FEATURED ARTICLE: POST-QUANTUM CRYPTOGRAPHY: THE FIRST RESULTS OF STANDARDIZATION

Yurii I. Gorbenko
Candidate of Sciences (Engineering), Academician of the Academy of Applied Radioelectronics Sciences, Researcher of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University, Ukraine. Areas of scientific interests: applied cryptology.
Email: gorbenkou@iit.kharkov.ua

Kateryna O. Kuznetsova
Researcher of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University, Ukraine. Areas of interests: security information systems and technologies.
Email: kate7smith12@gmail.com

Ivan D. Gorbenko
Doctor of Sciences (Engineering), Full Professor, Academician of the Academy of Applied Radioelectronics Sciences, Professor of the Department security information systems and technologies of the
V. N. Karazin Kharkiv National University, Ukraine. Areas of scientific interests: applied cryptology, post-quantum cryptography and authentication, methods of information security in computer systems.
Email: I.d.gorbenko@karazin.ua

Alexandr A. Kuznetsov
Doctor of Sciences (Engineering), Full Professor, Professor of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University, Ukraine. Visiting Professor at the University of Macerata, Italy. Visiting Professor at the University of Macerata, Italy. Areas of scientific interests: cryptography and authentication, steganography, cybersecurity.
Email: kuznetsov@karazin.ua

1. Introduction

Cryptographic information security is an important component of information security. It is directly related to overcoming current problems and challenges in cyberspace, new threats to information security in critical infrastructures in defense and security, industry, banking, economy, etc. New promising information technologies, which in the face of modern challenges and threats can radically change the architecture of new information systems, are particularly interesting.

Rapid improvement of new computing facilities based on the principles and effects of quantum physics (so-called universal quantum computers) jeopardizes current and standardized at the national and international levels mechanisms (protocols, algorithms etc.) public-key cryptography. In the near future, due to the possibility of effective use of quantum computers for solving cryptographic analysis problems, the vast majority of public-key algorithms existing today will become vulnerable and will not be able to provide even the lowest level of security. And the mathematical transformations of such cryptographic means will go down in history of cryptographic science.

Thus, the main task of modern cryptographic science is to theoretically substantiate the reliable, fast and secure cryptographic protocols in the conditions of possible use of quantum means of cryptographic analysis. On the one hand, it is a response to new challenges o information security. On the other hand, these are new opportunities for creating international information systems with the provision of electronic trust services with a guaranteed level of information and cybersecurity.

This article focuses on the results obtained from the development and research of post-quantum cryptographic algorithms (PQC) and the first results on their standardization. In particular, it provides brief information on the intermediate results of the open competition of post-quantum cryptographic algorithms from the US National Institute of Standards and Technology (NIST). It also shows the first results of national standardization obtained in Ukraine. In our opinion, this is one of the first examples of successful implementation of the latest cryptographic algorithms at the state level. Such experience can be used in the future for international standardization and for the implementation of post-quantum algorithms in modern information systems and networks.

2. Intermediate results of development and research of post-quantum cryptographic algorithms

According to the National Security Agency (NSA) [1], NIST USA [2], the European Telecommunications Standards Institute (ETSI) [3] and the world's leading scientists [4], full-scale universal quantum computers may become available to cybercriminals in the next 10-15 years. In 2016 NIST announced a global competition of post-quantum cryptographic algorithms (PQC) [5] to prevent such security threats. It involves the most experienced and reputable research institutions, including the Institute of Quantum Computing (IQC), European Institute of Telecommunications Standards ETSI international PQCrypto project, etc.

All studies of post-quantum cryptography are focused on several areas:

- Lattice-based cryptography
- Multivariate cryptography
- Hash-based cryptography
- Code-based cryptography
- Supersingular elliptic curve isogeny cryptography.

Another area is symmetric cryptography. But most modern algorithms will be able to provide the required level of stability due to large lengths of symmetric keys and system-wide parameters.

Therefore, algorithms and protocols of public-key cryptographic transformations are the most relevant:

- Public-Key Encryption and Key-Establishment Algorithms (PKE/KEM);
- Digital Signature Algorithms (DSA).

To date, there are the results of the second round of the PQC competition from NIST USA [6]. The next, third stage, has been announced. Intermediate results of research of the second stage are described in [7]. The results of research and comparative analysis of the candidates of the second round using PLD are presented in [8]. A detailed description of the algorithms-finalists of the third round is given in [9].

NIST has published several finalists of the third round, which are expected to be later standardized.

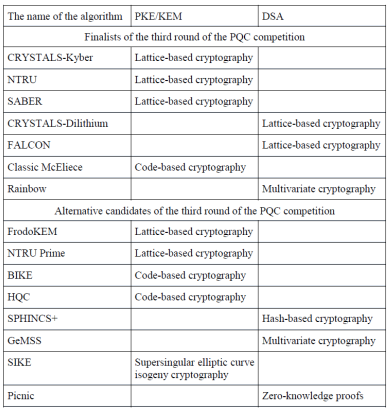
In particular, the following were selected as finalists PKE/KEM:

- Classic McEliece;
- CRYSTALS-KYBER;
- NTRU;
- SABRE.
- As for the DSA:
- CRYSTALS-DILITHIUM,
- FALCON
- Rainbow

These algorithms will be considered in detail and investigated for possible standardization.

In addition, eight other algorithms were selected as alternative candidates: BIKE, FrodoKEM, HQC, NTRU Prime, SIKE, GeMSS, Picnic and SPHINCS+.

General information on all algorithms is given in table 1.



The name of the algorithm	PKE/KEM	DSA
Finalists of the third round of the PQC competition		
CRYSTALS-Kyber	Lattice-based cryptography	
NTRU	Lattice-based cryptography	
SABER	Lattice-based cryptography	
CRYSTALS-Dilithium		Lattice-based cryptography
FALCON		Lattice-based cryptography
Classic McEliece	Code-based cryptography	
Rainbow		Multivariate cryptography
Alternative candidates of the third round of the PQC competition		
FrodoKEM	Lattice-based cryptography	
NTRU Prime	Lattice-based cryptography	
BIKE	Code-based cryptography	
HQC	Code-based cryptography	
SPHINCS+		Hash-based cryptography
GeMSS		Multivariate cryptography
SIKE	Supersingular elliptic curve isogeny cryptography	
Picnic		Zero-knowledge proofs

Table 1. Brief information about the finalists of the third round NIST PQC

As can be seen from Table 1, the most promising in terms of future standardization are post-quantum cryptographic algorithms, which are based on mathematical transformations in rings of polynomials (lattice-based cryptography). This direction was chosen by Ukrainian scientists for the national standardization of post-quantum cryptography and its further implementation at the state level.

2. The first results of standardization of post-quantum cryptography

Researchers from Ukraine have made the greatest progress in standardizing of post-quantum cryptography. In particular, based on the results of the last few years, Ukraine has managed to develop and bring to the level of national standardization three algorithms for post-quantum cryptography. The results and achievements of the international scientific community were taken into account, including the NIST PQC international competition [6-9].

2.1 Public-Key Encryption and Key-Establishment Algorithms (national standard of Ukraine DSTU 8961:2019 «Skelya»)

This standard describes key encryption and encapsulation algorithms that use Lattice-based cryptography. The authors of the standard took into account the experience and research results of the works presented at the NIST PQC competition.

The encryption algorithm uses an asymmetric key pair, i.e. a public key to encrypt blocks of information (data) by the sender, and a private (secret) key to decrypt encrypted blocks by the recipient.

The key encapsulation algorithm (protocol) also uses an asymmetric key pair, i.e. the private (secret) session key to encapsulate the session key by the sender, and the public session key to decapsulate the session key by the recipient.

The recipient, based on the personal (secret) decryption key and decapsulated sender's session key,and the sender, based on the recipient's public encryption key and the personal (secret) session key, produce a common «secret» (common key). Later, the common key can be used to encrypt information (data) in communication channels during the information exchange.

Key encapsulation is the process of cryptographically transforming a session key and other data to ensure their confidentiality, integrity (authenticity) and cryptographic resistance, as well as matching the symmetric encryption key between sender and receiver in the future. Decapsulation is the process of verifying the integrity and authenticity of an encapsulated session key and agreeing on a data protection key between the recipient and the sender.

Encryption and encapsulation of keys are performed on the basis of mathematical transformations in a ring of polynomials over a finite field.

The standard takes into account the requirements for cryptographic stability against special attacks based on leakage through technical channels, as well as potential classical and quantum attacks, in particular in the transition and post-quantum periods. The standard is developed taking into account the experience of creating and applying ISO / IEC 18033-2 and the results presented in [10-17].

This standard is intended to use by developing cryptographic information security in the provision of confidentiality, integrity, indisputability, availability, etc. In particular, to protect against special attacks, as well as attacks in the post-quantum period, in information, telecommunication and information-telecommunication systems.

Depending on the level of cryptographic resistance against classical and quantum attacks that must be provided, there are three modes:

- Mode SKELYA–KEM 256/128 – 256 protection bits against classic attacks and 128 bits of protection against quantum attacks, as well as protection against special attacks;
- Mode SKELYA–KEM 384/192 – 384 protection bits against classic attacks and 192 bits of protection against quantum attacks, as well as protection against special attacks;
- Mode SKELYA–KEM 512/256 – 512 protection bits against classic attacks and 256 bits of protection against quantum attacks, as well as protection against special attacks.

The following cryptographic transformations can be also separately applied in each of the operating modes:

- independent algorithm (function) of asymmetric encryption;
- key encapsulation protocol (function) based on the use of asymmetric cipher function;
- symmetric encryption and authentication mechanism (function) based on asymmetric encryption and key encapsulation functions.

Each mode of operation due to the use of cryptographic transformations in the rings of polynomials and finite fields provides services of confidentiality, integrity, authenticity, availability and cryptographic survivability of the session key and its coordination between sender and receiver.

2.2 Digital Signature Algorithms with deviations (draft national standard of Ukraine «Vershina», expected adoption by the end of 2022)

This draft standard («Vershina») provides cryptographic algorithms of digital signature based on mathematical transformations of the algebraic lattice with deviations in rings of polynomials Zq[X]/(Xn+1) and Z3[X]/(Xn+1) degree n for an integer q.

The algorithms use an asymmetric key pair: private (secret) key and public key. To create the DS the signer's private (secret) key is used, and for the verification of the DS the verifier's public key is used. The signer's integrity, authenticity and irrefutability are decided based on the verification of the DS.

Algorithms, depending on the level of cryptographic resistance against classical and quantum attacks, as well as attacks by third-party channels that need to be provided, can be used in four modes:

- Mode VERSHINA–128/64 (mode = 1) – 128 bit of protection against classical attacks and 64 bits of protection against quantum attacks, protection against special attacks (stability margin corresponds to symmetric cipher AES - 128);
- Mode VERSHINA–256/128 (mode = 2) – 256 bit of protection against classical attacks and 128 bits of protection against quantum attacks, protection against special attacks (stability margin corresponds to symmetric cipher AES - 256);
- Mode VERSHINA–384/192 (mode = 3) – 384 bit of protection against classical attacks and 192 bits of protection against quantum attacks, protection against special attacks (stability margin corresponds to symmetric cipher with a key 384 bits);
- Mode VERSHINA–512/256 (mode = 4) – 512 bit of protection against classical attacks and 256 bits of protection against quantum attacks, protection against special attacks (stability margin corresponds to symmetric cipher with a key 512 bits).

Cryptographic transformations and corresponding hashing functions can be used in each of the operating modes.

Public key cryptographic transformation algorithms based on algebraic lattices with deviations with different security parameters are used for modes of operation due to the use of DS to provide integrity, authenticity, accessibility and indisputability services, which allows to obtain different security levels and technical and economic and technical and operational characteristics (indicators).

2.3 Digital Signature Algorithms with a given sample (draft national standard of Ukraine «Sokil», expected adoption by the end of 2023)

This draft standard (the designation «Sokil») uses digital signature algorithms on algebraic NTRU lattices with a given sample. They are designed to ensure the integrity, authenticity, accessibility and integrity of the information and resources that underpin the provision of electronic trust services in the interaction of two or more entities that trust the provider of electronic trust services. Digital signature can be the basis for electronic identification, electronic authentication, advanced and qualified digital signature, printing and creation of electronic documents.

The draft standard describes DS algorithms that use two main components: 1) a class of cryptographic lattices based on the NTRU lattice; 2) fast Fourier sampling technology. An algorithm [18] is used as a prototype, which has been extended to provide greater cryptographic resistance while using quantum computers.

The main approach to the design of the DS mechanism is to use the "hash-and-signature" paradigm [18-20]. Its main advantage is the evidence stability within the quantum random oracle model. Another advantages of DS «Sokil» are the minimum length of public key size and signature size, compared to all other DS algorithms, the efficient DS signing and verification algorithms. The main disadvantage is the slow key generation. However, DS «Sokil» can be easily integrated into existing protocols and applications and provides acceptable overall performance. Also while using DS «Sokil» it is possible to implement it as a message recovery technology [18, 19]. DS «Sokil» corresponds to the requirements for cryptographic stability, including in the post-quantum period. It is effective in terms of technical, economic and operational characteristics. The main essences of calculations and transformations in DS «Sokil» are polynomials of degree n of the form φ = xn + 1 with integer coefficients, which are calculated by modulo. Calculations are also performed modulo the polynomial φ = xn + 1, always only for values n = 512, 1024 and 2048.

Cryptographic transformations are performed using asymmetric key pairs: for the DS using the subscriber's private key, and for the verification of the DS using the verifier’s public key.

Standard provides protection against existing and future classical and quantum attacks, as well as against special attacks through third-party channels.

Depending on the required level of security and restrictions on technical, operational and economic characteristics, the standard can be applied with 1, 2 and 4 levels of security and cryptocurrency, respectively, providing 128, 256 and 512 bits of security against classical cryptanalysis and 64, 128 and 256 security bits against quantum cryptanalysis, as well as providing protection against special attacks.

Conclusions

Thus, the development and research of post-quantum cryptographic algorithms are in the final phase. According to the results of the NIST PQC competition, possible candidates for international standardization have already been selected. In particular, there are several applicants for PKE / KEM and DSA. At the final stage of the competition, crucial tests and trials are conducted. It is expected that in the coming years new standards of cryptographic transformation will be adopted and put into practice, which will ensure a secure transition to the post-quantum technological era. A good example of such innovations are the latest Ukrainian standards, which have been developed and implemented taking into account the experience of NIST PQC.

REFERENCES

1. Post-Quantum Cybersecurity Resources. https://www.nsa.gov/what-we-do/cybersecurity/post-quantum-cybersecurity-resources/

2. NISTIR 8105 Report on Post-Quantum Cryptography. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

3. Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges. https://portal.etsi.org/Portals/0/TBpages/QSC/Docs/Quantum_Safe_Whitepaper_1_0_0.pdf

4. Neal Koblitz and Alfred J. Menezes. A Riddle Wrapped in an Enigma. https://eprint.iacr.org/2015/1018.pdf

5. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms

6. NISTIR 8309 Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf

7. 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings. https://link.springer.com/book/10.1007/978-3-030-44223-1

8. Kris Gaj. Implementation and Benchmarking of Round 2 Candidates in the NIST Post-Quantum Cryptography Standardization Process Using FPGAs. https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/seminars/oct-2020-gaj-kris-presentation.pdf

9. Round 3 Submissions. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

10. American National Standard X9.98-2010. Lattice-based polynomial public key encryption algorithm, Part 1: key establishment, Part 2: data encryption. – 2010.

11. Daniel J. Bernstein NTRU Prime / Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal // Електронний ресурс. – Режим доступу: https://ntruprime.cr.yp.to/ntruprime-20160511.pdf.

12. Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, Damien Stehlé. CRYSTALS-Dilithium. Algorithm Specifications and Supporting Documentation. // Електронний ресурс. – Режим доступу: https://pq-crystals.org/dilithium/data/dilithium-specification.pdf

13. Gorbenko I. D. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability / I. D. Gorbenko, A. M. Oleksiychuk, O. H. Kachko, M. V. Yesina, V. A. Bobukh, S. O. Kandyi // Радіотехніка. – Х. : Харківський національний університет радіоелектроніки, 2018. – Вип. 195. – С. 1726

14. I. D. Gorbenko, O. G. Kachko, M. V. Yesina Analysis of Asymmetric NTRU Prime IIT Ukraine Encryption Algorithm with Regards to Known Attacks / Telecommunications and Radio Engineering, Volume 77, 2018, Issue 9, pp. 799-816

15. Gorbenko I. D. Analysis, assessment and proposals regarding the method for generation of system parameters in NTRU-like asymmetric systems / I. D. Gorbenko, O. G. Kachko, K. A. Pogrebnyak, L. V. Makutonina // Telecommunications and Radio Engineering. Volume 76, 2017

16. Gorbenko I. D. General statements and analysis of the end-to-end encryption algorithm NRTU Prime IIT Ukraine / I. D. Gorbenko, O. G. Kachko, M. V. Yesina // Радіотехніка. – Х. : Харківський національний університет радіоелектроніки, 2018. – Випуск 193 – С. 5–16

17. Lily Chen Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai- Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone – Access mode: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

18. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU Specification v1.2 — 01/10/2020. Pierre-Alain Fouque Jeffrey Hoffstein Paul Kirchner. [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

19. Falcon. [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

20. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, 40th ACM STOC, pages 197–206, Victoria, BC, Canada, May 17–20, 2008. ACM Press.