© Milevskyi S., Voropay N., Korol O., Yevseiev S., Aksonova I. SSL/TLS protocol on post-quantum algorithms // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 150-156. ©

DOI: 10.18372/2225-5036.30.18616

SSL/TLS PROTOCOL ON POST-QUANTUM ALGORITHMS

Stanislav Milevskyi, Natalya Voropay, Olha Korol, Serhii Yevseiev, Iryna Aksonova

National Technical University "Kharkiv Polytechnic Institute", Ukraine

Stanislav MILEVSKYI, candidate of economic sciences, associate professor
Date and place of birth: 1979, Murom, Volodymyr region.
Education: Kharkiv National University of Economics, 2001.
Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: information protection in socio-cyberphysical systems.
Publications: more than 60 scientific publications, including monographs, textbooks, articles and patents.
E-mail: milevskiysv@gmail.com.
Orcid ID: 0000-0001-5087-7036.

Natalya VOROPAY, candidate of technical sciences, associate professor
Date and place of birth: 1984, Alushta, Crimea.
Education: National Technical University "Kharkiv Polytechnic Institute", 2008.
Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: protection models in socio-cyberphysical systems.
Publications: more than 30 scientific publications, including monographs, textbooks, articles.
E-mail: voropay.n@gmail.com.
Orcid ID: 0000-0003-1321-7324.

Olha KOROL, candidate of technical science, associate professor
Date and place of birth: 1981, Dzhankoy, Crimea.
Education: Kharkiv National University of Economics, 2005.
Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: information protection in socio-cyberphysical systems, authentication mechanisms.
Publications: more than 140 scientific publications, including monographs, textbooks, articles and patents.
E-mail: korol.olha2016@gmail.com.
Orcid ID: 0000-0002-8733-9984.

Serhii YEVSEIEV, doctor of technical science, professor
Date and place of birth: 1969, Khartsyzsk, Donetsk region.
Education: Kharkov Military University, 2002.
Position: Head of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: protection of information resources, post-quantum cryptography, security in socio-cyber-physic.
Publications: more than 300 scientific publications, including monographs, textbooks, articles and patents.
E-mail: serhii.yevseiev@gmail.com.
Orcid ID: 0000-0003-1647-6444.

Iryna AKSONOVA, candidate of economic sciences, associate professor
Date and place of birth: 1973, R. Lozovaya, Dergachevsky district, Kharkiv region.
Education: Kharkiv National University of Economics, 1995.
Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: quantitative methods for assessing and analyzing information.
Publications: more than 120 scientific publications, including monographs, textbooks, articles and copyrights.
E-mail: ivaksyonova@gmail.com.
Orcid ID: 0000-0003-2605-0455.

Abstract. *The development of mobile technologies and their integration with Internet of Things and smart technologies form both cyber-physical and socio-cyber-physical systems. In such systems, as a rule, wireless communication channels are used, in which SSL/TLS protocols are used to provide security services (confidentiality, integrity and authenticity). However, this protocol is not only vulnerable to "Meeting in the Middle", POODLE, BEAST, CRIME, BREACH attacks, but with the advent of a full-scale quantum computer, it can be broken. The article proposes a protocol based on quantum algorithms – crypto-code constructions, which will ensure not only resistance to current attacks, but also stability in the post-quantum period. To ensure the "hybridity" of services, it is proposed to use McEliece and Niederreiter crypto-code constructions and the improved UMAC algorithm based on McEliece crypto-code design. The use of crypto-code constructions provides not only resistance to attacks, but also simplifies the formation of a connection – the parameters of elliptic curves are used for the transmission of the common key. This approach significantly reduces the time of connecting mobile gadgets and simplifies the procedure of agreement before data transfer.*

Keywords: *SSL/TLS protocol, crypto-code constructions, UMAC algorithm, algebraic geometric codes, lossy codes.*

Introduction

The development of modern information and communication technologies, mobile technologies and the Internet of Things has significantly expanded the range of digital services and formed a trend in the formation of cyber-physical systems based on the integration of these technologies with cyberspace. The growth in the capabilities of mobile Internet technologies and wireless channels makes it possible to form mesh networks and expand the areas of smart technologies.

Analysis of existing studies

In such systems, as a rule, the SSL/TLS protocol stack is used to provide security services, which makes it possible to provide services of authenticity, integrity, and confidentiality [1–5]. The paper proposes an approach to improve the SSL/TLS v.1.3 protocol stack based on the integration of post-quantum algorithms – McEliece crypto-code constructions on algebrogeometric codes and the improved UMAC algorithm [6, 7].

In addition, the proposed approach provides not only an increase in the level of resistance and "elimination" of the possibility of implementing threats when using this protocol ("handshake" mode), but also allows its use in the post-quantum cryptoperiod. The post-quantum cryptoperiod is understood as the emergence of a full-scale quantum computer and the possibility of implementing Grover quantum algorithms (breaking symmetric algorithms) and Shor quantum algorithms (breaking asymmetric cryptography algorithms).

Purpose and statement of the task

Thus, the analysis showed that in order to "eliminate" (minimize) the existing threats to the SSL/TLS protocol, it is proposed to use either network traffic monitoring or use post-quantum cryptography and elliptic curve cryptography algorithms. The first approach does not eliminate the reasons for the implementation of threats, and the second does not provide the required level of performance and use in smart technologies based on smart chips with limited computing resources.

The main part of the study

Development of a protocol based on post-quantum algorithms

To ensure the security of mesh-, sensor networks technologies using wireless channel standards: mobile technologies LTE, IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE-802.11, Bluetooth, new approaches to providing security services are needed. In the context of the emergence of a quantum computer, it is necessary not only to use post-quantum cryptoalgorithms, but also a new approach to ensuring the security of socio-cyber-physical systems. Such algorithms require an increase in key sequences to 512 bits for symmetric cryptosystems (this provides a safe time of about 60 years), or the use of post-quantum asymmetric cryptosystems (PQAS – post-quantum asymmetric cryptosystems). Among the contestants of the third round of the competition, there are algorithms built on the integration of the theory of error-correcting coding and cryptography [6-12]. Crypto-code constructions of McEliece and Niederreiter on algebrogeometric codes (elliptic codes over the field GF (2^8), which provide protection against the Sidelnikov attack and reduce energy consumption. In addition, they provide an integrated error correction in the information sequence [2].

To ensure authenticity in the post-quantum cryptoperiod, it is proposed to use the improved UMAC algorithm based on the crypto-code structures of McEliece (Niederreiter) [18, 28], which makes it possible to meet the requirements for the efficiency of processing information flows, to ensure the "preservation" of the universality property.

The scheme for transmitting a message from the sender to the recipient and checking the integrity of the received message by comparing the codegrams and hash codes using the McEliece CCC on the MEC is shown (fig. 1).

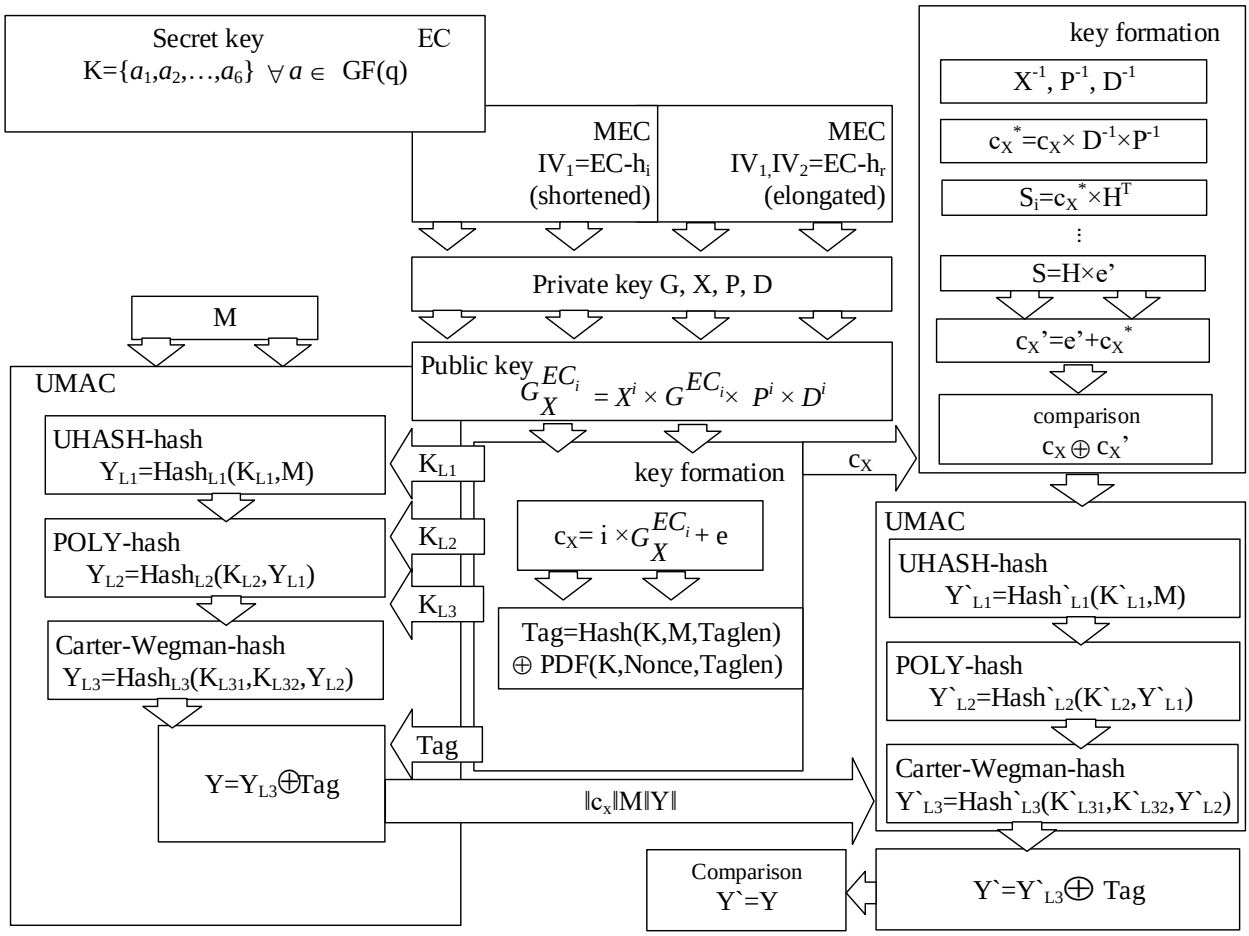


Fig. 1. Structural diagram of the UMAC protocol on the McEliece CCC with MEC

The crypto-code construction of McEliece on elliptic codes (MEC) acts as an algorithm for the formation of the substrate. The application of modification changes to elliptic codes reduces the load on computing resources and leads to an increase in the efficiency of generating MAC codes in real time. At the heart of the SSL/TLS protocol enhancements are complex algorithms based on post-quantum algorithms that allow the provision of security services, taking into account the elimination of vulnerabilities based on the use of the handshake phase.

At the present stage, two versions of the SSL/TLS protocol versions v.1.2, v.1.3 are used, their architecture consists of two protocols:

I – handshake protocol (appointment - authentication and key exchange), according to which the Client and Server perform the following procedures:

- protocol version negotiation;
- choice of cryptographic algorithm or cipher suite;
- authentication with asymmetric cryptography;
- determining the shared secret key to be used for symmetric encryption at the next level;

II – recording protocol. At this level, the following procedures are performed:

- all outgoing messages are encrypted with the secret key set during the handshake;
- encrypted messages are transmitted from the Client to the Server;
- server checks received encrypted messages for changes;
- if no changes are made, encrypted messages are decrypted using the secret key.

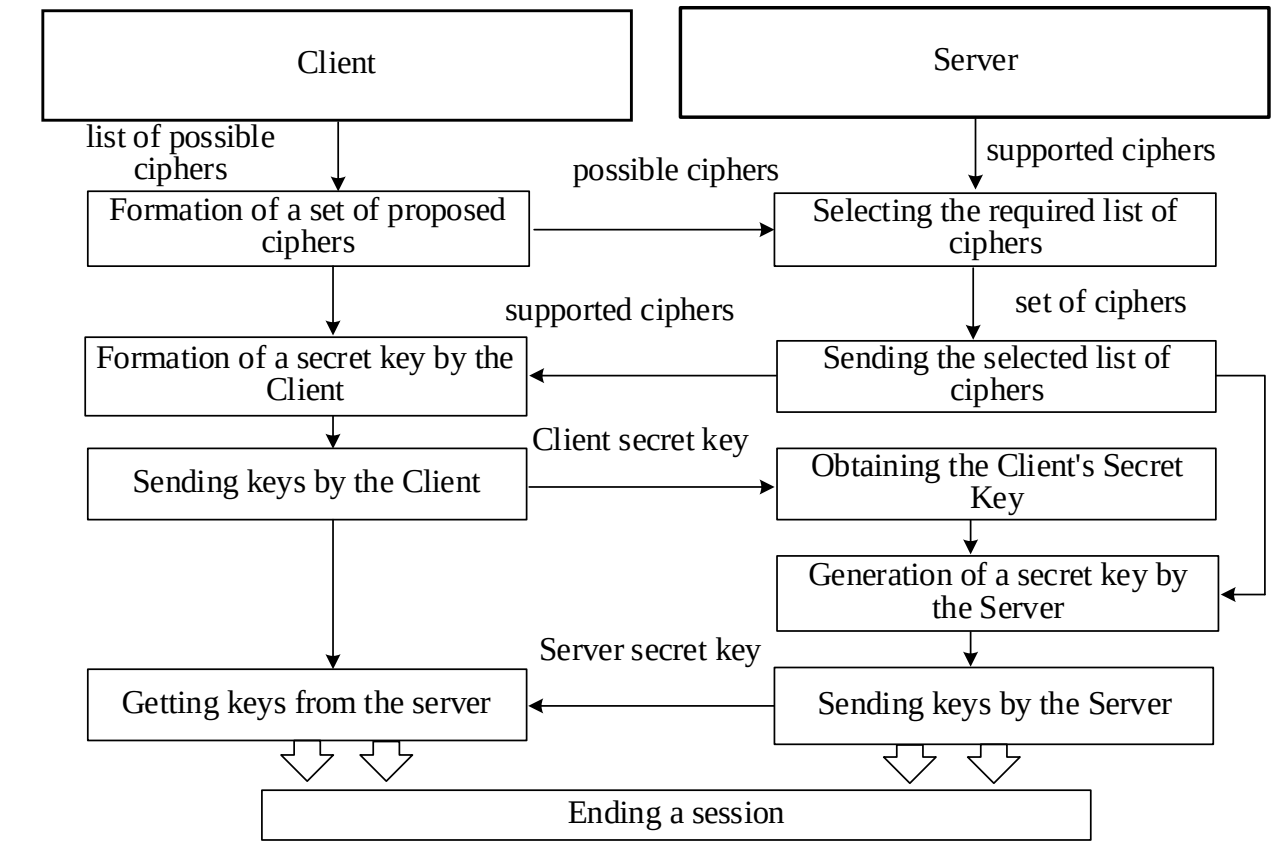
To ensure that an encrypted message has not been altered during transmission, the TLS v.1.3 protocols use authenticated encryption (AEAD mode), in Figure 1-3. Figure shows the differences between the versions of the SSL/TLS protocol stack (fig. 2).

The fundamental difference between version 1.2 and version 1.3 is the rejection of the choice of various symmetric encryption algorithms (version 1.2 was the choice) and the use of complex algorithms for generating an authenticated message in AEAD mode (version 1.3). However, even in version 1.3, the handshake protocol (phase) remains vulnerable, in which a secret (shared) key is exchanged for general use in the selected symmetric cryptoalgorithm, both on the server and on the client side.

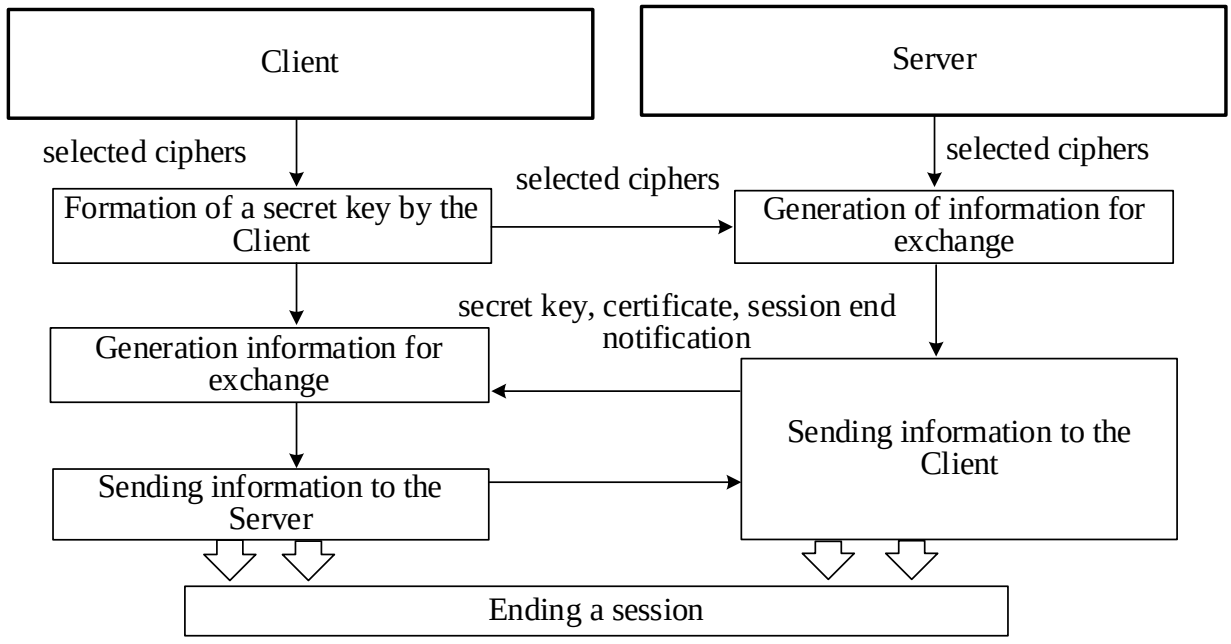
In addition, the algorithms used in version 1.2 and version 1.3 are not post-quantum algorithms and cannot guarantee the required level of security in the context of the emergence of a full-scale quantum computer. To provide security services and eliminate vulnerabilities in the handshake phase of the SSL/TLS protocol, it is proposed to transmit only the parameters of the equation of the curve, as well as, if necessary, the initialization vectors of the modified elliptic codes.

Thus, to generate key data both on the server side and on the client side, it is enough to transfer only the coefficients a1, a2, a3, a4, a5, a6, that is, a binary sequence of five characters. At the same time, both parties will be able to

form the necessary matrices and be ready to exchange information. In addition, there is no need to use additional asymmetric algorithms (Diffie-Hellman, RSA) to transfer key data for a symmetric algorithm (in the proposed case, asymmetric cryptosystems are used with a crypto transformation rate comparable to symmetric cryptoalgorithms). Figure shows an improved scheme of the SSL/TLS protocol (fig. 3).



a)



b)

Fig. 2. Block diagrams of the SSL/TLS protocol: a) version 1.2, b) version 1.3

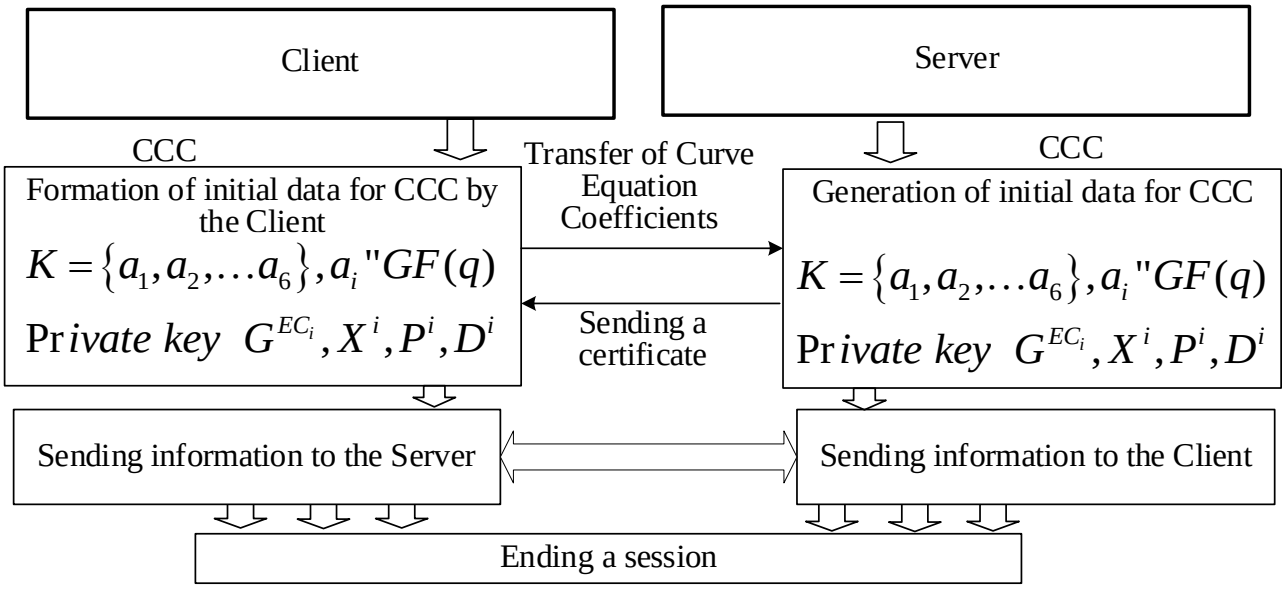


Fig. 3. Advanced SSL/TLS Protocol Scheme

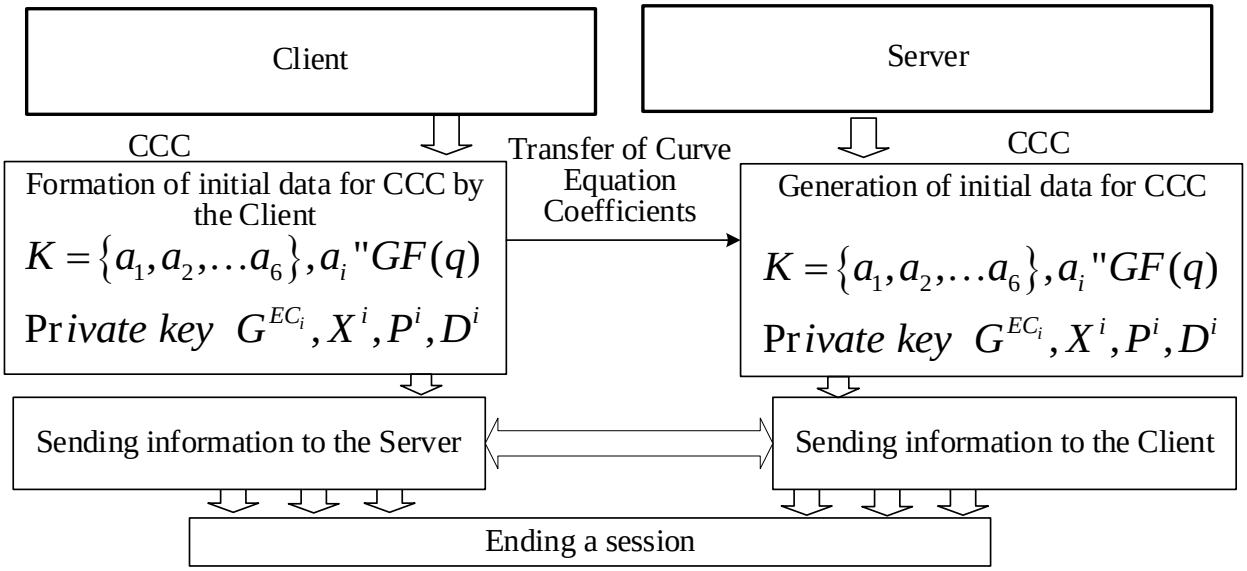


Fig. 4. Enhanced SSL/TLS Block Diagram in 0-RTT Mode

If it is necessary to "restore" the session in 0-RTT mode, there is also no need to exchange key data and part of the encrypted code to verify the correctness of the shared key definition. It is enough for the client to send only the coefficients of the curve for the server to determine the key data for the CCC. The use of the error vector *e* when transmitting information allows it to be considered as a session key for each individual packet, which significantly increases the security level. Figure 4 shows the block diagram of the enhanced SSL/TLS protocol in 0-RTT mode. This approach eliminates possible replay attack vulnerabilities and provides the required level of security (perfect forward secrecy). The use of asymmetric cryptoalgorithms (post-quantum algorithms – crypto-code constructions of McEliece (Niederreiter) on MEC, flawed codes, "simplifies" key exchange and does not require additional energy (computational) costs for the use of asymmetric cryptoalgorithms. In addition, the use of noise-immune codes allows "vary" by the error vector indicator *e* (session password for each packet) and provide either an increase in the level of security or an increase in the level of reliability. Thus, an improvement is proposed for the most common protocol for providing security services at the transport level SSL/TLS based on post-quantum algorithms – crypto-code constructions based on modified (shortened and/or extended) elliptic codes. This approach significantly reduces the "possibility" of known vulnerabilities to the SSL/TLS protocol. This ensures the required level of security in the post-quantum cryptoperiod, computational and energy-intensive requirements for use in cyber-physical systems based on smart technologies.

Conclusions. The proposed SSL/TLS transport layer protocol is based on complex algorithms – McEliece (Niederreiter) crypto-code constructions on MECs (flawed codes) with an improved cascade hashing algorithm. This approach significantly reduces the "possibilities" of known vulnerabilities to the SSL/TLS protocol by using only asymmetric cryptosystems, and by "simplifying" the handshake phase. The proposed protocol improvement eliminates the need to exchange a separate key before trans-

ferring data, use asymmetric encryption algorithms to exchange key data (certificates). This ensures the required level of security in the post-quantum cryptoperiod, computational and energy-intensive requirements for use in cyber-physical systems based on smart technologies.

References

[1]. Arora, J., K R, R., R, S., Ghantasala, G.S.P. Securing web documents by using piggybacked framework based on Newton's forward interpolation method (2023) Journal of Information Security and Applications, URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85153277373&doi=10.1016%2fj.jisa.2023.103498&partnerID=40&md=02f8677ebd2fb80a4ff29ac6d01c50ec. DOI: 10.1016/j.jisa.2023.103498.

[2]. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. Kharkiv: PC TECHNOLOGY CENTER, 2022. 196 p.

[3]. Saribas, S., Tonyali, S. Performance Evaluation of TLS 1.3 Handshake on Resource-Constrained Devices Using NIST's Third Round Post-Quantum Key Encapsulation Mechanisms and Digital Signatures (2022) Proceedings - 7th International Conference on Computer Science and Engineering, UBMK 2022, pp. 294-299. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85141847461&doi=10.1109%2fUBMK55850.2022.9919545&partnerID=40.

[4]. Khan, N.A., Khan, A.S., Kar, H.A., Ahmad, Z., Tarmizi, S., Julaihi, A.A. Employing Public Key Infrastructure to Encapsulate Messages during Transport Layer Security Handshake Procedure (2022) Proceedings - AiIC 2022: 2022 Applied Informatics International Conference: Digital Innovation in Applied Informatics during the Pandemic, pp. 126-130. URL: https://www.scopus.com/ inward / record.uri?eid = 2-s2.0-85141365676&doi=10.1109 %2fAiIC54368.2022.9914605&partnerID=40.

[5]. Ramraj, S., Usha, G. Signature identification and user activity analysis on WhatsApp Web through network data (2023) Microprocessors and Microsystems, 97, URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146098976&doi=10.1016%2fj.micpro.2023.104756&partnerID=40&md5.

[6]. Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. Kharkiv: PC TECHNOLOGY CENTER, 2021. 188 p.

[7]. Gavrilova A. Development of a modified UMAC Algorithm based on crypto-code constructions / A. Gavrilova, I. Volkov, Yu. Kozhedub, R. Korolev, O. Lezik, V. Medvediev, O. Milov, B. Tomashevsky, A. Trystan, O. Chekunova // Eastern-European Journal of Enterprise Technologies. 2020. № 4/9 (106). C. 45-63.

[8]. 19. Guide for Cybersecurity Event Recovery, 2022. URL: https: // nvlpubs.nist.gov / nistpubs /.../ NIST.SP. 800-184.pdf.

[9]. Security requirements for cryptographic modules, 2020, URL: https://csrc.nist. gov/publications/fips/fips 140-2/fips1402. pdf.

[10]. Guide to LTE Security, 2020, URL: https:// csrc.nist.gov / publications / drafts / 800-187 /sp800_187_ draft.pdf.

[11]. Report on Post-Quantum Cryptography, 2022, URL: https: // csrc.nist.gov / publications/detail/nistir/ 8105/final.

[12]. Daniel J. Bernstein Johannes Buchmann Erik Dahmen. Post-Quantum Cryptography, 2020, URL: https://www.researchgate.net /profile/Nicolas_Sendrier / publication / 226115302_Code -Based _ Cryptography/ links/ 540d62d50cf2df04e7549388 / Code-Based-Cryptography.pdf.

УДК 004.056.4: 004.272

Мілевський С., Воропай Н., Король О., Євсеєв С., Аксьонова І. Протокол SSL/TLS на постквантових алгоритмах

Анотація. *Розвиток мобільних технологій та їх інтеграція з Інтернетом речей і розумними технологіями формують як кіберфізичні, так і соціально-кіберфізичні системи. У таких системах, як правило, використовуються бездротові канали зв'язку, в яких для надання послуг безпеки (конфіденційності, цілісності та автентичності) використовуються протоколи SSL/TLS. Однак цей протокол не тільки вразливий до атак "Meeting in the Middle", POODLE, BEAST, CRIME, BREACH, але з появою повномасштабного квантового комп'ютера його можна зламати. У статті запропоновано протокол на основі квантових алгоритмів – криптокодових конструкцій, який забезпечить не лише стійкість до поточних атак, а й стабільність у постквантовий період. Для забезпечення «гібридності» сервісів пропонується використовувати конструкції криптокодів МакЕліса і Нідеррайтера і вдосконалений алгоритм UMAC на основі дизайну криптокодів МакЕліса. Використання криптокодових конструкцій забезпечує не тільки стійкість до атак, але й спрощує формування з'єднання – для передачі загального ключа використовуються параметри еліптичних кривих. Такий підхід значно скорочує час підключення мобільних гаджетів і спрощує процедуру узгодження перед передачею даних.*

Ключові слова: *протокол SSL/TLS, криптокодові конструкції, алгоритм UMAC, алгебраїчні геометричні коди, коди з втратами.*

Мілевський Станіслав Валерійович, кандидат економічних наук, доцент кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут», Україна.
Stanislav Milevskyi, candidate of economic sciences, associate professor of cybersecurity department National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Воропай Наталія Ігорівна, кандидат технічних наук, доцент кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна.
Natalya Voropay, candidate of technical sciences, associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Король Ольга Григорівна, кандидат технічних наук, доцент кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут», Україна.
Olha Korol, candidate of Technical Science, associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Євсеєв Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут», Україна.
Serhii Yevseiev, doctor of technical science, professor, head of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Аксьонова Ірина Вікторівна, кандидат економічних наук, доцент кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут», Україна.
Iryna Aksonova, candidate of economic sciences, associate professor of cybersecurity department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Отримано *7 березня 2024 року*, затверджено редколегією *1 квітня 2024 року*