УДК 004.056.55+530.145(083.73)
DOI: 10.31673/2409-7292.2024.020013

Berestiana T.

RESEARCH IN THE FIELD OF QUANTUM-SAFE CRYPTOGRAPHY

Quantum computing, based on the principles of quantum mechanics, is rapidly gaining momentum as a promising field of information technology. However, with the growing capabilities of quantum computing comes a new level of cybersecurity. Quantum-secure cryptography is emerging as a response to the potential threats posed by quantum computers to traditional cryptographic methods. The main goal of quantum-secure cryptography is to ensure the security of data in information systems, as quantum computing becomes more and more accessible. In this study, we thoroughly studied the essence of quantum-secure cryptography, its fundamental principles and applications. We have explored the advantages and limitations of this new cryptographic paradigm and discussed the potential challenges that arise in the context of its implementation. In addition, we analyzed the current state of research in the field of quantum-secure cryptography and highlighted the prospects for further development of this intriguing technology. We have researched potential threats and possible ways to solve them. Additionally, we reviewed a quantum risk assessment methodology that helps identify and manage threats in the context of quantum security. Finally, we trace existing examples and recent developments in the field of quantum-secure cryptography, revealing their potential to improve information security in the future. Overall, the research allows for a better understanding of the importance and prospects of quantum-secure cryptography in today's digital world.

Ключові слова*:* Quantum computing, cryptography, encryption, Quantum Key Distribution.

Introduction

Quantum computing, based on the principles of quantum mechanics, is rapidly gaining momentum as a promising field of information technology. Its computational power unlocks a wide range of possibilities that were previously considered unattainable with classical computing systems. However, along with the growing capabilities of quantum computing comes a new level of cybersecurity. Quantum-safe cryptography emerges as a response to the potential threats posed by quantum computers to traditional cryptographic methods. It offers new algorithms and protocols specifically designed to protect information from quantum attacks. The primary goal of quantum-safe cryptography is to ensure the security of data in information systems as quantum computing becomes increasingly accessible [1].

In this research, I have thoroughly examined the essence of quantum-safe cryptography, its fundamental principles, and applications. I have explored the advantages and limitations of this new cryptographic paradigm and discussed potential challenges that arise in the context of its implementation. Additionally, I have analyzed the current state of research in the field of quantum-safe cryptography and highlighted the prospects for further development of this intriguing technology.

What is cryptography and what types of cryptography exist today

Cryptography is the practice of using encoding algorithms, hashes, and signatures to protect information. Information can be stored (for example, a file on a hard disk), transmitted (for example, electronic communication exchanged between two or more parties), or used (during data computation). Cryptography employs various low-level cryptographic algorithms to achieve one or more goals of information security. These tools include encryption algorithms, digital signature algorithms, hash algorithms, and other functions.

Symmetric encryption is a widely used method of encrypting data, in which a single secret key is used for both encryption and decryption of data. Symmetric encryption is one of the most common encryption methods and one of the oldest, dating back to the times of the Roman Empire. The Caesar cipher, named after Julius Caesar, who used it to encrypt his military correspondence, is a well-known historical example of symmetric encryption. Symmetric encryption encrypts and decrypts data using either a stream cipher or a block cipher. Modern stream ciphers transform plaintext into ciphertext one byte at a time, while block ciphers transform entire units or blocks of plaintext using a pre-defined key length (such as 128, 192, or 256 bits). Senders and receivers transmitting data to each other using symmetric encryption must know the secret key so that the sender can encrypt the data they intend to share with the receiver, and the receiver can decrypt and read the encrypted data provided, along with any other necessary encrypted responses [2].

Popular examples of symmetric encryption include
- Data Encryption Standard (DES);
- Triple Data Encryption Standard (Triple DES);
- Advanced Encryption Standard (AES);
- International Data Encryption Algorithm (IDEA);
- SSL protocol.

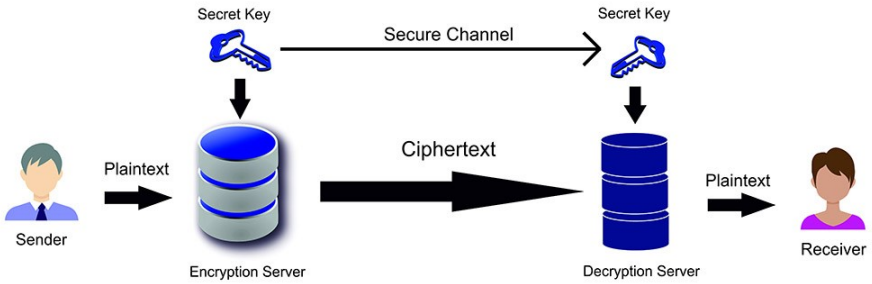

Fig. 1. "Symmetric Cryptography" [2]

Asymmetric encryption, also known as public-key encryption, is a relatively new method compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt plaintext. The exchange of secret keys occurs over the Internet or a large network, ensuring that attackers cannot abuse the key. It is important to note that anyone with the key can decrypt the message, so asymmetric encryption uses two related keys to enhance security. The public key is free for anyone who wants to send you a message. The second private key is kept secret and known only to you. Messages encrypted with the public key can only be decrypted with the private key, and messages encrypted with the private key can only be decrypted with the public key. The security of public keys is not necessarily required, as they are publicly accessible and can be transmitted over the Internet. Asymmetric keys provide much better security for transmitted information during communication [3].

Examples of asymmetric encryption include:
- Rivest-Shamir-Adleman (RSA);
- Digital Signature Standard (DSS), which includes the Digital Signature Algorithm (DSA);
- Elliptic Curve Cryptography (ECC);
- Diffie-Hellman key exchange method;
- TLS/SSL protocol;

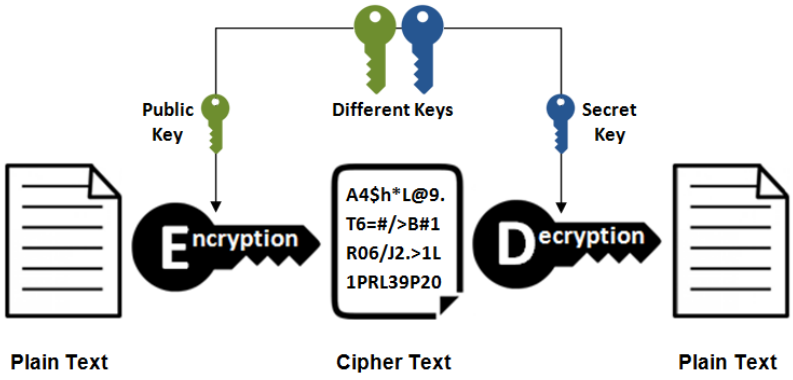

Fig. 2. "Asymmetric Cryptography" [3]

© Berestiana, T. (2024). Research in the Field of Quantum-Safe Cryptography. Сучасний захист інформації, 2(58), 109–116. https://doi.org/10.31673/2409-7292.2024.020013.

What is Quantum Cryptography and Post-Quantum Cryptography?

Post-Quantum Cryptography (PQC) is an advancement of classical cryptography. Like classical cryptography, PQC is based on mathematical problems. However, PQC extends the properties of classical cryptography to quantum computers. To achieve this, PQC employs more complex mathematical problems that are considered impossible to solve even by quantum machines. The fact that both classical and post-quantum systems rely on mathematical problems leads to an interesting advantage: PQC solutions can be easily implemented in code and deployed to any device through software updates. While most post-quantum cryptosystems are asymmetric (public-key), symmetric cryptosystems have also been developed. The reason why PQC systems tend to be asymmetric lies in the fact that symmetric cryptography is not so vulnerable to quantum computing. In asymmetric cryptography, the secret key is mathematically related to the public key. This means that, with sufficient computational power, a hacker can derive the secret key from the public key (which is visible to everyone). This is impossible on a classical computer, but with a quantum machine, it becomes very easy. Hackers can use your public key as an entry point into your corporate network. Symmetric algorithms do not have this weakness because encryption and decryption keys never become public. That's why most PQC algorithms are currently asymmetric or public-key [4].

Like post-quantum cryptography, the goal of quantum cryptography is to protect data from quantum threats. However, the mechanism is very different. Quantum cryptography (sometimes referred to as quantum cryptology) is based on physics and utilizes the properties of quantum mechanics to protect data. Quantum cryptography leverages the unpredictable nature of matter at the quantum level for message encryption and decryption, ensuring communication security. While information in classical and post-quantum cryptography is encoded in bits, quantum cryptography uses quantum bits. In this sense, quantum cryptography resembles quantum computing. The most well-known example of quantum computer cryptography is Quantum Key Distribution (QKD), which allows two parties to exchange data securely, unbreakably, and without eavesdropping. Unlike other methods, QKD helps communicating parties detect eavesdropping attempts. Due to the properties of quantum mechanics, such as the no-cloning theorem, hackers cannot directly measure data transmitted through QKD connections. Furthermore, if a hacker attempts to directly measure data transmitted through QKD connections, errors will occur in the quantum bits, immediately alerting the communicating party that the connection is compromised. Additionally, quantum cryptography theoretically can withstand increases in computational power of quantum computers. Regardless of how powerful a quantum computer becomes; it is believed that quantum cryptography will never be breached. Since computational power cannot violate the laws of physics, quantum cryptography is protected by the laws of nature itself. With this in mind, it is important to emphasize the "theoretical" nature of QKD when considering its advantages. Poor implementation of QKD is much less secure than PQC; establishing a QKD communication channel requires careful configuration and appropriate hardware. In terms of hardware, QKD requires special optical fiber connections and photon emitters for sending and receiving encrypted data. Building QKD infrastructure at an enterprise scale can cost millions of dollars. Software updates cannot provide standard QKD in infrastructure, and dedicated hardware channels are a prerequisite for QKD. However, some quantum cybersecurity service providers are working on digital alternatives to QKD. These alternatives retain the beneficial characteristics of standard QKD but are much easier to deploy [5, 6].

What Problems May Arise Due to the Development of Quantum Cryptography and How They Can Be Solved

The potential impact of quantum computing on many industries, especially those requiring complex problem-solving and data processing, is immense. However, the greatest breakthrough potential of quantum computing lies in their ability to challenge existing approaches to cryptography. Cryptography heavily relies on mathematical problems that are currently difficult or impossible to solve using conventional computing. With their powerful computational capabilities, quantum computing can undermine existing cryptographic approaches and pose significant security risks to many systems, including blockchain technology. Failure to prepare for quantum threats creates

© Berestiana, T. (2024). Research in the Field of Quantum-Safe Cryptography. Сучасний захист інформації, 2(58), 109–116. https://doi.org/10.31673/2409-7292.2024.020013.

significant security risks, and organizations cannot afford to ignore the importance of implementing PQC solutions.

At the core of RSA cryptography, a widely used public-key cryptosystem, lies the complexity of factoring large prime numbers. Many digital security protocols rely on this cryptographic technique. Quantum computers can break the RSA cipher much faster than conventional computers, and algorithms specifically designed for quantum computers, such as Shor's algorithm, can quickly solve the prime factorization problem, jeopardizing the security provided by the RSA cipher.

Cryptographic hash functions, such as SHA-256, are essential for ensuring data integrity and authentication. They are widely used in a broad range of cryptographic applications, including blockchain. While hash functions are considered resistant to quantum attacks, they are not entirely secure. Collision attacks, such as Grover's algorithm, theoretically can expedite the process of identifying input data in hashes, though not as significantly as their impact on RSA or ECC.

The National Institute of Standards and Technology (NIST) has played a key role in the development and standardization of PQC algorithms. Recognizing the quantum threat at an early stage, NIST initiated a process of solicitation, evaluation, and standardization of one or more post-quantum cryptographic algorithms. The goal is not only to develop algorithms that can withstand quantum attacks but also to make them efficient and easy to implement.

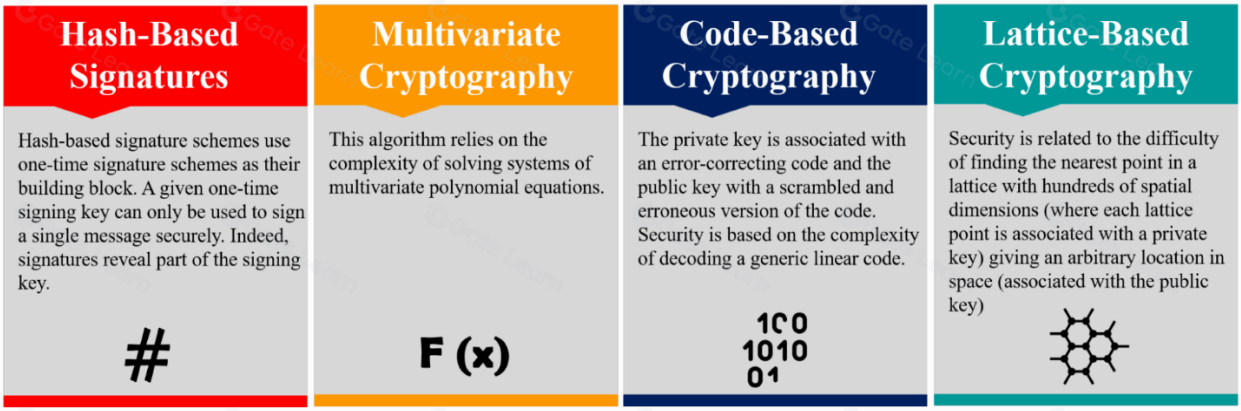

Figure 3 "NIST algorithms"

From the many submissions received, NIST selected seven algorithms based on different cryptographic approaches for further evaluation. According to recent data, four algorithms show great promise:

Lattice-based cryptography: These algorithms are based on the lattice problem of finding the shortest or closest vector in a multi-dimensional lattice. They are difficult to solve even on a quantum computer. Examples include the Learning With Errors (LWE) problem and its variants.

Code-based cryptography: An algorithm derived from error-correcting codes and based on the difficulty of decoding general linear codes. It has been studied for decades and is known for its resistance to quantum attacks.

Multivariate polynomial cryptography: An algorithm that solves systems of multivariate polynomials. It is attractive due to its efficiency and small key size.

Hash-based cryptography: Utilizes hash functions to create digital signatures. The security of these algorithms depends on the resistance of the hash function to collisions, pre-image attacks, and second pre-image attacks.

Quantitative Risk Assessment Methodology

Quantum risk assessment provides organizations with the necessary knowledge to understand the extent of quantum cyber risk and the timeframes within which quantum threats may arise. This gives organizations a basis for proactively responding to quantum risks, building a path to a quantum-safe state, and implementing and testing quantum-safe solutions as part of regular lifecycle management, rather than as a crisis reaction. Quantum Risk Assessment (QRA) does not replace

© Berestiana, T. (2024). Research in the Field of Quantum-Safe Cryptography. Сучасний захист інформації, 2(58), 109–116. https://doi.org/10.31673/2409-7292.2024.020013.

traditional Cyber Risk Assessment (RA). QRA is typically conducted concurrently with or after traditional RA, as some of the information gathered during RA is also needed in quantum processes. However, QRA focuses on specific security issues arising in quantum computing and does not address some aspects of the traditional assessment process. Several years ago, Mosca proposed a model for assessing quantum risk. The six-phase QRA process described below aligns with risk assessment models such as those of NIST and includes Mosca's "x, y, z" quantum risk model [7, 8].

Phase 1: "Identification and Documentation of Information Assets and their Current Cryptographic Protection"

Like any other risk assessment, QRA begins with an inventory of critical assets. Primary focus is given to confidential or valuable information assets that need protection through cryptography according to the organization's security policy. It's important to identify the nature of cryptography used, methods of cryptographic key generation, storage, and application, as well as sources of tools and devices used in these processes.

Phase 2: "Investigation of the State of Quantum Computers and Quantum-Safe Cryptography. Evaluation of the Availability Timing of these technologies. Impact on the development and verification of quantum-safe cryptography"

This stage is not specific to any particular QRA but rather for a group of quantum technology experts who will use the information to understand the challenges and advancements facing certain areas of quantum research, forecast possible delivery timelines for quantum computers, and understand the impact on the organization's cybersecurity. Current processes that can be utilized. There are groups worldwide conducting original research and applying different approaches to developing quantum computers and quantum-safe cryptography. It's important to have access to experts who can monitor developments in both fields and analyze them to predict their impact on cybersecurity. Ideally, the results of this stage of QRA will influence the development of quantum-safe cryptography. Working with quantum experts who have close ties to the academic and research community, real-world problems identified by QRA can influence the direction of quantum security research.

Phase 3: "Identification of Threat Actors and Assessment of the Time Required for them to Access Quantum Technology 'z'"

Any security-conscious organization will be aware of all threats to its most critical assets and will have a list of previous attempts to penetrate their cyber defenses. The report will consider the likelihood of these threats being able to leverage quantum computers, and During QRA, attention will be focused on the timeframes within which these threats could leverage quantum computers, and the impact of quantum computers on these threats will be considered. It's also necessary to consider new threat actors that may emerge after quantum computers become a reality. Together, they constitute part of the Collapse Time(z) model by Mosca, which is the time required for modern cyber defenses to collapse before threats with access to quantum technologies. This process also requires ongoing assessment by experts knowledgeable about cybersecurity and quantum computing developments.

Phase 4: "Determining the Lifespan of Your Assets 'x' and the Time Required to Transition the Organization's Technical Infrastructure to a Quantum-Safe State 'y'"

Determining the lifespan of business information is crucial for understanding an organization's quantum vulnerability. How long will encrypted information remain valid if intercepted and archived by an adversary? This depends on the nature of the business, product, customer, and regulatory requirements applicable to the organization. Evaluate the tools available to counter quantum threats. How effective are current policies and procedures for protecting the organization's encrypted information from internal and external threats? Study the strength of existing cryptographic methods and how effectively they are applied and utilized. Explore available quantum-safe cryptographic methods and determine if they can replace existing cryptographic methods. Consult with suppliers whose products the organization uses to determine if new algorithms and protocols can be integrated into existing tools and devices or if hardware upgrades are necessary. Assess whether quantum security can be integrated into IT lifecycle management processes in the organization by analyzing

© Berestiana, T. (2024). Research in the Field of Quantum-Safe Cryptography. Сучасний захист інформації, 2(58), 109–116. https://doi.org/10.31673/2409-7292.2024.020013.

the policies, management, and procurement processes applied to the organization's IT infrastructure and security infrastructure. With this information, the remaining values of the Mosca model can be calculated, namely the organization's data retention period (x) and the transition time to the new infrastructure (y).

Phase 5: "Determining Quantum Risk by Calculating Whether Business Assets Will Become Vulnerable Before the Organization Can Protect Them (x+y>z?)"

Using the information gathered to date, risks organizations face when implementing quantum computers can be assessed. The lifespan of confidential data, including the potential for leakage, is considered. This is compared to the period during which quantum technologies will be available to relevant threat actors. Together, they can provide a reasoned assessment of when organizations need to take proactive measures to reduce quantum risks. Depending on the lifespan of the data and current data protection processes, some organizations may already face this risk. The next step is to assess the impact of expected changes on business processes [9].

Phase 6: "Identifying and Prioritizing Measures Needed to Support Awareness and Transitioning the Organization's Technologies to a Quantum-Safe State"

Quantum risk assessments provide information and recommendations regarding the current state of quantum security, but it is unlikely that this state can be achieved with tools and technologies available today. Quantum technologies continue to evolve, as does understanding the strengths and weaknesses of quantum security approaches. Transition plans must also keep pace with these changes, as suppliers incorporate these developments into their products and tools. It is important to be aware of all this, and most organizations should have a plan to address immediate concerns and be able to adopt new quantum technologies as they become available.

Existing Examples and Latest Developments in Quantum-Safe Cryptography

iMessage with PQ3: The new state of the art in quantum-secure messaging at scale

On February 21, 2024, Apple Security Engineering and Architecture (SEAR) announced the most significant update to cryptographic security in the history of iMessage with the introduction of PQ3, a revolutionary post-quantum cryptographic protocol that enhances the current level of end-to-end secure messaging. Thanks to its breakthrough encryption resistant to breaches and extensive protection against even highly sophisticated quantum attacks, PQ3 becomes the first messaging protocol to achieve what is referred to as level 3 security, providing a level of protection that surpasses that of all other widely deployed messaging applications. To the best of our knowledge, PQ3 boasts the strongest security properties of any messaging protocol worldwide [10].

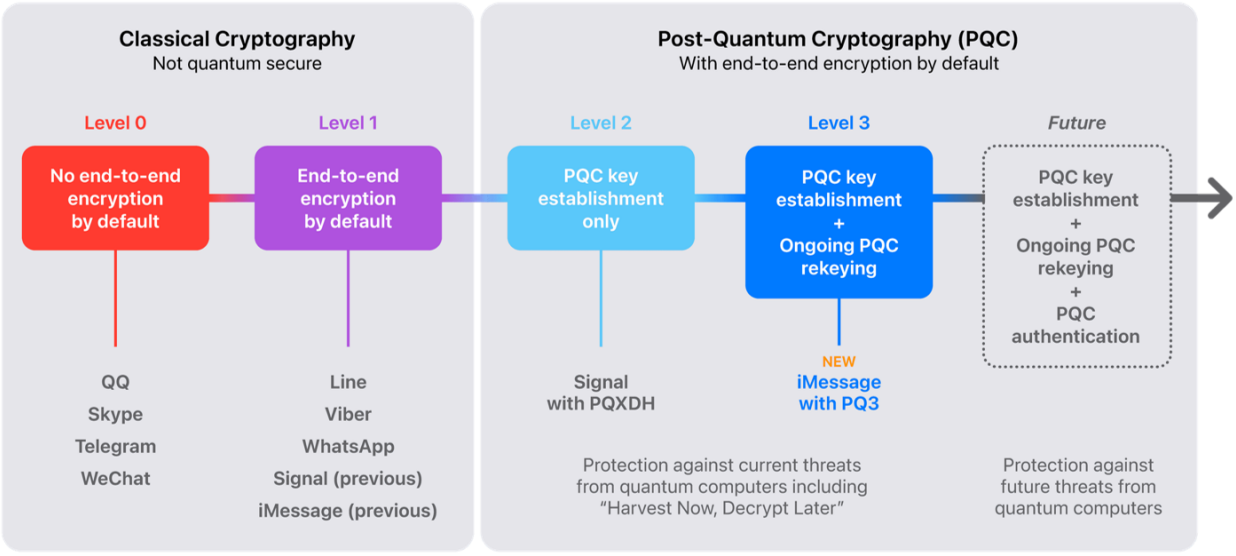

Fig. 4. "Quantum-secure Cryptography in Messaging Apps"

In recent years, significant innovations have emerged in the field of end-to-end message encryption, including post-quantum encryption using the PQXDH protocol from Signal and key transparency through the Auditable Key Directory from WhatsApp. Building on its legacy as the first widely adopted messaging app offering end-to-end encryption by default, iMessage continues to provide enhanced security that surpasses existing systems. iMessage Contact Key Verification is the most advanced and widely deployed key transparency system in the world, representing the latest achievement in automated key verification. Additionally, the new cryptographic protocol iMessage PQ3 combines post-quantum key establishment with three state-of-the-art mechanisms for recovering compromised keys, setting the global contemporary standard for message protection against HarvestNow, DecryptLater attacks, and future quantum computers.

An important step towards improved quantum computers by Google

First published in October 2022, their article "Non-Abelian vertex entanglement in a superconducting processor" is now featured in Nature, so they are pleased to share peer-reviewed findings. This work reports the first observation of non-Abelian exchange behavior. Non-Abelian anyons could pave the way for quantum computations, where researchers perform quantum operations by exchanging particles around each other, much like strings exchanging around each other, creating braids. Implementing this novel exchange behavior on a superconducting quantum processor could offer an alternative path to so-called topological quantum computing, which is immune to noise from the surrounding environment, a major challenge for quantum computing today [11].

Advancing science: Microsoft and Quantinuum demonstrate the most reliable logical qubits on record with an error rate 800x better than physical qubits

Here's why today is such a historic moment: for the first time in history, we are transitioning from basic level 1 to robust level 2 quantum computing. We are now entering the next stage of addressing significant challenges with reliable quantum computers. Microsoft's qubit virtualization system, which filters and corrects errors, combined with the Quantinuum hardware, demonstrates the largest gap between physical and logical error rates recorded to date. This is the first demonstrated system with four logical qubits that improves the level of logical error compared to the physical by such a large order. Importantly, they can now also diagnose and correct errors in logical qubits without destroying them − this is called "active syndrome extraction." This represents a huge leap forward for the field as it ensures more reliable quantum computing. With this system, they have conducted over 14,000 individual experiments without any errors [12].

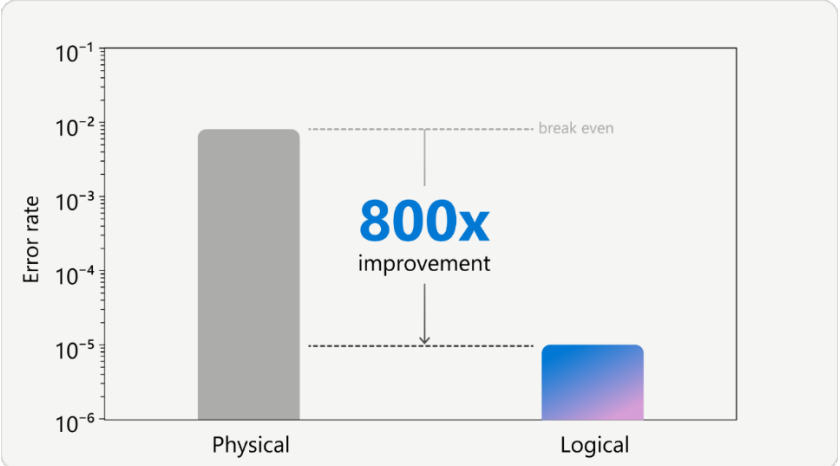

Fig. 5. "The largest gap between physical and logical error rates"

Conclusion

In conclusion to the research, I have explored a wide range of aspects related to this innovative field of cryptography. Specifically, I have analyzed the concept of cryptography and its various types,

© Berestiana, T. (2024). Research in the Field of Quantum-Safe Cryptography. Сучасний захист інформації, 2(58), 109–116. https://doi.org/10.31673/2409-7292.2024.020013.

including modern methods of information protection. Furthermore, I delved into the essence of quantum cryptography and its role in ensuring security in the face of threats associated with the development of quantum computing. By examining the challenges that may arise due to this development, I have investigated potential threats and possible ways to address them. Additionally, I have reviewed the methodology of quantum risk assessment, which helps identify and manage threats in the context of quantum security. Finally, I have traced existing examples and recent developments in the field of quantum-safe cryptography, revealing their potential to enhance the level of information protection in the future. Overall, the research allows for a better understanding of the importance and prospects of quantum-safe cryptography in the modern digital world.

References

1. What is Cryptography? https://aws.amazon.com/what-is/cryptography/
2. Brett, Daniel. (2021). Symmetric vs. Asymmetric Encryption: What's the Difference? https://www.trentonsystems.com/en-us/resource-hub/blog/symmetric-vs-asymmetric-encryption
3. Nikita, Gupta. (2022). Symmetric vs. Asymmetric Encryption – What are differences? https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
4. What Are The Differences between Classical, Quantum and Post-Quantum Cryptography? https://www.quantropi.com/differences-between-classical-quantum-post-quantum-cryptography/
5. Quantum Resistance and the Signal Protocol. https://signal.org/blog/pqxdh/
6. Post-Quantum Cryptography in Blockchain Security. https://www.gate.io/uk/learn/articles/post-quantum-cryptography-in-blockchain-security/1061
7. Strategy: Quantum Risk Assessment And Data Protection. https://cybersecurityventures.com/strategy-quantum-risk-assessment-and-data-protection/
8. Michele Mosca, John Mulholland. A Methodology for Quantum Risk Assessment. (2017) https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/
9. Secure socket layer application program apparatus and method. https://patents.google.com/patent/US5657390
10. iMessage with PQ3: The new state of the art in quantum-secure messaging at scale. (2024) https://security.apple.com/blog/imessage-pq3/
11. Trond, Andersen, Yuri, Lensky. (2023). An important step towards improved quantum computers. https://blog.google/technology/research/an-important-step-towards-improved-quantum-computers/
12. Jason, Zander. (2024). Advancing science: Microsoft and Quantinuum demonstrate the most reliable logical qubits on record with an error rate 800x better than physical qubits. https://blogs.microsoft.com/blog/2024/04/03/advancing-science-microsoft-and-quantinuum-demonstrate-the-most-reliable-logical-qubits-on-record-with-an-error-rate-800x-better-than-physical-qubits/

Надійшла 21.05.2024