

# POST-QUANTUM CRYPTOGRAPHY: CURRENT STATE OF STANDARDIZATION AND DEPLOYMENT

Tomáš Sochor<sup>1,2</sup>, Hana Sochorová<sup>3</sup>

<sup>1</sup>Department of Informatics, Faculty of Business and Economics, Mendel University in Brno, Zemědělská 1, 613 00 Brno, Czech Republic

<sup>2</sup>European Research University, Sokolská 33, 702 00 Ostrava, Czech Republic

<sup>3</sup>Institute of Laboratory medicine, Institute of Medical Biophysics and Medical Information Technology, Faculty of Medicine, University of Ostrava, Syllabova 19, 703 00 Ostrava, Czech Republic

**DOI:** [https://doi.org/10.11118/ecos2026\\_034](https://doi.org/10.11118/ecos2026_034)

## ABSTRACT

The paper reviews the quantum computing advances and their impact on classical cryptography. the aspect of potential breaking of present (believably secure) cryptographic algorithms. Recent progress in the abilities of quantum computers as well as the standardization of new generation of cryptographic algorithms resistant to quantum-computing attacks is summarized. The classical cryptographic algorithms are reviewed and corresponding threats from quantum algorithms were summarized. In addition, existing symmetric and hash algorithms under quantum attacks is discussed and recommendations for improving security in long-term are formulated.

**Keywords:** quantum computing, cryptographic algorithm, post-quantum cryptography, symmetric cryptography, asymmetric cryptography, hashing, key exchange

**JEL Code:** O33, L86, C81

## 1 INTRODUCTION

Communication through the internet (as well as through of other computer networks) is often vulnerable to various types of attacks ranging from eavesdropping through blocking up to silent modifications. Original insecure application protocols belonging to TCP/IP protocol suite (like telnet, FTP, SMTP, later prevailed by HTTP) massively used in early stages of internet have been later gradually replaced by their more secure alternatives (e.g. SSH and HTTPS) so that the above risks were eliminated. However, even the design of such secure protocols has been proposed decades ago reflecting the 1990's knowledge in cryptography when potential breaking of cryptographic algorithms like RSA, SHA and DES (or later AES) seemed to be aeons away.



This article is licensed under CC BY-SA 4.0 Attribution-ShareAlike 4.0 International license.  
<https://creativecommons.org/licenses/by-sa/4.0/deed.en>

Nevertheless, recent progress in quantum computing (as described e.g. by Gill *et al.* 2025) has changed the perspective a lot. Now, the question does not seem to sound whether quantum computers will be able to perform computational operations for wide public but when they are going to do so. As a result, so far rather theoretical algorithms applicable to quantum computers able to solve some problems much quickly than classical computers (like factorization of large integers) will become widely available not only for researchers, academia and industry, but also for hackers. This could pose a significant threat to the security of information and communication systems relying on classical cryptography and therefore it is necessary to reflect this threat in near-future improvement of them, namely by implementation of quantum-attack-resistant algorithms.

## 2 RELEVANT EXISTING RESEARCH

Despite quantum computers of various types have been investigated for at for several decades, the real implementations started to emerge just in recent years. Although all present quantum computers are still rather experimental devices with very limited (inf any) practical impact, it is almost impossible when they overcome their experimental status and start their availability for real calculations.

Among the most promising applications, in addition to simulation of complex physical, chemical and other natural systems, there are calculations allowing significant simplifying (lowering the complexity) of computations problems having non-polynomial (exponential) computational complexity. Most of such non-polynomial-complex problems (e.g. problem of factorization of large numbers) have been and still are a fundament of various cryptographical systems, starting from RSA in 1970's (see Rivest, Shamir, Adleman 1977).

Such a threat (in the form of future potential availability of quantum computers being able to decrypt/break such cryptosystems quickly) poses a significant risk to all systems relying on cryptographic algorithms potentially prone to quantum-computing break. The reason is simple: many systems cannot change their cryptographic algorithms to more resistant quickly enough. Moreover, even if the decryption of vulnerable communication is not feasible now, still potentially sensitive communication can be captured by attackers now and decrypted later. This approach is called "Harvest now, decrypt later" (see Singh, 2024). For certain portion of data, it is still a significant risk, even though most of the encrypted communication would not feel compromised when decryption will happen in, say, 5 or 10 years from now, as demonstrated by Mascelli& Rodden M. 2025. Among the identified use-cases, bitcoin and its underlying middleware blockchain could be at risk because of later unauthorized decryption of their communication.

There are numerous papers and articles devoted to the topic of post-quantum cryptography focusing on various aspects thereof. Among them, Kumar& Pattnaik (2020) provides a review of existing solutions, Joseph *et al.* (2022) focuses on PQC transition, and Lysenko *et al.* (2024) emphasizes general security aspects of post-quantum cryptography.

## 3 CRYPTOGRAPHIC ALGORITHMS REVIEW FROM QUANTUM COMPUTING PERSPECTIVE

### 3.1 Symmetric encryption algorithms

Currently, AES (as standardized by National Institute of Standards and Technology 2001) is the dominant symmetric encryption algorithm, definitely (see e.g. Ganes *et al.* 2025) and in fact, there is no real competition for it since 3DES as the last remaining alternative was deprecated by NIST in 2023.

Several recent studies (e.g. Hosseini, S.M. and Pilaram, H., 2024.) demonstrate that AES is relatively well prepared for quantum computing era. Despite the fact that Grover quantum algorithm reduces the time necessary for cracking AES encryption order of this type of search from  $O(n)$  to  $O(\sqrt{n})$ , no other risks for AES have been presented. Therefore, one can conclude that for the near “quantum” future, it is sufficient to increase (ideally double) the key length to keep the same security level. Even though the current AES standard offers only three key lengths (128, 192 and 256 bits, respectively), with mostly used the maximum, it would not be difficult to extend the algorithms for its usage with longer keys.

### 3.2 Asymmetric encryption and digital signature algorithms

Asymmetric encryption applications do not date far in the history because RSA as the first asymmetric cryptographic algorithm was described in Rivest, Shamir, Adleman 1977. Since then, other asymmetric cryptosystems, namely Elliptic Curve Cryptography (ECC) and ElGamal, have been developed (see e.g. Zhang 2021), and asymmetric cryptosystems have spread rapidly because they have a significant advantage over symmetric algorithms, namely they can operate safely without having a covert channel for distributing a shared secret that is necessary for symmetric algorithms.

On the other hand, a significant drawback of asymmetric algorithm lies in their higher computational complexity reflecting in significantly higher number of operations necessary to encrypt or decrypt a chunk of data in comparison to adequately strong symmetric algorithm. Therefore, a combination of symmetric and asymmetric encryption is massively applied in practical implementations. The more detailed description of the combination is given in section 4.

There is a significant threat from a quantum-computer-run Shor algorithm because it converts the exponentially complex problem of finding of secret factors into a problem with polynomial complexity. Therefore, public availability of quantum computers that is expected in the near future, will pose a threat to the security of any cryptosystem that does not replace them with post-quantum alternatives that are summarized in Section 3.5.

To summarize those observations and findings, one must conclude that virtually all classical asymmetric encryption algorithms are not quantum-attack-resistant and therefore they must be replaced with post-quantum alternatives so that to keep the cryptosystem security in the long-term. The same is true for digital signature algorithms because they are mostly based on the same or very similar mathematical fundamentals to asymmetric encryption.

Unlike for symmetric algorithms, here, replacement is necessary. Fortunately, despite of the fact that there is no direct replacement algorithm among those standardized as post-quantum (see section 3), we can still find a solution in combination of FIPS203 that can efficiently replace the asymmetric cryptography in the most frequent use-case, namely the key negotiation (key exchange) as a part of TLS handshaking between www server and a web browser.

### 3.3 Hashing algorithms

Together with encryption algorithms, hashing completes the cryptographic algorithmic triad necessary to perform a safe encryption. Similarly to encryption, hashing algorithms could be also potentially threatened by quantum simplification of certain operations necessary to break hashing algorithms, typically by simplifying finding collisions.

The most significant threat come from Grover quantum algorithm that can reduce the time necessary for performing pre-image or collision attacks to  $O(\sqrt{n})$ , or  $O(\sqrt[3]{n})$ , respectively (see Hosseini&Pilaram 2024). This means that a short-term solution to mitigate the threat could be an increase of the hash length (with existing hashing algorithm offering a reasonable reserve for that) while in long-term, replacing of existing hashing algorithms with quantum-resistant is the only feasible way.

### 3.4 Key exchange algorithms

Among cryptographic protocols, key exchange plays an important complementary role. Key exchange algorithms do not serve only for seldom operation of replacing the old keys with new ones, but they are employed every day, for instance at every key negotiation phase of TLS connection that is mentioned in section 4.

The most commonly key exchange algorithm class, Diffie-Hellman, is based on similar mathematical problem like RSA and therefore it is also threatened by Shor algorithm when run on a quantum computer. Therefore, the recommendation for Diffie-Hellman algorithm is almost the same as for RSA: the only way how to keep any cryptosystem long-term secure is the replacement of Diffie-Hellman algorithm with its post-quantum alternatives. Here, the new FIPS203 standard provides a solution.

### 3.5 Standardization of quantum-resistant algorithms

In response to rapidly emerging threat to classical algorithms from rapidly improving quantum computers, several new quantum-attack-resistant algorithms have been developed and some of them have been NIST-standardized recently. Despite the standardization process started already in 2016, first final PQC standards were presented in 2024. The following specifies the first generation of post-quantum cryptography:

- FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), derived from the CRYSTALS-KYBER submission. ML-KEM is a KEM (for key establishment) based on module-LWE. It includes parameter sets ML-KEM-512, ML-KEM-768, and ML-KEM-1024 (increasing security levels). This KEM can be used in hybrid TLS or other protocols for key exchange (e.g. combining with X25519). (National Institute of Standards and Technology 2024a)
- FIPS 204: Module-Lattice-Based Digital Signature Algorithm (ML-DSA), derived from CRYSTALS-Dilithium. ML-DSA provides three parameter sets (ML-DSA-44, -65, -87) corresponding to different security categories. It yields signatures comparable in size to existing ECC schemes and is intended for general-purpose signing (certificates, code signing, etc.) (SEE National Institute of Standards and Technology 2024B).
- FIPS 205: Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), derived from SPHINCS+. SLH-DSA is a hash-based signature scheme with parameter variants (128s/128f, 192s/192f, 256s/256f) that trade off signature size and speed. It provides long-term security even against quantum adversaries, at the cost of larger signature sizes. Details are available in National Institute of Standards and Technology 2024c.

**Tab. 1** Overview of NIST Post-quantum cryptographic standards

| Algorithm name     | Purpose                                         | Security assumption                                       | Parameter sets (FIPS)                                          | Deployment                                                                                    |
|--------------------|-------------------------------------------------|-----------------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| ML-KEM (FIPS 203)  | Key-encapsulation (key exchange/ establishment) | Module-LWE (lattice-based)                                | ML-KEM-512, ML-KEM-768, ML-KEM-1024                            | TLS key exchange (incl. hybrid with X25519); larger key shares may impact bandwidth/ latency. |
| ML-DSA (FIPS 204)  | Digital signatures (general-purpose)            | Module-lattice (Module-LWE / Module-SIS)                  | ML-DSA-44, ML-DSA-65, ML-DSA-87                                | PKI, code-signing, firmware signing; larger signatures/public keys than ECDSA/ Ed25519.       |
| SLH-DSA (FIPS 205) | Stateless hash-based digital signatures         | Hash function properties (preimage/ collision resistance) | 128s/128f, 192s/192f, 256s/256f (SHA-256 / SHAKE-256 variants) | Conservative choice; suitable for long-term signatures (e.g., firmware); larger signatures.   |

Sources: National Institute of Standards and Technology 2024a- 2024c

The description of new post-quantum standards by NIST is provided in Table 1.

As the research results mentioned in section 2, there are quantum-attack-resistant algorithms available. On the other hand, available implementations in existing systems are still quite rare – see details in section 5.

## 4 APPLICATION OF CURRENT CRYPTOGRAPHIC ALGORITHMS

Among the applications of current cryptographic algorithms, the Transport Layer Security protocol (TLS) plays a dominant role because it is a fundamental component of HTTPS (Secure HTTPS) that is massively used (nowadays at about 95% of HTTP traffic uses TLS as statistics show, e.g. Google, 2026, and Kerschbaumer *et al.* 2025). TLS was standardized by IETF in several versions starting with version 1.1 in 1999, followed by version 1.2 in RFC5246 in 2008. Currently last version 1.3 comes from 2018, 8446 (Rescorla E., 2018).

The operation of TLS combines multiple cryptographic techniques so that the encryption operates both securely and quickly. In the beginning, the TLS client should rely on the asymmetric key of the server from its certificate only. Here, the client can send the small data chunks to the server (encrypted using slower asymmetric algorithm) as a part of Diffie-Hellman key-exchange process in establishing the session key. After successful key exchange, the rest of the communication involving encryption of large data files is performed using a symmetric encryption algorithm that is significantly faster.

Other secure protocols (like SSH, and even IPsecure) follow a similar pattern: they use classical asymmetric cryptographic algorithms for distribution or exchange of temporary session key, and symmetric cryptography for payload encryption. All these classical asymmetric cryptographic components (certificates, key exchange etc.) need post-quantum cryptography replacements.

## 5 AVAILABLE IMPLEMENTATIONS

The above-mentioned post-quantum cryptographic algorithms have been implemented partly in some major software packages (see Demir 2025). Another recent study (Ahmed *et al* 2025) demonstrates that for some libraries, developers work hard on supporting post-quantum cryptography. A recent news from OpenSSL developers announced that starting April 2025, the above mentioned standard post-quantum cryptographic algorithms are implemented since version 3.5. It seems likely that implementations in other popular libraries will follow but it is a good idea to verify the status before use of a specific library.

## 6 CONCLUSIONS

As the above results demonstrate, all classes of cryptographic algorithms, with a small expectation of relatively few impacted symmetric ones, are threatened by potential availability of quantum computers in relatively near future. Therefore, it is critical so that the existing cryptosystems are modified so that potentially weak cryptographic algorithms are promptly replaced with post-quantum alternatives. These alternative cryptographic algorithms are already available thank to their recent standardization by NIST so there are no formal obstacles preventing information and communication system administrators and owners to start the process of replacement.

In summary, the transition to quantum-safe cryptography is underway. With standards in hand and growing support in cryptographic libraries, organizations can begin implementing post-quantum cryptography now to safeguard against the coming quantum era.

### Acknowledgements

This paper was supported by the project CZ.02.1.01/0.0/0.0/16\_017/0002334 Research Infrastructure for Young Scientists, which is co-financed from the Operational Programme Research, Development and Education.

## REFERENCES

- AHMED, N., ZHANG, L., GANGOPADHYAY, A. 2025. August. A survey of post-quantum cryptography support in cryptographic libraries. In: *2025 IEEE International Conference on Quantum Computing and Engineering (QCE)*. Vol. 1, pp. 906-917. IEEE.
- BARRETT-DANES, F., AHMAD, F. 2025. Quantum computing and cybersecurity: a rigorous systematic review of emerging threats, post-quantum solutions, and research directions (2019–2024). *Discover Applied Sciences*. 7(10), 1083.
- DEMIR, E. D., BILGIN, B., ONBASLI, M. C. 2025. Performance analysis and industry deployment of post-quantum cryptography algorithms. *arXiv preprint arXiv:2503.12952*.
- GILL, S. S., CETINKAYA, O., MARRONE, S., CLAUDINO, D., HAUNSCHILD, D., SCHLOTE, L., WU, H., OTTAVIANI, C., LIU, X., MACHUPALLI, S. P., KAUR, K. 2025. Quantum computing: Vision and challenges. In: *Quantum Computing*. pp. 19-42. Morgan Kaufmann.
- GANESH, R., KHAN, B. U. I., KHAN, A. R., KAMSIN, A. B. 2025. A panoramic survey of the advanced encryption standard: from architecture to security analysis, key management, real-world applications, and post-quantum challenges. *International Journal of Information Security*. 24(5), 1-45.

- GOOGLE. 2026. *HTTPS encryption on the web*. [Accessed: 2026-01-07] <https://transparencyreport.google.com/https/overview?hl=en>
- HOSSEINI, S. M., PILARAM, H. 2024. *A Comprehensive Review of Post-Quantum Cryptography: Challenges and Advances*. Cryptology ePrint Archive.
- JOSEPH, D., MISOCZKI, R., MANZANO, M., TRICOT, J., PINUAGA, F. D., LACOMBE, O., LEICHENAUER, S., HIDARY, J., VENABLES, P. AND HANSEN, R. 2022. Transitioning organizations to post-quantum cryptography. *Nature*. 605(7909), 237-243.
- KERSCHBAUMER, C., BRAUN, F., FRIEDBERGER, S., JÜRGENS, M. 2025. The State of https Adoption on the Web. *Mozilla Research*. [Accessed: 2026-04-14] [https://research.mozilla.org/files/2025/03/the\\_state\\_of\\_https\\_adoption\\_on\\_the\\_web.pdf](https://research.mozilla.org/files/2025/03/the_state_of_https_adoption_on_the_web.pdf)
- KUMAR, M., PATTNAIK, P. 2020. September. Post quantum cryptography (pqc)-an overview. In: *2020 IEEE High Performance Extreme Computing Conference (HPEC)*. pp. 1-9. IEEE.
- LYSENKO, S., BOKHONKO, O., VOROBİYOV, V., GAJ, P. 2024. Method for identifying cyberattacks based on the use of social engineering over the phone. In: *IntelITSIS*. pp. 318-329. [Accessed: 2026-01-11] <https://ceur-ws.org/Vol-3675/paper23.pdf>
- MASCELLI, J., RODDEN, M. 2025. *"Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks*. FEDS Working Paper No. 2025-93. [Accessed: 2026-01-12] [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=5956313](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5956313)
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2001. FIPS 197: Advanced Encryption Standard (AES). *Nist.org* [Accessed: 2026-01-07] <https://doi.org/10.6028/NIST.FIPS.197-upd1>
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2024a. *FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard*. [Accessed: 2026-01-12] <https://csrc.nist.gov/pubs/fips/203/final>
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2024b. *FIPS 204. Module-Lattice-Based Digital Signature Standard*. [Accessed: 2026-01-12] <https://csrc.nist.gov/pubs/fips/204/final>
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2024c. *FIPS 205. Stateless Hash-Based Digital Signature Standard*. [Accessed: 2026-01-12] <https://csrc.nist.gov/pubs/fips/205/final>
- RESCORLA, E. 2018. The Transport Layer Security (TLS) Protocol Version 1.3. *IETF*. [Accessed: 2026-01-12] <https://datatracker.ietf.org/doc/html/rfc8446>
- RIVEST, R. L., SHAMIR, A., ADLEMAN, L. 1977. *On Digital Signatures and Public-Key Cryptosystems* (No. MITLCSM82).
- SINGH, H. 2024. Managing the Quantum Cybersecurity Threat: Harvest Now, Decrypt Later. In: *Quantum Computing*. pp. 142-158. CRC Press.
- ZHANG, Q. 2021. An overview and analysis of hybrid encryption: the combination of symmetric encryption and asymmetric encryption. In: *2021 2<sup>nd</sup> international conference on computing and data science (CDS)*. pp. 616-622. IEEE.

### Contact information

Tomáš Sochor: e-mail: [tomas.sochor@mendelu.cz](mailto:tomas.sochor@mendelu.cz), e-mail: [tomas.sochor@eruni.org](mailto:tomas.sochor@eruni.org)

Hana Sochorová: email: [hana.sochorova@osu.cz](mailto:hana.sochorova@osu.cz)