IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 October 2023, accepted 6 November 2023, date of publication 14 November 2023, date of current version 21 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3333020

TOPICAL REVIEW

Enabling Secure and Trustworthy Quantum Networks: Current State-of-the-Art, Key Challenges, and Potential Solutions

SAMED BAJRIĆ
Laboratory for Open Systems and Networks, Jožef Stefan Institute, 1000 Ljubljana, Slovenia
e-mail: samed@e5.ijs.si

This work was supported in part by the Slovenian Research and Innovation Agency under Grant P2-0037, and in part by the Slovenian Quantum Communication Infrastructure Demonstration (SiQUID) Project through the European Union's Digital Europe Program under Grant 101091560.

ABSTRACT Quantum networks hold the promise of enabling secure and trustworthy communication and computation. However, they also pose significant challenges in terms of security, privacy, and trust. In this paper, we have explored the current state-of-the-art in the field of quantum network security, privacy, and trust, with a focus on quantum key distribution, quantum-resistant cryptography, quantum hacking, trust establishment, and privacy-enhancing technologies. We have identified key challenges and open research questions in these areas, and presented potential solutions to enable the realization of secure and trustworthy quantum networks. As quantum networks continue to evolve, addressing these challenges will be crucial to realizing their full potential for secure communication and computation.

INDEX TERMS Privacy-enhancing technologies, quantum hacking, quantum key distribution, quantum networks, quantum-resistant cryptography.

I. INTRODUCTION

The rapid advancement in quantum communication research has resulted in a significant progress in the field of quantum networking. Quantum networking holds a lot of promise in terms of enhancing the overall functional benefits of the Internet and enabling applications with no counterpart in the classical world. It is a breakthrough technology that could pave the way for an unimaginable future. In a quantum network, the source and destination may be connected by quantum repeaters/routers for facilitating qubit transmissions. The quantum network of the future is envisioned to pervade the entire globe, relying on terrestrial components, satellites, airplanes, ships, and other vehicles. It is anticipated that it will support nearly unconditional security, super-computing power, large network capacity, even at high velocity. This large network capacity, combined with the security features offered by quantum mechanics, has been empirically validated and opens up a new era of communication and computation possibilities that are not feasible within classical network frameworks. For instance, the Beijing-Shanghai Quantum Key Distribution (QKD) network, with a total length exceeding 2,000 km, demonstrates the practical implementation of high-capacity quantum communication over long distances, providing a tangible example of the network's capabilities [50]. Additionally, privacy is a fundamental concern in quantum networking, and these networks are designed with privacy-enhancing technologies to protect sensitive information, further underscoring the potential of quantum networking to revolutionize the way we communicate, compute, and secure our digital interactions.

However, the design of a quantum network presents several challenges that are fundamentally different from those in classical networks [11]. The features of quantum mechanics, such as the Haisenberg's uncertainty principle [9], indistinguishable particles [2], the quantum no-cloning theorem [47], entanglement and superposition [23], pose significant constraints on the design of quantum networks. To realize the promise of quantum networking, the entire protocol stack, spanning from the physical layer enabling

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

techniques to the application layer, requires a dedicated collaborative effort from a large fraction of the engineering and physics community.

Security, privacy, and trust are critical components of any communication network, and quantum networks are no exception. Quantum networks have the potential to provide nearly unconditional security, but the unique features of quantum mechanics also present significant challenges for designing secure and reliable quantum networks. The secure transmission of information in a quantum network requires the use of QKD and quantum-resistant cryptography. However, there are practical limitations to implementing QKD, such as distance limitations, noise, and loss in the transmission channel, which can reduce its effectiveness [39]. Despite the promise of secure key distribution through QKD, quantum networks are not invulnerable. They are susceptible to various forms of hacking and malicious attacks. Adversaries might attempt to exploit weaknesses in the quantum devices or implement sophisticated attack strategies to compromise the network's security [38]. Trust is an indispensable element in the functioning of any communication network. In quantum networks, establishing trust becomes even more challenging. Verifying the correctness and integrity of quantum devices is a complex task [44], as any compromise could have severe consequences for network security. Additionally, detecting attacks or unauthorized access in a quantum network requires advanced monitoring and intrusion detection mechanisms. Privacy is critical for many applications of quantum networks, such as secure communication and data sharing. However, the privacy implications of quantum networks are still being explored.

In this paper, we focus on the critical issues of security, privacy, and trust in the context of quantum networks. Specifically, we explore the challenges and opportunities in quantum key distribution, quantum-resistant cryptography, quantum hacking, trust establishment, and privacy-enhancing technologies. Our goal is to provide a comprehensive overview of the state-of-the-art in quantum network security and privacy, identify the key challenges, and present potential solutions to enable the realization of secure and trustworthy quantum networks.

II. TERMS AND DEFINITIONS

The following terms and definitions are used in the paper:

- **quantum network** - a communication network that utilizes the principles of quantum mechanics to transmit and process information, typically using quantum bits or qubits, which can exist in multiple states simultaneously due to the phenomenon of superposition.
- **quantum key distribution** - a procedure or method for creating and sharing symmetric cryptographic keys, offering information-theoretic security by leveraging the principles of quantum information theory.
- **quantum key distribution protocol** - a set of rules and procedures that enable the secure exchange of cryptographic keys using quantum communication principles.
- **quantum encryption** - a cryptographic technique that leverages the principles of quantum mechanics to secure communication between two parties. It uses quantum properties, such as the superposition and entanglement of quantum bits or qubits, to encode and decode information in a way that is theoretically immune to attacks by classical or quantum computers.
- **quantum signature** - an ultra-secure digital signature generated using quantum principles, ensuring the authenticity and integrity of the messages.
- **quantum firewall** - a theoretical concept for an advanced cybersecurity system that uses quantum computing and communication principles to enhance network security and protect against quantum-based attacks.
- **plug-and play protocol for QKD** - a type of QKD implementation that aims to simplify the deployment of QKD systems by providing easy integration into existing communication networks. They are characterized by their user-friendly setup, allowing users to "plug in" the QKD devices and use them without complex adjustments or calibration, hence the name "plug-and-play."

III. AN OVERVIEW OF THE CURRENT STATE-OF-THE-ART IN THE FIELD OF QUANTUM NETWORK SECURITY, PRIVACY, AND TRUST

A. QUANTUM KEY DISTRIBUTION (QKD)

QKD has been extensively studied in both theoretical and experimental domains over the past few decades. The first QKD protocol was proposed in 1984 by Bennett and Brassard, which is known as the BB84 protocol [4]. Since then, numerous QKD protocols have been proposed, each with different characteristics and the potential for high levels of security. There are two main categories of QKD protocols: prepare-and-measure protocols and entanglement-based protocols [32].

In prepare-and-measure protocols, the sender (Alice) randomly prepares a series of quantum states, typically using one of two non-orthogonal quantum states. She then transmits these states to the receiver (Bob), who performs measurements on the received states. The security of these protocols is based on the no-cloning theorem, which guarantees that an eavesdropper cannot copy the transmitted states without being detected. The most well-known prepare-and-measure protocol is the BB84 protocol, where Alice prepares qubits in one of four possible states (two bases, each with two non-orthogonal states), and Bob randomly chooses measurement bases to determine the final key. These protocols are relatively straightforward to implement and are known for their simplicity.

Entanglement-based protocols, on the other hand, rely on the creation and manipulation of entangled quantum states between Alice and Bob. These entangled states are generated

in a way that ensures any attempt by an eavesdropper to gain information about the key will disrupt the entanglement and be detected. Entanglement-based protocols offer the potential for extremely high levels of security. A well-known entanglement-based protocol is the E91 protocol [16], which utilizes pairs of entangled particles to establish a shared key. However, they can be more complex to implement due to the need for entanglement sources and specialized quantum operations.

While QKD protocols offer the potential for high security levels, it's important to note that achieving formal mathematical proofs for unconditional security is an ongoing research endeavor. Additionally, practical limitations such as distance restrictions, key generation rates, and vulnerability to certain attacks have been identified in some QKD implementations. For example, protocols like the coherent-one-way protocol have specific distance limitations [45]. To address these challenges, there is ongoing research into improving the efficiency, security, and practicality of QKD protocols and systems. Furthermore, researchers are exploring the integration of QKD with classical cryptography, such as hybrid encryption schemes that combine QKD with classical encryption algorithms, to enhance overall security and address practical limitations.

Overall, QKD is a rapidly evolving field, and ongoing research efforts aim to maximize its security potential while addressing real-world constraints.

B. QUANTUM-RESISTANT CRYPTOGRAPHY

Quantum computers have garnered significant attention due to their potential to break many widely used public-key encryption algorithms, such as RSA [48], and Elliptic Curve Cryptography (ECC) [37]. These classical encryption methods rely on the presumed computational difficulty of factoring large numbers or solving discrete logarithm problems, which quantum computers can potentially solve efficiently. Therefore, there has been an extensive research effort to develop new cryptographic algorithms that are resistant to attacks by quantum computers.

One primary approach to quantum-resistant cryptography involves the use of post-quantum cryptographic algorithms. These algorithms are specifically designed to remain secure against attacks by both classical and quantum computers. Post-quantum cryptography encompasses several families of algorithms, including lattice-based, code-based, and hash-based cryptography. Among these, lattice-based cryptography stands out as the most widely studied and promising approach. Schemes like NTRUEncrypt [19] and Kyber [7] have emerged as secure alternatives that withstand quantum attacks.

Another strategy for quantum-resistant cryptography involves the use of quantum cryptographic algorithms that are secure against both classical and quantum adversaries. One example of such an algorithm is the quantum-resistant version of the McEliece cryptosystem [3], which relies on error-correcting codes and is currently considered one of the most promising quantum-resistant cryptosystems.

In addition to algorithm development, considerable research has focused on the practical implementation and standardization of quantum-resistant cryptographic techniques. Notably, the National Institute of Standards and Technology (NIST) has been conducting a Post-Quantum Cryptography Standardization process since 2016 [42]. The objective of this initiative is to identify and select quantum-resistant cryptographic algorithms that will eventually replace the existing public-key encryption and digital signature standards. This standardization effort is crucial to ensuring the adoption of robust security measures in the post-quantum era.

Overall, quantum-resistant cryptography is an active and rapidly evolving field, with ongoing research efforts to develop and standardize new quantum-resistant cryptographic algorithms.

C. QUANTUM HACKING

Quantum hacking [49] refers to attacks on quantum cryptographic systems or classical cryptographic systems that rely on assumptions that are broken by quantum computers. Quantum hacking techniques can be divided into two categories: attacks on quantum key distribution (QKD) systems and attacks on classical cryptographic systems [14], [49].

In the case of QKD systems, quantum hacking attacks typically involve exploiting vulnerabilities within the QKD protocol's implementation. These vulnerabilities may arise due to imperfections in the quantum devices used or sub-optimal classical post-processing algorithms employed. Over recent years, researchers have successfully demonstrated various quantum hacking attacks on QKD systems. These include attacks based on photon number splitting [24], which involves an eavesdropper diverting a portion of the transmitted photons, and time-shifted photon detection [34], where an attacker intercepts and resends photons to gain unauthorized access. It is important to note that while these attacks showcase potential vulnerabilities, they often necessitate a high level of technical expertise and specialized equipment. As of now, they do not pose a significant threat to practical QKD systems.

Quantum hacking extends its reach to classical cryptographic systems, specifically those whose security relies on mathematical assumptions that quantum computers can efficiently break. One example of such an algorithm is Shor's algorithm [5], which can factor large numbers and break RSA and ECC in polynomial time using a quantum computer. However, the current state-of-the-art in quantum computers is not yet sufficient to implement Shor's algorithm on a large scale, and it is uncertain when this will become possible.

Overall, quantum hacking is an area of active research, with ongoing efforts to develop new quantum hacking techniques and defenses against these attacks. As quantum computers continue to develop, the threat posed by quantum

hacking will become more significant, making it essential to continue advancing the field of quantum-safe cryptography.

D. TRUST ESTABLISHMENT

Trust establishment plays a pivotal and multifaceted role in the realm of quantum networks, as the security and reliability of quantum communications hinge on the trustworthiness of network components and the accurate execution of cryptographic protocols. In essence, trust establishment in quantum networks encompasses the following key aspects: verifying the identities of network components, ensuring the integrity of transmitted messages, and proactively detecting and responding to security breaches.

One common approach to trust establishment in quantum networks involves the utilization of trusted third parties (TTPs), such as certification authorities or key distribution centers. TTPs serve as trusted entities responsible for authenticating network components and laying the groundwork for initial trust relationships. However, it's important to acknowledge that this approach may not always be practical or suitable, particularly in decentralized or ad-hoc network scenarios.

An alternative approach to trust establishment within quantum networks leverages the concept of quantum signatures [33]. Quantum signatures are digital signatures that derive their security from the principles of quantum mechanics, offering unconditional security guarantees. These signatures can be employed to authenticate messages and identify potential tampering, providing an additional layer of trust. However, the practical implementation of quantum signatures presents significant challenges, necessitating high-quality quantum sources and precise control over quantum states.

Recent research efforts in trust establishment within quantum networks have been dedicated to the development of innovative protocols and technologies aimed at enhancing both efficiency and security. For instance, a promising proposal put forth in [15] introduces the use of quantum-secure multi-party computation to establish trust within decentralized networks, reducing reliance on TTPs. Additionally, the integration of machine learning and artificial intelligence techniques has been explored as a means to detect and respond to security breaches in quantum networks [28].

Overall, trust establishment in quantum networks remains a dynamic and evolving field, with continuous endeavors to create new protocols and technologies that improve both the efficiency and security of trust establishment mechanisms. As the prevalence of quantum networks continues to grow, trust establishment assumes even greater significance, emphasizing the need for ongoing advancements in this crucial domain.

E. PRIVACY-ENHANCING TECHNOLOGIES

Privacy-enhancing technologies constitute a crucial component of quantum networks, serving to safeguard the confidentiality and integrity of quantum communications while also providing measures to maintain anonymity and unlinkability between communicating parties. These technologies are engineered to thwart unauthorized access, interception, or observation of quantum transmissions, thus ensuring the privacy and security of sensitive information.

One approach to privacy-enhancing technologies in quantum networks is the deployment of quantum encryption. Quantum encryption harnesses the principles of quantum mechanics to encode and decode quantum transmissions, rendering them invulnerable to eavesdropping attempts. The inherent properties of quantum states make it exceedingly challenging for adversaries to intercept or observe quantum transmissions without detection by legitimate parties [38]. Quantum encryption offers the prospect of unconditional security, as any unauthorized access attempt disrupts the quantum states and triggers alarms. However, practical implementation of quantum encryption remains a formidable challenge, demanding high-quality quantum sources and precise control over quantum states.

An alternative strategy for enhancing privacy in quantum networks is the application of classical encryption and authentication techniques. This encompasses symmetric-key cryptography, public-key cryptography, and digital signatures. These techniques can provide strong security for classical communications in quantum networks, but may not be sufficient to protect the privacy of the quantum transmissions. Recent advancements in privacy-enhancing technologies for quantum networks have led to the development of innovative protocols and technologies aimed at enhancing both efficiency and security. For instance, researchers in [35] have introduced a hybrid approach that combines quantum key distribution and classical encryption techniques, offering robust security and privacy protection for quantum communications. Another avenue explores the integration of quantum-secure multi-party computation and zero-knowledge proofs to provide anonymity and unlinkability to quantum transmissions [43].

Overall, privacy-enhancing technologies in quantum networks remain an active area of research, with ongoing efforts to develop new protocols and technologies that can improve the efficiency and security of privacy protection. As quantum networks become more prevalent and sensitive information is transmitted over them, the importance of privacy protection will only continue to grow, making it essential to continue advancing the field in this area.

IV. ADDRESSING KEY CHALLENGES AND IDENTIFYING POTENTIAL SOLUTIONS

A. QUANTUM KEY DISTRIBUTION (QKD)

After analyzing the current state-of-the-art in quantum network security, privacy, and trust, it is clear that QKD is a promising cryptographic technique that allows for secure key generation over a quantum channel. However, several key challenges must be addressed to enable the realization of secure and trustworthy quantum networks:

1) Implementation complexity: The practical implementation of QKD is complex and requires precise control of the quantum communication channels and equipment [27].
2) Channel loss and noise: QKD is sensitive to channel loss and noise, which can cause errors and reduce the range of the communication [41].
3) Eavesdropping attacks: While QKD is theoretically secure against eavesdropping attacks, practical implementations are vulnerable to attacks such as side-channel attacks [1], [8] and Trojan horse attacks [21].
4) Limited range: QKD is currently limited to relatively short distances due to the attenuation of the quantum signals over long distances [20].
5) Scalability: QKD systems must be scalable to support large-scale quantum networks, which requires the development of new technologies and protocols [22].
6) Cost: The cost of QKD systems is currently high compared to classical cryptographic systems, which may limit their adoption in some applications [13].

Considering the current state-of-the-art and the identified key challenges for QKD, the following potential solutions can be explored and implemented to address these challenges and enable the realization of secure and trustworthy quantum networks:

1) Improving QKD protocols: One potential solution is to develop more efficient and robust QKD protocols that can overcome the current limitations of channel loss, noise, and eavesdropping attacks. This can involve the use of novel techniques such as multi-photon sources, entangled photon pairs, and quantum memories to improve the rate and range of QKD.
2) Developing practical QKD systems: Another potential solution is to develop practical QKD systems that can be easily integrated into existing communication infrastructures. The commercial availability of plug-and-play protocols for QKD [30] has already made strides in this direction, simplifying integration and deployment. Looking ahead, there are also some promising avenues for further reducing costs and enhancing the practicality of QKD systems such as utilizing silicon photonics to integrate QKD components or researching quantum dot sources for reliable photon generation.
3) Hybrid QKD solutions: A hybrid QKD solution, combining the best of classical cryptography and quantum key distribution, can be considered to overcome the challenges in implementing QKD at a large scale. Such hybrid solutions can use classical encryption techniques to ensure the security of the message, while using QKD to distribute and refresh the keys.
4) QKD network architectures: Another potential solution is to develop QKD network architectures that can support long-distance QKD over multiple hops. This can involve the use of quantum repeaters, which can amplify and regenerate quantum signals over long distances, or the use of satellite-based QKD to enable global QKD networks.

In addition, the potential solutions identified above can help address the key challenges in implementing QKD and enable the realization of secure and trustworthy quantum networks. However, further research is required to fully explore the feasibility and effectiveness of these solutions in practical quantum network deployments.

B. QUANTUM-RESISTANT CRYPTOGRAPHY

Quantum-Resistant Cryptography faces significant challenges in the realization of secure and trustworthy quantum networks. Some of the key challenges for Quantum-Resistant Cryptography include:

1) Lack of standardized algorithms: Though the NIST has announced the first four algorithms for post-quantum cryptography [31], there is still no consensus on a standardized set of quantum-resistant cryptographic algorithms.
2) Post-quantum security analysis: Many proposed quantum-resistant cryptographic algorithms have not yet undergone sufficient analysis to confirm their security in a post-quantum computing environment [25].
3) Interoperability with existing systems: Quantum-resistant cryptography must be compatible with existing systems and protocols, which may require significant modifications or updates [6].
4) Performance overhead: Many quantum-resistant cryptographic algorithms are computationally intensive and may require significant computational resources, which could affect the performance of systems and applications [6].
5) Quantum computing progress: The progress of quantum computing itself presents a challenge, as the development of more powerful quantum computers could eventually render current quantum-resistant cryptographic algorithms obsolete [10].

To address these challenges and enable the realization of secure and trustworthy quantum networks, several potential solutions are being explored:

1) Standardization of quantum resistant algorithms: Efforts are underway, led by organizations like NIST, to identify and standardize the most promising quantum-resistant cryptographic algorithms.
2) Post-quantum cryptography (PQC): As a promising solution to address the limitations of QKD, PQC has garnered significant attention. PQC is designed to offer resilience against attacks from both classical and quantum computers, making it a compelling choice for securing modern communication networks. Researchers are actively developing and refining quantum-resistant cryptographic schemes, including lattice-based cryptography, code-based cryptography,

and hash-based cryptography. These innovative cryptographic techniques are tailored to withstand the unique threats posed by quantum computers.
3) Hardware-based Solutions: Beyond software-based approaches, there is also research into hardware-based solutions for quantum-resistant cryptography. These solutions, such as hardware security modules and quantum-resistant smart cards [46], aim to provide secure and efficient implementations of post-quantum cryptographic algorithms in practical settings.

In addition, to enable the realization of secure and trustworthy quantum networks, it is crucial to continue research efforts in developing and standardizing post-quantum cryptographic algorithms, integrating them into existing network protocols and architectures, and exploring efficient hardware-based implementations.

C. QUANTUM HACKING

Based on the current state-of-the-art and the existing literature on quantum hacking, a number of key challenges have been identified in this area:

1) Limited availability of quantum computers: Quantum hacking techniques typically require the use of quantum computers, which are currently limited in availability and expensive to build and maintain [12].
2) Noise and error correction: Quantum hacking techniques may be vulnerable to noise and error correction issues [26], which can affect the accuracy and reliability of quantum computations.
3) Complexity of quantum algorithms: Quantum hacking techniques may require the use of complex quantum algorithms [11], which can be difficult to implement and may require significant computational resources.
4) Limited understanding of quantum phenomena: The field of quantum computing and quantum mechanics is still relatively new, and there is much that is not yet fully understood. This can make it challenging to develop and test quantum hacking techniques in a reliable and consistent manner.
5) Rapidly evolving technology: The field of quantum computing and quantum hacking is rapidly evolving, and new breakthroughs and developments are occurring at a rapid pace. Keeping up with these developments and ensuring that hacking techniques remain effective over time can be a significant challenge.

Quantum hacking poses a significant threat to the security of quantum networks. However, the field of quantum security is rapidly advancing, and there are potential solutions that can enable the realization of secure and trustworthy quantum networks. Some of these potential solutions include:

1) Post-quantum cryptography: This involves the development of cryptographic protocols that can withstand attacks from quantum computers.
2) Quantum-resistant key exchange: Researchers are developing new key exchange protocols that can resist attacks from quantum computers. One such protocol is the new hybrid key exchange protocol, which combines classical Diffie-Hellman key exchange with quantum key distribution to provide quantum-resistant key exchange [17].
3) Quantum random number generators: Quantum random number generators are a promising solution for generating truly random numbers that can be used to generate cryptographic keys. These generators are based on the randomness of quantum phenomena, such as the polarization of photons or the position of electrons.
4) Quantum firewall: A quantum firewall is a security mechanism that can detect and prevent quantum hacking attacks. It works by monitoring the state of the quantum network and detecting any attempts to manipulate or intercept quantum information [18].
5) Quantum intrusion detection systems: Quantum intrusion detection systems can be used to monitor the quantum network for any unauthorized access attempts. These systems work by analyzing the quantum signals to detect any anomalies that may indicate a hacking attempt.
6) Quantum error-correcting codes: Quantum error-correcting codes are a promising solution for protecting quantum information from hacking attacks. These codes work by adding redundancy to the quantum information, making it possible to detect and correct errors caused by hacking attempts.

However, further research is needed to improve the efficiency and practicality of these solutions and ensure their suitability for large-scale quantum networks.

D. TRUST ESTABLISHMENT

In the context of quantum networks, trust establishment poses several significant challenges that need to be addressed. Some of the major challenges are:

1) Lack of established standards: There are currently no widely accepted standards for trust establishment in quantum networks, which can make it challenging to develop interoperable and scalable solutions.
2) Limited understanding of quantum phenomena: As with quantum hacking, trust establishment in quantum networks relies on a thorough understanding of quantum mechanics and quantum computing. This understanding is still developing, and there may be aspects of quantum networks that are not yet fully understood.
3) Complexity of quantum protocols: Quantum protocols for trust establishment can be complex, requiring the use of advanced mathematical concepts and techniques. This complexity can make it challenging to develop and implement effective trust establishment mechanisms.
4) Interference from outside sources: Quantum networks can be vulnerable to interference from outside sources,

such as malicious actors or environmental factors [38]. This interference can disrupt trust establishment protocols and compromise the security and reliability of the network.

5) Integration with classical infrastructure: Quantum networks must be integrated with existing classical infrastructure, such as the internet and other communication networks [36]. This integration can introduce additional complexity and challenges for trust establishment, particularly in ensuring that the security of the quantum network is not compromised by vulnerabilities in the classical infrastructure

One potential solution for trust establishment in quantum networks is to develop and deploy trusted hardware and software components that can be used to securely authenticate and authorize network users and devices. This could include the use of secure enclaves, such as Intel SGX or ARM TrustZone [29], to protect critical system components and prevent unauthorized access or tampering. Another approach is to leverage blockchain technology to create a decentralized trust framework for quantum networks. This could involve the use of smart contracts and digital signatures to establish trust between network participants and ensure the integrity of network transactions. Furthermore, it is essential to develop and implement standardized protocols for trust establishment and management in quantum networks. These protocols could incorporate mechanisms for verifying the identity and credentials of network participants, as well as detecting and mitigating attacks on the network. Lastly, ongoing research efforts are needed to identify new and emerging threats to trust in quantum networks and develop effective countermeasures to address these threats. This could involve the development of new cryptographic techniques, as well as the integration of machine learning and artificial intelligence into trust management systems to improve their ability to detect and respond to attacks.

E. PRIVACY-ENHANCING TECHNOLOGIES

It can be observed that the development of privacy-enhancing technologies for quantum networks is fraught with several challenges. Some of the most significant challenges in this context are:

1) Achieving efficient and scalable protocols: One of the main challenges is to develop privacy-enhancing protocols that are efficient and can be implemented on a large scale [22]. This is particularly important for applications that require high-speed data transfers, such as cloud computing and online transactions.
2) Preserving privacy in the presence of quantum attacks: Privacy-enhancing technologies must be designed to withstand quantum attacks, which can potentially compromise the confidentiality and integrity of the communication. Developing quantum-resistant privacy-enhancing technologies is therefore a critical challenge.
3) Balancing privacy and functionality: Another challenge is to strike a balance between privacy and functionality. While strong privacy protection is desirable, it may come at the cost of reduced functionality or usability. Privacy-enhancing technologies must be designed to provide strong privacy protection without compromising the usability of the system.
4) Addressing legal and regulatory challenges: Privacy-enhancing technologies may face legal and regulatory challenges, particularly in the areas of data protection and privacy laws. Developers of these technologies must be aware of these challenges and ensure that their solutions comply with relevant regulations and laws.

The following potential solutions can be proposed:

1) Integration of privacy-preserving mechanisms: Researchers can develop novel privacy-preserving mechanisms that can be integrated with existing quantum network protocols to protect sensitive information from unauthorized access.
2) Multi-party computation (MPC): it is a technique that allows multiple parties to jointly compute a function on their private inputs without revealing their inputs to each other. By integrating MPC into quantum network protocols, sensitive information can be processed securely without revealing it to any single entity.
3) Zero-knowledge proofs (ZKP): ZKPs allow one party to prove to another party that a statement is true without revealing any additional information about the statement. They can be used in quantum network protocols to prove that a party has the right to access certain information without revealing the information itself.
4) Quantum anonymous communication (QAC): it allows parties to communicate with each other anonymously using quantum cryptography. QAC can be used to protect the identity of parties involved in quantum network protocols and ensure the privacy of their communication.
5) Blockchain-based solutions: Blockchain technology can be used to establish trust and security in quantum networks by creating a decentralized and tamper-proof ledger of network transactions [40]. This can help to prevent malicious actors from compromising the network and ensure the integrity of the network's data.

Overall, the above solutions can be used to address the key challenges of privacy-enhancing technologies in quantum networks and enable the realization of secure and trustworthy quantum networks.

V. CONCLUSION

The realization of secure and trustworthy quantum networks is a complex and challenging task that requires the development and integration of multiple technologies and solutions. The current state-of-the-art in quantum network security, privacy, and trust provides promising approaches for achieving this goal, including quantum key distribution,

quantum-resistant cryptography, trust establishment, and privacy-enhancing technologies. However, these approaches also face significant challenges such as the scalability, efficiency, and robustness of the solutions, as well as the potential for new types of quantum-based attacks. Addressing these challenges and advancing the state-of-the-art in quantum network security will require collaboration and innovation from researchers, industry experts, and policymakers. With continued effort and investment, we can work towards realizing the full potential of quantum networks in enabling secure and trustworthy communication and computation in the digital age.

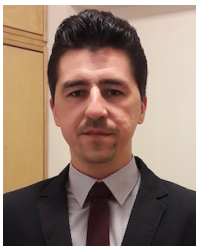
ACKNOWLEDGMENT

The author Samed Bajrić extend his sincere appreciation to the anonymous reviewers whose valuable insights and constructive feedback greatly enhanced the quality and rigor of this paper. Their meticulous review and thoughtful suggestions contributed significantly to shaping the final version of this work. He is also grateful for their time, expertise, and dedication in reviewing this manuscript.

REFERENCES

[1] P. Arteaga-Díaz, D. Cano, and V. Fernandez, "Practical side-channel attack on free-space QKD systems with misaligned sources and countermeasures," *IEEE Access*, vol. 10, pp. 82697–82705, 2022.
[2] A. Bach, "The concept of indistinguishable particles in classical and quantum physics," *Found. Phys.*, vol. 18, no. 6, pp. 639–649, Jun. 1988.
[3] D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), vol. 5299, J. Buchmann and J. Ding, Eds. Cincinnati, OH, USA: Springer, Oct. 2008.
[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. Int. Conf. Comput., Syst. Signal Process.*, 1984, pp. 175–179.
[5] V. Bhatia and K. R. Ramkumar, "An efficient quantum computing technique for cracking RSA using Shor's algorithm," in *Proc. IEEE 5th Int. Conf. Comput. Commun. Autom. (ICCCA)*, Greater Noida, India, Oct. 2020, pp. 89–94.
[6] N. Bindel, U. Herath, M. McKague, and D. Stebila, "Transitioning to a quantum-resistant public key infrastructure," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), T. Lange and T. Takagi, Eds., vol. 10346. Utrecht, The Netherlands: Springer, Jun. 2017.
[7] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle, "CRYSTALS–kyber: A CCA-secure module-lattice-based KEM," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2018, pp. 353–367.
[8] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130502.
[9] P. Busch, T. Heinonen, and P. Lahti, "Heisenberg's uncertainty principle," *Phys. Rep.*, vol. 452, no. 6, pp. 155–176, 2007.
[10] G. T. Byrd and Y. Ding, "Quantum computing: Progress and innovation," *Computer*, vol. 56, no. 1, pp. 20–29, Jan. 2023.
[11] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, 2nd Quart., 2022.
[12] M. T. Dejpasand and M. S. Ghamsari, "Research trends in quantum computers by focusing on qubits as their building blocks," *Quantum Rep.*, vol. 5, no. 3, pp. 597–608, Sep. 2023.
[13] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Inf.*, vol. 2, no. 1, p. 16025, Nov. 2016.
[14] C. Ding, S. Wang, Y. Wang, Z. Wu, J. Sun, and Y. Mao, "Machine-learning-based detection for quantum hacking attacks on continuous-variable quantum-key-distribution systems," *Phys. Rev. A, Gen. Phys.*, vol. 107, no. 6, Jun. 2023, Art. no. 062422.
[15] Y. Dulek, A. Grilo, S. Jeffery, C. Majenz, and C. Schaffner, "Secure multi-party quantum computation with a dishonest majority," in *Advances in Cryptology—EUROCRYPT 2020*. Zagreb, Croatia: Springer, May 2020, pp. 729–758.
[16] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.
[17] D. Fischer, "Quantum diffie–hellman key exchange," Cryptol. ePrint Arch., Paper 2021/1279, 2021.
[18] D. Harlow and P. Hayden, "Quantum computation vs. firewalls," *J. High Energy Phys.*, vol. 2013, no. 6, Jun. 2013, Art. no. 85, doi: 10.1007/JHEP06(2013)085.
[19] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, "Choosing parameters for NTRUEncrypt," Cryptol. ePrint Arch., Paper 2015/708, 2015.
[20] B. Huttner, R. Alléaume, E. Diamanti, F. Fröwis, P. Grangier, H. Hübel, V. Martin, A. Poppe, J. A. Slater, T. Spiller, W. Tittel, B. Tranier, A. Wonfor, and H. Zbinden, "Long-range QKD without trusted nodes is not possible with current technology," *npj Quantum Inf.*, vol. 8, no. 1, Sep. 2022, Art. no. 108, doi: 10.1038/s41534-022-00613-4.
[21] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Risk analysis of trojan-horse attacks on practical quantum key distribution systems," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 168–177, May 2015.
[22] W. Kozlowski and S. Wehner, "Towards large-scale quantum networks," in *Proc. 6th Annu. ACM Int. Conf. Nanosc. Comput. Commun. (NANOCOM)*, Dublin, Ireland, Sep. 2019, pp. 1–7.
[23] T. Li and Z.-Q. Yin, "Quantum superposition, entanglement, and state teleportation of a microorganism on an electromechanical oscillator," *Sci. Bull.*, vol. 61, no. 2, pp. 163–171, Jan. 2016.
[24] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack," *New J. Phys.*, vol. 4, pp. 44.1–44.9, Jul. 2002.
[25] J. P. Mattsson, B. Smeets, and E. Thormarker, "Quantum-resistant cryptography," 2021, *arXiv:2112.00399*.
[26] D. McMahon, "Quantum noise and error correction," in *Quantum Computing Explained*. Wiley, 2008, pp. 251–278.
[27] M. Mehic, O. Maurhart, S. Rass, and M. Voznak, "Implementation of quantum key distribution network simulation module in the network simulator NS-3," *Quantum Inf. Process.*, vol. 16, no. 10, p. 253, Oct. 2017.
[28] H. A. Al-Mohammed, A. Al-Ali, E. Yaacoub, U. Qidwai, K. Abualsaud, S. Rzewuski, and A. Flizikowski, "Machine learning techniques for detecting attackers during quantum key distribution in IoT networks with application to railway scenarios," *IEEE Access*, vol. 9, pp. 136994–137004, 2021.
[29] M. A. Mukhtar, M. K. Bhatti, and G. Gogniat, "Architectures for security: A comparative analysis of hardware security features in Intel SGX and ARM TrustZone," in *Proc. 2nd Int. Conf. Commun., Comput. Digit. Syst. (C-CODE)*, Mar. 2019, pp. 299–304.
[30] A. Müller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "'Plug and play' systems for quantum cryptography," *Appl. Phys. Lett.*, vol. 70, no. 7, pp. 793–795, 1997.
[31] (Jul. 2022). *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*. [Online]. Available: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
[32] A. I. Nurhadi and N. R. Syambas, "Quantum key distribution (QKD) protocols: A survey," in *Proc. 4th Int. Conf. Wireless Telematics (ICWT)*, Nusa Dua, Indonesia, Jul. 2018, pp. 1–5.
[33] Y. Pelet, I. V. Puthoor, N. Venkatachalam, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, Ž. Samec, M. Stipčević, R. Ursin, E. Andersson, J. G. Rarity, D. Aktas, and S. K. Joshi, "Unconditionally secure digital signatures implemented in an eight-user quantum network," *New J. Phys.*, vol. 24, no. 9, Sep. 2022, Art. no. 093038.
[34] B. Qi, C.-H.-F. Fung, H.-K. Lo, and F.-X. Ma, "Time-shift attack in practical quantum cryptosystems," *Quantum Inf. Comput.*, vol. 7, nos. 1–2, pp. 73–82, Jan. 2007.
[35] S. Ren, Y. Wang, and X. Su, "Hybrid quantum key distribution network," *Sci. China Inf. Sci.*, vol. 65, no. 10, Oct. 2022, Art. no. 200502.
[36] J. Rabbie, K. Chakraborty, G. Avis, and S. Wehner, "Designing quantum networks using preexisting infrastructure," *npj Quantum Inf.*, vol. 8, no. 1, p. 5, Jan. 2022.
[37] M. Roetteler, M. Naehrig, K. M. Svore and K. Lauter, "Quantum resource estimates for computing elliptic curve discrete logarithms," in *Advances in Cryptology—ASIACRYPT 2017*. Hong Kong, China: Springer, Dec. 2017, pp. 241–270.

[38] T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, M. Hajdušek, and R. V. Meter, "Attacking the quantum Internet," *IEEE Trans. Quantum Eng.*, vol. 2, pp. 1–17, 2021.
[39] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: Real implementation problems," *Theor. Comput. Sci.*, vol. 560, no. 1, pp. 27–32, Dec. 2014.
[40] P. Sharma, K. Choi, O. Krejcar, P. Blazek, V. Bhatia, and S. Prakash, "Securing optical networks using quantum-secured blockchain: An overview," *Sensors*, vol. 23, no. 3, p. 1228, Jan. 2023.
[41] V. Sharma, K. Thapliyal, A. Pathak, and S. Banerjee, "A comparative study of protocols for secure quantum communication under noisy environment: Single-qubit-based protocols versus entangled-state-based protocols," *Quantum Inf. Process.*, vol. 15, no. 11, pp. 4681–4710, Nov. 2016.
[42] *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process, Official Call for Proposals*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Dec. 2016. [Online]. Available: http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-final-dec-2016.pdf
[43] K. Sutradhar and H. Om, "An efficient simulation for quantum secure multiparty computation," *Sci. Rep.*, vol. 11, no. 1, p. 2206, Jan. 2021.
[44] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, "Resource-efficient verification of quantum computing using Serfling's bound," *npj Quantum Inf.*, vol. 5, no. 1, Apr. 2019, Art. no. 27.
[45] R. Trényi and M. Curty, "Zero-error attack against coherent-one-way quantum key distribution," *New J. Phys.*, vol. 23, no. 9, Sep. 2021, Art. no. 093005.
[46] Q. Wang, D. Wang, C. Cheng, and D. He, "Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 1, pp. 193–208, Jan. 2023.
[47] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.
[48] B. Yan et al., "Factoring integers with sublinear resources on a superconducting quantum processor," 2022, *arXiv:2212.12372*.
[49] Y. Zhao, C.-H.-F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 4, Oct. 2008, Art. no. 042333.
[50] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng and J.-W. Pan, "Large scale quantum key distribution: Challenges and solutions," *Opt. Exp.*, vol. 26, no. 18, pp. 242–260, 2018.



SAMED BAJRIĆ is currently a Researcher with the Laboratory for Open Systems and Networks, Jožef Stefan Institute. Over the years, he has established himself as a prominent figure in the field of cryptology. He has dedicated significant efforts toward the design and analysis of cryptographic Boolean functions, which are fundamental in ensuring the security and robustness of cryptographic systems. In recent years, he has also delved into the realm of quantum cryptography, exploring its potential implications and applications in the ever-evolving landscape of cryptographic research. His research interest includes cryptology, with a specific focus on symmetric-key cryptography.