Vladyslav KHVOSTENKO[1], Olha KOROL[2]

Scientific supervisor: Serhii YEVSEIEV[3]

DOI: https://doi.org/10.53052/9788366249868.07

PROTOKÓŁ PRYWATNOŚCI KANAŁU GSM DOTYCZĄCY KONSTRUKCJI KRYPTO-KODÓW

Streszczenie: Opracowano nowy protokół zapewniający poufność kanału GSM w oparciu o algorytmy postkwantowe - konstrukcje kryptokodów Mal-Elisa i Niederreitera na algebraicznych kodach geometrycznych. Zastosowanie zmodyfikowanych i/lub wadliwych kodów pozwala konstrukcjom krypto-kodu zachować poziom bezpieczeństwa i znacznie zmniejszyć moc pola Galois. Artykuł proponuje zasadniczo nowy kierunek wykorzystania struktur krypto-kodu w postaci urządzenia programowo-sprzętowego, które pozwala na opracowanie systemu bezpieczeństwa dla wiadomości głosowych w trybie offline, przy jednoczesnym zapewnieniu opłacalności i bezpieczeństwa protokołów głównego ruchu mobilnego kanału internetowego. Takie podejście umożliwia świadczenie podstawowych usług bezpieczeństwa w szerokim zakresie zastosowań praktycznych opartych nie tylko na mobilnym kanale internetowym, ale także na kanałach bezprzewodowych, przy tworzeniu systemów opartych na technologiach Internetu rzeczy, sensorów i sieci Mesh .

Słowa kluczowe: kryptoalgorytmy post-kwantowe, konstrukcje kryptokodowe McEliece'a i Niederreitera, Internet mobilny.

GSM CHANNEL CONFIDENTIALITY PROTOCOL ON CRYPTO-CODE CONSTRUCTIONS

Summary: A new protocol has been developed to ensure the confidentiality of the GSM channel. This protocol is based on post-quantum algorithms - crypto-code constructions of McEliece and Niederreiter on algebraic geometric codes. The use of modified and / or defective codes allows to maintain the level of security and significantly reduce the power of the Galois field by crypto-code constructions. The article proposes a fundamentally new direction of using crypto-code constructions (CCC) in the form of a software and hardware device that allows to form a security complex for voice messages in offline mode, that ensuring the profitability and

[1] Associate Prof., PhD, Simon Kuznets Kharkiv National University of Economics, a Associate Professor of Department of Cyber Security and Information Technology vladyslav.khvostenko@gmail.com

[2] Associate Prof., PhD, Simon Kuznets Kharkiv National University of Economics, a Associate Professor of Department of Cyber Security and Information Technology olha.korol@hneu.net

[3] Senior Research. D.Sc., Simon Kuznets Kharkiv National University of Economics, a head

safety of the main traffic of the mobile Internet channel protocol. This approach allows the possibility to provide basic security services in a wide range of practical applications based on not only the mobile Internet channel, but also on wireless channels, in case of forming systems based on the technologies of the Internet of things, sensor- and Mesh-networks.

Keywords: post-quantum cryptoalgorithms, crypto-code constructions of McEliece and Niederreiter, mobile Internet

1. Introduction

The development of computing and mobile technologies determined the vector of development not only of digital services based on the mobile Internet, but also significantly increased the number of attacks on mobile applications, while the analysis of threats to mobile Internet channels, operating systems and technologies confirms their integration, synergy and hybridize [1–6]. Moreover, the emergence of a full-scale quantum computer can lead to a significant decrease in the level of resistance of symmetric and asymmetric cryptosystems, partial or complete destruction / hacking of network architectures. This result can reduce the range of digital services significantly. The main advantage over computer networks of LTE (4G) technology is a high data transfer rate than in IEEE 802.X. However, with all the advantages, there is a significant drawback - the almost complete absence of security services, which largely does not allow users to receive the required level of service quality. This disadvantage is inherent in the new generation networks of 4G – 6G technology based on the Diameter protocol. This protocol provides 3A services (identification, authorization and authentication), however, the provision of confidentiality services (ensuring the protection of information during transmission from passive attacks), and integrity (ensuring protection during storage and the possibility of modification only by an authorized user in networks based on the Diameter protocol is not provided). This approach allows attackers to use mobile Internet channels not only as channels of information leakage, but also as the main channels of access to computer networks and systems [1–6].
Thus, the task of ensuring the required level of safety in the post-quantum period is urgent.

2. Analysis of the last researches and publications

To provide security services in the post-quantum period, it is necessary to introduce new post-quantum cryptography algorithms. To this end, the US National Institute of Standards and Technology (NIST) opened a competition for post-quantum cryptography algorithms in February 2019. At the third stage, among the four applicants for an asymmetric post-quantum cryptography algorithm, the classical scheme of McEliece's crypto-code construction is presented. However, in [7], the studies carried out confirm that the construction of a classical scheme that will provide the required level of resistance in the post-quantum period is necessary over GF (2^{10}–2^{13}), which significantly narrows their application. In order to eliminate this drawback, the works [7–10] proposed schemes of crypto-code constructions by

McEliece and Niederreiter on modified elliptic codes (algebraic geometric codes based on coding theory algorithms using elliptic curve parameters). The development and analysis of the construction of crypto-code constructions on algebraic geometric codes are described in [7–10]. In [7], models and practical algorithms for the use of hybrid crypto-code constructions on defective codes are proposed, which significantly reduces the power of the Galois field (the power of the alphabet of the post-quantum algorithm) and allows to implement of crypto-code constructions on smart and microchips practically.

3. Research problem

Investigation of the possibility of closing the voice mobile Internet channels in offline mode based on a complex of post-quantum algorithms - crypto-code constructions of McEliece and Niederreiter.
2. Development of a protocol for closing the voice channel of the mobile Internet.
To close the GSM voice channel, it is proposed to use a hardware and software complex that provides offline confidentiality of voice messages on the basis of post-quantum encryption algorithms – McEliece and Niederreiter crypto-code constructions on algebraic geometric codes. The block diagram of the communication organization is shown in Fig. 1.

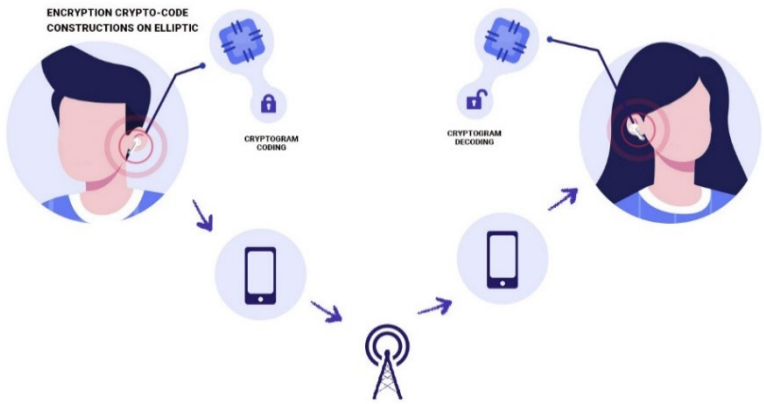

Figure 1. Block diagram of GSM voice channel closure

To ensure the closure, specialized chipsets are used in which encryption algorithms are implemented based on the McEliece crypto-code construction. In this case, the analog signal of the message after entering the headset is converted into digital form and immediately goes to the encoder. The encrypted message is transmitted via the Bluetooth channel to the mobile gadget. After that, the protocols of the GSM mobile Internet channel are used. This approach makes it possible to use standard procedures for subsequent transformations, ignore manufacturers and modifications of both headsets and mobile gadgets, and ignore modifications of both the Bluetooth channel and the mobile Internet technology. In addition, it can significantly reduce the cost of

production and implementation of this approach. To implement the protocol for closing a voice GSM channel, it is proposed to use a mobile messenger and a key data server presented in Fig. 2.

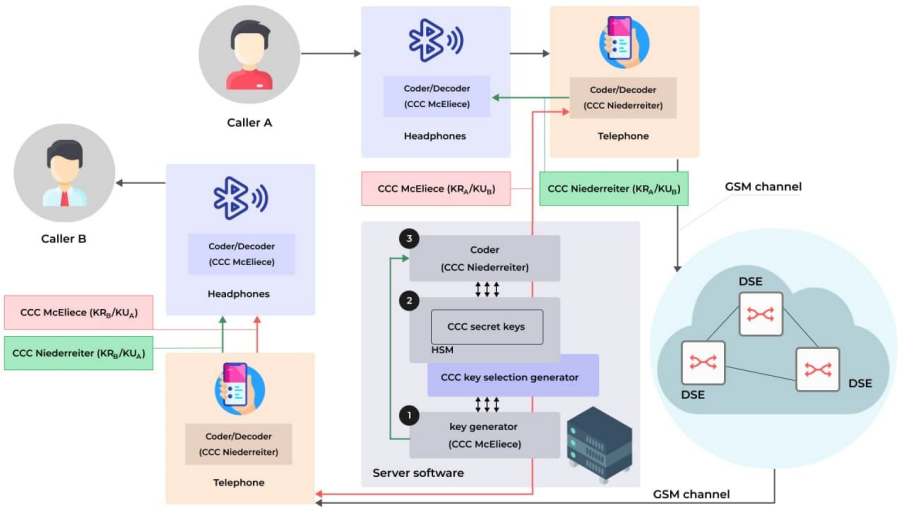

Figure 2. Block diagram of the protocol for closing a voice GSM-channel based on CCC

The complex of means of protection is built taking into account the most modern developments in the field of post-quantum cryptography based on crypto-code constructions. At the same time, the complex provides maximum protection of your conversations from unauthorized access. To ensure security, only the session password is recorded in the headphones, depending on the role (sender, recipient), which are recorded from the mobile application. After the end of the conversation, they are deleted.

To ensure the security of the transmission of key data for conducting a conversation, the channel between the mobile application and the server is encrypted based on an asymmetric cryptosystem – a post-quantum algorithm of the Niederreiter crypto-code construction.

To ensure the security of the server side, after the keys are generated for the conversation and their transfer to the sender and the recipient, the RAM is reset to zero. The secret keys of the McEliece and Niederreiter crypto-code constructions change with different periods of time. Consider a voice message security protocol based on post-quantum algorithms:

CALLER A (initiator of the call)

1. Opens the telephone line software and finds the corresponding caller in the list of callers (CALLER B)

2. Sends a request to caller B through the server.

3. Receives on the phone software through a private channel (encryption based on the Niederreiter's CCC in the EC is used) a private key, and a public key of caller B.

4. Confirms the willingness to talk. In this case, the personal key (KRA) and the public key KUB are transmitted from the phone software via the Bluetooth channel.

5. The key is recorded in the Bluetooth headset in the encoder (C/DC).

6. After recording the key, a ready signal is generated.

7. After confirmation of the readiness of caller B, the conversation is carried out.

SERVER SOFTWARE

1. At the request of subscriber A in (2), the CCC key selection generator randomly selects the key parameters and transmits it to (1).

2. In (1) secret keys are received from HSM (masking matrices – X, P, D, and generating matrix GEC).

3. In (1), KR_A (personal key of McEliece CCC of caller A) and KU_A (public key of caller A) are generated.

4. At the response of caller B, a public key KU_B is generated and transmitted to caller A.

5. The generated KRA and KU_A come to (3) from (1), after the keys are transferred to (1), the data is erased.

6. In (3) KR_A and KU_A, KU_B are encrypted.

7. From (3), respectively, KR_A, KU_B are sent to caller A (the caller who initiates the call), KU_A – to caller B (the caller who is called), after the keys are transferred to (3), the data is erased.

CALLER B (call recipient)

1. Receives a request from the server to the phone software to transfer the public key (KU_A).

2. Confirms the request to the server, sends KR_B.

3. Receives the public key KU_A to the phone software through a private channel (encryption based on the Niederreiter CCC on the EC is used).

4. Confirms the willingness to talk. In this case, the public key (KU_A) is transmitted from the phone software via the Bluetooth channel.

5. In the Bluetooth headphones, the key is recorded in the decoder (C/DC).

6. After recording the key, a ready signal is generated.

7. After confirming that it is ready, caller B sends a signal to the server that it is ready to talk.

Thus, the proposed protocol ensures the closure of the mobile Internet channel using a complex of software and hardware. The use of a hardware solution for closing (encrypting) a voice message in a headset will provide resistance to almost all threats, and the use of a key server provides a tunnel mode, which excludes the possibility of "eavesdropping" of voice messages.

4. Conclusions

A protocol for closing a voice mobile Internet channel based on post-quantum algorithms, which uses the complex proposed by the authors and based on the crypto-code constructs of McEliece and Niederreiter. This approach provides the required

level of strength (cryptographic strength at the level of 1030-1035 group operations), efficiency (the speed of cryptographic transformations is provided - encoding / decoding of a codeword / cryptogram at the level of the speed of cryptographic transformations of symmetric block ciphers with a key length of 128 bits) and the reliability of voice messages ($P_{error} = 10^{-9}–10^{-12}$) in the post-quantum period.

REFERENCES

1. Report on Post-Quantum Cryptography // [Online], available: *http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR. 8105.pdf*
2. Protokol DIAMETR. Tehnicheskie materialy IBM // URL: *http://www.ibm.com/developerworks/ru/library/wi-diameter/*
3. A Comprehensive Survey of Prominent Cryptographic Aspects for Securing Communication in Post-Quantum IoT Networks // URL: *https://www.sciencedirect.com/science/article/pii/S2542660520300159.*
4. Ugrozy bezopasnosti jadra paketnoj seti 4G // URL: *https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/* (data obrashhenija: 20.04.2020).
5. Ujazvimosti protokola Diameter v setjah 4G // URL: *https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/* (data obrashhenija: 20.04.2020).
6. STEPANOVA I.V.: Analiz perspektivnyh podhodov k povysheniju nadezhnosti konvergentnyh korporativnyh setej svjazi / I. V. Stepanova, Ahmed Abdulvasea, Ndajinkunda Zhuv // T-Comm: Telekommunikacii i transport. – 2015. – Tom 9. – №12. – S. 44 – 51.
7. YEVSEIEV S. (ed), PONOMARENKO V., LAPTIEV O., MILOV O.: Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
8. YEVSEIEV S., TSYHANENKO O., GAVRILOVA A., GUZHVA V., MILOV O., MOSKALENKO V. et. al. (2019): Development of Niederreiter hybrid crypto-code structure on flawed codes. Eastern-European Journal of Enterprise Technologies, 1 (9 (97)), 27–38. doi: http://doi.org/10.15587/1729-4061.2019.156620
9. YEVSEIEV S., TSYHANENKO O., IVANCHENKO S., ALEKSIYEV V., VERHELES D., VOLKOV S. et. al. (2018): Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. doi: http://doi.org/10.15587/1729-4061.2018.150903.
10. YEVSEIEV S., HRYHORII K., LIEKARIEV Y. (2016): Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. doi: http://doi.org/10.15587/1729-4061.2016.86175