THE NEXT DIGITAL ERA: POST-QUANTUM CRYPTOGRAPHY

Zoltán Rajnai, PhD
Donát Bánki Faculty of Mechanical and Safety Engineering, Óbuda University
Budapest, Hungary

Attila Nagy, PhD Student[1]
Doctoral School on Safety and Security Sciences, Óbuda University
Budapest, Hungary

INTRODUCTION

A Chinese study claimed that by 2025, quantum computers will be able to crack the RSA algorithm. (B. Yan et al., 2022) If this is true, people's privacy or countries' data will be in big trouble, and we may have to stop communicating on the Internet. Our economies have switched to fast communication, which is why this would be a big break for societies. Fortunately, a year later, another study refuted the Chinese study, having showed that we would not be able to crack RSA encryption by 2025 (Khattar & Yosri, 2023). This is a great relief for us, but still, we have to be careful and prepare for Q-day. The SNDL attack is also a source of danger. SNDL (Store Now, Decrypt Later) attack is one of the most significant threats that arise in connection with the development of quantum technologies. In this attack method, attackers currently collect and store data with the goal of hacking it later when quantum computers are available. This can be especially dangerous for data that requires long-term secrecy, such as military or state secrets. (*Quantum Computing: The Growing Threat Of SNDL*, 2024) We don't know how to defend against this attack. Countries and organizations are still spying to find out who is doing what. We assume that there will still be surprises in this area in the future. Investing in the development of quantum technologies requires significant resources. Investments in quantum research and development of some major countries are presented below. The US has invested billions of dollars in quantum research, including the National Quantum Initiative (NQI), which provided $1.2 billion in funding over five years. (The National Quantum Initiative Supplement to the President's FY 2024 Budget, 2023) China devotes significant resources to the development of quantum technologies, having invested more than 15 billion dollars in the establishment of the National Quantum Computing Science and Technology Center. (*How Is China Investing in Quantum Technology?*, 2023) Russia announced an investment of 790 million dollars in the development of quantum technologies by 2024. (*Russian Scientists Expect A 50-Qubit Quantum Computer By End Of 2024*, 2024) The European Union has invested 1 billion euros in the Quantum Flagship program, which supports quantum research and innovation for ten years. Since 2018, the EU and its member states have spent more than 8 billion euros on quantum technologies. (*European Industry Is yet to Embrace the Potential of Quantum Technologies,* 2024) Based on these statistics, it can be seen that the great powers of the world are devoting serious resources to the development of quantum technologies, realizing their potential. Developments are taking place in many areas, such as materials science, cyber security, as well as pharmaceutical research and artificial intelligence. These efforts could bring significant breakthroughs in many aspects of technology. In the following

1 attila.nagy@bgk.uni-obuda.hu

section of the paper, we present which algorithms have been compromised and which may become the new standard, so that our societies are prepared for the Q-Day.

ALGORITHMS

Rivest-Shamir-Adleman Algorithm

In cryptography, there are three main types of encryption methods: symmetric algorithms, asymmetric algorithms, and hash functions. RSA encryption was published in 1977 by RL Rivest, A. Shamir, and L. Adleman. The name RSA came from the initials of the researchers' names (Rivest-Shamir-Adleman). The RSA encryption algorithm is an asymmetric encryption process or method. In the RSA algorithm, messages are encrypted using the public key, and only the owner of the private key can decrypt them. This is the basis of asymmetric encryption methods. The special feature of the RSA encryption algorithm is that publishing the public key does not mean publishing the private key, which has two important consequences. First, it is not necessary to use couriers or other secure means to transmit the keys, since the message can be encrypted with the recipient's public key, and only he can decrypt it with his own private key. Second, a message can be "signed" with the private key, and anyone can verify this signature with the public key. Signatures cannot be forged, and the signer cannot later deny the validity of the signature. This can also be useful in electronic correspondence and electronic financial transactions. In the RSA encryption process, a message is represented as a number that is raised to a publicly specified power and then the remainder is taken with another publicly specified number that is the product of two large secret primes. Decryption is done in a similar way, but a different, secret power is used. Part of the security of RSA is based on the difficulty of factoring the published number.

Details of the RSA Algorithm

The message is encrypted with a public key consisting of a pair of numbers (e, n), where n is the product of two large primes. Encryption is done as follows: the message is represented as a number, then it is raised to the e power and the remainder is divided by n. Decryption is done with the private key, which consists of another pair of numbers (d, n), where d is a specially chosen number.

In practice, when using the RSA algorithm, each user publishes their public key while keeping their private key secret. Anyone can use the public key to encrypt the message, but only the owner of the private key can decrypt it. The RSA algorithm was a major advance in cryptography as it enabled secure communication without the need for keys to be transmitted securely and enabled the use of digital signatures that could be authenticated and non-repudiated. (Rivest et al., 1978)

Elliptic Curves

Elliptic curve cryptography (ECC) is one of the strongest and most efficient techniques in modern cryptography. The strength and efficiency of ECC is based on the use of mathematical operations that work with elliptic curves. ECC is more secure than many other cryptographic methods and plays a prominent role in the security of web and mobile applications. The encryption system of ECC consists of the following elements: the plaintext, the key and the secret text. The key can be public, private, or partially public and partially private. When generating the keys for ECC, we randomly choose two points on the elliptic curve and determine the private and public keys. ECC encryption and decryption is based on mathematical operations that use curve addition and multiplication. The advantages

of ECC include greater security and shorter key lengths, which require less storage space and enable faster operations. The ECC key is 256 bits long, which provides the same security as a 3072-bit RSA key. The disadvantage of ECC is its calculation requirement, which results in low efficiency. ECC is used in many fields, such as the Elliptic Curve Digital Signature Algorithm (ECDSA) and the SM2 algorithm. ECDSA enables the creation and authentication of digital signatures that ensure data integrity and authenticity. Elliptic curve cryptography is one of the most important modern cryptographic methods, providing greater security than many other encryption methods. ECC can be further improved through the development of accelerators and algorithms, and it can be effectively used in many application areas. (Y. Yan, 2022)

Diffie – Hellman Key Exchange Algorithm

The Diffie-Hellman key exchange algorithm, developed by Whitfield Diffie and Martin Hellman and published in 1976, showed new directions in the field of cryptography. The goal of this study was to develop new types of cryptographic systems that minimize the need for secure key distribution channels and are equivalent to written signatures.

Key exchange: Two parties can generate a shared key by exchanging public information that cannot be decrypted by a third party.

Public key system: The encryption and decryption keys are separate, so the encryption key can be made public without compromising the decryption key.

Digital signatures: Allows messages to be authenticated in such a way that the encryption key is public, while the key needed to create the signature remains private.

The problems of cryptography began to be solved in parallel with the theoretical development of communication and computer science. The security of cryptography largely depends on how computationally demanding the determination of the decryption key is. This problem falls into the fields of computational complexity and algorithm analysis, which examine the difficulty of solving computational problems. The Diffie-Hellman algorithm and their publication showed new directions in cryptography, enabling secure communication without the need for secure transmission of keys and promoting the use of digital signatures that could be authenticated and not forged. (Diffie & Hellman, 1976)

Shor's algorithm is dangerous for all three encryption methods mentioned above. In the next section, the Peter Shor algorithm is presented.

Shor's Algorithm

Peter Shor first presented his algorithm in 1994, offering an efficient solution for prime factorization and discrete logarithms for quantum computers. The basis of the algorithm is the quantum Fourier transform and the superposition of quantum states. The most important steps and concepts are Quantum Fourier Transform, Superposition and Interference, Prime Factorization, Discrete Logarithms. Quantum Fourier transform: The Quantum Fourier transform (QFT) is the basic tool of the Shor algorithm. This enables the rapid transformation of quantum states, which greatly increases the computational speed compared to classical computers. Superposition and Interference: The algorithm uses quantum mechanical properties such as superposition and interference to perform computational tasks. Through superposition, the quantum computer manages several possible states at the same time, while interference helps to choose the correct solution. Prime factorization: The Shor algorithm can efficiently determine the prime factors of a large number. This compromises the security of tradi-

tional RSA encryption, as RSA relies on the difficulty of factoring integers. Discrete logarithms: The algorithm can also be used to solve the discrete logarithm problem, which forms the basis of many other cryptographic systems such as elliptic curves and Diffie-Hellman key exchange. The importance of the Shor algorithm lies in the fact that it showed that quantum computers can fundamentally change the security basis of current cryptographic protocols. Although practical quantum computers are still under development, the theoretical foundations already demonstrate the potential applicability and future challenges in the field of cryptography. (Shor, 1997)

QUANTUM COMPUTERS

Quantum computers are computers that use the phenomena of quantum mechanics to perform computational tasks. Their basic unit is the quantum bit (qubit), which can be both 0 and 1 at the same time due to the principle of quantum superposition. This property allows quantum computers to perform multiple calculations in parallel, significantly increasing their computing capacity compared to classical computers. A quantum bit, or qubit, is a quantum mechanical system that can take two states: |0 ” and |1 ”. However, superposition can take any linear combination of them, such as a|0 ” + b|1 ”, where a and b are complex numbers and |a|^2 + |b|^2 = 1. This ability is the basis of parallel computing, which is one of the most important advantages of quantum computers. Another basic principle of the operation of quantum computers is entanglement, which allows a quantum mechanical connection to develop between two or more qubits. Its intertwined states of qubits are connected, so a change in the state of one qubit immediately affects the state of another qubit, regardless of their distance. This entanglement enables the efficiency and speed of quantum algorithms. In 1982, Richard Feynman explained that quantum mechanical simulations could make calculations more efficient by overcoming the limitations of classical computers. In 1994, Peter Shor published his algorithm, which showed that quantum computers can efficiently factorize large numbers, which fundamentally shook classical encryption systems. In 1996, Grover developed a fast database search algorithm that demonstrated further applications of quantum computers. The development of quantum computers involves many technical challenges, such as making qubits fault-tolerant and maintaining stable quantum states over long periods of time. Currently, Google, IBM, Intel and Rigetti are leading the development of multi-qubit systems, but these machines are not yet widely available to the public. Quantum computers can make significant advances in solving complex problems such as factorization, search algorithms, molecular modeling, and cryptography. Quantum algorithms can perform special tasks more efficiently than classical algorithms. For example, the Shor algorithm is suitable for factoring large numbers, while the Grover algorithm is suitable for fast database searches. These algorithms use a series of quantum gates that form quantum circuits. Quantum computers have significant potential to increase computing capacity and develop new cryptographic methods, although the technology is still in its early stages of development. Quantum computers are innovative devices that can significantly increase computing capacity by utilizing the principles of quantum mechanics. Through superposition and entanglement, they perform parallel computations and provide new possibilities in many areas such as cryptography and modeling of complex systems. The technology is still developing, but quantum computers are already attracting a lot of interest from the scientific community and the technology industry. (Amundson & Sexton-Kennedy, 2019; Ishita Ray, 2011; Yanofsky, 2007)

POST-QUANTUM CRYPTOGRAPHY

Quantum encryption and post-quantum cryptography are part of quantum communication, but they are separate fields. Post-quantum cryptography (PQC) is also called quantum-safe or quantum-resistant cryptography. Quantum encryption includes a quantum key distribution (QKD) and associated protocols such as BB84 or B92. This also includes quantum networks. (Nagy & Rajnai, 2024) Post-quantum cryptography will be presented in detail below.

The National Institute of Standards and Technology (NIST) is an agency of the US government whose main task is to define and maintain technological and scientific standards. For example, NIST is responsible for maintaining a digital library of mathematical functions and popularizing the metric system in the United States. The emergence of quantum computers poses a serious challenge to current cryptographic systems. To address this, NIST announced a competition in 2016 to develop and standardize post-quantum cryptographic standards. This competition is currently ongoing and seeks to find new cryptographic algorithms that can withstand the threats posed by quantum computers. NIST's third round report examines various types of post-quantum cryptography based on different mathematical problems to provide protection against quantum computers. Four algorithms were standardized, and four other algorithms advanced to the next round. We will now move on to deal with the family of encryption algorithms and describe the four standardized algorithms. (Alagic et al., 2022)

Lattice-based Cryptography: Lattice-based cryptography is based on the mathematical structures of grids, where the grid points are located in a space. These systems often use problems like Shortest Vector Problem (SVP) and Learning With Errors (LWE), which prove difficult to solve even for quantum computers. Such algorithms offer a high level of security and are highly scalable, which is why they are popular in post-quantum cryptography. Code-based Cryptography: Code-based cryptography is based on error-correcting codes, such as Goppa codes. One of the best-known code-based cryptosystems is McEliece, a cryptosystem that provides strong protection against attacks by quantum computers. These algorithms have been known and studied for decades and have proven to be very secure, although they often have large public key sizes. Multivariate Cryptography: Multivariate cryptography uses multivariate polynomials as the basis for encryption and signature schemes. Such systems are usually fast and efficient, but their security depends heavily on the complexity of the polynomials. Rainbow and Unbalanced Oil and Vinegar (UOV) algorithms are examples of multivariate cryptographic methods. Hash-based Cryptography: Hash-based cryptography uses the properties of hash functions for secure communication and data protection. One of the best-known hash-based signature schemes is based on Merkle trees, which enable efficient and secure digital signatures. SPHINCS+ is an example of a hash-based signature algorithm that can be considered quantum secure. Isogeny-based Cryptography: Isogeny-based cryptography is based on isogenies of elliptic curves, which are difficult to calculate even for quantum computers. One of the best-known examples of this type of cryptography is Supersingular Isogeny Key Exchange (SIKE), which has a small key size and high security. These algorithms are of particular interest in quantum-resistant key exchange protocols. Non-commutative Cryptography: Non-commutative cryptography is based on non-commutative algebras such as quaternions or certain groups. These systems use structures in which the order of elements matters, which can provide special security advantages. This type of cryptography is still relatively new and an area of research, but it offers promising possibilities in quantum-resistant cryptography, although the non-commutative cryptography type did not make it to the third or fourth round. Each of these different types of cryptography offers different advantages and challenges, and together they provide the diversity and robustness of post-quantum cryptography. (Alagic et al., 2022) Now let us look at the four standardized algorithms.

CRYSTALS- Kyber

CRYSTALS-Kyber is the key encapsulation mechanism (KEM) selected by NIST in the post-quantum cryptography standardization process. The algorithm is based on the Modulated Learning with Errors (MLWE) problem, which offers significant efficiency advantages over similar schemes based on MLWE. Kyber is an IND-CPA-secure public key cryptography (PKE) scheme that is transformed into an IND-CCA-secure KEM using a Fujisaki-Okomoto-type transformation. The basic PKE scheme comes from the MLWE problem, which is defined in a cyclotomic power-of-2 ring. The rank of the module can be k = 2, 3 or 4, which corresponds to the security categories (1, 3, 5). Other parameters of Kyber include an integer modulus q = 3329 and a public matrix of polynomials generated from a uniformly random 256-bit string. In the Kyber encryption process, a message is encrypted using a polynomial vector, then the result is encoded using another polynomial vector and adding an error product. During decryption, the secret key is used to recover the message after the ciphertext is properly "decompressed". Kyber inherits a strong theoretical security foundation from the decade-long literature of grid-based cryptography. The MLWE problem has been widely studied, and there is evidence that increasing the rank of a module improves performance without significantly degrading security. Kyber uses a variant of the FO transformation to achieve IND-CCA security, and its security proofs are tight in the ROM model and not tight in the Quantitative Random Oracle Model (QROM). Kyber offers fast key generation, encapsulation and decapping in a software environment. A number of optimization works have been done on the software and hardware implementations of Kyber, showing excellent performance in both environments. Kyber's key and ciphertext sizes are acceptable for most applications, and its performance is outstanding in FPGA implementations. Overall, based on security and performance data, Kyber is an excellent choice for post-quantum cryptographic environments that NIST wants to standardize. (Alagic et al., 2022)

CRYSTALS- Dilithium

CRYSTALS-Dilithium is the digital signature algorithm selected by NIST in the post-quantum cryptography standardization process. This algorithm is based on a combination of grid-based cryptography and the Fiat-Shamir paradigm, which has strong security and performance characteristics. The Dilithium algorithm is built around the ring Rq: = Zq [X]/ (X256 + 1), where q is a prime number. The public key basically consists of a Modulated Learning with Error (MLWE) pattern of the form (A, t: = As1 + s2), where A is a matrix in the ring Rq and s1 and s2 are error vectors. A distinctive feature of Dilithium is that the error vectors use a uniform distribution, as opposed to the truncated Gaussian distribution typically used. Dilithium is the "Fiat-Shamir with aborts" approach introduced by Lyubashevsky. This procedure uses a three-message lattice-based authentication scheme that allows the prover to convince the verifier that he has the secret key (s1, s2) without revealing it. In the signature scheme, the prover generates a vector consisting of the higher order bits of Ay. The verifier randomly chooses a polynomial, then the prover responds with the vector z: = y + cs1 may leak information from s1, so careful sampling steps are required to ensure its coefficients are of the correct magnitude. The security of Dilithium starts from the decision Module-LWE assumption, which ensures that the public key does not leak information about the private key. Additional assumptions, such as SelfTargetMSIS, allow Dilithium to be strongly unforgeable in the QROM. Dilithium offers several parameter settings that increase security, although increased security sometimes results in larger keys and slower performance. Dilithium uses pseudo randomness and truncated storage techniques to improve performance. The elements of Rq are computed and stored using an NTT-based implementation for fast polynomial multiplication. Along with FALCON, Dilithium is one of the most effective signature

protocols of the third round. FALCON generally offers shorter keys and signatures, although Dilithium does not require floating-point arithmetic, which may be beneficial for some implementations. CRYSTALS-Dilithium is an efficient, relatively easy-to-implement signature scheme with a strong theoretical security foundation and an encouraging cryptanalytic history. It is an excellent choice for a wide range of cryptographic applications and was therefore selected by NIST as the primary signature algorithm for standardization. (Alagic et al., 2022)

FALCON

FALCON (Fast Fourier Lattice-based Compact Signatures over NTRU) is a grid-based digital signature scheme based on the "hash-and-sign" paradigm. FALCON was selected by NIST for its post-quantum cryptographic standardization process, especially for applications with low bandwidth and fast authentication requirements. FALCON follows the Gentry, Peikert and Vaikuntanathan (GPV) framework introduced in 2007. This framework uses grid-based trapdoor functions to generate signature schemes using preimage sampling. FALCON uses NTRU lattices, which are generated in the following form: the secret key consists of polynomials (f, g, F, G ∈ Z[x] / (x^n + 1)) satisfying fG - gF ≡ q relationship. The public key is h = g/f. The FALCON trapdoor preimage sampling algorithm is relatively complex and requires floating-point arithmetic, which can be challenging for secure implementations. FALCON's data structures, such as the FALCON tree, add further complexity but ensure compact public key and signature sizes. The theoretical security of FALCON is based on the difficulty of the SIS problem over NTRU grids. FALCON is probably unfalsifiable in the QROM. The FALCON core's SVP safety is conservatively estimated to be similar to that of Dilithium. Certain desired "beyond tamperproof" security features are not offered by FALCON but can be added with a simple transformation with minimal performance loss. Among the third-round digital signature schemes, FALCON offers the smallest bandwidth (public key and signature size combined). Signature verification is fast, while signature generation is slightly slower compared to Dilithium, and key generation is significantly slower. Due to its low bandwidth and fast authentication, FALCON can be advantageous in certain limited protocol scenarios. FALCON was chosen for standardization because NIST trusts its security (provided it is implemented correctly) and because its low bandwidth may be essential in some applications. FALCON's low bandwidth and fast authentication make it an ideal choice for applications where bandwidth and authentication speed are critical. (Alagic et al., 2022)

SPHINCS+

SPHINCS+ is the digital signature algorithm chosen by NIST, which is hash-based and stateless. This algorithm provides excellent security based solely on the security of symmetric primitives, thus providing a robust defense against quantum computers. SPHINCS+ combines single signatures, multiple signatures, Merkle trees, and hypertrees to create a general-purpose digital signature scheme. One of its most important features is that it does not require state preservation between different signatures, in contrast to other hash-based signature schemes, which are faster and result in smaller signatures, but require state management. SPHINCS+ is based on three different hash functions: SHAKE256, SHA-256 and Haraka. The cryptographic security of SPHINCS+ is based solely on the security of the underlying hash functions. This security assumption is independent of other finalist signature schemes such as Dilithium and FALCON, so SPHINCS+ can serve as a useful backup in case of unexpected cryptanalytic attacks. However, the complexity of the algorithm can be a problem for implementation security, and evaluating the security of the entire system can be more difficult for a more complex algorithm. SPHINCS+ key generation and verification is much faster than signature genera-

tion. SPHINCS+ public keys are very short, but signatures are relatively long. Even at security category 1, the signature with the smallest and slowest parameters is around 8 KiB, much larger than alternative signature schemes such as FALCON or Dilithium. At the beginning of the third round, new parameters were chosen for security categories 1 and 3. Also, during the third round, a bug was discovered in SPHINCS+'s security reduction, which was fixed. Two attacks have surfaced that challenge the SHA-256-based versions of SPHINCS+ Category 5 security parameters. The first attack occurred in February 2021, and a month later the SPHINCS+ team proposed a fix. The second attack was disclosed in April 2022 and similarly affected SHA-256-based parameters, but the previously proposed patch did not resolve the issue. SPHINCS+ was chosen for standardization because this algorithm provides the necessary security, although it is larger and slower than grid-based signatures. SPHINCS+ is a mature scheme that provides an alternative solution for defense against quantum computers, minimizing the risk that any cryptanalytic breakthrough will leave NIST without a viable signature scheme. (Alagic et al., 2022)

Algorithms that Made it to the Fourth Round

Based on NIST's third round report, the following algorithms remained in the competition for the fourth round. These algorithms are undergoing further evaluation and analysis before final standardization decisions are made.

BIKE (Bit Flipping Key Encapsulation):

It is based on binary linear quasi-cyclic medium density parity check codes (QC-MDPC). It was originally designed to use ephemeral keys, but it is said to work with static keys as well. It rests on a strong theoretical foundation and has proven resistant to many attacks. (Alagic et al., 2022)

Classic McEliece:

It is based on traditional code-based cryptography that uses Goppa codes. It is characterized by a high level of security and has been studied for a long time. It is secure as it is resistant to quantum attacks and is supported by well-known cryptanalytic results. (Alagic et al., 2022)

HQC (Hamming Quasi-Cyclic):

Based on error correcting codes and quasi-cyclic structures, it offers good performance in both software and hardware environments. It is based on a solid theoretical foundation and many attack scenarios have been considered in its evaluation. (Alagic et al., 2022)

SIKE (Supersingular Isogeny Key Encapsulation):

It is based on isogenies of elliptic curves. It offers small key sizes, which can be beneficial in certain applications. It is based on special mathematical problems that are currently resistant to quantum computer attacks. (Alagic et al., 2022)

For the sake of transparency, we have compiled the standardized algorithms, those awaiting standardization and those that have been eliminated from the competition in a table.

Table 1. *Post-Quantum Cryptography*

NIST competition	Algorithms	Encryption family	Category
Winner of round 3	CRYSTALS- Kyber	Grid-based Cryptography	SPY
Winner of round 3	CRYSTALS- Dilithium	Grid-based Cryptography	Digital signature
Winner of round 3	FALCON	Grid-based Cryptography	Digital signature
Made it to the 4th round	Classic McEliece	Code-based Cryptography	Public key encryption
Made it to the 4th round	BIKE	Code-based Cryptography	SPY
Made it to the 4th round	HQC	Code-based Cryptography	SPY
Fell out	Rainbow	Multivariate Cryptography	Digital signature
Winner of round 3	SPHINX +	Hash-based Cryptography	Digital signature
Made it to the 4th round	SIKE	Isogeny-based Cryptography	SPY

CONCLUSION

The paper discusses the challenges associated with the advent of quantum computers and the importance of post-quantum cryptography. Advances in quantum technologies could have a major impact on current cryptographic systems, especially the RSA encryption algorithm, which some predict quantum computers will be able to break by 2025.

SNDL (Store Now, Decrypt Later) is a method of an attack wherein attackers currently collect and store data with the goal of hacking it later when quantum computers become available. This is especially dangerous for information requiring long-term secrecy, such as military or state secrets.

The importance of global investments is also detailed in the study. The USA, China, Russia and the European Union are devoting significant resources to quantum research and development. The United States, for example, has invested $1.2 billion over five years under the National Quantum Initiative (NQI) program. China has earmarked more than $15 billion for the establishment of the National Quantum Computing Science and Technology Center. Russia has announced an investment of 790 million dollars by 2024, while the European Union has invested 1 billion euros in the Quantum Flagship program.

The post-quantum cryptographic algorithms that NIST (National Institute of Standards and Technology) standardized the third round are the following four: CRYSTALS- Kyber, CRYSTALS- Dilithium, FALCON and SPHINCS+. Four other algorithms - Classic McEliece, BIKE, HQC and SIKE - remained in the competition for the fourth round. These algorithms are based on various mathematical problems, providing protection against quantum computers.

The paper describes in detail the different types of cryptography and their advantages, and presents the algorithms selected by NIST and their properties. Finally, it emphasizes the importance of post-quantum cryptography for future secure communication and privacy.

REFERENCES

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022). *Status report on the third round of the NIST Post-Quantum Cryptography Standardization process* (NIST IR 8413; p. NIST IR 8413). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8413

Amundson, J., & Sexton-Kennedy, E. (2019). Quantum Computing. *EPJ Web of Conferences*, *214*, 09010. https://doi.org/10.1051/epjconf/201921409010

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

European industry is yet to embrace the potential of quantum technologies. (2024). https://sciencebusiness.net/news/quantum-computing/european-industry-yet-embrace-potential-quantum-technologies#:~:text=In%202018%2C%20the%20EU%20launched,results%20closer%20to%20industrial%20exploitation.

How is China Investing in Quantum Technology? (2023). https://www.azoquantum.com/Article.aspx?ArticleID=435

Ishita Ray. (2011). *Quantum Computing*. https://doi.org/10.13140/2.1.1021.7286

Khattar, T., & Yosri, N. (2023). *A comment on "Factoring integers with sublinear resources on a superconducting quantum processor."* https://doi.org/10.48550/ARXIV.2307.09651

Nagy, A., & Rajnai, Z. (2024). Introduction to Quantum Communication. *INNOVATIVE TECHNOLOGIES IN THE DIGITALIZATION ENVIRONMENT OF HIGHER EDUCATION : PROBLEMS AND SOLUTIONS-2024 (2024) Pp. 559-563. , 5 p.*

NATIONAL QUANTUM INITIATIVE SUPPLEMENT TO THE PRESIDENT'S FY 2024 BUDGET. (2023).

Quantum Computing: The Growing Threat Of SNDL. (2024). https://www.cybersecurityintelligence.com/blog/quantum-computing-sndl-threats-are-increasing-7427.html

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

Russian Scientists Expect A 50-Qubit Quantum Computer By End Of 2024. (2024). https://thequantuminsider.com/2024/02/24/russian-scientists-expect-a-50-qubit-quantum-computer-by-end-of-2024/#:~:text=Initially%20part%20of%20a%20project,over%20the%20next%20five%20years.

Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, *26*(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

Yan, B., Tan, Z., Wei, S., Jiang, H., Wang, W., Wang, H., Luo, L., Duan, Q., Liu, Y., Shi, W., Fei, Y., Meng, X., Han, Y., Shan, Z., Chen, J., Zhu, X., Zhang, C., Jin, F., Li, H., … Long, G.-L. (2022). *Factoring integers with sublinear resources on a superconducting quantum processor*. https://doi.org/10.48550/ARXIV.2212.12372

Yan, Y. (2022). The Overview of Elliptic Curve Cryptography (ECC). *Journal of Physics: Conference Series*, *2386*(1), 012019. https://doi.org/10.1088/1742-6596/2386/1/012019

Yanofsky, N. S. (2007). *An Introduction to Quantum Computing* (arXiv:0708.0261). arXiv. http://arxiv.org/abs/0708.0261