Cryptographic protection of classified information in military radio communication faced with threats from quantum computers

Robert Wicik, Mariusz Borowski
Military Communication Institute, Warszawska 22A, 05-130 Zegrze, Poland

ABSTRACT

Classified information protection is regulated by dedicated acts and related laws that require use of necessary physical, personal, information and communication technologies, electromagnetic and cryptographic security measures. Equipment and tools for cryptographic protection of classified information should be examined and assessed by the designated government services. Certificates issued by these services authorize the use of cryptographic devices to protect classified information, but this is not a sufficient condition. Each ICT system intended for processing classified information is subject to accreditation. All this makes the process of reaching the right level of protection for this type of information long and expensive – especially if this protection should be effectively provided in the battlefield. Additional specific requirements are put on information protection measures for radio communication, especially military, where radio transmission is characterized by uncertainty of establishing and maintaining connections, bit rates are lower than in cable or fiber optic connections, most often there is no full duplex. All this has an impact on the methods of cryptographic synchronization and implementation of cryptographic functions. A different approach to information protection is required by classic narrowband radio communications, a different one in time-division multi-access mode, and another one in broadband packet data transmission. Systems designed for the protection of classified information in radio communications implement appropriate operating modes of operation for cryptographic algorithms and protocols. Latest threats from quantum computers pose new challenges to the cryptographic protection, especially in systems using public key cryptography, because there are algorithms that can be used to attack public-key schemes with polynomial complexity.

Keywords: classified information protection, cryptography, cryptanalysis, quantum computers

1. INTRODUCTION

Classified information must be processed in conditions preventing its unauthorized disclosure. Secure ICT (Information and Communication Technologies) systems used for this purpose should be accredited by government services. Cryptographic devices and electromagnetic protection measures used within these systems must be assessed and certificated. These rules also apply to radio communication systems where classified information is transmitted. Cryptographic modules for narrowband and broadband radios are currently being developed. These projects must take into account the specifics of radio transmission in poor propagation conditions and with intentional interferences. Some aspects of the approach to information protection in radio communications are described in the following chapters.

The latest threats from cryptanalysis methods using quantum computers have an impact on cryptographic algorithms and protocols implemented to protect classified information. In the case of symmetric cryptography (with secret keys) there is a need to extend the keys. On the other hand, for asymmetric cryptography (with public key) additional security mechanisms should be used, and ultimately algorithms and protocols resistant to cryptanalysis on quantum computers should be developed.

2. PROTECTING CLASSIFIED INFORMATION

2.1 Statutory requirements

Today, statutory requirements regulate the principles of protecting classified information. Legal provisions describe the rules for classifying, processing and organizing the protection of classified information. Such information must be processed under conditions that prevent its unauthorized disclosure. Required level of security is defined depending on the clause of protected information. In particular, these rules apply to the protection of classified information in ICT

Radioelectronic Systems Conference 2019, edited by Piotr Kaniewski, Jan Matuszewski, Proc. of SPIE
Vol. 11442, 114420Q · © 2020 SPIE · CCC code: 0277-786X/20/$21 · doi: 10.1117/12.2565467

systems and there is no reduced tariff for systems operated in battlefield conditions. Each ICT system processing classified information should have accreditation certificate, i.e. admission to the processing of this type of information, which is confirmed on the basis of approved security documentation and the results of the ICT system security audit. This also applies to systems using radio means.

In ICT systems may be used electromagnetic protection devices and cryptographic devices and tools. A system prepared for classified information protection should use only certified devices. The certification process is intended to confirm the ability of the device to protect classified information. The current law does not allow the use of non-certified devices or tools for protecting classified information.

When building a cryptographic system for the protection of classified information, one must take into account potential threats, specify security features, perform the design and implementation, conduct security tests, and then ensure the proper implementation for use. It is an extremely costly process, requiring the participation of specialists from many fields and burdened with a high risk of changes and delays in implementation stages.

2.2 Cryptography and cryptanalysis

Cryptography and cryptanalysis are complementary parts of cryptology – a field that includes knowledge about secure storage and transfer of information. Cryptography deals with methods to ensure the confidentiality, integrity and availability of information, while cryptanalysis deals with attacks that allow an adversary to break these protections.

Algorithms and protocols are an important element of any cryptographic system. Cryptographic algorithms are constructed and used to provide services such as confidentiality, integrity, authentication and non-repudiation. Cryptographic protocols are used, among others, for authentication and key agreeing. All cryptographic algorithms and protocols need cryptographic data for operating, i.e. keys, passwords, random data, identification data. The security provided by these algorithms and protocols depends largely on keeping keys secret. Cryptographic algorithms and protocols are divided into two types: standard, commonly available algorithms (Suite B) and algorithms that have been developed under the supervision of the government services whose specification is not widely available (Suite A). The security of the algorithms themselves is based on their design and the lack of effective methods of cryptanalysis.

All cryptographic algorithms and protocols used to protect classified information must be accepted by national or NATO/EU services. The selection of appropriate algorithms and protocols and their operating modes depends not only on the protected information clause, but also on the specificity of a given system – including threats and transmission possibilities. Special cryptography modes and dedicated security profiles are often specified for radio communication. The latest threats from quantum computers also affect the selection of cryptography.

2.3 Encryption devices for special systems

Electronic, digital encryption devices have been designed for decades mainly for the needs of the army and special services, including those used to protect classified information in radio communication. One of the first devices of this type was developed in the 70s of the 20th century and used by the Land Forces and the Navy for the protection of data transmission in HF channels. In the following years, work was continued on encrypted data transmission devices and a complete digital radio with encryption was developed. One of the most important types of devices designed in the previous century were link and bulk encryption devices – used not only to protect information on wired routes, but also on radio links.

The end of the 20th century brought significant changes in the approach to the protection of classified information. We began to use standards in designing and assessing the security of cryptographic systems. We have started to use FPGA programmable systems, 32-bit RISC processors, multi-layer printed circuit boards, surface mount technology and electromagnetic information protection. Modern sets of cryptographic algorithms have been designed to meet security requirements. Efficient hardware methods for random numbers generation and complete systems for planning, generation and distribution of keys have been developed. Statutory requirements in the field of the protection of classified information has forced a formal approach to the certification of cryptographic devices and the accreditation of information protection systems.

The use of the newest electronic technologies, mechanical and electromagnetic security as well as newly designed cryptographic algorithms has allowed the construction of encryption devices to successfully pass the certification processes. Many certificates for encryption devices and key management systems have been issued over the last years. These include bulk and link encryptors and also devices for information protection in ISDN and IP networks. Link encryption devices are used to protect information in telecommunications systems using also radios. The IP encryptor can be used to protect information in radio networks too, if the packet data exchange is available.

Currently, research and development and also implementation works are underway, as well as certification processes for devices dedicated to radio transmission – narrowband, broadband also with Internet Protocols. These devices implement specific protocols for establishing encrypted connections and implementing encryption in operating modes dedicated to radio transmission.

2.4 Key management subsystems

An important element of any information protection system is the cryptographic key management subsystem, which is designed to meet the needs of cryptographic devices for cryptographic keys and other materials necessary for their work. Such subsystems are usually built with several modules responsible for:

- preparing a plan of secret connections – in radio networks this is based on the radio plan;
- generating cryptographic keys for a prepared plan;
- distribution of cryptographic keys to encryption devices – for this purpose telecommunications channels or courier distribution on electronic media are used;
- monitoring and management of the encrypted communication network – through encrypted and authenticated management channels.

Key management for the purpose of information protection in radio networks has its own specifics, hence keys loaded from electronic media directly to devices are often used to ensure their long-term operation even without radio communication with the management center. Also, establishing encrypted connections and agreeing session keys should be simplified – protocols with a small number of runs (sometimes with only one) and resistant to high error rates are used.

3. PROTECTION OF INFORMATION IN MILITARY RADIO COMMUNICATIONS

Military radio communication is characterized by the uncertainty of establishing and maintaining connections. Even if radios ensure high efficiency and quality of connections, in battlefield conditions, in the presence of an enemy actively affecting radio space, this statement is highly probable. The above has an impact on cryptographic algorithms and protocols used to protect information in radio communication, their modes of operation and key management subsystems.

3.1 Narrowband systems

Narrowband radio communication systems are most often organized to work in HF or VHF radio networks which enable the transmission of voice signals or serial data [3]. Some radios are equipped with built-in COMSEC or TRANSEC security modules designed for communication, transmission protection. Some have implemented more advanced modes of operation, e.g. ALE. There are also those that support packet data transmission (IP), selected services such as e-mail or tracking the position of troops [4]. A cryptographic module has been developed for this type of systems, which, as an external device, can be attached to any type of radio, if only it provides a compatible type of communication interface. Such a common interface turned out to be a synchronous serial interface, which is made available by modems of most narrowband HF and VHF radios.

The cryptographic module works synchronously with the clock given from the radio – so the type and transmission speed settings are made only in the radio, and the module adapts to them. The module can be connected with a handset and terminal devices via a synchronous or asynchronous serial interface. This module, like radios, works in simplex mode – one encrypts data at the transmitting radio and another one or more decrypts data at the receiving radios. Data transmission is controlled by send and receive signals (RTS, CTS, etc.), which allows it to be organized in half-duplex mode.

Voice signal, in order to be secret, is first transformed into digital form in the cryptographic module. Voice in the receiving modules, after decryption, is decoded to analog. The voice signal is controlled by the tangent of the handset attached to the cryptographic module. Encrypted voice signal is transmitted as serial data between the module and the transmitting radio, next to the receiving radios and the cryptographic modules attached to them.

Tests have shown effective cooperation of the cryptographic modules with many HF and VHF radios in various operating conditions and various modes of serial transmission. The use of the module did not affect the effectiveness of establishing connections and did not degrade the quality of voice and data transmission. This was possible thanks to the use of an appropriate cryptographic connection protocol – setting session keys and cryptographic synchronization, resistant to poor transmission conditions – high error rate, as well as a cipher mode adapted to simplex or half-duplex operation, which does not duplicate any transmission errors that may occur, while the radios maintain the continuity of transmitting and receiving clocks. It was also possible to obtain secret connections between radios of different manufacturers when they worked in compatible data transmission modes.

The main limitation introduced by the cryptographic module in cooperation with radios is the need to separate user signals, which should be kept secret by this module, from radio control signals that should reach the radio in an uncovered form. An additional disadvantage may be the additional delay in data and voice transmission introduced by the cryptographic module. The cryptographic module allows encryption at speeds adapted to the mode of operation of the radio, i.e. from 50 bit/s to even several dozen kb/s. This is quite enough for narrowband radios.

3.2 Broadband systems

Broadband radios allow us to build more advanced communications networks in terms of organization and management, throughput available to users and support for many types of services [2]. And just, as in narrowband radios, packet transmission is rather an addition to operating modes, so in broadband radios it is a standard. Hence, the approach to cryptographic information protection for broadband radios may be closer to classic IP networks. But, the specificity and limitations of radio systems still need to be taken into account. So, cryptographic protocols for authentication and agreeing of session keys should not delay the establishment of encrypted connections and also encryption modes should not overload the transmission channels with additional data.

Currently, broadband radios and standards implemented in them are being developed among allies. In the area of military radio communication so-called waveforms are developed defining a number of functions implemented in the radio that transform the user signals into signals emitted by the radio antenna. In addition, this type of radio has built-in intelligence enabling highly automated establishing and maintaining the appropriate quality of connections, organizing extensive wireless communication networks (also working in motion) and supporting the implementation of various services and applications for users. Examples of this type of waveforms are: ESSOR HDR (European Secure Software Defined Radio Program High Data Rate Waveform) and Coalition Wideband Networking Waveform (COALWNW).

In the area of information security, cryptographic protocols and algorithms with their operating modes and profiles specifying the specifics of their use are standardized within NATO, including those dedicated to radio communication [5]. The Secure Communications Interoperability Protocol (SCIP) standard [10] based on the American Future Narrowband Digital Terminal (FNBDT) project is dedicated to protect information transmitted over switched narrowband channels. SCIP operates at the application layer and allows establishing a secure voice connection or data transmission on a previously established duplex channel. SCIP operating on pre-placed keys (PPK) can also be used for communication on simplex radio channels and for point-to-multipoint communication. A version of this protocol is also defined over IP, which allows its use in broadband radios, but not all required operating modes have been covered by this standard so far. That is why NATO NII IP Network Encryption (NINE) standard [11] based on the American High Assurance Internet Protocol Encryptor (HAIPE) is designed to ensure the security of IP packet communications, also using radios. NINE uses the set of IPsec protocols to provide encryption and authentication of data sent in IP networks after prior authentication and key agreement of the communicating parties.

Cryptography in radios is used to ensure transmission security (TRANSEC), security of organized networks (NETSEC) and security of transmitted user information (COMSEC). Broadband radios provides interfaces, where in the data link layer dominates Ethernet and in the network layer – IP technology. Therefore, cryptographic solutions designed to protect information should be tailored to these technologies. The NINE standard is suitable for implementation in broadband radios based on IP packet transmission. The radio profile for NINE is being defined. Taking into account the specificity of radio communication, to the profile should be chosen those operating modes that burden the available communication channels as little as possible, and thus minimize the use of a trusted third party for authenticating and use pre-placed keys to establish secret relationships faster (compared to multi-pass authentication protocols and session key agreeing).

Key management is another important issue for secure connectivity. For SCIP and NINE standards, we can use asymmetric cryptography with public key or symmetric cryptography with secret keys. Secret keys (PPK, APPK) provided before the mission to communicating radios will allow faster and more reliable establishment of encrypted connections. This is beneficial in radio communication where there are deficits in the available bit rates. In addition, point-to-multipoint connections can be established only with secret pre-placed keys. Again, the use of public-key cryptography makes the encrypted connections more flexible, but requires a trusted third party, as well as authentication protocols and session key agreement that overload communication channels. Hence, the selection of the appropriate key management method must be preceded by an analysis to match the solution to the capabilities of radio networks as well as to the needs of users and security requirements.

4. THREATS TO CONTEMPORARY CRYPTOGRAPHY FROM THE CRYPTANALYSIS USING QUANTUM COMPUTERS

Symmetric cryptography algorithms are used to ensure data confidentiality, integrity and authentication. These algorithms are computationally effective, and their security is based on a secret, shared cryptographic keys. Such keys must be securely delivered to users, which will challenge the subsystem for the generation and distribution of cryptographic data. Also the flexibility (e.g. adding a new user) of symmetric key systems has some limitations.

Since the late 1970s of the 20th century, we have been observing the development of asymmetric cryptography with public-private key pairs and asymmetric key agreement protocols based on public parameters. Cryptography and protocols of this type allow to provide flexibility in the operation of telecommunication systems. Subsequent system users can join secure communication when they authenticate their public keys and parameters and keep their private keys secret. Protocols for key agreement of symmetric session keys, which are then used to protect the confidentiality of transmitted data, base on public-key cryptography [1].

Simultaneously with the development of public-key cryptography, we are observing the progress in their cryptanalysis. The previously known algorithms for solving computationally difficult problems, which are behind the security of public key cryptography, have the exponential complexity (memory or time) in the model of attack using classical computers. Unfortunately, in the model of attack using quantum computers, there are algorithms [9] that can be used to attack public-key schemes with polynomial complexity. For example, the Shor algorithm provides exponential acceleration of the factorization problem by using the superposition of quantum states [9]. Quantum computers also have a negative impact on the security of symmetric key cryptographic algorithms, because the Grover algorithm [7] and Simon's algorithm [8] allow the construction of effective, quantum attacks on this type of cryptographic transformations. For the practical implementation of the algorithms of Shor, Grover, Simon, which were developed in the 90s of the 20th century, there is a lack (for now) of efficient quantum computers with an industrial scale of application [1].

4.1 Security degradation of session key agreement protocols based on asymmetric cryptography

The possibility of launching an attack using a quantum computer has serious implications for the security of currently used cryptographic mechanisms applied during agreement of the session key using public key algorithms. Asymmetric algorithms and protocols (with public-private key pairs or with public parameters), based on difficult computational problems: factorization of integers (e.g. RSA) or discrete logarithm (e.g. DH, MQV, DSA, ECDH, ECMQV, ECDSA) [6], in the model of attack using a quantum computer, they no longer provide security [1]. This is due to the fact that there are algorithms that can be performed on a quantum computer, which significantly reduce the computational complexity of cryptosystems based on these problems.

Having a quantum computer, that will be able to effectively implement the Shor algorithm, it can be stated that cryptographic algorithms based on the factorization and discrete logarithm problems will lose their significance regardless of the length of the cryptographic key used, which is illustrated in Table 1. The *Effective key* column indicates the number key bits of a symmetric algorithm that would give a comparable level of security to the asymmetric algorithm listed in a given row of this table.

Table 1. Comparison of security of asymmetric algorithms.

Algorithm	Key length (bits)	Effective key length (bits)	
		Classical computer	Quantum computer
RSA-3072	3072	128	**0**
RSA-7680	7680	192	**0**
RSA-15360	15360	256	**0**
ECC-256	256	128	**0**
ECC-384	384	192	**0**
ECC-521	521	256	**0**

The security degradation, presented above, results from the fact that the time needed to break these cryptosystems will be much less than the time they need to effectively perform their cryptographic functions (e.g. confidentiality of the agreed key, or digital signature security).

4.2 Reduction of the security of symmetrical algorithms that ensure confidentiality

The Grover algorithm is an implementation of searching for an element that meets certain conditions in an unordered set with $N = 2^n$ elements. For example, it can be a name search by phone number stored in the classic phone book. This is a *BQP* (*Bounded-error Quantum Polynomial time*) computational problem. Classical algorithms require $O(N)$ operations, while the Grover algorithm requires only $O(\sqrt{N})$ operations, which gives a quadratic gain in performance. Let's consider a symmetric block algorithm using a cryptographic key with a length of k bits. Then the classical attack has the complexity of $O(N = 2^k)$, while the attack using the Grover algorithm on a quantum computer has the complexity of $O(N = 2^{k/2})$. In its operation, the Grover algorithm uses superposition of states, but the main distinguishing feature of the algorithm class to which it belongs is amplification and the use of features that distinguish amplitude from probability [7].

The effectiveness of an attack using the Grover algorithm does not depend on the currently used symmetric algorithm that ensures confidentiality, but only on the bit length of the cryptographic key used, as illustrated in Table 2.

Table 2. Comparison of security of symmetrical algorithms.

Algorithm	Key length (bits)	Effective key length (bits)	
		Classical computer	Quantum computer
AES-256	256	256	128
MEDLEY-256	256	256	128
CAST-256	256	256	128

Scientific analyzes indicate that in the case of symmetric algorithms ensuring confidentiality (in the context of quantum computers) security can be ensured by extending the cryptographic keys from 256 bits up.

4.3 Security reduction of cryptographic hash functions

The family of cryptographic hash functions is also vulnerable to a quantum attack using the Grover search algorithm [7]. The Grover algorithm can be used to find collisions for cryptographic hash functions, with complexity being the square root of the complexity resulting from the length of the hash generated by the function, as is the case with searching a disordered database. In addition, it has been proven that it is possible to combine the Grover algorithm with the birthday paradox – we will then get a quantum birthday attack method. By creating an array of size $\sqrt[3]{N}$ and using the Grover algorithm to find collisions, it is possible to construct an effective quantum attack. This means that in order to provide b-bit security against an attack using the Grover algorithm running on a quantum computer, the cryptographic hash function must generate a 3·b bit hash. Therefore, in order to ensure 128-bit security of the integrity of information secured using the SHA-3 hash function, it is necessary to use its version designating the 384-bit hash. Table 3 presents a comparison of the security of cryptographic hash functions in a classical birthday attack method and a birthday quantum attack method. The *Attack Efficiency* column contains the base 2 logarithm of the attack complexity on the cryptographic hash function in both classical and quantum attack models.

Table 3. Comparison of security of cryptographic hash functions.

Algorithm	**Hash (bits)**	**Attack effectiveness ($\log_2$)**	
		Classical computer	**Quantum computer**
SHA-2-256	256	128	85
SHA-3-256	256	128	85
SHA-2-384	384	192	128
SHA-3-384	384	192	128

The cryptographic functions SHA-2 and SHA-3, which determine the hash of at least 384 bits, remain secure against attacks using quantum computers.

4.4 Loss of security of data authentication modes applying symmetric algorithms

Data authentication modes are designed to guarantee the authenticity of the message. The standard security model is that it is difficult to forge a message with a valid tag, even having access to the oracle, which calculates the MAC (Message Authentication Code) tag of each selected message (of course, for a forged message the oracle cannot be asked). In order to transfer this concept of security to a quantum case, it is assumed that the opponent receives an oracle that accepts the quantum superposition of the message as input and calculates the superposition of the corresponding MAC [8]. In the quantum attack model, the Simon algorithm helps to solve the following problem.

Simon's problem for a given Boolean function

$$f: \{0, 1\}^n \rightarrow \{0, 1\}^n \tag{1}$$

is to find such an n-bit mask s that:

$$f(x) = f(y) \Leftrightarrow x \oplus y \in \{0^n, s\} \tag{2}$$

This problem can be solved classically by looking for a collision. The time complexity of finding a solution to this problem is $\Theta(2^{n/2})$. On the other hand, Simon's algorithm solves this problem with $O(n)$ quantum complexity.

The Simon algorithm performed on a quantum computer allows an attack with polynomial complexity on the following authentication modes using symmetric algorithms as ideal permutations: CBC-MAC, PMAC, GMAC, GCM, OCB, causing the loss of authenticity of secured data [8]. The computational complexity of the attack is only $O(n)$, where n is the length in bits of the data block processed by the symmetric algorithm, and is generally 128. Loss of authentication security in an attack model using a quantum computer immediately translates into the security problem of the mentioned above NINE standard using the set of IPsec protocols ensuring encryption and authentication of data sent in IP networks, also using the authenticated GCM encryption mode. The success of the attack on the authentication mode does not depend on the currently used symmetric algorithm.

5. SUMMARY

Building a cryptographic system for the protection of classified information we must consider various aspects of potential threats, security features, design and implementation, security tests, and implementation for use. This process requires the participation of specialists from many fields and is at risk of changes and delays. Equipment and systems designed for cryptographic protection of classified information should be examined and assessed by the government services. Additional specific requirements are put on information protection measures for radio communication, especially military, where radio transmission is characterized by uncertainty of establishing and maintaining connection, bit rates are lower than in cable or fiber optic connections, most often there is no full duplex. All this has an impact on implementation of cryptographic algorithms and protocols, which should use simplified operating modes. This applies in various ways to narrowband and broadband radios. Also, key management systems operating for a cryptographic protection of radio communications should not be too heavy for this communication.

We are currently facing further challenges related to information security, also in radio communications. Available scientific analyzes indicate that cryptographic algorithms are at risk from quantum computers. Symmetric algorithms ensuring confidentiality should be strengthened by extending the cryptographic keys from 256 bits up. However, this will affect their performance and probably will require an analysis of resistance to other cryptographic attacks. It is also possible to use cryptographic hash functions which are safe in the classical model, determining a hash of at least 384 bits, which remain resistant to attacks using quantum computers. Also other secure modes can be selected for data authentication that use symmetric algorithms.

It will probably take several years to build quantum computers useful to cryptanalysis. However asymmetric algorithms should be made today resistant to the specific properties of quantum computers, for example by using symmetric techniques. In the near future, these algorithms must be replaced with new ones. United States NIST has initiated a process to evaluate and standardize quantum-resistant public-key cryptographic algorithms. The second round of the competition is already underway. Newly developed asymmetric algorithms, resistant to cryptanalysis using quantum computers, should be used especially in classified information protection systems with the highest security levels.

The above-mentioned recommendations should be implemented in the cryptographic modules being developed to protect classified information in radio communication systems to ensure an adequate level of security, not only today, but also in the future, when the threat from quantum computers will be real.

REFERENCES

[1] Borowski M., Gocałek J., Wicik R., *Zabezpieczenia protokołu uzgadniania kluczy sesji przed kryptoanaliza przy wykorzystaniu komputerów kwantowych*, KSTiT, Wrocław, Przegląd telekomunikacyjny nr 7/2019.

[2] Matyszkiel R., Kaniewski P., Polak R., Laskowski D., *The results of transmission tests of polish broadband SDR radios*, IEEE Communication and Information Technologies, 2017.

[3] Wiśniewski M., Dobkowski A., Matyszkiel R., Kaniewski P., Grochowina B., *Test results of Polish SDR narrowband radio*, IEEE Communication and Information Technologies, 2017.

[4] Małowidzki M., Kaniewski P., Matyszkiel R., Bereziński P., *Standard tactical services in a military disruption-tolerant network: Field tests*, IEEE Military Communications Conference (MILCOM), 2017.

[5] Różański G., *Strategie bezpiecznej komunikacji w sieciach wydzielonych*, KSTiT, Gliwice, Przegląd telekomunikacyjny nr 8-9/2016.

[6] Dąbrowski P., Gliwa R., Szmidt J., Wicik R., *Generation and Implementation of Cryptographically Strong Elliptic Curves*, Number Theory Methods in Cryptology (NuTMiC), Warszawa, LNCS 10737, 2017, p. 25-36.

[7] Grover L. K., *A fast quantum mechanical algorithm for database search*, Bell Labs, 1996.

[8] Kaplan M., Laurent G., Leverrier A., Naya-Plasencia M., *Breaking symmetric cryptosystems using quantum period finding*, Advances in Cryptology – CRYPTO 2016, LNCS vol. 9815, Springer, 2016.

[9] Shor P., *Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer*, SIAM Journal on Computing, Volume 26 Issue 5, 1997, p. 1484-1509.

[10] STANAG 5068, Secure Communications Interoperability Protocol (SCIP).

[11] STANAG 4787, Network and Information Infrastructure (NII) Internet Protocol Network Encryption (NINE).