonstrates that information security becomes a major issue for businesses of all kinds.

Traditionally, asymmetric cryptography has been relied upon in conventional security solutions, including SSL/TLS protocols and Public Key Infrastructure (PKI), to protect private data. While SSL/TLS protocols create a secure link between a client and a server, thereby preserving data during transmission, PKI consists of generating, administering, and using digital certificates that offer authentication and data encryption. Still, cryptographers face difficulties, especially as the number and value of transmitted data have surged to 402.74 million terabytes daily, with an expected annual data volume of 147 zettabytes. As stated in [2], such increasing data demands require stronger cryptographic measures to handle potential weaknesses and threats.

To maintain data integrity, confidentiality, and authenticity in the modern digital landscape ahead of adversaries, cryptographers must continue developing new information security techniques. Cryptographic science helps to partial-

ly assure the CIA triad – confidentiality, integrity, availability – relevant to information systems security. The difficulty of factoring large numbers prevents unauthorized access, hence preserving the integrity of traditional cryptographic methods. The RSA algorithm forms the basis of security in these systems. It has been shown in [3] that breaking SHA-3 or compromising an RSA encryption key could require protracted brute-force attacks over several years. For example, running the 10^{40} operations required to break an RSA-2048 key by brute force would take over 19.8 quadrillion years, well beyond the age of the universe (13.8 billion years). This explains why RSA-2048 remains secure against brute force attacks using conventional computers.

However, quantum technology could fundamentally change this security paradigm. The paper [4] presents that Peter Shor developed an algorithm based on quantum computing that can effectively factor large integers, thus supporting cryptosystems like RSA. It is shown that Shor's approach significantly decreases the time required for cryptanalysis, potentially reducing it from quadrillions of years to mere hours or minutes with quantum computers. This breakthrough led to the development of post-quantum cryptography, which aims to create cryptographic techniques resistant to quantum computer attacks, as presented in [5]. Conversely, quantum cryptography based on quantum mechanics offers data transfer methods naturally safe against hacking and interception.

Quantum physics, utilizing qubits, offers substantial advantages over conventional data processing techniques. Quantum computers can process exponentially more information than classical bit-based computers, as qubits can reside in a superposition state, concurrently representing both 0 and 1. By employing properties like light polarization and photon pulses, approaches can solve challenging problems and create new opportunities in various domains.

A highly promising application of quantum technologies is secure data transmission. The paper [6, 7] present that quantum cryptography, introduced in 1979, uses quantum mechanics to generate secret keys that can be securely shared between two parties. Shown that this method provides an unmatched level of data protection compared to traditional encryption, which relies on computational complexity. Through quantum superposition and the Heisenberg uncertainty principle, the Quantum Key Distribution (QKD) protocol offers enhanced security. Any attempt to intercept and measure qubits is quickly detected since the change in the qubits' state indicates an intrusion.

Safe key exchange is facilitated by several QKD protocols like BB84 and E91. The paper [8] shows that the BB84 protocol, introduced in 1984, employs four different photon polarization states for information transmission, while the paper [9] presents that the E91 protocol, introduced in 1991, relies on quantum entanglement to detect interference. Based on quantum physics, QKD theoretically provides absolute security, and it has been shown in [10] that the security of the QKD technique has been demonstrated in multiple studies. Two primary approaches for implementing QKD are discrete variables (DV), which encode information in the quantum state of an individual photon, and continuous variables (CV), which use coherent states of weak light pulses. Shown that CV-based systems provide benefits such as rapid key transfer over short distances, cost efficiency, and compatibility with current telecommunications technology.

The development of quantum technologies and networks depends on their fit for current communication infrastructures. With a high level of protection against interception and the use of quantum states of photons for information transfer, quantum networks present a promising route for improving data security and transmission efficiency. The transition from classical to quantum networks requires hybrid systems that integrate the advantages of both paradigms, thereby enabling incremental integration of quantum technologies and reducing the risks and expenses associated with infrastructure upgrades.

Thus, as it aims to improve data security and adaptability in contemporary multi-user network contexts, research devoted to the development of distributed quantum key distribution protocols based on superposition is highly relevant [11–14].

2. Literature review and problem statement

Early in the 2000s, studies started extending ideas of quantum key distribution (QKD) to multiparty environments. Research conducted in 2007 [15] introduced a technique that allowed three parties to create a shared secret bit sequence without obfuscation, guaranteeing security even against potentially limitless computing capacity of attackers. Based on CSS (Calderbank-Shor-Steane) codes, this protocol demonstrated the viability of multi-party QKD without entangled states, thereby enabling practical implementation. Nevertheless, this method was limited to point-to-point networks, and applying it to larger, more complex networks remains an unsolved challenge.

In 2012, significant advancements were made, as noted in [16], which contributed to the development of more effective multilateral QKD systems. This work explored techniques such as CDMA and TDMA in passive star networks to improve QKD efficiency and security in networked environments. Moreover, a listen-before-send protocol was also implemented to enhance key generation efficiency and support scalable network topologies using standard telecommunications components. However, the complexity of managing key distribution grows significantly with network size, despite these improvements, indicating a need for further advancements to scale these systems for larger networks.

Further research into N-particle entanglement continued by 2017 [17], with a focus on hypothetically increasing QKD speeds in networks. It was shown that multilateral entangled states could improve security thresholds and distribution rates. However, the technical hurdles associated with maintaining and synchronizing entanglement across multiple nodes pose significant challenges to applying N-particle entanglement in practical networks.

In the same year, researchers [18] developed a semi-quantum key distribution (MSQKD) and secret exchange system utilizing GHZ-like states to enable communication between quantum and classical entities. This protocol proved to be adaptable and efficient for multilateral quantum communications and permitted conversions between MSQKD and MSQSS. However, the protocol's reliance on specialized states and dedicated communication channels restricts its application in larger, more heterogeneous networks, making further investigation into its scalability necessary.

The study conducted in 2018 [19] presented multi-level QKD methods involving multi-dimensional and multi-sided entanglement. These approaches optimized the use of quan-

tum channels, allowing them to be adapted for intricate network topologies, thereby significantly improving exchange efficiency. Nonetheless, the practical viability of multi-dimensional entanglement is limited by the complexity of its control, especially in real-world scenarios where stability remains a key issue.

Another approach, introduced in 2019 [20], proposed a multi-party QKD system using phase shift manipulation to encode key sequences in EPR pairs, thus providing a simpler implementation strategy. Although this method simplifies key distribution, its real-world deployment is hindered by increased sensitivity to phase stability and environmental factors. This finding highlights the necessity of developing solutions capable of maintaining robustness under varied conditions.

In 2020, a confirmed multiparty QKD agreement based on two-dimensional Poisson was presented [21]. This approach highlighted the potential of hybrid systems that combine quantum and classical techniques to facilitate key distribution among multiple participants. However, combining quantum and classical methods introduces computational overhead, which can hamper real-time performance, particularly as network sizes grow.

The research in [22] described a multi-user QKD strategy employing a Bell state encoding approach, using unitary operations and custom algorithms to generate secure session keys among multiple users. While the system increased security, the paper also highlighted that operational complexity and resource constraints might hinder its adoption in larger networks, suggesting that further optimization is essential to enhance scalability.

In the same year, a blind multiparty quantum computing protocol featuring mutual authentication was established [23], using MDI-QKD to support secure key distribution. This work aimed to improve the reliability of quantum computing in networked environments. Despite these contributions, broader applicability remains hindered by synchronization and standardization challenges across different network infrastructures.

A novel methodology for generating shared secret keys across separate quantum channels was introduced in 2023 [24]. The proposed system underscored the potential for scalable QKD in practical settings, emphasizing low hardware requirements for intermediate nodes and utilizing abstract cryptographic frameworks to ensure high security. However, scalability for larger networks is significantly impeded by hardware limitations, which necessitates the creation of innovative solutions to minimize the reliance on specialized components.

Recently, researchers [25] introduced a hybrid QKD framework for multi-user networks, enhancing conventional QKD using twin-field algorithms that provide both scalability and improved security over more extensive networks. While this approach maintained high-security standards and reduced resource consumption, it was concluded that further enhancements are needed to ensure real-time adaptability and consistent performance in large-scale quantum networks.

From theoretical advancements to practical applications, each step forward has built upon prior contributions and introduced new methodologies and technology. However, current methods continue to face considerable challenges in terms of scalability, complexity, and integration with existing communication infrastructure. Addressing these gaps is crucial to ensure that QKD systems can meet the demands for secure, reliable communication in the modern digital environment. Therefore, additional research is essential to address these issues and develop robust, scalable QKD systems for secure quantum communication in today's digital world.

3. The aim and objectives of the study

The aim of the study is to develop a decentralized, scalable quantum key distribution (QKD) protocol that enhances data security in multi-user network settings by utilizing principles of quantum superposition.

To achieve the aim, the following objectives are accomplished:

– to develop a key negotiation process for legitimate nodes in a full mesh decentralized network;

– to develop qubit processing with quantum superposition and qubit state rotation;

– to develop a key extraction process for each side of a legitimate connection.

4. Materials and methods

4. 1. Object and hypothesis of the study

The object of this study is the security of communication networks, particularly in decentralized, multi-user environments, where robust data protection, confidentiality, and integrity are critical. The hypothesis of this research is that a distributed Quantum Key Distribution (QKD) protocol based on quantum superposition can significantly improve the resilience, scalability, and security of communication networks, making them robust against both classical and quantum cyber threats.

Several assumptions were made during the study. It is assumed that the communication channels between nodes include secure quantum channels and classical communication links. The principles of quantum mechanics, particularly quantum superposition, are considered reliable for secure key exchange. Additionally, all nodes in the network are assumed to be equipped with the necessary quantum and classical hardware, such as optical components, quantum detectors, and quantum sources.

To simplify the analysis, noise in the quantum channels and potential losses are not modeled and are assumed to be minimal under ideal conditions. Synchronization and time delay issues between nodes are also considered negligible for the scope of this protocol. Furthermore, any eavesdropping attempts are assumed to cause detectable perturbations in the quantum states, enabling the detection of intrusions.

4. 2. Protocol design

The decentralized Quantum Key Distribution (QKD) protocol functions on the principles of quantum superposition, specifically engineered for safe key exchange inside a multi-node network using a full-mesh architecture. Every node in this topology can create a simple, secure communication link with all other nodes, ensuring resilience against eavesdropping and improving data security throughout the network.

The protocol's security is based on quantum mechanics principles, wherein any effort at eavesdropping results in observable perturbations in the quantum states of the transmitted qubits. This intrinsic characteristic enables the detection and prevention of unwanted access. Encoding essential information in qubits that exist in superposition ensures the security of any communication channel, as any

effort to measure or monitor the qubits disturbs their states, indicating the presence of an intruder.

In this full-mesh architecture (Fig. 1), each node must create distinct keys with every other node, resulting in exponential increases in the number of connections as the network enlarges. This method necessitates meticulous design and optimization to manage the escalating complexity, as the quantity of connections increases with each additional node. The protocol's design incorporates methods to ensure and uphold high scalability, facilitating safe communication and efficient key distribution in large network contexts.

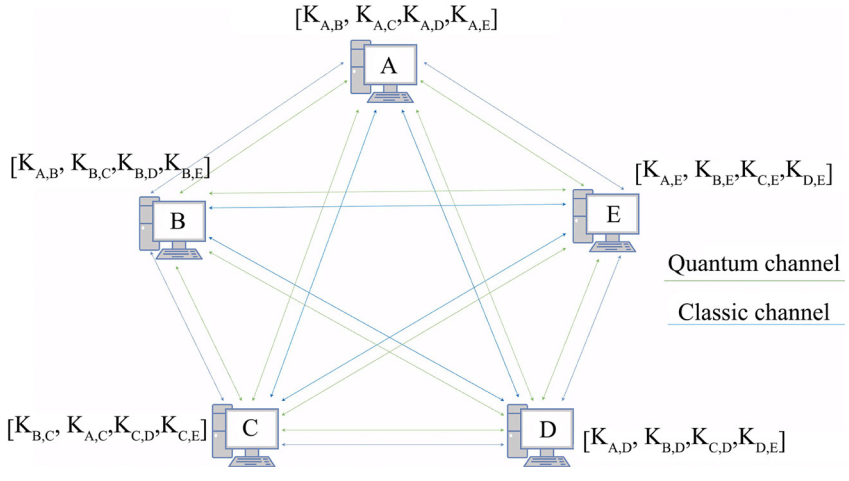

Fig. 1. Network depiction of the protocol with annotated connections among the nodes

This arrangement offers a scalable answer for networks as well as enhances the security of communication. The protocol improves the resilience of the network against external attacks by allowing every node to create direct and safe channels with all other nodes, therefore guaranteeing effective and safe key distribution even as the network increases in size and complexity.

4. 3. Protocol implementation

The execution of this QKD protocol adheres to a systematic procedure encompassing the generation and manipulation of qubits, the rotation of their states, and the extraction of a secure key between each pair of nodes in a fully interconnected network. The procedures are outlined as follows:

1. Key Length Generation: The protocol initiates by producing a random key length for each inter-node connection. The length is established by a pseudorandom number generator (*PRNG*) on the one hand, which initiates the interaction, which guarantees variety in key size of each connection.

2. Qubit Initialization: Each node randomly establishes an initial array of qubit states corresponding to the specified key length. These states are arbitrarily selected to exist in one of two configurations: $|-\rangle$ or $|+\rangle$. The starting configurations are characterized as superpositions (2):

$$|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle). \quad (1)$$

The initial superpositions create the foundation for subsequent operations that will incorporate greater randomness into the qubit states.

3. Qubit Generation and Rotation: After the initial configuration, each qubit is subjected to a rotation determined by a randomly assigned angle, θ, produced by the PRNG. The rotation transformation $Rx(\theta)$ is executed on each qubit state to alter its probability amplitudes. The rotation matrix $Rx(\theta)$ is defined as (2):

$$R_X(\theta)=\exp\left(-i\frac{\theta}{2}X\right)=\cos\left(\frac{\theta}{2}\right)I-i\cdot\sin\left(\frac{\theta}{2}\right)X.$$

In this context, $Rx(\theta)$ denotes the rotation operator by an angle θ about the X-axis, X represents the Pauli operator, and I signifies the identity matrix. Each user randomly chooses a rotation angle between 0 and 2π.

4. Qubit Transmission and Measurement: The rotating qubits are subsequently communicated over secure quantum channels between nodes. Upon arrival at the receiving node, the state of each qubit collapses into a classical bit value of $|0\rangle$ or $|1\rangle$ upon measurement. The likelihood of each occurrence is dictated by the amplitude values derived from the rotating state (3):

$$P(|0\rangle)=|a|^2, P(|1\rangle)=|b|^2,$$

where a and b represent the coefficients from the rotated state. This measurement phase produces a discrete bit value determined by the probability of each outcome.

5. Key Extraction: To determine the final shared key, nodes compare their processed qubit states and utilize a Boolean XOR function to derive a unique key bit for each qubit pair. The XOR operation is characterized as $key\_bit=p1\_bit\oplus p2\_bit$. In this context, $p1\_bit$ and $p2\_bit$ denote the classical bit values obtained from the probability amplitudes of the qubit measurements at each node. The XOR technique guarantees that each pair of nodes produces a corresponding key bit alone when their measurements coincide, so establishing a shared, secure key for that connection.

6. Full-Mesh Network Exchange: This protocol operates within a full-mesh network setup, wherein each node establishes a distinct key with every other node in the network. For every node pair, the protocol produces, spins, and measures qubits, subsequently applying the XOR operation to produce a unique key for that connection. This guarantees that each node-to-node link is independently secured, and the ultimate collection of keys enables secure communication between every node in the network.

By adhering to these procedures, the QKD protocol creates a resilient and decentralized network in which each connection is safeguarded by a distinct, randomly generated key, hence ensuring security throughout the whole communication network.

5. Results of the study of a superposition-based quantum key distribution protocol in decentralized full mesh networks

5. 1. Key negotiation process for legitimate nodes in full mesh decentralized network

The pseudo randomly generated angles for each qubit in the links between Alice and her nodes are specified as follows. The angles introduce randomization into qubit states through rotations, ensuring that measurement outcomes vary across

connections, resulting in distinct key bits. Details of the random bit generation for each connection are provided in Table 1.

Table 1

Results of the random bit generation for each node

Connection	PRNG for Alice's bit sequence	PRNG for N's bit sequence
ConnectionAB	1011010	0000010
ConnectionAB	0000101	1011010
ConnectionAB	0101011	1100000
ConnectionAB	1101101	0000100

The rotation angles determine the modifications executed on each qubit prior to measurement, leading to diverse probability distributions for outcomes.

For every link, Alice and her corresponding node produce a sequence of qubits, each designated a certain rotation angle. Upon executing the rotation, the qubit is depicted in a terminal state determined by its probability amplitudes for the $|0\rangle$ and $|1\rangle$ results. Presented below are the comprehensive tables of qubit states pertaining to Alice's interactions with Bob, Charlie, Dave, and Elise.

5. 2. Qubit processing with quantum superposition and qubit state rotation

This section delineates the results of the Quantum Key Distribution (QKD) protocol between Alice and her associated nodes: Bob, Charlie, Dave, and Elise. The following tables (Tables 2–9) provide specific details of Alice's qubit preparation and processing in relation to each of these nodes. Alice's qubits are initially generated in either state $|0\rangle$ or $|1\rangle$ during this process. Subsequently, they endure a rotation to achieve a superposition state. This guarantees that the qubits are adequately randomized, and any attempts to intercept them would result in detectable changes.

Table 2

Results of Alice's qubit preparation process in connection with Bob

Bit	Z	X	θ	Result state $\|\psi_{nn}\rangle=\alpha_{nn}\|0\rangle+\beta_{nn}\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	635	$\|\psi_{a1}\rangle=0.9990\|0\rangle-0.0436\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	341	$\|\psi_{a1}\rangle=-0.8141\|0\rangle-0.5807\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	231	$\|\psi_{a1}\rangle=-0.9426\|0\rangle-0.3338\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	143	$\|\psi_{a1}\rangle=-0.4462\|0\rangle-0.8949\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	706	$\|\psi_{a1}\rangle=0.7880\|0\rangle+0.6157\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	526	$\|\psi_{a1}\rangle=0.6157\|0\rangle+0.7880\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	494	$\|\psi_{a1}\rangle=0.3746\|0\rangle-0.9272\|1\rangle$

Table 3

Results of Bob's qubit preparation process in connection with Alice

Bit	Z	X	θ	Result state $\|\psi_{nn}\rangle=\alpha_{nn}\|0\rangle+\beta_{nn}\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	635	$\|\psi_{b1}\rangle=0.9990\|0\rangle-0.0436\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	341	$\|\psi_{b1}\rangle=-0.8141\|0\rangle-0.5807\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	231	$\|\psi_{b1}\rangle=-0.9426\|0\rangle-0.3338\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	143	$\|\psi_{b1}\rangle=-0.4462\|0\rangle-0.8949\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	706	$\|\psi_{b1}\rangle=0.7880\|0\rangle+0.6157\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	526	$\|\psi_{b1}\rangle=0.6157\|0\rangle+0.7880\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	494	$\|\psi_{b1}\rangle=0.3746\|0\rangle-0.9272\|1\rangle$

Table 4

Results of Alice's qubit preparation process in connection with Charlie

Bit	Z	X	θ	Result state $\|\psi_{nn}\rangle=\alpha_{nn}\|0\rangle+\beta_{nn}\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	249	$\|\psi_{a2}\rangle=-0.9833\|0\rangle+0.1822\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	674	$\|\psi_{a2}\rangle=0.9272\|0\rangle+0.3746\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	394	$\|\psi_{a2}\rangle=-0.4695\|0\rangle-0.8829\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	161	$\|\psi_{a2}\rangle=-0.5807\|0\rangle+0.8141\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	145	$\|\psi_{a2}\rangle=-0.4617\|0\rangle-0.8870\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	14	$\|\psi_{a2}\rangle=0.6157\|0\rangle+0.7880\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	21	$\|\psi_{a2}\rangle=0.5664\|0\rangle-0.8241\|1\rangle$

Table 5

Results of Charlie's qubit preparation process in connection with Alice

Bit	Z	X	θ	Result state $\|\psi_{nn}\rangle=\alpha_{nn}\|0\rangle+\beta_{nn}\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	229	$\|\psi_{c1}\rangle=-0.9367\|0\rangle-0.3502\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	59	$\|\psi_{c1}\rangle=0.2672\|0\rangle+0.9636\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	350	$\|\psi_{c1}\rangle=-0.7660\|0\rangle+0.6428\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	160	$\|\psi_{c1}\rangle=-0.5736\|0\rangle-0.8192\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	319	$\|\psi_{c1}\rangle=-0.9100\|0\rangle-0.4147\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	121	$\|\psi_{c1}\rangle=-0.2672\|0\rangle+0.9636\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	269	$\|\psi_{c1}\rangle=-0.9913\|0\rangle-0.0087\|1\rangle$

Table 6

Results of Alice's qubit preparation process in connection with Dave

Bit	Z	X	θ	Result state $\|\psi_{nn}\rangle=\alpha_{nn}\|0\rangle+\beta_{nn}\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	536	$\|\psi_{a3}\rangle=0.6820\|0\rangle-0.7314\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	466	$\|\psi_{a3}\rangle=0.1392\|0\rangle+0.9903\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	197	$\|\psi_{a3}\rangle=-0.8039\|0\rangle+0.5948\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	654	$\|\psi_{a3}\rangle=0.9781\|0\rangle-0.2079\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	246	$\|\psi_{a3}\rangle=-0.9781\|0\rangle+0.2079\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	301	$\|\psi_{a3}\rangle=-0.9636\|0\rangle-0.2672\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	289	$\|\psi_{a3}\rangle=-0.9863\|0\rangle-0.1650\|1\rangle$

Table 7

Results of Dave's qubit preparation process in connection with Alice

Bit	Z	X	θ	Result state $\|\psi_{nn}\rangle=\alpha_{nn}\|0\rangle+\beta_{nn}\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	656	$\|\psi_{d1}\rangle=0.9744\|0\rangle-0.2250\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	517	$\|\psi_{d1}\rangle=0.5519\|0\rangle+0.8339\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	628	$\|\psi_{d1}\rangle=0.9998\|0\rangle-0.0175\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	313	$\|\psi_{d1}\rangle=-0.9304\|0\rangle-0.3665\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	339	$\|\psi_{d1}\rangle=-0.8241\|0\rangle-0.5664\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	332	$\|\psi_{d1}\rangle=-0.8572\|0\rangle-0.5150\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	717	$\|\psi_{d1}\rangle=0.7254\|0\rangle+0.6884\|1\rangle$

Table 8

Results of Alice's qubit preparation process in connection with Elise

Bit	Z	X	θ	Result state $\|\psi_{nn}\rangle=\alpha_{nn}\|0\rangle+\beta_{nn}\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	58	$\|\psi_{a4}\rangle=0.2756\|0\rangle-0.9613\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	145	$\|\psi_{a4}\rangle=-0.4617\|0\rangle-0.8870\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	610	$\|\psi_{a4}\rangle=0.9848\|0\rangle-0.1736\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	162	$\|\psi_{a4}\rangle=-0.5878\|0\rangle-0.8090\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	407	$\|\psi_{a4}\rangle=-0.3665\|0\rangle+0.9304\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	513	$\|\psi_{a4}\rangle=0.5225\|0\rangle-0.8526\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	97	$\|\psi_{a4}\rangle=-0.0610\|0\rangle-0.9981\|1\rangle$

Table 9

Results of Elise's qubit preparation process in connection with Alice

Bit	Z	X	θ	Result state $\|\psi_{nn}\rangle=\alpha_{nn}\|0\rangle+\beta_{nn}\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	656	$\|\psi_{e1}\rangle=0.9744\|0\rangle+0.2250\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	546	$\|\psi_{e1}\rangle=0.7431\|0\rangle-0.6691\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	110	$\|\psi_{e1}\rangle=-0.1736\|0\rangle+0.9848\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	189	$\|\psi_{e1}\rangle=-0.7604\|0\rangle+0.6494\|1\rangle$
1	$\|1\rangle$	$\|-\rangle$	157	$\|\psi_{e1}\rangle=-0.5519\|0\rangle-0.8339\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	118	$\|\psi_{e1}\rangle=-0.2419\|0\rangle+0.9703\|1\rangle$
0	$\|0\rangle$	$\|+\rangle$	659	$\|\psi_{e1}\rangle=0.9681\|0\rangle+0.2504\|1\rangle$

The results in these tables confirm the effectiveness of quantum superposition and rotation in generating unpredictable and secure qubit states for key distribution. The QKD process's resilience against potential surveillance attempts is illustrated by the variations in angles and final qubit states that are present in each node interaction.

5. 3. Key extraction process for each side of a legitimate connection

Once the qubits are processed and exchanged between Alice and her associated nodes, the next phase involves extracting secure keys from the shared quantum states. Each legitimate connection between Alice and the other nodes yields a unique key based on the comparison of their measured qubit states. Table 10 below provides the generated keys for each connection in the network representation, ensuring that only Alice and her intended partner share a secret key, while any interception would be immediately evident due to changes in the quantum state.

Table 10

Generated keys of all connected edges in the network representation of the protocol

Connection	Generated key
Alice and Bob	1001101
Alice and Charlie	0110101
Alice and Dave	1000000
Alice and Elise	1111001

The QKD protocol's successful implementation is demonstrated by the generated keys, which generate unique, secure keys for each connection between Alice and the other nodes. The QKD protocol's scalability in a decentralized full mesh network is confirmed by the established keys, which guarantee that each pairwise connection can establish a secure communication channel independently of the others.

This information shows how well the protocol generates original keys for every connection in the network, thereby guaranteeing that all nodes may interact securely without running key overlap or reuse risk. Since every connection has a unique isolated cryptographic sequence, the approach enhances protection against eavesdropping by producing separate keys. In multi-user quantum networks, where preserving data integrity and secrecy across all connections depends on individual key creation, this structure is very beneficial.

6. Discussion of the outcomes of the QKD protocol based on superposition

The practical applications of the developed protocol include secure communication in critical sectors such as healthcare, government, and finance. The protocol is particularly effective in scenarios requiring decentralized and scalable security solutions against quantum and conventional cyber threats. For instance, it can be deployed to protect electronic health records or secure interbank financial transactions.

In order to improve the security and scalability of multi-user networks, a distributed quantum key based on superposition was designed in this work. Leveraging quantum mechanics ideas to prevent eavesdropping, the proposed protocol guarantees the safe exchange of keys between several nodes in a full mesh network. The results show how well the QKD system can independently create safe keys across several nodes, hence guaranteeing resilience without depending on centralized control.

The efficiency of the qubit preparation process emphasizes the robustness of quantum superposition and rotation in reaching secure communications: this is seen in the interaction between Alice and her corresponding nodes (Bob, Charlie, Dave, and Elise). Tables 2–9 show the special states produced during qubit preparation and rotation, therefore enabling the detection of any interception attempt by means of state perturbation. This helps to stop efforts at illegal access and ensures the integrity of the key exchange system.

The suggested technology offers many advantages in relation to current centralized QKD systems and conventional cryptography techniques. This protocol's distributed character improves resilience and dependability unlike centralized systems, which sometimes include a single point of failure. For example, although centralized methods depending on a single authority to control important distribution are prone to targeted attacks [26], our distributed approach lets each node in the network create safe keys independently, therefore removing this important vulnerability. Post-quantum encryption techniques such as upgraded SSL/TLS protocols also clearly show similar issues whereby centralized components could become points of failure [27].

Moreover, our efforts help to address security issues, especially the weaknesses related to centralized key management and the challenges presented to conventional encryption methods by quantum computing. The main distribution mechanism of the suggested protocol is naturally resistant to both classical and quantum assaults, therefore improving the general security of data communication on the network. As security studies of cyber-physical systems [28] emphasize, the dependence on quantum superposition and state rotation essentially closes the holes found in the centralized models.

Though it has benefits, the research turned up certain limits. The fundamental constraint is the technological complexity required to keep exact synchronization across many of nodes. High-quality quantum hardware is necessary for precise qubit state preparation and rotation; this limits the current usability of the protocol in large-scale practical environments. Furthermore, this study was carried out under ideal circumstances for quantum state transmission, which might not fairly represent the noise and disturbances usually found in practical quantum channels.

Furthermore, lacking in the suggested protocol are some shortcomings. The primary shortfall is from the pragmat-

ic difficulties preserving entanglement at long distances, which might limit system scalability. Furthermore, lacking strong error correcting systems, which are essential in noisy surroundings to enhance important generating efficiency, is the existing implementation. Unless significant technological developments are made, these shortcomings could restrict the viability of implementing the protocol in high-volume communication contexts.

Still, the results of the carried out pragmatic tests highlighted the importance of the suggested distributed network. These tests showed, even under demanding circumstances, distributed key generation utilizing quantum superposition can securely encrypt communications in a multi-user network. The focus on resource economy while preserving security reveals the possible relevance of the protocol in practical situations.

Further research directions include:

– developing a sophisticated synchronization mechanism to enhance coherence and efficiency in full mesh networks;

– implementing robust error correction protocols to improve reliability in noisy quantum channels;

– investigating alternative quantum states, such as entangled states, to enhance key generation and distribution, which could address the challenges related to maintaining entanglement over extended distances.

7. Conclusions

1. A key negotiation process for legitimate nodes in a full mesh decentralized network was successfully developed, demonstrating that secure key exchange can be established autonomously between nodes. The successful implementation of this decentralized approach across multiple network configurations has ensured that each node can independently generate keys without centralized management, thereby enhancing network resilience by eliminating reliance on a central authority.

2. Qubit processing that involved the rotation of qubit states and quantum superposition was effectively executed. The resulting data demonstrated that the unpredictability of qubit states was effectively guaranteed by quantum superposition and random rotations, thereby substantially reducing the risk of eavesdropping.

3. A key extraction process was developed and validated for each side of a legitimate connection, resulting in successful generation of shared secret keys between connected nodes. The experimental results indicated that the proposed key extraction mechanism yielded consistent and dependable results, with all generated keys matching on both sides of the connection. This discovery confirms that the protocol that was devised effectively facilitates secure and efficient key exchange in a multi-user network environment.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

This research 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 KazNRTU named after K. I. Satbayev.

Data availability

Manuscript has no associated data.

Use of artificial intelligence

The authors have used artificial intelligence technologies within acceptable limits to provide their own verified data, which is described in the research methodology section.

References

1. Global Data Breaches and Cyber Attacks in 2024 (2024). IT Governance. Available at: https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024
2. Data generated per day, 2024. Exploding Topics. Available at: https://explodingtopics.com/
3. Rivest, R. L., Shamir, A., Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21 (2), 120–126. https://doi.org/10.1145/359340.359342
4. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134. https://doi.org/10.1109/sfcs.1994.365700
5. Algazy, K., Sakan, K., Khompysh, A., Dyusenbayev, D. (2024). Development of a New Post-Quantum Digital Signature Algorithm: Syrga-1. Computers, 13 (1), 26. https://doi.org/10.3390/computers13010026
6. Wiesner, S. (1983). Conjugate coding. ACM SIGACT News, 15 (1), 78–88. https://doi.org/10.1145/1008908.1008920
7. Brassard, G. (2005). Brief history of quantum cryptography: a personal perspective. IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005., 19–23. https://doi.org/10.1109/itwtpi.2005.1543949
8. Bennett, C. H., Brassard, G. (1984). An Update on Quantum Cryptography. Advances in Cryptology, 475–480. https://doi.org/10.1007/3-540-39568-7_39
9. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67 (6), 661–663. https://doi.org/10.1103/physrevlett.67.661
10. Bennett, C. H., Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 560, 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

11. Muller, A., Herzog, T., Huttner, B., Tittel, W., Zbinden, H., Gisin, N. (1997). "Plug and play" systems for quantum cryptography. Applied Physics Letters, 70 (7), 793–795. https://doi.org/10.1063/1.118224
12. Wang, J., Qin, X., Jiang, Y., Wang, X., Chen, L., Zhao, F. et al. (2016). Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units. Optics Express, 24 (8), 8302. https://doi.org/10.1364/oe.24.008302
13. Mo, X.-F., Zhu, B., Han, Z.-F., Gui, Y.-Z., Guo, G.-C. (2005). Faraday-Michelson system for quantum cryptography. Optics Letters, 30 (19), 2632. https://doi.org/10.1364/ol.30.002632
14. Zhang, C.-H., Zhou, X.-Y., Ding, H.-J., Zhang, C.-M., Guo, G.-C., Wang, Q. (2018). Proof-of-Principle Demonstration of Passive Decoy-State Quantum Digital Signatures Over 200 km. Physical Review Applied, 10 (3). https://doi.org/10.1103/physrevapplied.10.034033
15. Matsumoto, R. (2007). Multiparty quantum-key-distribution protocol without use of entanglement. Physical Review A, 76 (6). https://doi.org/10.1103/physreva.76.062316
16. Razavi, M. (2012). Multiple-Access Quantum Key Distribution Networks. IEEE Transactions on Communications, 60 (10), 3071–3079. https://doi.org/10.1109/tcomm.2012.072612.110840
17. Epping, M., Kampermann, H., Macchiavello, C., Bruß, D. (2017). Multi-partite entanglement can speed up quantum key distribution in networks. New Journal of Physics, 19 (9), 093012. https://doi.org/10.1088/1367-2630/aa8487
18. Yu, K.-F., Gu, J., Hwang, T., Gope, P. (2017). Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing. Quantum Information Processing, 16 (8). https://doi.org/10.1007/s11128-017-1631-x
19. Pivoluska, M., Huber, M., Malik, M. (2018). Layered quantum key distribution. Physical Review A, 97 (3). https://doi.org/10.1103/physreva.97.032312
20. Li, L., Li, Z. (2019). A multi-party quantum key distribution protocol based on phase shift operation. Laser Physics, 29 (10), 105201. https://doi.org/10.1088/1555-6611/ab3845
21. Li, L., Li, Z. (2020). A verifiable multiparty quantum key agreement based on bivariate polynomial. Information Sciences, 521, 343–349. https://doi.org/10.1016/j.ins.2020.02.057
22. Ma, X., Wang, C., Li, Z., Zhu, H. (2021). Multi-Party Quantum Key Distribution Protocol with New Bell States Encoding Mode. International Journal of Theoretical Physics, 60 (4), 1328–1338. https://doi.org/10.1007/s10773-021-04758-4
23. Shan, R.-T., Chen, X., Yuan, K.-G. (2021). Multi-party blind quantum computation protocol with mutual authentication in network. Science China Information Sciences, 64 (6). https://doi.org/10.1007/s11432-020-2977-x
24. Doosti, M., Hanouz, L., Marin, A., Kashefi, E., Kaplan, M. (2024). Establishing Shared Secret Keys on Quantum Line Networks: Protocol and Security. 2024 International Conference on Quantum Communications, Networking, and Computing (QCNC), 176–183. https://doi.org/10.1109/qcnc62729.2024.00035
25. Begimbayeva, Y., Zhaxalykov, T., Makarov, M., Ussatova, O., Tynymbayev, S., Temirbekova, Zh. (2024). Development of a Hybrid Quantum Key Distribution Concept for Multi-User Networks. International Journal of Advanced Computer Science and Applications, 15 (9). https://doi.org/10.14569/ijacsa.2024.0150940
26. Yevseiev, S., Pohasii, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I. et al. (2021). Development of a method for assessing the security of cyber-physical systems based on the Lotka-Volterra model. Eastern-European Journal of Enterprise Technologies, 5 (9 (113)), 30–47. https://doi.org/10.15587/1729-4061.2021.241638
27. Yevseiev, S., Havrylova, A., Milevskyi, S., Sinitsyn, I., Chalapko, V., Dukin, H. et al. (2023). Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies, 3 (9 (123)), 33–48. https://doi.org/10.15587/1729-4061.2023.281795
28. Rasool, A. A., Abbas, N. M., Sheikhyounis, K. (2022). Determination of optimal size and location of static synchronous compensator for power system bus voltage improvement and loss reduction using whale optimization algorithm. Eastern-European Journal of Enterprise Technologies, 1 (8 (115)), 26–34. https://doi.org/10.15587/1729-4061.2022.251760