Mankovskyy, S. V. (2024). Post-Quantum Cryptography trends and perspectives. *Actual Issues of Modern Science. European Scientific e-Journal, 29*, 7-14. Ostrava: Tuculart Edition, European Institute for Innovation Development.

DOI: 10.47451/inn2024-03-01

The paper is published in Crossref, ICI Copernicus, BASE, Zenodo, OpenAIRE, LORY, Academic Resource Index ResearchBib, J-Gate, ISI International Scientific Indexing, ADL, JournalsPedia, Scilit, EBSCO, Mendeley, and WebArchive databases.

Spartak V. Mankovskyy, Candidate of Technical Sciences (Ph.D.), Senior Lecturer, Department of Radioelectronic Devices and Systems, Institute of Telecommunications, Radioelectronics and Electronic Engineering, Lviv Polytechnic National University. Lviv, Ukraine.
ORCID: 0009-0008-5217-6290, Scopus ID: 36021406800

Post-Quantum Cryptography trends and perspectives

Abstract: This paper devoted to overview impact of quantum computing to modern cryptography and to analyze possible trends of cryptography development in the next years. Quantum computing became more popular these days and performance obtained using quantum computers promises to be extremely high. This trend causes to the security risks of current cryptographic algorithms usage without sufficient feasibility and analysis. It means that extremely high performance of quantum computers will be able to break some of existing cryptographic algorithm and produce the risk in security at all. To avoid such situation many cryptography specialists within whole world start research in the direction of so-called Post-quantum Cryptographic algorithms. Currently there are several projects performing research in this direction. Actuality of this topic is confirmed by many scientific papers in this direction. So, this paper contains overview of cryptography trends considering quantum computing coming in the nearest future.

Keywords: cryptography, postquantum, quantum computers, cybersecurity.

Abbreviations:
AES – Advanced Encryption Standard,
ECC – Elliptic Curve Cryptography,
DES – Data Encryption Standard,
KEM – key encapsulation mechanism,
LWE – learning-with-errors,
NIST – National Institute of Standards and Technology,
SIS – short integer solution.

Introduction

Cryptography is the science of mathematical methods for ensuring the confidentiality, integrity and authenticity of information. In recent decades, the scope of cryptography has expanded to include not only secret data transmission, but also methods for verifying message integrity, sender identification, authentication, digital signatures, interactive confirmations, and secure communication technologies. Widespread use of computer networks, in particular, the global Internet, development of electronic banking technologies, increases the amount of

restricted information transferring of state, military, commercial and private data. This leads to development of new directions in cryptography, including public key distribution systems and electronic key distribution systems and electronic digital signature systems. Today it is difficult to find an information or telecommunication system, which would not use the mechanisms of cryptographic information security mechanisms. Today we are at the new step in cryptography development which is related with invention of quantum computers. Due to quantum computers performance cryptographic algorithms need to be improved or the new algorithms developed. The direction of cryptographic algorithms development that shall be reliable in the era of quantum computers is called post-quantum cryptography.

Cryptography history overview

Cryptography, as the science of protecting information from unauthorized access, has a long history. The beginnings of cryptography can be traced back to ancient civilizations that used various encryption methods to preserve significant data and communication confidentiality. However, an expanded description of cryptography as a modern science with mathematical and computer foundations began to develop in the 20th century with the advent of electronic devices and computers that required more sophisticated encryption methods to ensure data security. Thus, cryptography has become a key branch in cybersecurity and information security.

In ancient times, cryptography was already used to protect significant information and ensure the confidentiality of communications. One of the most famous examples is Caesar's cipher, where each letter of a text was replaced by another letter at a certain offset in the alphabet. Ancient cryptography methods also include the more complex Atbash cipher, which used the replacement of letters of the alphabet with their "reverse" letters, and other methods of replacing characters. Ancient civilizations such as Egypt, Greece, and Rome also played a significant role in the development of cryptography, using ciphers for communication and military purposes.

In the 20th century significant development in cryptography happened due to the emergence of new technologies and mathematical methods that have significantly increased the complexity of information security. During World War I, cryptography became a significant tool for military area, e.g., the German Enigma cipher was considered extremely difficult to decipher, but was cracked by British and Polish cryptanalysts, which significantly influenced the course of the war. In the 1970s and 1980s, the mathematical foundations of modern cryptography were developed, such as asymmetric ciphers and protocols based on complex mathematical problems such as the factorization of large numbers and the discrete logarithm. With the development of computers, new opportunities have occurred for the development and use of cryptographic algorithms. Computer cryptography has become a significant field, providing security for electronic communications and transactions (*Maqsood et al., 2017*; *Rathidevi et al., 2017*).

Starting from 1970s and 1980s, the first standards for cryptographic algorithms were created, such as DES. Later, other standards such as AES appeared, which are widely used around the world till these days.

At the beginning of the 21st century, the active study of quantum cryptography was started, which is based on the principles of quantum mechanics. This branch of cryptography has the potential to ensure absolute security of communications (*Bernstein et al., 2009*).

Quantum computing principles

Quantum computers began to appear on the horizon of science and technology in the second half of the 20th century, when scientists began to explore the possibilities of using the principles of quantum mechanics for computing. One of the key moments was the publication of the Shor`s factorization algorithm by Peter Shor in 1994, which demonstrated the potential of quantum computers in solving complex problems such as factorizing large numbers.

Since then, significant advances have been made in the development of hardware for quantum computing, such as qubits, quantum gates, and quantum computing devices. In addition, a variety of quantum algorithms have been created that can be used to solve a variety of problems, including cryptography, optimization, simulation of quantum systems, and many others (*Bernstein & Lange, 2017*; *Maqsood et al., 2017*).

Today, quantum computers remain at the early stages of development and their capabilities and limitations are still being studied. Nevertheless, they have the potential to become a promising technology for solving complex computing problems that currently require a large number of resources of traditional computers.

The principle of a quantum computer is based on the peculiarities of processing and storing information using qubits, the basic quantum analogues of classical bits. Qubits represent the states of a quantum system, which can be in a vertical or horizontal position, corresponding to the "0" or "1" values of classical bits. However, qubits can also be in a superposition of states, which allows them to store and process information faster and more efficiently than classical bits.

There are some other often used terms in quantum commuting: Quantum gates, Quantum algorithms and Quantum assembly. *Quantum gates* are similar to classical logic gates and perform operations on qubits such as rotation, superposition storage, state mixing, etc. These gates allow a quantum computer to perform computations and logical operations. *Quantum assembly* allows you to read information stored in qubits and convert this information into a classical output that can be interpreted by humans or other classical computers. Quantum computers use special *Quantum algorithms* that exploit the unique properties of quantum mechanics to solve complex computational problems such as significant for cryptography factorization of large numbers.

Quantum computing is based on the next three principles: superposition, entanglement and decoherence. Superposition, like in other scientific fields, means that adding two or more quantum states produces another valid quantum state. Quantum entanglement is phenomena when quantum state of two or more objects are described in relation to each other, even if the individual objects are separated in space. Finally, quantum decoherence is the loss of the quantum state in a qubit.

In general, the operation of a quantum computer is based on the use of quantum principles and algorithms to perform computations and process information, which can be much faster and more efficient (*Paquin et al., 2020*).

Impact of quantum computers to cryptographic algorithms

The impact of quantum computers on modern cryptography is a significant topic of discussion in information security. The main aspect of this impact includes breaking of existing cryptographic algorithms.

Some modern cryptographic algorithms, such as RSA and ECC, are based on complex mathematical problems, such as factorizing large numbers or calculating the discrete logarithm. Quantum computers can use algorithms that effectively break these mathematical problems, which leads to lose of security of such cryptographic systems. However, the development of quantum cryptography, which is based on the principles of quantum mechanics, may provide new methods of protecting information from quantum attacks, e.g., quantum cryptography can use the principles of quantum key exchange to ensure absolute confidentiality of data transmission.

The introduction of quantum computers may cause to potential challenges to existing information security systems, as cryptographic algorithms previously considered secure may be vulnerable to quantum attacks. This may require a review and update of cryptographic protocols and algorithms to ensure resilience to quantum computing.

The purpose of post-quantum cryptography is to develop cryptographic methods and protocols that remain resistant to attacks that can be carried out using quantum computers. Since quantum computers can break some modern cryptographic algorithms, such as RSA and ECC, by using algorithms that effectively solve the complex mathematical problems on which these algorithms are based, post-quantum cryptography creates new methods of protecting information.

Post-quantum cryptography uses the principles of quantum mechanics to solve complex mathematical problems that form the basis of cryptographic algorithms. Post-quantum cryptography involves the development of new cryptographic protocols and algorithms that remain resistant to attacks by quantum computers. These algorithms can be based on other mathematical problems that are considered difficult for quantum computers or on quantum principles such as quantum key exchange. It is significant to note that some of existing cryptographic protocols can be adapted to protect against attacks by quantum computers by using longer keys or other security measures.

Considering this, the impact of quantum computers on modern cryptography creates not only both potential threats and also open new opportunities for the development of new methods of information protection. It is significant to continue researching these aspects and developing strategies to adapt to the new challenges.

Post-quantum projects overview

There are many projects in post-quantum cryptography that aim to develop and apply new methods of protecting information in the face of threats from quantum computers. Some of the most famous projects are mentioned and supported by NIST Post-Quantum Cryptography page. A project of the NIST aimed at creating post-quantum cryptography standards to protect information from quantum attacks. This project evaluates various candidates for post-quantum cryptography standards and develops recommendations for their use (*Moody et al., 2016*).

The most famous Post-Quantum Cryptography algorithms are: CRYSTALS-Dilithium, CRYSTALS-Kyber, Falcon. The information below is mostly taken from the official sites of these algorithms and contains some detailed explanation of these algorithms.

CRYSTALS-Dilithium is a digital signature scheme that is strongly secure under chosen message attacks based on the hardness of lattice problems over module lattices (*Cryptographic*

Suite …, 2018). The security notion means that an adversary having access to a signing oracle cannot produce a signature of a message whose signature he has not yet seen, nor produce a different signature of a message that he already saw signed. Dilithium is one of the candidate algorithms submitted to the NIST Post-quantum cryptography project. The design of Dilithium is based on the "Fiat-Shamir with Aborts" technique of Lyubashevsky which uses rejection sampling to make lattice-based Fiat-Shamir schemes compact and secure. The scheme with the smallest signature sizes using this approach is the one of Ducas, Durmus, Lepoint, and Lyubashevsky which is based on the NTRU assumption and crucially uses Gaussian sampling for creating signatures. Because Gaussian sampling is hard to implement securely and efficiently, we opted to only use the uniform distribution. Dilithium improves on the most efficient scheme that only uses the uniform distribution, due to Bai and Galbraith, by using a new technique that shrinks the public key by more than a factor of 2. To the best of our knowledge, Dilithium has the smallest public key + signature size of any lattice-based signature scheme that only uses uniform sampling. Performance overview is shown in the table of the Appendix (*Table 1*).

CRYSTALS-Kyber is an IND-CCA2-secure KEM, whose security is based on the hardness of solving the LWE problem over module lattices. Kyber is one of the finalists in the NIST Post-quantum cryptography project as well. The submission lists three different parameter sets aiming at different security levels. Specifically, Kyber-512 aims at security roughly equivalent to AES-128, Kyber-768 aims at security roughly equivalent to AES-192, and Kyber-1024 aims at security roughly equivalent to AES-256. The design of Kyber has its roots in the seminal LWE-based encryption scheme of Regev. Since Regev's original work, the practical efficiency of LWE encryption schemes has been improved by observing that the secret in LWE can come from the same distribution as the noise and also noticing that "LWE-like" schemes can be built by using a square (rather than a rectangular) matrix as the public key. Another improvement was applying an idea originally used in the NTRU cryptosystem to define the Ring-LWE and Module-LWE problems that used polynomial rings rather than integers. The CCA-secure KEM Kyber is built on top of a CPA-secure cryptosystem that is based on the hardness of Module-LWE.

Falcon is a cryptographic signature algorithm submitted to NIST Post-quantum Cryptography Project on November 30th, 2017 (*Fast-Fourier …, 2017*). Falcon is based on the theoretical framework of Gentry, Peikert and Vaikuntanathan for lattice-based signature schemes. It instantiates that framework over NTRU lattices, with a trapdoor sampler called "fast Fourier sampling". The underlying hard problem is the SIS problem over NTRU lattices, for which no efficient solving algorithm is currently known in the general case, even with the help of quantum computers. Falcon offers the following features:

- Security: a true Gaussian sampler is used internally, which guarantees negligible leakage of information on the secret key up to a practically infinite number of signatures (more than 264).
- Compactness: thanks to the use of NTRU lattices, signatures are substantially shorter than in any lattice-based signature scheme with the same security guarantees, while the public keys are around the same size.
- Speed: use of fast Fourier sampling allows for very fast implementations, in the thousands of signatures per second on a common computer; verification is five to ten times faster.

- Scalability: operations have cost O (n log n) for degree n, allowing the use of very long-term security parameters at moderate cost.
- RAM Economy: the enhanced key generation algorithm of Falcon uses less than 30 kilobytes of RAM, a hundredfold improvement over previous design such as NTRUSign. Falcon is compatible with small, memory-constrained embedded devices.

  Performance of Falcon algorithm is shown in the table of the Appendix (*Table 2*).

Conclusion

Impact of quantum computers on modern cryptography creates not only both potential threats and also opens new opportunities for the development of new methods of information protection. It is significant to continue researching these aspects and developing strategies to adapt to the new challenges. Quantum computers can use algorithms that effectively break famous cryptographic algorithms like RSA and ECC, which leads to lose of security of such cryptographic systems. From another side, development of quantum cryptography, provides new methods of protecting information from quantum attacks, e.g., post-quantum cryptography can ensure absolute confidentiality of data transmission.

There are many projects in post-quantum cryptography that aim to develop and apply new methods of protecting information in the face of threats from quantum computers. The most famous projects are supported by National Institute of Standards and Technology and described on their web page.

Actuality of post-quantum cryptography is confirmed by many scientific papers related to this topic.

References:

Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). *Post-quantum cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg.

Bernstein, D., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*, 188-194. https://doi.org/10.1038/nature23461

Buchmann, J. A., Butin, D., Göpfert, F., & Petzoldt, A. (2016). Post-quantum cryptography: state of the art. *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, 88-108.

Cryptographic Suite for Algebraic Lattices. (2018, June 19). CRYSRALS. https://pq-crystals.org/

Fast-Fourier Lattice-based Compact Signatures over NTRU. (2017, December 13). https://falcon-sign.info/

Fernández-Caramés, T. M. (2019). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet of Things Journal*, *7*(7), 6457-6480.

Gagnidze, A., Iavich, M., & Iashvili, G. (2017). Analysis of post quantum cryptography use in practice. *Bulletin of Georgian National Academy of Science*, *11*(2), 29-36.

Ghosh, B., Aich, R., Khag, A., Nayak, S., & Kumar, P. (2020). Cryptography. *Journal of Mathematical Sciences & Computational Mathematics*, *1*(2), 225-228.

Katz, J., & Lindell, Y. (2007). *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC.

Maqsood, F., Ahmed, M., Ali, M. M., & Shah, M. A. (2017). Cryptography: A comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications*, *8*(6).

Moody, D., Jordan, S.P., Chen, L., & Li, Y.-K. (2016). NIST Report on post-quantum cryptography. *National Institute of Standards and Technology Internal Report*, *12*, *8105*. Gaithersburg, MD, USA.

Mosca, M. (Ed.). (2014). *Post-quantum cryptography*. Springer International Publishing.

Niederhagen, R., & Waidner, M. (2017). *Practical post-quantum cryptography*. Fraunhofer SIT.

Paquin, C., Stebila, D., & Tamvada, G. (2020). Benchmarking post-quantum cryptography in TLS. *Post-Quantum Cryptography: 11th International Conference*, *PQCrypto 2020*, 72-91. Paris, France, April 15-17, 2020. Springer International Publishing.

Pornin, T. (2019). *New efficient, constant-time implementations of falcon*. Cryptology ePrint Archive.

Raavi, M., Wuthier, S., Chandramouli, P., Balytskyi, Y., Zhou, X., & Chang, S. Y. (2021, June). Security comparisons and performance analyses of post-quantum signature algorithms. *International Conference on Applied Cryptography and Network Security*, 424-447. Cham: Springer International Publishing.

Rathidevi, M., Yaminipriya, R., & Sudha, S. V. (2017, March). Trends of cryptography stepping from ancient to modern. *2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT), 1-9*. IEEE.

Sharma, N. (2017). A review of information security using cryptography technique. *International Journal of Advanced Research in Computer Science*, *8*(4).

Shoukat, I. A., Bakar, K. A., & Iftikhar, M. (2011). A survey about latest trends and research issues of cryptographic elements. *International Journal of Computer Science*, *8*(3), 140-149.

Song, F. (2014). A Note on Quantum Security for Post-Quantum Cryptography. In: M. Mosca. (Ed.). *PQCrypto 2014: Post-Quantum Cryptography*, *8772* (pp. 246-265). Springer, Cham. https://doi.org/10.1007/978-3-319-11659-4_15

Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Computer Science Review*, *47*, 100530.

Appendix

Table 1. Performance Overview of CRYSTALS-Dilithium algorithm

Dilithium2					
Sizes (in bytes)		**Skylake cycles (ref)**		**Skylake cycles (avx2)**	
		gen:	300751	**gen:**	124031
pk:	1312	**sign:**	1355434	**sign:**	333013
sig:	2420	**verify:**	327362	**verify:**	118412
Dilithium3					
Sizes (in bytes)		**Skylake cycles (ref)**		**Skylake cycles (avx2)**	
sk:		**gen:**	544232	**gen:**	256403
pk:	1952	**sign:**	2348703	**sign:**	529106
sig:	3293	**verify:**	522267	**verify:**	179424
Dilithium5					
Sizes (in bytes)		**Skylake cycles (ref)**		**Skylake cycles (avx2)**	
sk:		**gen:**	819475	**gen:**	298050
pk:	2592	**sign:**	2856803	**sign:**	642192
sig:	4595	**verify:**	871609	**verify:**	279936

(Source: *Cryptographic Suite …, 2018*)

Table 2. Performance Overview of Falcon algorithm

variant	**keygen (ms)**	**keygen (RAM)**	**sign/s**	**verify/s**	**pub size**	**sig size**
Falcon-512	8.64	14336	5948.1	27933.0	897	666
Falcon-1024	27.45	28672	2913.0	13650.0	1793	1280

(Source: *Fast-Fourier …, 2017*)