PROTOCOLS FOR SYMMETRIC SECRET KEY ESTABLISHMENT - MODERN APPROACH

Meiran Galis[a], *Tomislav* B. Unkašević[b], *Zoran* Đ. Banjac[c], *Milan* M. Milosavljević[d]

[a] Institute VLATACOM, Belgrade, Republic of Serbia; Scytale, Tel Aviv, State of Israel, e-mail: meiran.galis@vlatacom.com, ORCID iD: https://orcid.org/0000-0003-3017-9542

[b] Institute VLATACOM, Belgrade, Republic of Serbia, e-mail: tomislav.unkasevic@vlatacom.com, **corresponding author**, ORCID iD: https://orcid.org/0000-0002-6456-9250

[c] Institute VLATACOM, Belgrade, Republic of Serbia, e-mail: zoran.banjac@vlatacom.com, ORCID iD: https://orcid.org/0000-0001-8195-8576

[d] Singidunum University, Belgrade, Republic of Serbia, e-mail: mmilosavljevic@singidunum.ac.rs, ORCID iD: https://orcid.org/0000-0001-9630-804X

DOI: 10.5937/vojtehg70-36607;https://doi.org/10.5937/vojtehg70-36607

FIELD: Mathematics, Computer sciences, Telecommunications

ARTICLE TYPE: Original scientific paper

Abstract:

Introduction/purpose: The problem of efficient distribution of cryptographic keys in communication systems has existed since its first days and is especially emphasized by the emergence of mass communication systems. Defining and implementing efficient protocols for symmetric cryptographic keys establishment in such circumstances is of great importance in raising information security in cyberspace.

Methods: Using the methods of Information Theory and Secure Multiparty Computation, protocols for direct establishment of cryptographic keys between communication parties have been defined.

Results: The paper defines two new approaches to the problem of establishing cryptographic keys. The novelty in the protocol defined in the security model based on information theory is based on the source of common randomness, which in this case is the EEG signal of each subject participating in the communication system. Experimental results show that the amount of information leaking to the attacker is close to zero. A

ACKNOWLEDGMENT: The authors are grateful for the financial support from VLATACOM to project EEG and symmetric key establishment, project code: P-164

novelty in the second case, which provides security with keys at the level of computer security by applying Secure Multiparty Computation, is in the new application field, namely generation and distribution of symmetric cryptographic keys. It is characteristic of both approaches that within the framework of formal theories, it is possible to draw conclusions about their security characteristics in a formal way.

Conclusions: The paper describes two new approaches for establishing cryptographic keys in symmetric cryptographic systems with experimental results. The significance of the proposed solutions lies in the fact that they enable the establishment of secure communication between comunication parties from end to end, avoiding the influence of a trusted third party. In that way, the achieved communication level security significantly increases in relation to classical cryptographic systems.

Key words: symmetric cryptographic key, key establishment, source of randomness, advantage distillation, information reconciliation, privacy amplification, secure multiparty computation.

Introduction

The rapid development of communication and network technologies as well as technological advances in the design and implementation of microprocessor devices has led to information and communication connectivity of a large number of heterogeneous devices resulting in the creation of intelligent systems capable of monitoring and managing complex processes. Communication connectivity based on Internet infrastructure and protocols enables the establishment of complex management network systems, such as Wireless Sensor Networks (WSN) and the Internet of Things (IoT). This kind of progress brings the comfort of everyday life by advancing many technological and life processes through smart cities, autonomous vehicles, robotics and intelligent robot behavior (Mohamed, 2019; Atlam et al., 2018). In this way, a symbiotic community of people and machines is formed - Cyberspace. In this context, information security has a very important role in maintaining the integrity and privacy of data because their disruption in such an integrated world can cause serious damage, even to the level of general disaster (Ziegler, 2019; Mahmood, 2019; Banday, 2019). Therefore, in addition to security mechanisms built into Internet protocols, additional security mechanisms are used in devices and systems themselves to prevent external induction of their unwanted behavior. Almost all security mechanisms are realized by applying cryptographic

methods based on cryptographic algorithms and their cryptographic keys. Accordingly, the basic precondition for the reliability of the created security mechanisms essentially depends on the quality of the designed cryptographic algorithms and the quality of the generated cryptographic keys. Each of these topics, the design of reliable cryptographic algorithms and the generation and management of cryptographic keys, represents an extensive research area. Techniques for efficient generation and management of cryptographic keys have been the subject of research throughout the history of cryptology, and the need to establish a high level of security in cyberspace has further emphasized this issue.

Managing cryptographic keys involves control over their life cycle. The life cycle of cryptographic keys assumes their generation, storage, implementation, activation, use, deactivation, revocation and destruction. In this process, the processes of generation and distribution cryptographic keys are of essential importance. The basic assumption of the quality of cryptographic solutions is that cryptographic keys are generated in a completely random way and that the parties intended to protect communications come into their possession in a way that prevents unauthorized parties from accessing their content. Until the beginning of the 1980s, classical cryptology was focused on a direct or centralized way of managing cryptographic keys:

- **Direct way of exchanging cryptographic keys** when protected communication actors exchange cryptographic keys in direct contact, Figure 1.

Figure 1 – Cryptographic key delivery by direct contact
Рис. 1 − Передача криптографических ключей путем прямого контакта
Слика 1 – Размена кључева у директном контакту

- **The Center for Distribution of Cryptographic Keys** can function in several different forms:
  - Predefined communication network and cryptographic keys when the communication network is defined in advance, who can com-

municate with whom, and each participant in communication is assigned a set of predefined cryptographic keys.

– Predefined communication network and assignment of cryptographic keys on request when a member of the communication system marked as A wants to protect his communication by a symmetric cryptographic algorithm with another member of the system marked as B. The initiator of the communication A addresses the Center for Generation and Distribution of Cryptographic Keys T, with the requirement for cryptographic key to communicate with B. The key assignment scenario is as follows:

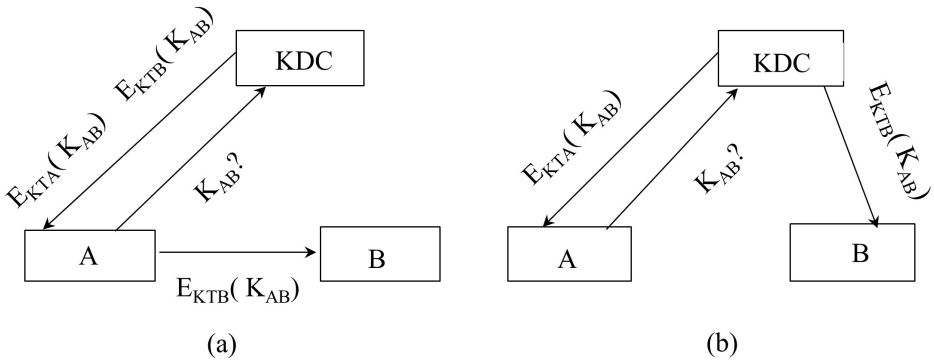

Figure 2 – Models of the cryptographic key delivery by the Key Distribution Center
Рис. 2 − Модели передачи криптографических ключей через Центр распределения криптографических ключей
Слика 2 – Модели уручења криптографских кључева преко Центра за дистрибуцију криптографских кључева

1. T generates a cryptographic key for the communication A and B denoted K_{AB}.
2. Then T form the ciphers $E_{K_{TA}}(K_{AB})$ and $E_{K_{TB}}(K_{AB})$.
3. The generated ciphers are delivered to the parties A and B, according to the agreed protocol, Figure 2

- **Predefined communication network and forwarding of cryptographic keys** when a member of the network, A, creates a cryptographic key K_{AB} and cipher $E_{K_{TA}}(K_{AB})$ and forwards it to center T with a request to forward it to the user B. The Center T deciphers the received message, forms $E_{K_{TB}}(K_{AB})$ and forwards it to B, Figure 3.

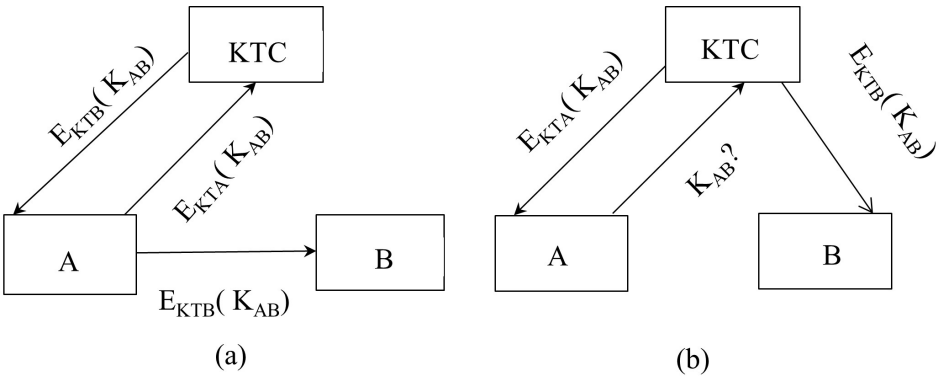

Figure 3 – Models of the Key translation center functioning
Рис. 3 − Модели функционирования Центра передачи криптографических ключей
Слика 3 – Модели уручења криптографских кључева преко Центра за пренос криптографских кључева

A more detailed overview and analysis of centralized systems for generating and distributing cryptographic keys can be found in (Menezes, 1997).

With the emergence and expansion of mass communication networks, and the need for information security, the centralized model of managing cryptographic proved to be inadequate. There are several reasons for this:

- Initial establishment of the system implies the distribution of cryptographic keys to users by the center for the generation and distribution of cryptographic keys in a secure manner (Trusted third party). In the initial phase when there are no secure data exchange channels, this is usually reduced to courier delivery of the subject keys, which in the case of mass networks, from the point of view of communication volume and number of participants, is uneconomical and inefficient.
- Achieving agreement on a single central entity for the generation and distribution of cryptographic keys is not realistic to expect according to required and necessary operational capacity as well as user needs, n^2 problem.
- A special issue is the realization of universal trust in the hypothetical center for the distribution and generation of cryptographic keys, which is, after all, the value attitude of each individual user. In today's world, which is divided over many issues, it is difficult to agree on a common high level of trust in one such entity and ways to control it.

- Attempts to the problem relaxation have led to the creation of complex hybrid models that have induced the creation of complex organizational structures resulting in demanding administration and maintenance procedures.

Searching for more efficient and comfortable solutions in the late 1970s, protocols for establishing cryptographic keys based on asymmetric cryptographic algorithms were discovered. The security of asymmetric cryptographic algorithms that are in mass use today is based on ignorance of efficient computer algorithms for factoring natural numbers, solving discrete logarithms and related problems. The theory of complexity of computer algorithms for this group of problems has no provable lower limits of complexity for algorithms that solve the mentioned problems, and accordingly their security cannot be absolute. Therefore, it is considered that this class of cryptographic protocols belongs to practically secure cryptographic algorithms, but there is no formal evidence for that. On the other hand, it has been shown that these problems are effectively solved in the quantum computer model of computation and therefore their security and usability is lost with the realization of quantum computers. In the early 1980s, ideas began to be developed to define protocols for which it would be possible to formally prove the level of security they provide to their users in relation to available computing resources, similar to Shannon's OTP encryption system. Researchers focused on the construction of protocols with the following properties:

– Elimination of the trusted third party from the process of creating and distributing cryptographic keys, which results in the possibility of establishing individual secure "end to end" communication systems.

– For defined protocols, formal security models can be formed and theoretical conclusions can be drawn about the achieved level of security, while eliminating the need for the existence of the trusted third party.

In this context, two formal models of security of cryptographic solutions stand out:

1. Security model based on Information Theory
2. Security model based on Theory of computability and algorithm complexity

Galis, M. et al, Protocols for symmetric secret key establishment - modern approach, pp.604–635

Information theoretically secure protocols for key establishment

In his seminal papers (Shannon, 1948a,b) Shannon defined the concept of cryptographic security using Information Theory and formulated the concept of absolutely secure cipher systems. Shannon's formulation did not need to take into account possible attacks and the power of a potential attacker for the simple reason that the security of cryptographic algorithms as defined by Shannon implied unlimited computing power of the attacker. In the case of cryptographic key protocols, the situation is somewhat more complex and the attacker's ability to access the messages exchanged by the protocol, the way in which it can affect protocol execution, and the ability to reconstruct the cryptographic key obtained by the protocol must be considered.

The first works on this topic appeared in the second half of the 1970s (Wyner, 1975; Maurer, 1993; Ahlswede & Csiszar, 1993) with the idea that, during the execution of the protocol illegitimate protocol observers who have access to exchanged messages cannot collect the necessary amount of information about the established cryptographic key with the aim of its restoration in an efficient manner. Over time, the importance of this type of protocol for establishing cryptographic keys has been recognized, and with the increase in security requirements in cyberspace, more and more attention has been paid to them.

The basic model of the environment in which protocols of this type are defined and analyzed is given in (Maurer, 1993). According to the symbols common in the literature, the environment in which the protocol takes place is defined in the following way. Alice and Bob are actors who want to achieve mutual protected communication using a symmetric cryptographic algorithm, and for that they need a common secret key. Eve is curious and interested in the information that Alice and Bob exchange and she knows the protocol according to which they exchange messages and the cryptographic algorithm they will use. The only way Eve can access Alice and Bob's information, provided the applied cryptographic algorithm is safe, is to somehow get their cryptographic key. It is assumed that Eve has an insight into all the messages that are exchanged during the protocol between Alice and Bob. Based on the information gathered, Eve tries to reconstruct the cryptographic key that Alice and Bob perform after the protocol is completed. The initial data, the strings of symbols, which are used in the exe-

cution of the protocol for establishing the cryptographic key Alice, Bob and Eve get in the following way. In a common source, a series of symbols is generated by some random process, denoted by $U^n = \{u_1, u_2, \ldots, u_n\}$, through independent binary symmetric channels of known characteristics are sent to Alice, Bob and Eve who register them as strings of symbols $X^n = \{x_1, x_2, \ldots, x_n\}$, $Y^n = \{y_1, y_2, \ldots, y_n\}$, $Z^n = \{z_1, z_2, \ldots, z_n\}$ respectively. The model is shown in Figure 4.

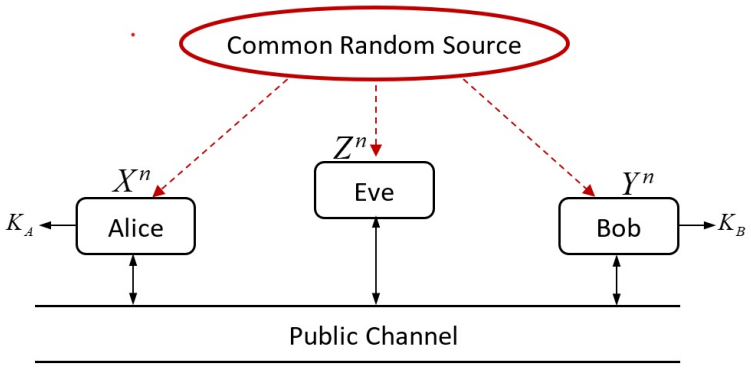

Figure 4 – Model of the execution environment for the Information theoretic based symmetric key establishment protocol
Рис. 4 – Изображение среды выполнения протокола установления криптографических ключей в рамках теоретико-информационной модели
Слика 4 – Графички приказ окружења извршавања протокола за установљавање криптографских кључева у информационо-теоретском моделу

The result of the protocol execution is to obtain a series of symbols K_A, K_B, with the objectives:

1. The probability that the resulting arrays are equal, $P(K_A = K_B)$, is close to unity. At the end of the protocol, a procedure, which does not violate the security of the process, can be performed to determine this equality, and the resulting symbol string is denoted by $K^{m(n)} = K_A = K_B$ where $m(n)$ is the length of the string symbols obtained after the protocol execution.
2. The protocol is safe from the point of view of the obtained key, $K^{m(n)}$, in the sense that Eve is not able to reconstruct the value of $K^{m(n)}$

which is expressed by

$$I\left(K^{m(n)}, Z^n\right) = 0. \tag{1}$$

This condition has proven to be quite limiting in practice and its somewhat weaker variant expressed with

$$\lim_{n\to\infty} I\left(K^{m(n)}, Z^n\right) = 0. \tag{2}$$

where n is the length of the initial string of symbols.

Condition (2) essentially means that Eve has the information about $K^{m(n)}$ but it is not enough to effectively approximate or reconstruct the key $K^{m(n)}$. In this way, the computing and algorithmic power that Eve has is abstracted, similar to the definition of the security of cryptographic algorithms in Shannon's book, (Shannon & Weaver, 1963).

General structure of the information theoretically secret key establishment protocols

According to the functional model shown in Figure 4, the protocol takes place in several steps. In the first step, a common source of randomness generates a series of random symbols $U^n = \{u_1, u_2, \ldots, u_n\}$ which by a discrete symmetric communication channels without the memory of known characteristics, P_{XYZ}, forwards to Alice, Bob and Eve who register them as strings of symbols X^n, Y^n, Z^n respectively. In the described communication channel (P_{XYZ}, X^n, Y^n, Z^n) errors can occur during transmission, in the general case the sequences X^n, Y^n, Z^n are different from each other. In the next phase, Alice and Bob exchange messages via a public authenticated channel to detect parts of the initial set of symbols that are common to them. The way of communication is constructed so that the similarity of their symbol strings increases and the similarity of Eve's string of symbols with Alice's/Bob's string of symbols either does not change or decreases despite the known content of the exchanged messages. A measure appropriate to the situation is taken as a measure of similarity, most often Hamming's distance. This phase is called advantage distillation. After that, in the third phase of the protocol, Alice and Bob exchange messages through a publicly authenticated channel that allows them to extract identical parts in their symbol strings and thus arrive at a string of symbols that is common

to both. Here, too, it is understood that Eve's knowledge of the obtained common set of symbols does not increase. This phase is called the phase of Information reconciliation. In the final part of the protocol, Alice and Bob construct a common symmetric key by applying a pre-agreed publicly known function to the derived common symbol string, and this step is called Privacy amplification.

Common randomness source sequence distribution

The primary requirement in the process of generating cryptographic keys is that the created cryptographic key has maximum entropy in relation to its length and that the entropy of the plain text messages is not greater than the entropy of the space of possible keys. Systems that meet this condition are known to be secure against an attacker with unlimited computing resources (processor speed, memory, power). This includes the attacker's approach to quantum computers. Probability theory and mathematical statistics have developed techniques by which realizations of random variables with different probability distribution functions under certain conditions can be transformed into realizations of random variables with uniform distribution. With this in mind, the idea of an information-theoretical approach in this context is to identify and extract equal parts with sufficiently high entropy from two mutually correlated signals. According to the nature of the randomness sources used in this phase, we distinguish two models:

1. Random processes that are not connected to the communication channel - source model, such as in (Galis et al., 2021).
2. Random processes related to the communication channel model are used as a source of randomness, such as in (Maurer, 1993).

Advantage distillation phase

In accordance with the model shown in Figure 4, we can consider that the binary symmetric channels through which Alice, Bob and Eve get their strings X^n, Y^n, Z^n are mutually independent and characterized by error probabilities p_A, p_B,and p_E respectively with $0 < p_A, p_B, p_E < \frac{1}{2}$. For practical applications, the relevant situation is when $0 < p_E < min\ \{p_A, p_B\}$. In this context, it can be considered that Alice sends her symbol string X^n through a binary symmetric channel to Bob who receives it as a string Y^n

with an error probability

$$\begin{aligned} p_{AB} &= P\left(x_i \neq y_i\right) = \\ &= P\left(x_i \neq y_i \mid x_i = u_i\right) \cdot P\left(x_i = u_i\right) + P\left(x_i \neq y_i \mid x_i \neq u_i\right) \cdot P\left(x_i \neq u_i\right) \\ &= P\left(y_i \neq u_i\right) \cdot P\left(x_i = u_i\right) + P\left(y_i = u_i\right) \cdot P\left(x_i \neq u_i\right) = \\ &= p_B \cdot (1 - p_A) + (1 - p_B) \cdot p_A \end{aligned} \tag{3}$$

The relationship between Alice's and Eve's set of symbols is observed in the same way, and the probability of error in that binary symmetric channel is given by

$$p_{AZ} = p_Z \cdot (1 - p_A) + (1 - p_Z) \cdot p_A \tag{4}$$

The aim of this part of the protocol for Alice and Bob is to exchange messages via a public authenticated channel and to select subsets of symbols from X^n, Y^n where the error will be less than (3) without revealing too much information to Eve and the error in her channel will not be less than (4). Below we will describe the most commonly used protocols of this type.

The repetition code advantage distillation protocol (RCAD) This protocol is described in (Maurer, 1993; Bloch & Barros, 2011; Tan et al., 2020). For the selected segment of the initial bit string of the length N, Alice randomly generates the bit r $\left(P\left(r=0\right) = P\left(r=1\right) = \frac{1}{2}\right)$ and the code word $R^N = \left(\overbrace{r, r, \ldots r}^{N}\right)$. Then she calculated

$$X^N + R^N = (r + x_1, r + x_2, \ldots, r + x_N)$$

and the resulting vector is sent to Bob. Upon receiving Alice's message, Bob calculates

$$Y^N + X^N + R^N = (y_1 + r + x_1, y_2 + r + x_2, \ldots, y_N + r + x_N)$$

If as a result Bob gets $\left(\overbrace{r, r, \ldots r}^{N}\right)$ where $r \in \{0, 1\}$ he assumes that his and Alice's sequences coincide. Bob in response to Alice sends the bit F

$$F = \begin{cases} 1 & \text{Bob gets } \left(\overbrace{r, r, \ldots r}^{N}\right) \\ 0 & \text{otherwise} \end{cases}.$$

If $F = 1$, that sequences are considered equal on both sides and participate in the construction of a new bit string, otherwise that bit sequence is omitted from the further process. The value of the parameter N is determined according to the situation and optimized so that the probability of matching is maximal and the level of information leakage to Eve is minimal. It can be shown that, on the accepted segments after the end of the RCAD protocol, the next statements are valid, (Bloch & Barros, 2011; Wang et al., 2015):

1. On the accepted segment of the length N between Alice and Bob the error probability is

$$p_{AB}^{RCAD} = \frac{(p_{AB})^N}{(p_{AB})^N + (1 - p_{AB})^N}$$

   and p_{AB} is the probability of error on the segment of the length N before starting the protocol execution.

2. Since $X^N + R^N$ is transmitted through a public channel, Eve can calculate $Z^N + X^N + R^N$ and then the error between Eve's and Alice's segment is expressed with

$$p_{AE}^{RCAD} = \frac{1}{(p_{AE})^N + (1 - p_{AE})^N} \cdot \sum_{w=\lceil \frac{N}{2} \rceil}^{N} \binom{N}{w} p_w$$

   where p_w is probability that vector of length N has Hamming weight w.

3. Data remaining efficiency, as a quotient between the length of the initial string and the length of the string obtained after the protocol execution, is given with the next equation (Wang et al., 2015)

$$\mu_{AB}^{RCAD}(p_{AB}) = \frac{(p_{AB})^N + (1 - p_{AB})^N}{N}.$$

The significance of this solution lies primarily in the fact that the possibility of implementing secure protocols for establishing cryptographic keys from the Information theory point of view elimination of trusted third parties has been demonstrated in a constructive way. The main drawback of this protocol lies in the fact that in the case when p_E is significantly less than p_A, p_B it is quite inefficient in terms of the length of the derived key. A more efficient variant of this protocol is described in (Maurer, 1993).

The bit pair iteration advantage distillation protocol (BPIAD) The BPIAD protocol is an iterative protocol that, starting from the initial bit strings X^n, Y^n in each iteration, generates a sequence for the next iteration. The result of the last iteration is processed in the next stages of the key establishment protocol. The following steps are performed in each iteration of the AD protocol, (Wang et al., 2015):

(1) In the $s-$th iteration Alice and Bob have strings of symbols of the length n_s bits and form blocks of two consecutive bits.

(2) Alice computes the parity bit for each block $\left\{X_{2i+1} \oplus X_{2i},\, i = 0, 1, \ldots, \left\lfloor \frac{n_s}{2} \right\rfloor\right\}$ and send them to Bob.

(3) Bob computes his parity bits $\left\{Y_{2i+1} \oplus Y_{2i},\, i = 0, 1, \ldots, \left\lfloor \frac{n_s}{2} \right\rfloor\right\}$ and compares them with Alice's parity bits. For every i for which is $X_{2i+1} \oplus X_{2i} \neq Y_{2i+1} \oplus Y_{2i}$ pairs X_{2i+1}, X_{2i} and Y_{2i+1}, Y_{2i} are removed from the further process. In the case that $X_{2i+1} \oplus X_{2i} = Y_{2i+1} \oplus Y_{2i}$ bit X_{2i+1} is included in Alice's string and bit Y_{2i+1} is included in Bob's string for the next iteration $s+1$.

It turns out that it is at the end of the $s-$th iteration, (Wang et al., 2015):

$$\begin{aligned} p_{AB_s}^{BPIAD} &= \frac{\left(p_{AB_0}\right)^{2^s}}{\left(p_{AB_0}\right)^{2^s} + \left(1 - p_{AB_0}\right)^{2^s}} \\ p_{AE_s}^{BPIAD} &= p_{AE_0}^{BPIAD} \\ \mu_{AB_s}^{RCAD}\left(p_{AB_0}\right) &= \frac{\left(p_{AB_0}\right)^2 + \left(1 - p_{AB_0}\right)^2}{2^s} \end{aligned} \tag{5}$$

The analysis of the described protocol and the results given in (5) concludes that the number of iterations depends on the size p_{AB_0} and that with its increase the required number of iterations increases so that the symbol strings obtained in this phase can be productively used in the following, $p_{AB_s}^{BPIAD} < p_{AE_s}^{BPIAD}$. Also, the protocol is extremely inefficient in terms of the ratio of the lengths of the initial and obtained bit strings, because according to the third equation in (5), the length of the obtained bit string decreases exponentially with the number of iterations.

The bit pair iteration advantage distillation/degeneration protocol (BPIADD) The fact that during the BPIAD protocol the probability of error in Eve's bit string remains constant during the execution of the protocol

remains constant, the second equality in (5) indicates the possibility of increasing Eve's capacity to obtain more information about Alice's bit string during the next protocol phase. In order to reduce these possibilities and provide more favorable initial conditions for the next phase, Information reconciliation, the BPIADD protocol is defined as follows, (Wang et al., 2015):

(1) Alice computes $A_k = X_{2k-1} \oplus X_{2k}$ $k = 1, 2, \ldots$.and sends A_k to Bob.

(2) Bob computes $B_k = Y_{2k-1} \oplus Y_{2k}$ $k = 1, 2, \ldots$.and sends B_k to Alice.

(3) For every $k = 1, 2, \ldots$ the following procedure is performed:

- If $A_k \neq B_k$ then Alice deletes X_{2k-1}, X_{2k} from X and Bob deletes Y_{2k-1}, Y_{2k} from Y.
- If $A_k = B_k$ then Alice checks if $X_{2k} = 1$. If it is, then she deletes X_{2k-1} from X and if not, she deletes X_{2k} from X. Bob does the same in the case of the string Y.

It turns out that after the first iteration of this protocol, the following relations are valid (Wang et al., 2015):

$$\begin{aligned} p_{AB_1}^{BPIADD} &= \frac{1}{2} \cdot \frac{\left(p_{AB_0}\right)^2}{\left(p_{AB_0}\right)^2 + \left(1 - p_{AB_0}\right)^2} < p_{AB_0} \\ p_{AE_1}^{BPIADD} &= \frac{p_{AE_0}}{2} + p_{AE_0}\left(1 - p_{AE_0}\right) > p_{AE_0} \\ \mu_{AB_1}^{RCAD}\left(p_{AB_0}\right) &= \frac{\left(p_{AB_0}\right)^2 + \left(1 - p_{AB_0}\right)^2}{2} \end{aligned} \tag{6}$$

From the first and second expressions in (6) it is clear that the error in the Alice and Bob's sequence decreases monotonically and the error in the Alice and Eve's series increases monotonically. By applying the protocol in several iterations using (6) we get that in the $s-$th iteration in order, the following is valid:

$$\begin{aligned} p_{AB_s}^{BPIADD} &= \frac{1}{2} \cdot \frac{\left(p_{AB_{s-1}}\right)^2}{\left(p_{AB_{s-1}}\right)^2 + \left(1 - p_{AB_{s-1}}\right)^2} < p_{AB_{s-1}} \\ p_{AE_s}^{BPIADD} &= \frac{p_{AE_{s-1}}}{2} + p_{AE_{s-1}}\left(1 - p_{AE_{s-1}}\right) > p_{AE_{s-1}} \\ \mu_{AB_s}^{RCAD}\left(p_{AB_{s-1}}\right) &= \frac{\left(p_{AB_{s-1}}\right)^2 + \left(1 - p_{AB_{s-1}}\right)^2}{2} \end{aligned} \tag{7}$$

In this way, the difference between Eve's and Alice's string becomes large enough and the difference between Alice's and Bob's string becomes small enough that the process of information reconciliation and the amount of information that leaks to Eve during it does not have a significant impact on the derived cryptographic key.

Information reconciliation After completing the previous phase, advantage distillation, Alice and Bob have reached a situation where they have an advantage over Eve in terms of the amount of mutual information about their bit strings. In this phase of the protocol, Alice and Bob's goal is to use an authenticated public channel for communication to exchange information that will allow them to correct any differences in the current bit strings they formed during previous phases of the protocol. All messages exchanged through the public channel are also available to Eve. The more information Eve can extract from this communication imply the shorter length of the secret key at the end of the process.

The first such protocol is described in (Bennett et al., 1992). From the point of view of mass application and efficiency, several widely used solutions have crystallized:

- In practice, the CASCADE protocol defined in (Brassard & Salvail, 1992) is widely used today. The protocol is iterative in its nature and in the $i-$th iteration it takes place in the following way. According to a pre-agreed permutation, Alice and Bob permute $X^n\,Y^n$. The resulting bit strings are divided into blocks of length k_i bits. Alice calculates the parity bit for each of her blocks and sends them to Bob. Bob compares Alice's parity bits to his parity bits on matching positions. If there is a discrepancy between Alice and Bob's parity bit for some block they apply the binary search algorithm on that block and the exchange additional parity bits for some sub-blocks of the current block with the aim to detect an incorrect bit. Upon incorrect bit detection, Bob changes its value. Bob then analyzes the effect of the changed bit on the previous iterations and eventually detects and corrects previously masked errors. This procedure is repeated for each block of bits that does not agree with Alice's corresponding blocks. Since all blocks in this iteration are processed, the next iteration is taken with $k_{i+1} = 2 \cdot k_i$. The initial choice of the block length, k_1, is critical for the efficiency of the algorithm. Many papers have dealt with experimental

and theoretical analyses of this problem in order to achieve an optimal performance (Bennett et al., 1988; Cachin & Maurer, 1997; Carleial & Hellman, 1977; Csiszar & Korner, 1978). Sugimoto and Yamazaki in their papers (Sugimoto & Yamazaki, 2000; Yamazaki & Sugimoto, 2000) defined certain modifications of this algorithm and showed that such a modified protocol has a performance close to the theoretical limits of efficiency. He also confirmed that four iterations are enough to reconcile the values of bit strings. On the other hand, the communication complexity of the protocol during the execution can be great, which results in a small length of the obtained string in order to minimize the amount of information that Eve has.

- The Winnow protocol is introduced in (Buttler et al., 2003) with the aim of reducing communication complexity by eliminating the use of a binary search algorithm for error detection and correction. The author's idea is to use Hamming's error detection and correction code to correct errors. Both sides, Alice and Bob, split their bit strings into blocks of equal length. Two corresponding blocks are denoted by M_a and M_b and their syndromes, S_a and S_b, are calculated using the generator matrix G and the check matrix H, $G \cdot H^T = 0$. Alice sends Bob S_a who calculates $S_d = S_a \oplus S_b$. If $S_d = 0$ then M_a and M_b are considered equal, otherwise Bob transforms M_b by changing the minimum number of positions and recalculating S_b for such a modified block to get $S_d = 0$. Analyses have shown that from the point of view of execution speed, achieved string length and security characteristics, the protocol has good performance with appropriate p_{AB}, (Elkouss et al., 2009; Buttler et al., 2003).
- The aforementioned protocols do not consider the situation when there are significant limitations in the communication environment in terms of loss of communication packets, limited time for protocol execution and limited communication and computational complexity, for example in satellite connections. Gallagher's Low Density Parity Check Codes (Gallager, 1962) were candidates for such environments as a promising solution. In this context, LDPC codes were first mentioned in (Elliott et al., 2005). The advantage of LDPC codes in these applications is that they provide low communication complexity, inherent and pronounced asymmetry in terms of computing resources of communication parties.

Decoding LDPC codes requires more computing and memory resources than the Cascade and Winnow protocols but its significance is in communication resources and complexity reduction as it requires only one message to be exchanged. In resource-constrained networks, this feature provides a significant advantage in achieving large gains in execution time and security.

Other ideas in this context have emerged recently. One of them is the application of neural networks in the process of error correction during this phase of the protocol. (Niemiec, 2019).

More details on this topic with an exhaustive list of references can be found in (Bloch, 2016; Mehic et al., 2020; Gronberg, 2005)

Privacy amplification

This is the last phase in the process of the protocol which is carried out by Alice and Bob in order to obtain a cryptographic key that is information-theoretically secure in relation to Eve. At this point, Alice and Bob have a string of bits in common and know the estimate of the upper limit of the amount of information Eve has about that string. Nevertheless, Eve's information shows that Alice and Bob can extract from their strings a certain string of bits S_{AB} about which Eve knows nothing or

$$I\left(S_{AB}, S_E\right) = 0$$

where S_E is Eve's version of S_{AB} constructed based on the information Eve collected. Eve knows that $S_{AB} \neq S_E$ but does not know in which positions the sequences differ. Using the publicly known selected appropriate deterministic function f, Alice and Bob calculate the required cryptographic key as $k = f(S_{AB})$. Knowing the function f and S_E does not provide any knowledge to Eve about k because she does not know how the errors from S_E spread during the calculation of f and affect its result. Consequently, $f\left(S_E\right)$ does not give any information about k to Eve.

Precise formalizations and proofs are based on the notion of Rényi entropy and its derivatives, collision entropy and min-entropy.

Detailed references to protocols and formalizations can be found in (Bloch, 2016).

The common source of randomness choice

The previously described process of cryptographic keys establishment implies that Alice, Bob and Eve get their initial strings of symbols X^n, Y^n, Z^n from a common source of randomness as shown in Figure 4. This generally implies the participation of a trusted third party in the process itself. The level of communication security is increased when it is possible to eliminate the influence of the trusted third party and achieve protection of communication between Alice and Bob by controlling the generation of cryptographic keys and using proven cryptographic algorithms. One of the first examples of this communication protection type was the Quantum key exchange protocol (QKD) BB84, (Bennett & Brassard, 1984). An interesting and in some ways biometrical oriented approach is described in the works (Milosavljević et al., 2018) and (Galis et al., 2021). The authors used digitized recorded electroencephalogram (EEG) brain signals as a source of randomness for Alice and Bob during identical mental activities, looking at the image of the White Angel in (Milosavljević et al., 2018) and during the Wisconsin Card Sorting Test (WCST) in (Galis et al., 2021). Intuitively, Alice's and Bob's brain is stimulated by the same input stimulus but due to individual physiological differences it is registered as correlated but different and independent signals, for example in the case of an image the general image content is the same but color perceptions, physical dimensions and other characteristics may differ. So the digitalized form of Alice's EEG becomes X^n and the digitalized form of Bob's EEG becomes Y^n. In that situation, Eve has no information about X^n, Y^n and her only possibilities may be:

1. To be able to recognize in a set of registered EEG signals on the same stimulus, which does not contain Alice's and Bob's EEG, the one closest to them, measured by the Hamming's metric - Strong Eve
2. That the set of registered EEG signals includes both Alice's and Bob's EEG, but that Eve does not know the identity of the person from whom the EEG signals originate - Medium Eve
3. Eve has no information about Alice's and Bob's EEG signal, but she knows the process for obtaining it and the device for recording and digitizing it - weak Eve.

In (Galis et al., 2021), the authors used 76 of EEG signals from different individuals during WCST. For all registered samples, the previously described procedure of performing cryptographic keys in the information-

theoretical model, advantage distillation, information reconciliation, private amplification was performed. A summary of the results is given in Table 1.

Table 1 – Experimental results of cryptographic keys establisment using EEG
Таблица 1 – Экспериментальные результаты создания криптографических ключей при использовании ЭЭГ
Табела 1 – Експериментални резултати успостављања криптографских кључева применом ЕЕГ-а

Type of Eve	Strong	Medium	Weak
Established key length	1301.55 ±502.16	1290.53 ± 496.85	1301.76 ± 502.44
Efficiency	4.79%	4.75%	4.79%
Hamming distance(A,E)	0.4997± 0.0147	0.5005± 0.0149	0.4999± 0.0147
Successfully established pairs	100%	100%	100%

The table shows the results in relation to the assumed strength of Eve. The second row labeled Established key length shows the mean length value and the standard deviation of the established cryptographic keys lengths in the $(76 \cdot 75)/2$ implemented protocols. The third row shows the efficiency of the applied protocols expressed as the ratio of the length of the obtained cryptographic keys and the length of the initially used string. At first glance, it seems that the efficiency is small and unsatisfactory, but the length obtained, on average over a thousand bits, is many times higher than the currently accepted standards for cryptographic key lengths of secure symmetric cryptographic algorithms. The fourth row shows the Hamming distance between the keys obtained by Alice and Eve at the end of the process, normalized by the length of the key obtained, and the table shows that this value is practically 0.5, which is a characteristic value for independent and randomly generated arrays. In the end, the table shows that the procedure was successful in all cases in which it was carried out. In addition, it should be noted that the obtained sets of cryptographic keys were tested by the NIST package to check the randomness of the data and all requirements were met.

A full description of the basic idea, methodology, applied protocols and experimental results can be found in (Galis et al., 2021).

Computationally secure protocols for key establishment

With the expansion of information and communication systems, the distribution of cryptographic keys in a centralized way through a trusted third party has become a bottleneck in achieving security in the information and communication world. The first solutions that reduced and relatively eliminated this problem were defined in the second half of the 1970s with the discovery of asymmetric cryptographic algorithms, electronic signature and digital envelope techniques (Diffie & Hellman, 1976; Rivest et al., 1978; Menezes, 1997). However, such solutions assumes the existence of an infrastructure for generation and management of cryptographic keys for asymmetric cryptographic systems and digital certificates based on them (Public Key Infrastructure -PKI). This enables the introduction of digital identity in the digital world. This, in turn, means involving a trusted third party in the process of establishing cryptographic keys. Today's trend in the protection of messages in information and communication traffic is the creation of direct secure channels between the parties in communication and the development of techniques for establishing cryptographic keys directly between them in a secure way.

The first reflections on the protocol for secure decentralized computing of functions are presented in (Yao, 1982). The described approach considers the possibilities for defining a protocol by which n participants denoted by P_i and each has a private data x_i $i = 1, 2, \ldots, n$ for a given function f calculate the value $(y_1, y_2, \ldots, y_n) = f(x_1, x_2, \ldots, x_n)$ in such a way that:

1. After protocol execution, the generated value $(y_1, y_2, \ldots, y_n)$ is the exact value of the function f for the arguments $(x_1, x_2, \ldots, x_n)$ and each participant P_i received them as a result.
2. After protocol execution, each participant P_i knows only $(y_1, y_2, \ldots, y_n)$, x_i and nothing else.
3. Some participants in the protocol may behave maliciously in relation to the protocol in order to obtain information or influence the outcome of the protocol.

A graphical presentation of the Secure multiparty protocol is given in Figure 5.

Secure multiparty computing can be fully formally described thus createing a formal theory within which it is possible to infer conclusions about the security features of the created protocols in a logically based way.

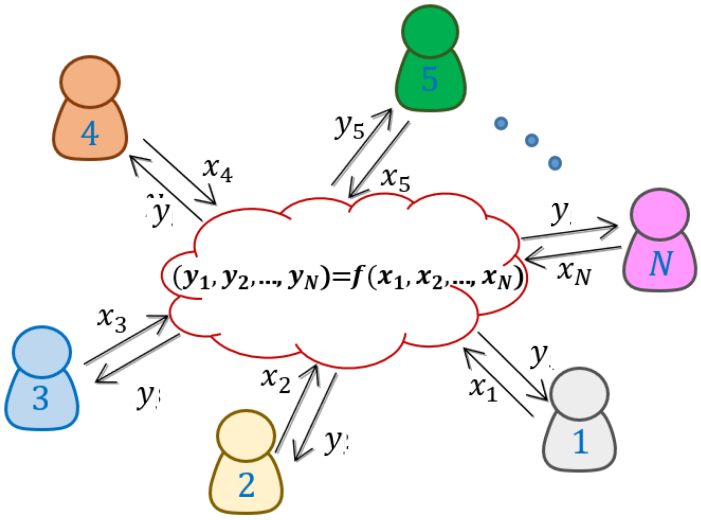

Figure 5 – Graphical presentation of the secure multiparty protocol
Рис. 5 – Графическое представление протокола безопасного многопартийного вычисления
Слика 5 – Графички приказ безбедног кооперативног рачунања

This formalization first defines the characteristics of network channels through which messages are exchanged during the execution of the protocol. Channels by their nature can be public, when the attacker has access to the content of messages but cannot change them, and private, when communication between each two participants is protected. As for the attacker, depending on the communication channel on which the protocol takes place, all messages can be available to him when the channel is public or only those received from malicious participants when the channel is private. According to the received messages, the attacker is passive when only by analysing the received messages he tries to reconstruct information inaccessible to him, or active when he can influence the malicious participants in the protocol available to him. In the case of an active attacker, his behavior does not have to be uniform, but he can adapt to the development of the situation during the execution of the protocol, and then he is called an adaptive active attacker. Some protocol participants under the influence of an attacker may behave in a way that affects the execution of the protocol and the types of such behavior can be described exactly. The protocol is considered safe if conditions listed on page 623 are met.

An interesting question is how to define security in a formal way. The idea is as follows.

By protocol history, we mean a collection of all non-private data used and constructed during protocol execution in an environment. The ideal environment is an abstract construction consisting of simulator S, a functional mechanism for executing protocol instructions that calculates f, and the attacker. All activities in an ideal environment are performed in the correct way, exactly as defined by the functionalities and protocol. The protocol to be executed is denoted by π, the attacker by $\mathcal{A}$, the protocol execution history by h and the security parameter by k. Since in an ideal environment, everything takes place in the right way, security threats and information leakage cannot be in it. Let us introduce the following two functions

$$R_{\pi,\mathcal{A}}(k,h) = \begin{cases} 1 & h \text{ belongs to real world} \\ 0 & \text{otherwise} \end{cases}$$

$$I_{\pi,\mathcal{A}}(k,h) = \begin{cases} 1 & h \text{ belongs to ideal world} \\ 0 & \text{otherwise} \end{cases}$$

Then we say that the protocol π safely calculates the function f in relation to the attacker $\mathcal{A}$ if there is a polynomial simulator S for which each execution with the security parameter k and each protocol history h next inequality is valid

$$\left|P\left(R_{\pi,\mathcal{A}}(k,h)=1\right) - P\left(I_{\pi,\mathcal{A}}(k,h)=1\right)\right| < \frac{1}{p(k)} \tag{8}$$

for a sufficiently large k, where $p(k)$ is an arbitrary positive polynomial. Inequality (8) essentially means that an attacker is unable to distinguish between protocol execution in an ideal and a real environment and, consequently, to gather additional information in addition to those already known. The exact formalization of this concept can be found in (Cramer et al., 2015; Hazay & Lindell, 2010).

The theory shows that in the case of public communication channels and the presence of an active attacker, each function f can be safely calculated in the previously stated sense, provided that the number of corrupt participants t is less than $\frac{n}{3}$. A detailed classification of the possibility of creating a protocol for secure multiparty computing depending on the type of attacker and communication model can be found in (Cramer et al., 2015).

Galis, M. et al, Protocols for symmetric secret key establishment - modern approach, pp.604–635

This method is applicable in any situation when it is necessary to calculate a function based on the private information of individual entities so that the result is accurate and does not compromise the privacy of the entities private data participating in the calculation. The problem of generation and distribution cryptographic keys for bilateral or conference secure communication by its nature completely fits into the class of problems this area deals with. The model of decentralized generation and distribution of symmetric cryptographic keys for bilateral secure communication can be described as follows. The participants P_1 and P_2 who want to achieve secure bilateral communication agree on a symmetric cryptographic algorithm through a public communication channel and the function $f(x, y)$ which they will use to derive the desired cryptographic key. Then the participant P_1 chooses a random value x_1 and the participant P_2 a random value x_1, implementing the appropriate protocol for secure multiparty computing, and using it to compute $k = f(x_1, x_2)$ which they will use for the selected symmetric cryptographic algorithm for communication protection. The realization of the system for the automatic establishment of cryptographic keys for symmetric cryptographic algorithms begins with the selection of one of the existing universal protocols for bilateral secure multiparty computing, (Hazay & Lindell, 2010). The implementation of the selected protocol implies the existence of the following subsystems implemented:

- System for automated translation of the selected function f into an equivalent vector Boolean function in the algebraic normal form and then construction of its equivalent Boolean circuit.
- System for automated generation of Yao's garbled computing system based on the obtained Boolean circuit.
- System for the implementation of oblivious transfer protocols.

The realization of such a software package resulted in a system for the direct establishment of cryptographic keys of parties who want to establish secure communication without the mediation of a trusted third party. For the security characteristics of the protocol in the bilateral case, the restrictions related to the number of malicious participants in the protocol are not important for the simple reason of the number of participants, two. If at least one of the participants is malicious, the protocol will not be successfully completed and the key will not be established.

Similarly, this concept can be used to establish the protection of group communication, such as conference calls or complete video meetings.

Comparative analysis of proposed solutions

By applying the previously described methods, we are able to solve the problem of secure generation and distribution of cryptographic keys. The levels of security that the methods offer are different, but they provide a significant advantage over classical cryptology, the elimination of a trusted third party. The benefits of eliminating a trusted third party are manifold. In the first place, the absence of a trusted third party reduces the complexity of the system and thus reduces the number of potential possibilities for its compromise, and further simplifies its administration and maintenance. An additional quality from the security point of view lies in the fact that both systems can be described in a completely formal mathematical way and accordingly analyze the defined protocols and make formal claims about the achieved level of security.

In the Information theory model, it is possible to formally define protocols that can achieve levels of absolute security for generating cryptographic keys and that can be used even in Shannon's OTP system. In this model of performing cryptographic keys, an additional quality is the fact that the source of common randomness can be different environments, which increases the application area of such systems.

In the model of secure multiparty computing on public communication channels, protocols for establishing symmetric cryptographic keys that reach the level of computer security can be formally defined. This lower level of security is a consequence of the characteristics of communication channels and the level of security of cryptographic mechanisms applied in the implementation of the subsystem oblivious transfer.

Although the described systems offer important, technological and security improvements in the field of generation and distribution of cryptographic keys, their application in this context is still small. The main reason lies in the complexity of their implementation and demonstrated performance. Conceptually, these solutions have been proven, but great research efforts are being made to find opportunities to improve their performance and more efficient implementation in terms of computing resources (processing power, amount of memory).

Galis, M. et al, Protocols for symmetric secret key establishment - modern approach, pp.604–635

Conclusion

One of the central problems of cryptology, from its inception to the present day, is the generation and distribution of cryptographic keys for symmetric cryptographic systems. The centralized system of generating and distributing cryptographic keys, characteristic of classical cryptology, has manifested its limitations with the expansion of information and communication systems and their network connection. The increased need for the application of cryptographic mechanisms in the protection of information systems has induced an increase in requirements. This paper presents two models by which the described problem can be solved in accordance with the security requirements of modern cryptology. Solutions based on the above proposals give users complete autonomy and end-to-end security protection. The applicability of solutions of this type allows

- Direct establishment of cryptographic keys between communication sites, people or machines, without the mediation of a trusted third party,
- Application of secure symmetric cryptographic algorithms in mass communication systems, IoT and WSN (Unkašević et al., 2019),
- Simplification of the complexity of security systems thus facilitating their administration, and
- By simplifying the complexity and administration of security systems, facilitation of their analysis, potential weaknesses detection and, overall, an in- crease of their security.

The described methods for the realization of direct establishment of cryptographic keys for symmetric cryptographic systems are in line with new trends in data protection in order to reduce the possibility of influence of entities that do not participate in communication directly. The applicability of these techniques in IoT and WSN significantly increases the possibilities of raising the level of security in cyberspace. This claim is supported primarily by the fact that the described methods support cryptographic algorithms with the highest degree of security.

References

Ahlswede, R. & Csiszar, I. 1993. Common randomness in information theory and cryptography. I. Secret sharing. *IEEE Transactions on Information Theory*, 39(4), pp. 1121–1132. Available at: https://doi.org/10.1109/18.243431.

Atlam, H.F., Walters, R.J. & Wills, G.B. 2018. Internet of Things: State-of-the-art, Challenges, Applications, and Open Issues. *International Journal of Intelligent Computing Research*, 9(3), pp. 928–938. Available at: https://doi.org/10.20533/ijicr.2042.4655.2018.0112.

Banday, M.T. (ed.) 2019. *Cryptographic Security Solutions for the Internet of Things*. IGI Global. Available at: https://doi.org/10.4018/978-1-5225-5742-5.

Bennett, C. & Brassard, G. 1984. Quantum cryptography: Public key distribution and coin tossing. In: *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*. Bangalore, India. December 9-12.

Bennett, C.H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. 1992. Experimental quantum cryptography. *Journal of Cryptology*, 5, pp. 3–28. Available at: https://doi.org/10.1007/bf00191318.

Bennett, C.H., Brassard, G. & Robert, J.M. 1988. Privacy Amplification by Public Discussion. *SIAM Journal on Computing*, 17(2), pp. 210–229. Available at: https://doi.org/10.1137/0217014.

Bloch, M. 2016. *Physical-Layer Security*. Cambridge University Press. ISBN 0521516501.

Bloch, M. & Barros, J. 2011. *Physical-Layer Security*. Cambridge University Press. Available at: https://doi.org/10.1017/cbo9780511977985.

Brassard, G. & Salvail, L. 1992. Secret-Key Reconciliation by Public Discussion. In: *Helleseth, T. (Eds.) Advances in Cryptology - EUROCRYPT '93*, vol. 765, pp.410–423. Springer Berlin Heidelberg. Available at: https://doi.org/10.1007/3-540-48285-7_35.

Buttler, W.T., Lamoreaux, S.K., Torgerson, J.R., Nickel, G.H., Donahue, C.H. & Peterson, C.G. 2003. Fast, efficient error reconciliation for quantum cryptography. *Physical Review A*, 67(5), p. 052303. Available at: https://doi.org/10.1103/physreva.67.052303.

Cachin, C. & Maurer, U. 1997. Unconditional security against memory-bounded adversaries. In: *Kaliski, B.S. (Eds.) Advances in Cryptology - CRYPTO '97*, vol. 1294, pp.292-306. Springer Berlin Heidelberg. Available at: https://doi.org/10.1007/bfb0052243.

Carleial, A. & Hellman, M. 1977. A note on Wyner's wiretap channel (Corresp.). *IEEE Transactions on Information Theory*, 23(3), pp. 387–390. Available at: https://doi.org/10.1109/tit.1977.1055721.

Cramer, R., Damgard, I.B. & Nielsen, J.B. 2015. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press. Available at: https://doi.org/10.1017/cbo9781107337756.

Csiszar, I. & Korner, J. 1978. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3), pp. 339–348. Available at: https://doi.org/10.1109/tit.1978.1055892.

Diffie, W. & Hellman, M. 1976. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), pp. 644–654. Available at: https://doi.org/10.1109/tit.1976.1055638.

Elkouss, D., Leverrier, A., Alleaume, R. & Boutros, J.J. 2009. Efficient reconciliation protocol for discrete-variable quantum key distribution. In: *IEEE International Symposium on Information Theory*. Seoul, South Korea, pp.1879-1883, June 28-July 3. Available at: https://doi.org/10.1109/isit.2009.5205475.

Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J. & Yeh, H. 2005. Current status of the DARPA quantum network (Invited Paper). In: *Donkor, E.J., Pirich, A.R. and Brandt, H.E. (Eds.) Proceedings Volume 5815, Quantum Information and Computation III, Defense and Security*. Orlando, Fl, March 28 - April 1. Available at: https://doi.org/10.1117/12.606489.

Galis, M., Milosavljević, M., Jevremović, A., Banjac, Z., Makarov, A. & Radomirović, J. 2021. Secret-Key Agreement by Asynchronous EEG over Authenticated Public Channels. *Entropy*, 23(10), p. 1327. Available at: https://doi.org/10.3390/e23101327.

Gallager, R. 1962. Low-density parity-check codes. *IEEE Transactions on Information Theory*, 8(1), pp. 21–28. Available at: https://doi.org/10.1109/tit.1962.1057683.

Gronberg, P. 2005. *Key reconciliation in quantum key distribution*. *Tech. rep.*, FOI-Swedish Defence Research Agency.

Hazay, C. & Lindell, Y. 2010. *Efficient Secure Two-Party Protocols*. Springer Berlin Heidelberg. Available at: https://doi.org/10.1007/978-3-642-14303-8.

Mahmood, Z. (ed.) 2019. *Security, Privacy and Trust in the IoT Environment*. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-18075-1.

Maurer, U.M. 1993. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3), pp. 733–742. Available at: https://doi.org/10.1109/18.256484.

Mehic, M., Niemiec, M., Siljak, H. & Voznak, M. 2020. Error Reconciliation in Quantum Key Distribution Protocols. In: *Ulidowski, I., Lanese, I., Schultz, U., Ferreira, C. (Eds.) Reversible Computation: Extending Horizons of Computing. RC 2020. Lecture Notes in Computer Science*. 12070, pp. 222–236. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-47361-7_11.

Menezes, A.J. 1997. *Handbook of applied cryptography*. Boca Raton: CRC Press. ISBN 9780849385230.

Milosavljević, M., Adamović, S., Jevremovic, A. & Antonijevic, M. 2018. Secret key agreement by public discussion from EEG signals of participants. In: *5th International Conference IcEtran 2018*. Palić, Serbia, June 11-14.

Mohamed, K.S. 2019. *The Era of Internet of Things*. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-18133-8.

Niemiec, M. 2019. Error correction in quantum cryptography based on artificial neural networks. *Quantum Information Processing*, 18(6, art.number:174). Available at: https://doi.org/10.1007/s11128-019-2296-4.

Rivest, R.L., Shamir, A. & Adleman, L. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), pp. 120–126. Available at: https://doi.org/10.1145/359340.359342.

Shannon, C.E. 1948a. A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27(3), pp. 379–423. Available at: https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

Shannon, C.E. 1948b. A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27(4), pp. 623–656. Available at: https://doi.org/10.1002/j.1538-7305.1948.tb00917.x.

Shannon, C.E. & Weaver, W. 1963. *The Mathematical Theory of Communication*. University of Illinois Press. ISBN 0252725484.

Sugimoto, T. & Yamazaki, K. 2000. A study on secret key reconciliation protocol "Cascade". *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E83-A(10), pp. 1987–1991.

Tan, E.Y.Z., Lim, C.C.W. & Renner, R. 2020. Advantage Distillation for Device-Independent Quantum Key Distribution. *Physical Review Letters*, 124(2, art.number:020502). Available at: https://doi.org/10.1103/PhysRevLett.124.020502.

Unkašević, T., Banjac, Z. & Milosavljević, M. 2019. A Generic Model of the Pseudo-Random Generator Based on Permutations Suitable for Security Solutions in Computationally-Constrained Environments. *Sensors*, 19(23, art.number:5322). Available at: https://doi.org/10.3390/s19235322.

Wang, Q., Wang, X., Lv, Q., Ye, X., Luo, Y. & You, L. 2015. Analysis of the information theoretically secret key agreement by public discussion. *Security and Communication Networks*, 8(15), pp. 2507–2523. Available at: https://doi.org/10.1002/sec.1192.

Wyner, A.D. 1975. The Wire-Tap Channel. *The Bell System Technical Journal*, 54(8), pp. 1355–1387. Available at: https://doi.org/10.1002/j.1538-7305.1975.tb02040.x.

Yamazaki, K. & Sugimoto, T. 2000. On secret reconciliation protocol - modification of "Cascade"protocol. In: *International Symposium on Information Theory and Its applications*. Honolulu, Hawaii, pp.223–226, Nov. 5-8.

Yao, A.C. 1982. Protocols for secure computations. In: *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*. Chicago, IL, USA, pp.160-164, November 3-5. Available at: https://doi.org/10.1109/sfcs.1982.38.

Ziegler, S. (ed.) 2019. *Internet of Things Security and Data Protection*. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-04984-3.

ПРОТОКОЛЫ УСТАНОВЛЕНИЯ СИММЕТРИЧНЫХ СЕКРЕТНЫХ КЛЮЧЕЙ – СОВРЕМЕННЫЙ ПОДХОД

Меиран Галис[а,в], *Томислав* Б. Ункашевич[а], **корреспондент**, *Зоран* Дж. Баняц[а], *Милан* М. Милосавлевич[б]

[а] Институт ВЛАТАКОМ, г. Белград, Республика Сербия

[б] Университет Сингидунум, г. Белград, Республика Сербия

[в] Scytale, Тель-Авив, Государство Израиль

РУБРИКА ГРНТИ: 27.47.17 Математическая теория информации
28.21.19 Теория кодирования
50.37.23 Защита от несанкционированного доступа. Физическая защита информации
49.33.35 Надежность сетей связи и защита информации

ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Проблема эффективного распределения криптографических ключей в системах связи появилась уже в первые дни их существования, но особенно она обострилась с появлением систем массовой связи. Определение и внедрение эффективных протоколов распределения криптографических ключей в таких условиях играет значительную роль в повышении информационной безопасности в киберпространстве.

Методы: С помощью методов теории информации и безопасных многосторонних вычислений были определены протоколы для прямого установления криптографических ключей между сторонами связи.

Результаты: В статье представлены два новых подхода к решению проблемы установления криптографических ключей. Новшество в протоколе, определенном в модели безопасности, согласно теории информации, основана на источнике общей случайности, которым в данном случае является сигнал ЭЭГ каждого отдельного субъекта, участвующего в системе связи. Экспериментальные результаты показывают, что объем информации, поступающей к противнику, близок к нулю. Новшество во втором случае, обеспечивающее безопасность ключам на уровне

компьютерной безопасности за счет применения безопасных многосторонних вычислений при наличии нескольких участников-злоумышленников, содержится в новом приложении одной вычислительной модели. Для обоих подходов характерно то, что в рамках формальных теорий можно формальным образом сделать выводы об их характеристиках безопасности.

Выводы: В статье описываются два новых подхода к управлению криптографическими ключами в симметричных криптографических системах, подкрепленных экспериментальными результатами. Значимость предлагаемых решений заключается в том, что они позволяют установить надежную связь между заинтересованными сторонами, избегая влияния третьей доверенной стороны. Достигнутый таким образом уровень безопасности связи значительно повышается по сравнению с классическими криптографическими системами.

Ключевые слова: симметричный криптографический ключ, управление криптографическими ключами, источник случайности, преимущества дистилляции данных, согласование информации, усиление конфиденциальности, безопасные многосторонние вычисления.

ПРОТОКОЛИ ЗА УСТАНОВЉАВАЊЕ ТАЈНИХ СИМЕТРИЧНИХ КЉУЧЕВА - САВРЕМЕН ПРИСТУП

Меиран Галис[а,в], *Томислав* Б. Ункашевић[а], **аутор за преписку**, *Зоран* Ђ. Бањац[а], *Милан* М. Милосављевић[б]

[а] Институт ВЛАТАКОМ, Београд, Република Србија

[б] Универзитет Сингидунум, Београд, Република Србија

[в] Scytale, Тел Авив, Држава Израел

ОБЛАСТ: математика, рачунарство, телекомуникације
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Проблем ефикасне дистрибуције криптографских кључева у комуникационим системима постоји одавно, а са појавом масовних комуникационих система постао је изражен. Дефинисање и имплементација ефикасних протокола за установљавање симетричних криптографских

Galis, M. et al, Protocols for symmetric secret key establishment - modern approach, pp.604–635

кључева у таквим околностима има велики значај у подизању информационе безбедности у сајбер простору.

Методе: Применом метода теорије информација и безбедног кооперативног рачунања дефинисани су протоколи за директно установљавање криптографских кључева између комуникационих страна.

Резултати: У раду су дефинисана два нова приступа проблему установљавања криптографских кључева. Новина у протоколу дефинисаном у безбедносном моделу заснованом на теорији информација заснива се на извору заједничке случајности који је у овом случају ЕЕГ сигнал сваког субјекта учесника у комуникационом систему. Експериментални резултати показују да је количина информација која отиче ка противнику блиска нули. Новина у другом случају који кључевима обезбеђује сигурност на нивоу рачунарске сигурности применом безбедног кооперативног рачунања у присуству више злонамерних учесника садржана је у новој примени једног рачунарског модела. За оба приступа је карактеристично да је у оквиру формалних теорија могуће на формалан начин изводити закључке о њиховим безбед носним својствима.

Закључак: Представљена су два нова приступа за установљавање криптографских кључева у симетричним криптографским системима са експерименталним резултатима. Значај предложених решења лежи у чињеници да омогућавају установљавање поуздане комуникације између заинтересованих страна са краја на крај, избегавајући утицај треће стране од поверења. На тај начин се значајно повећава постигнути ниво сигурности њихове комуникације у односу на класичне криптографске системе.

Кључне речи: симетрични криптографски кључ, успостављање кључа, извор случајности, дестилација предности, усклађивање информација, појачавање приватности, безбедно кооперативно рачунање.

Paper received on / Дата получения работы / Датум пријема чланка: 23.02.2022.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 22.06.2022.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 24.06.2022.