УДК 621. 391.3
doi:10.31799/1684-8853-2018-5-79-87

Articles

Theorem about key capacity of a communication network

A. D. Sinjuk[a], *PhD, Associate Professor, orcid.org/0000-0003-0608-4359*
O. A. Ostroumov[a], *PhD, Post-Graduate Student, orcid.org/0000-0003-1674-6248, oleg-26stav@mail.ru*
[a]*S. M. Budyonny Military Academy of Telecommunications, 3, Tikhoretskii Ave., 194064, Saint-Petersburg, Russian Federation*

Introduction: *An important aspect of cryptographic telecommunication systems is the encryption key control problem. The most complicated stages in its solution are the safe generation of the keys, their distribution, and their delivery to legitimate subscribers via protected communication channels, which is fairly expensive, sometimes slow and not always possible. As an alternative, the keys can be generated by transferring information via telecommunication channels, being possibly exposed to a violator. The known estimations of information efficiency look like a solution of sophisticated information theory problems for certain ways of open key coordination between two legitimate subscribers. Efficiency estimations for the conditions of network key generation are not known.* ***Purpose:*** *A strictly conclusive search for potential estimates of information efficiency of open network key generation.* ***Results:*** *Within the formulated statement of the problem, we have proposed a violator model and a network channel connectivity model which is a combination of a broadcast channel connecting three legitimate subscribers and an intercept channel at the output of which the violator controls the transferred information. The information exchange is based on the proposed models of a random coder and deterministic decoder with a specially developed asymptotic method of key generation. In order to assess the process, we introduce a system of quality indicators and requirements which differs from the known ones by its definition of "information" speed of network key generation. We also introduce a term of key network capacity which determines the asymptotic information efficiency of the key generation. We have formulated and rigorously proved a theorem about key capacity. The boundary values have been substantiated.* ***Practical relevance:*** *The obtained results develop the known scientific achievements in the field of open key coordination theory and can be used by specialists in the design and development of key control subsystems in modern cryptographic information security systems which provide closed network information exchange.*

Keywords *— communication network, legitimate subscribers, violator, network key, broadcast communication channel, intercept channel, random coder and deterministic decoder, joint information, asymptotic method of network secret key agreement by public discussion, quality indicators and requirements to a network key, network key generation speed, theorem about key capacity of a communication network of minimum size, key capacity assessment.*

Citation: Sinjuk A. D., Ostroumov O. A. Theorem about key capacity of a communication network. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 5, pp. 79–87. doi:10.31799/1684-8853-2018-5-79-87

Introduction

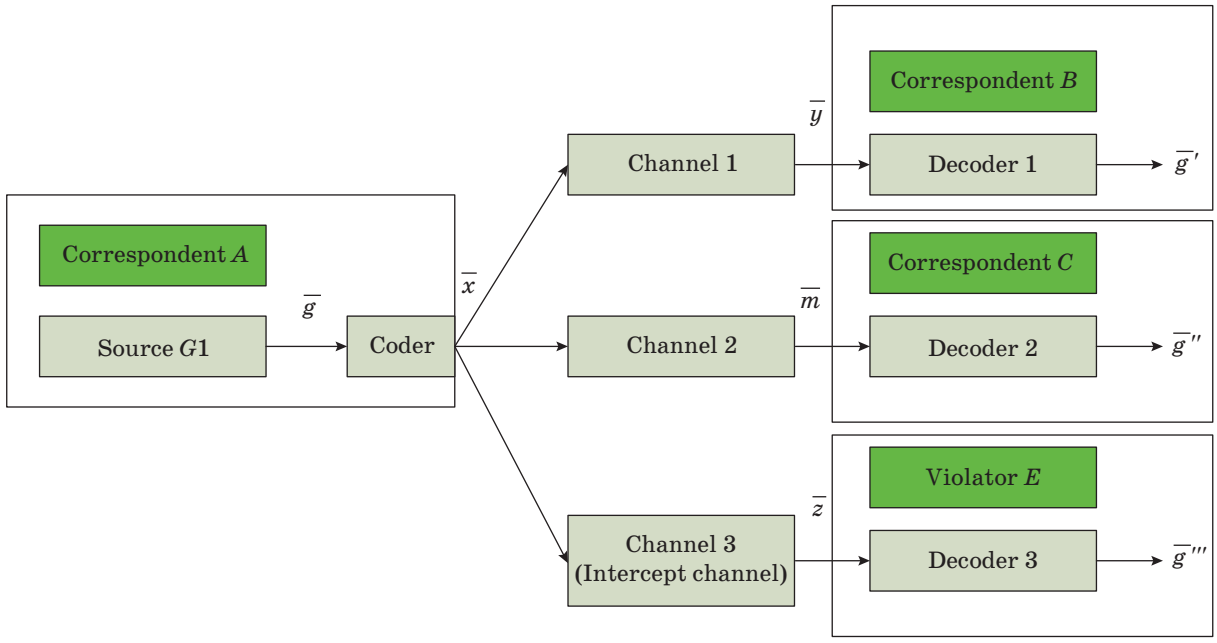
When ensuring information security of telecommunication systems which use cryptographic methods to protect information, it is most important to find an effective solution for the problem of forming, distributing and delivering keys to the subscribers. At the moment, this problem is solved by using protected communication channels, which is expensive, slow and not always possible. Therefore, it is of great practical interest to develop methods for generating these keys with open telecommunication channels. In these circumstances, we need to estimate the information efficiency of generating keys via open communication channels in order to optimize the secret key agreement by public discussion methods which are now under development. The obtained results develop the known scientific achievements in the network key sharing by public discussion [1–5].

Statement of the problem

We have to evaluate the information efficiency of generating a common key for legitimate subscribers (LS) of a communication network, called A, B and C, while exchanging data between them via channels available for a violator E. We need to ensure that a network key is promptly and reliably generated for the LS and the information about this key has a low level for E.

Let us consider the following generalized description of information transfer via the network [6, 7]. The LS A has a transmitter (coder). Two other LS B and C, and the violator E have three independently functioning receivers (decoders) whose inputs are fed with output signals of various channels. The transmitter gets messages $\overline{g}$ from a source $G1$ which LS A should simultaneously pass to the receivers 1, 2 and 3 (i. e. to the LS B and C, and the violator E). The channel connectivity model (CCM) of the network is shown in Fig.

Let the source $G1$ be described by a model of a discrete stationary source without memory [8–10]. The alphabet of the source is specified by a set G, consisting of t letters $G = \{g1, ..., g_t\}$. In every time unit, it independently chooses the i^{th} letter from the alphabet with a preset probability $p(g_i)$ [11], being specified by the assembly $\{G, p(g)\}$ [11]. Let the source generate a message $\overline{g}$, which is a sequence of



■ Channel connectivity model

k letters, and $\bar{g} \in G^k$, where G^k is a Cartesian k^{th} degree of the set G. The total number of the sequences from the source M_0 is

$$M_0 = t^k. \quad (1)$$

Generation probability $\bar{g}$ is equal to

$$p(\bar{g}) = \prod_{i=1}^{k} p\left(g^{(i)}\right), \quad (2)$$

where $g^{(i)}$ is the i^{th} element of the sequence $\bar{g}$.

Information parameter of the source is the entropy [8–10] which is equal to

$$H_S = H(G), \quad (3)$$

where $H(G)$ is the entropy of the assembly G.

Let us assume that all the communication channels in the CCM are described by models of discrete symmetric communication channels without memory (DSC) [10–12]. The complex of two channels with a common input (at the output of the coder LS A) and outputs (at the inputs of receivers 1 and 2 which are LS B and C respectively) can be described by a model of a broadcast channel (BC) [13–15] which binds the three LS in a framework of a loose network with the smallest number of subscribers [7, 8]. Signal transmission is determined by two channels with an input alphabet X, output alphabets Y and M, and matrices of transition probabilities $P_1 = \{p(y/x)\}$, $P_2 = \{p(m/x)\}$, $x \in X$, $y \in Y$, $m \in M$. Alphabets X, Y and M are finite. Let us denote the BC as $\{X, Y, M; p(y/x), p(m/x)\}$; the channels $\{X, Y; p(y/x)\}$ and $\{X, M; p(m/x)\}$ are components of the BC [13]. The DSC from the coder output of LS A to the input of the receiver 3 of violator E will be called an intercept channel (IC). Signal transmission via the IC $\{X, Z; p(z/x)\}$ is determined by the input alphabet X, output alphabet Z and a matrix of transition probabilities $P_3 = \{p(z/x)\}$, $x \in X$, $z \in Z$. The components of the BC and IC are independent channels:

$$p(y, m, z/x) = p(y/x)\, p(m/x)\, p(z/x).$$

Let us assume that the alphabets of $G1$, BC and IC coincide, and $|G| = |X| = |Y| = |M| = |Z| = t$.

Models of random coder and deterministic decoder

Let us build a random coder and a deterministic decoder which determine the asymptotic transmission of information for generating a network key in the model shown in Fig. Let a large n be specified. We need to build up a code (some approaches are discussed in [9, 16–18]) with which information will be transferred via the BC. We will consider only such codes for which the coder is an identity mapping on a set of code words. In this case, codes will be defined by sets of code words and decoding mappings, not by coders and decoders as it was in [9]. For information transmission, let us use a random coder. Out of a set X^n, we will choose a set of code words V; this set is a highly probable set of typical sequences [9, 11]. For building up V, the test channel method

can be used, discussed in details in [9]. Let the cardinality J of the set V be no more than

$$J = |V| < 2^{n(F(X;\,Y;\,M)\,-\,\tau)},$$

where $F(X; Y; M)$ is the average joint information (JI) of the BC defined in [19, 20], and τ is a certain positive number ($\tau > 0$).

A set of code words V specifies a certain (n, ε_1) code on X^n with the speed

$$R < F(X; Y; M) - \tau. \qquad (4)$$

In accordance with the direct BC coding theorem [6] for the (n, ε_1) code we provide an average probability of erroneous decoding no more than ε_1, $\varepsilon_1 > 0$. Let us split V into M_0 disjoint subsets C_i of the same cardinality. The cardinality D of any i^{th} subset C_i, where $i = 1, 2, ..., M_0$, is equal to $D = J / M_0$.

In accordance with the theorem of highly probable sets [9, 11], when n is large, probabilities of elements V are close to each other (i. e. the distribution of probabilities on the elements of the set V is close to uniform) and $P(V)$ is the total probability of all elements of the set V (the probability of (n, ε_1) code) is close to 1, i. e. for an arbitrarily small $\rho > 0$

$$P(V) > 1 - \rho. \qquad (5)$$

Then the probabilities of the elements C_i are also close to each other. The expression (5) means that for any sequence $\bar{x}, \bar{x} \in X^n$, with probability $p(\bar{x} \in C_i) \geq \tilde{n}$, we can find C_i to which $\bar{x}$ belongs. For each i^{th} sequence $\bar{g}_i$ of the source $G1$, a certain C_i is chosen. Let us consider random coding. Let $\bar{g}_i$ appear at the output of $G1$. The coder chooses C_i. Then randomly, with probability $1/D$, it chooses from the sequences C_i a code word and sends it to the input of the BC (and the IC). Such coding by (n, ε_1) code determines the probability distribution on X^n

$$p(\bar{x}) = \begin{cases} \dfrac{1}{D} p(\bar{g}_i), \text{ для всех } \bar{x} \in C_i, \text{ где } i = 1, \ldots, M_0 \\ 0, \text{ для всех остальных } \bar{x} \notin \bigcup\limits_{i=1}^{M_0} C_i. \end{cases} \qquad (6)$$

The next statement (proved in [6]) determines that JI does not grow when a $G1$ sequence is transferred by a code word as long as n characters with the use of random coding, as compared to the JI of the BC $F(X^n; Y^n; M^n)$.

Statement 1. Let $F(X^n; Y^n; M^n)$ be defined for (6) and $F(G^k; Y^n; M^n)$ be the average JI between the $G1$ output and the outputs of the BC. Then

$$F(G^k; Y^n; M^n) \leq F(X^n; Y^n; M^n), \qquad (7)$$

where G^k is Cartesian k^{th} degree of the set, and the equality in (7) is satisfied if C_i consists of just one code word.

Let us discuss the deterministic decoder model [6] and find the probability of correct decoding. LS B and C choose C_i as solving areas corresponding to $\bar{g}_i$, and $S^i \subseteq Y^n$, $Q^i \subseteq M^n$, where $i = 1, ..., M_0$. For each code word $u_i = 1, ..., M_0$, let us define a joint solving area L which would unite the solving areas $S^i \subseteq Y^n$, $Q^i \subseteq M^n$. Let $J1$ be a joint assemble of solutions which is a result of mapping of the assemble $Y^n M^n$ onto a set of solutions. Each couple of sequences $(\bar{y}, \bar{m}) \in Y^n M^n$ determines the solution $j \in J1$ according to the following rule:

$$j1 = \begin{cases} j1_i, \text{ если } (\bar{y}, \bar{m}) \in L_i, \; i = 1, \ldots, M_0, \\ j1_{M_0+1}, \text{ если } (\bar{y}, \bar{m}) \notin \bigcup\limits_{i=1}^{M_0} L_i. \end{cases} \qquad (8)$$

In [6] it is proved that after transmitting a $G1$ sequence by a code word of n characters with random coding and decoding by the rule (8), the uncertainty of the source with known outputs of the BC $HF(G^k/Y^n, M^n)$ does not exceed the uncertainty of the BC $HF(X^n/Y^n, M^n)$ specified in [6].

After transmitting a code word with probability distribution (6) and decoding by the rule (8), the full group of events is defined as

$$\Pr\left((\bar{y}, \bar{m}) \notin \bigcup_{i=1}^{M_0} L_i\right) + \Pr\left((\bar{y}, \bar{m}) \in \bigcup_{i=1}^{M_0} L_i\right) = 1, \qquad (9)$$

where $\Pr\left((\bar{y}, \bar{m}) \notin \bigcup\limits_{i=1}^{M_0} L_i\right)$ is the probability of making a decision j_{M0+1} (probability of giving up the decoding) by rule (8) or the probability of combination $(\bar{y}, \bar{m}) \in Y^n M^n$, which both stay "outside the (n, ε_1) code". Then, according to (5)

$$\Pr\left((\bar{y}, \bar{m}) \notin \bigcup_{i=1}^{M_0} L_i\right) < 1 - (1 - \rho)^2.$$

For $\Pr\left((\bar{y}, \bar{m}) \notin \bigcup\limits_{i=1}^{M_0} L_i\right)$, "inside the (n, ε_1) code", according to (8), let us write

$$\Pr\left((\bar{y}, \bar{m}) \in \bigcup_{i=1}^{M_0} L_i\right) = P_{ed} + P_{cd}, \qquad (10)$$

where P_{cd}, P_{ed} are the probabilities of correct and erroneous decoding of the (n, ε_1) code respectively, while $P_{ed} < \varepsilon_1$. Then the sought probability

$$P_{cd} \geq (1 - \rho^2) - \varepsilon_1. \qquad (11)$$

The model of a violator. Asymptotic method of forming a network key

The IC output for the violator E, if a $G1$ sequence is chosen and a random coder is used, is a random choice of a $G1$ message and uniform distribution of the input sequence at the IC input. It is assumed that the violator uses a *passive* strategy, observing the information exchange between the LS at the IC output. Other cases are discussed in [21–24]. It is assumed that E knows full descriptions of LS actions in forming a key, the (n, ε_1) code and the source $G1$. The violator's ignorance degree can be measured by the uncertainty rate ω [25]

$$\omega = H(G^k / Z^n). \qquad (12)$$

Here is a general description of the key generation method for a large n:

1. The LS A, using $G1$, randomly chooses $\overline{g}_i$, $\overline{g}_i \in G^k$, where $i = 1, ..., M_0$.

2. The LS A, using random coding, associates $\overline{g}_i$, $\overline{g}_i \in G^k$, with a code word $\overline{x}$, $\overline{x} \in V$ of n characters.

3. The LS A transmits $\overline{x}$, $\overline{x} \in V$ via the BC (and the IC), LS B, C (and E).

4. The LS B receives a sequence $\overline{y}$, $\overline{y} \in Y^n$ at the output of the first component BC. The LS C receives $\overline{m}$, $\overline{m} \in M^n$ at the output of the second component channel (the violator E receives $\overline{z}$, $\overline{z} \in Z^n$ at the IC output).

5. The LS B, with a probability higher than $1 - \rho$, according to the decoding rule which states that the receiver 1 makes a decision about the transferred code word, does the following: if $\overline{y} \in S_i$, where $i = 1, ..., M_0$, it makes a decision about the message $\overline{g}_i$ and gets $\overline{g}'$, $\overline{g}' \in G^k$, if $\overline{y} \notin \bigcup S_i$, the decision is to give up the decoding. The LS C, with a probability higher than $1 - \rho$, according to the decoding rule which states that the receiver 2 makes a decision about the transferred code word, does the following: if $\overline{m} \in Q_i$, where $i = 1, ..., M_0$, it makes a decision about the message $\overline{g}_i$ and gets $\overline{g}''$, $\overline{g}'' \in G^k$, if $\overline{m} \notin \bigcup Q_i$ (with a probability lower than ρ), the decision is to give up the decoding.

6. With a probability higher than $(1 - \rho)^2$, sequences $\overline{g}'$, $\overline{g}''$, $\overline{g}$ are chosen as a key for the LS B, C and A respectively.

The system of quality score and requirements to a key

The main quality indicators of a generated key can be reduced to reliable transmission of a large number of bits of a "good" key and a small leakage of information to the violator E. The term "good" means that the quality indicators of a key fit certain requirements adequate to the conditions of its generation and usage. The expression (9) shows that with a certain non-zero probability the keys may be not generated altogether. Furthermore, the keys (see expression (10)) may not coincide. Let us take into account all the cases in our estimation of probability P_ε. Apparently, P_ε is an addition to the correct decoding probability P_{cd} defined in (11). Then

$$P_\varepsilon = 1 - P_{cd} < 1 - (1 - \rho)^2 + \varepsilon_1.$$

As the next indicator, it would be expedient to choose the speed I_E with which the violator receives information about the key [25], i. e. the average amount of mutual information [9, 10, 12] between the assemblies of the source G^k and sequences at the IC output Z^n, assigned to the length n of a code word (CW) $I_E = I(G^k; Z^n)/n$.

The third indicator is the quality of the generated key Ω treated as closeness of its probability distribution to the uniform distribution of the probabilities of the key characters [11, 25]

$$\Omega = k(\log_2 t - H_s) / n, \qquad (13)$$

where k is the length of $G1$ messages, t is the volume of $G1$ alphabet, H_s is the entropy of $G1$ from (3).

Let us introduce the "information" speed of key generation.

Definition 1. A number H_3 is called speed of BC key generation if for a sufficiently large n and arbitrarily small $\varepsilon_2 > 0$, $\varepsilon_3 > 0$, $\varepsilon_4 > 0$ и $\varepsilon_5 > 0$, when the asymptotic method of key generation is used, a key is generated which meets the following requirements:

$$P_\varepsilon < \varepsilon_2; \qquad (14)$$
$$I_E < \varepsilon_3; \qquad (15)$$
$$\Omega < \varepsilon_4; \qquad (16)$$
$$H_3 < (H(G^k) - \varepsilon_5)/n. \qquad (17)$$

The introduced indicator determines the amount of information about the key generated, which includes one channel character of a code word transferred via the BC. From [8–10, 12] it is known that the code speed is equal to

$$R = (\log M)/n, \qquad (18)$$

where M is the code volume, and n is the code length.

It follows from definition 1 that H_3 is the "information" speed of the key generation, and from (18) it follows that R is the "information" speed of the transmission. Analysis of the asymptotic method of key generation shows that in the discussed method, a key is also transferred with random coding. The code speed in (18) is the maximum amount of information which can be transferred in a single channel character. Analysis of (17) and (18) shows that the maximum achievable H_3 does not exceed R, i. e.

$H_3 \le R$, and $H_3 = R$, provided that the violator's IC is "cut". We have to find the maximum H_3, as it determines the information efficiency of open generation of a network key, which will be represented as the key capacity. Therefore, we have to specify the bounds of R as a (n, ε_1) code parameter for any $\varepsilon > 0$ within

$$\left|\frac{1}{n}\log_2(M_0) - R\right| < \varepsilon, \qquad (19)$$

where M_0 is the volume of the set of $G1$ messages.

Then the research goal is reduced to finding the maximum achievable value of H_3 with a maximum possible R.

Key capacity theorem

In order to prove the theorem, let us prove the following statement:

Statement 2. Let $I(X^k; Z^n)$ be an average mutual information between the input and output of an IC by distribution (6), and let $I(G^k; Z^n)$ be an average mutual information between the output of the source $G1$ and output of the IC obtained with the use of a random coder. Then

$$I(X^k; Z^n) \ge I(G^k; Z^n) \qquad (20)$$

and

$$H(X^n / Z^n) \ge H(G^k / Z^n). \qquad (21)$$

The equality in (20) and (21) is achieved if each subset C_i of a random coder, where $i = 1, 2, ..., M_0$ consists of just one code word.

Proof

Let us consider mutual information $I(X^n, G^k); Z^n)$:

$$I((X^n, G^k); Z^n) = I(X^n, Z^n) + I(G^k; Z^n / X^n) = \\ = I(G^k; Z^n) + I(X^n; Z^n / G^k).$$

Taking into account that the output of the IC is determined only by its input, we have $H(Z^n / G^k, X^n) = H(Z^n / X^n)$, and hence $I(G^k; Z^n / X^n) = 0$. Then

$$I(X^n, Z^n) = I(G^k; Z^n) + I(X^n; Z^n / G^k). \qquad (22)$$

The expression (22) proves that the inequality (20) is true.

The analysis of the joint probability distribution law at $G1$ output in (2) and at the BC input in (6) shows that

$$H(X^n, G^k) = H(X^n) + H(G^k / X^n) = \\ = H(G^k) + H(X^n / G^k).$$

Taking into account (6), the BC input can uniquely determine the source output, then $H(G^k / X^n) = 0$. Therefore, we can write

$$H(X^n) = H(G^k) + H(X^n / G^k) \ge H(G^k). \qquad (23)$$

The equality sign in (23) is achieved if each C_i consists of just one code word. Let us unwind (22).

$$H(X^n) - H(X^n / Z^n) = H(G^k) - H(G^k / Z^n) + \\ + H(X^n / G^k) - H(X^n / Z^n, G^k).$$

Taking into account (23), we have

$$H(G^k / Z^n) = H(X^n / Z^n) - H(X^n / Z^n, G^k).$$

The last expression proves that the inequality (21) is true. The statement is proved.

Definition 2. The key capacity C_3 of a BC is the maximum achievable H_3 with which a key is generated meeting the requirements (14) – (17) for arbitrarily small $\varepsilon_2 > 0$, $\varepsilon_3 > 0$, $\varepsilon_4 > 0$ and $\varepsilon_5 > 0$:

$$C_3 = \max H_3.$$

Theorem. Let, in the above-described channel connectivity conditions, the subscribers of a connection network (BC) use the asymptotic method of key generation with uniform distribution of character probabilities at $G1$ output, a random coder of (n, ε_1) code for transmission and a deterministic decoder for reception in order to generate a network key. Let the violator follow a passive strategy of information intercept. Let the value of BC capacity C exceed the value of IC capacity C_w. Then

$$C_3 = C - C_w, \qquad (24)$$

where C is the capacity of the BC [8, 9, 15], and C_w is the capacity of the IC

$$C_w = \log_2 L + \sum_{j=1}^{L} p_j \log_2 p_j,$$

where L is the volume of the IC output alphabet, $p_1, ..., p_L$ are the elements in the first line of the transient probability matrix of the IC [9].

Proof

In accordance with the definition of BC uncertainty $HF(X^n / Y^n, M^n)$ from [6], using Fano's inequality [9, 12], let us write:

$$HF(X^n / Y^n, M^n) \le h(\lambda) + \lambda \log(M_0),$$

where λ is the average probability of a BC decoding error [6]. Then for any χ, $\chi > 0$, depending on ε_1, we can write

$$HF(X^n / Y^n, M^n) / n < \chi. \quad (25)$$

Let us find out how H_3 is interconnected with the violator's uncertainty speed ω from (12) when the requirements (14) – (17) are met, for arbitrarily small $\varepsilon_2 > 0$, $\varepsilon_3 > 0$, $\varepsilon_4 > 0$ and $\varepsilon_5 > 0$. Add up the left and right parts of the inequalities which determine the demands to the key (15) and (17), move I_E to the right-hand side, represent the latter as average mutual information [8, 9, 12] and finally get

$$H_3 < H(G^k / Z^n) / n + \varepsilon_3 - \varepsilon_5. \quad (26)$$

Now, taking into account the expression (21) and statement 1, we can rewrite (26) as

$$H_3 < H(X^n / Z^n) / n + \varepsilon_3 - \varepsilon_5. \quad (27)$$

If we add up the left and right parts of the inequalities (25) and (27) and move $HF(X^n / Y^n, M^n) / n$ to the right-hand side, we will get

$$H_3 < H(X^n / Z^n) / n - HF(X^n / Y^n, M^n) / n + \varepsilon_3 - \varepsilon_5 + \chi. \quad (28)$$

Adding and subtracting $H(X^n) / n$ in the right-hand side of (28), according to the definitions of JI and mutual information from [9, 22], will give us the following:

$$H_3 < F(X^n; Y^n; M^n) / n - I(X^n; Z^n) / n + \varepsilon_3 - \varepsilon_5 + \chi. \quad (29)$$

Using the results of the theorems about BC information capacity [6] and DSC information capacity [9], we can rewrite (29) as

$$H_3 < \max_{\{p(x)\}} F(X; Y; M) - \max_{\{p(x)\}} I(X; Z) + \varepsilon_3 - \varepsilon_5 + \chi. \quad (30)$$

Results of the theorems about average JI maximization [19, 20] and average mutual information maximization [9] $\max\limits_{\{p(x)\}} F(X; Y; M)$ and $\max\limits_{\{p(x)\}} I(X; Z)$ can be achieved with independent and uniform distribution of BC and IC input character probabilities. For (n, ε_1) code speed defined in (4), the following is true:

$$R < \max_{\{p(x)\}} F(X; Y; M) - \tau. \quad (31)$$

Let a sufficiently large n ($n \to \infty$) be chosen. Then, according to the theorem of highly probable sets [9, 11], the probability of (n, ε_1) code $P(V)$ will tend to 1, and $\rho \to 0$. Then at the input of the BC (and IC), uniformly distributed (with nearly equal probability) code words will appear. Due to this, the distribution of BC and IC input character probabilities is very close to uniform. The results of the theorem about average JI maximization and the direct theorem of BC coding [6] allow us to rewrite (31) (note that $\tau \to 0$ when $n \to \infty$):

$$R < C. \quad (32)$$

This means that (n, ε_1) code speed can be maximized as closely to the BC capacity value as we want, but will never exceed it. Consequently, $R \to \max$. Then it follows from the direct theorem of BC coding [6] that $\varepsilon_1 \to 0$, too. Now from $\rho \to 0$ it follows that $\varepsilon_2 \to 0$, too. Then the fulfillment of requirement (14) determines that $P_\varepsilon \to 0$. In this conditions, $HF(X^n / Y^n, M^n) \to 0$. From the inequality (25), we can see that $\chi \to 0$, too. Using the results of the theorems about information capacity and the direct theorem of DSC coding [9] with uniform distribution of code words at the IC input

$$\max_{\{p(x)\}} I(X; Z) = C_w, \quad (33)$$

Let us assume that $C > C_w$. When $n \to \infty$, we can find a code whose value R will satisfy the inequality

$$C_w < R < C. \quad (34)$$

Using the results of the information capacity theorem and the converse theorem about DSC coding from [9] for the left-hand side of (34), i. e. the condition $C_w < R$, we can claim that the average probability of erroneous decoding in the IC will be higher than a certain preset positive number. Consequently, $I(X^n; Z^n) \to 0$. Then, taking into account (20) the statement 2, we can say that

$$I(G^k; Z^n) \to 0. \quad (35)$$

From the analysis (35), we can conclude that $\varepsilon_3 \to 0$ in the requirement (15). Let us estimate how close the key assembly distribution is to uniform probability distribution using the parameter Ω defined in the requirement (16). If $n \to \infty$, then, according to the definition of R in (4) and the restriction (34), k (the length measured in characters of the generated sequence $\bar{g}$ of the source $G1$) will also grow, i. e. $k \to \infty$. Let a random probability distribution be specified at the source output. According to the highly probable set theorem [9], when $k \to \infty$, a sequence at the $G1$ output is split into a highly probable subset of typical sequences U and a subset of non-typical sequences $\bar{U}$. The probabilities of elements U are close to each other, and $P(U)$, the to-

tal probability of the elements U, will be close to 1. Taking this into account, we can write

$$\log_2(M_0) \geq H(G^k), \quad (36)$$

where M_0 is the volume of the set of $G1$ sequences defined in (1), and $H(G^k)$ is the entropy of its assembly. The equality sign in (36) is achieved when the probability distribution of the messages at the source output is uniform. For that, the discrete stationary memoryless source $G1$ must have a uniform distribution law for the character probabilities in its messages [8, 9, 11]. Therefore, let us choose this distribution law at $G1$ output. In this case, $\Omega \to 0$ in (13), and hence $\varepsilon_4 \to 0$ in the requirement (16). Taking into account the above-mentioned conditions and considering the joint functioning of the source and a random coder, we can see that when $n \to \infty$, the highly probable subset of $G1$ output sequences expands to a highly probable subset of code words at the output of a random coder of (n, ε_1) code (this takes place at the input of BC and IC). Further analysis of using the asymptotic method of key generation shows that the method can be reduced to transferring coded sequences via the BC so that the violator who can observe only the output of his/her IC (and who knows the code in use) cannot restore a message you send. Analysis of (36) shows that when $n \to \infty$, the speed R of (n, ε_1) code will tend to its maximum in (18) and hence $\varepsilon \to 0$ in (19). Since the information about a "higher quality" key is transferred via the BC, H_3 will tend to the maximum R and, consequently, in the requirement (17) $\varepsilon_5 \to 0$. Furthermore, taking into account the definition 2 and inequality (30), let us write

$$C_3 = \max_{\{p(x)\}} \left[F(X; Y; M) - I(X; Z)\right] + \varepsilon_3 - \varepsilon_5 + \chi. \quad (37)$$

Under the condition described above, the key requirement parameters (14) – (17) $\varepsilon_2 \to 0$, $\varepsilon_3 \to 0$, $\varepsilon_4 \to 0$, $\varepsilon_5 \to 0$, and $\chi \to 0$ in (25). Then, taking into account the fulfillment of (31) – (33), we can rewrite (37) as

$$C_3 = C - C_w. \quad (38)$$

Expression (38) coincides with expression (24) from the statement of the theorem. Thus the theorem is proved.

Estimating the boundary values of the key capacity

If $C \leq C_w$, then $C_3 = 0$. Consequently, the lower boundary of C_3

$$0 \leq C_3.$$

In order to find the upper boundary of C_3, let us use the following statement whose proof is given in [6].

Statement 3. C_3 is bounded above

$$C_3 \leq \max F(X; Y; M / Z),$$

where the equality sign is set in the case of statistical independence of the assembly X at the input and assembly Z at the output of the IC (the IC is "cut" [7, 10, 12]).

Conclusion

The work contains new scientific results about open generation of keys for a communication network which includes three subscribers of connected BCs. We propose models of a random coder, deterministic decoder, asymptotic generation method and a system of quality indicators and requirements to a network key. We introduce a term of key capacity of a BC. We have formulated and proved a theorem about the key capacity of a BC, which provides the ways to estimate the asymptotic information efficiency of the studied process. We also have shown its boundary values.

The problems for further research should be assessing the key capacity for information exchange within a binary BC, search for regularities which determine the ways of forming a "good" key, and establishing integral links with earlier scientific results in the filed of secret key agreement by public discussion. On the base of the latter, a comprehensive comparative analysis should be performed, with the development of a methodology for estimating the gain of the proposed key generation method. Another goal could be determining the conditions and developing new methods for providing higher key capacity of a BC.

The obtained results can be helpful for the specialists in the design and optimization of key control subsystems in modern cryptographic information security systems which provide uninterrupted closed network information exchange.

References

1. **Siavoshani M. J., Mishra S., Diggavi S. N., Fragouli Ch.** Group secret key agreement over state-dependent wireless Broadcast channels, *IEEE ISIT 2011*, 2011, pp. 1960–1964.
2. **Shimizu T., Iwai H., Sasaoka H.** Group secret key agreement based on radio propagation characteristics in wireless relaying systems. *IEICE Transactions* (IEICET), 2012, 95-B(7), pp. 2266–2277.
3. **Naito M., Watanabe Sh., Matsumoto R., Uyematsu T.** Secret key agreement by soft-decision of signals in

gaussian maurer's model. *IEICE Transactions* (IEICET), 2009, 92-A(2), pp. 525–534.
4. **Li Zh., Wang H., Fang H.** Group-based cooperation on symmetric key generation for wireless body area networks. *IEEE Internet of Things Journal*, 2017, no. 4(6), pp. 1955–1963.
5. **Halford T. R., Courtade T. A., Chugg K. M., Li X., Thatte G.** Energy-efficient group key agreement for wireless networks. *IEEE Transactions on Wireless Communications*, 2015, no. 14 (10). pp. 5552–5564.
6. **Sinjuk A. D.** *Formirovanie trekhstoronnego shifrkliucha po otkrytym kanalam sviazi s oshibkami* [Forming a three-way encryption key through open communication channels with errors], SPb, VAS, 2009. 360 p. (In Russian).
7. **Shangin V. F.** *Informacionnaja bezopasnost' komp'juternyh sistem i setej* [Information security of computer systems and networks]. Moscow, Forum Publ., 2013. 416 p. (In Russian).
8. **Sklar B.** *Digital communications: fundamentals and applications*. Los Angeles, University of California, 2007. 1104 p.
9. **Kolesnik V. D., Poltyrev G. Sh.** *Kurs teorii informacii* [The course of information theory]. Moscow, Nauka Publ., 1982. 416 p. (In Russian).
10. **Sannikov V. G.** *Teorija informacii i kodirovanija* [Theory of information and coding]. Moscow, MTUSI Publ., 2015. 96 p. (In Russian).
11. **Bure V. M., Parilina E. M.** *Teorija verojatnostej i matematicheskaja statistika* [Theory of Probability and Mathematical Statistics]. SPb, Lan' Publ., 2013. 416 p. (In Russian).
12. **Bikkenin R. R., Chesnokov M. N.** *Teorija jelektricheskoj svjazi* [The theory of electrical communication]. Moscow, Akademija Publ., 2010. 329 p. (In Russian).
13. **Nair Ch., Gamal. A.** The capacity region of a class of three-receiver Broadcast channels with degraded message sets. *IEEE Transactions on Information Theory* (TIT), 2009, no. 55(10), pp. 4479–4493.
14. **Gohary R. H., Davidson T. N.** The capacity region of a product of two unmatched physically degraded gaussian broadcast channels with three individual messages and a common message. *IEEE Transactions on Information Theory* (TIT). 2013, no. 59(1), pp. 76–103.
15. **Kim H., Gamal A.** Capacity theorems for broadcast channels with two channel state components known at the receivers. *IEEE Transactions on Information Theory*. 2016, no. 62 (12), pp. 6917–6930.
16. **Muramatsu J., Miyake Sh.** construction of codes for the wiretap channel and the secret key agreement from correlated source outputs based on the hash property. *IEEE Transactions on Information Theory* (TIT). 2012, no. 58(2), pp. 671–692.
17. **Gao Y., Tuncel E.** Wyner-Ziv coding over broadcast channels: hybrid digital/analog schemes. *IEEE Transactions on Information Theory* (TIT). 2011, no. 57(9), pp. 5660–5672.
18. **Liang Y., Kramer G.** rate regions for relay broadcast channels. *IEEE Transactions on Information Theory* (TIT). 2007, no. 53(10), pp. 3517–3535.
19. **Ostroumov O. A., Sinjuk A. D.** Study of joint information. *Informacija i kosmos*. 2017, no. 3, pp. 55 — 58 (In Russian).
20. **Ostroumov O. A., Sinjuk A. D.** The information-information model of transmission of the general information of the broadcasting channel. *Vestnik komp'juternyh i informacionnyh tehnologij*. 2017, no. 11, pp. 29–36 (In Russian).
21. **Yakovlev V., Korzhik V., Bakaev M.** Protocols of key formation based on communication channels with noise under conditions of active interception using ex-tractors. *Problems of Information Security. Computer systems*. 2006, no. 1, pp. 60 — 81(In Russian).
22. **Dodis Y., Kanukurthi B., Katz J., Reyzin L., Smith A.** Robust fuzzy extractors and authenticated key agreement from close secrets. *IEEE Transactions on Information Theory* (TIT). 2012, no) 58(9), pp. 6207–6222.
23. **Alezabi K. A., Hashim F., Hashim Sh. J., Ali B. M.** An efficient authentication and key agreement protocol for 4G (LTE) networks. *IEEE region 10 symposium*. 2014. pp. 502 – 507.
24. **Wazid M., Das A. K., Kumar N., Odelu V., Reddy A. G., Park K., Park Y.** Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks. *IEEE Access*. 2017, no. 5, pp. 14966 – 14980.
25. **Maurer U.** Secret key agreement by public discussion based on common information. *IEEE Trans. on IT*. 1993, no. 39, pp. 733–742.

УДК 621.391.3
doi:10.31799/1684-8853-2018-5-79-87

Теорема о ключевой пропускной способности сети связи

А. Д. Синюк[a], доктор техн. наук, доцент, orcid.org/0000-0003-0608-4359
О. А. Остроумов[a], канд. техн. наук, адъюнкт, orcid.org/0000-0003-1674-6248, oleg-26stav@mail.ru
[a]Военная академия связи им. Маршала Советского Союза С. М. Буденного. Тихорецкий проспект, 3, Санкт-Петербург, 194064, РФ

Введение: важнейшим аспектом функционирования криптографических телекоммуникационных систем представляется решение задачи управления ключами шифрования. Сложными этапами ее решения являются безопасное формирование, распреде-

ление и доставка ключей законным корреспондентам с использованием защищенных каналов связи, что достаточно дорого, не всегда оперативно и возможно. Альтернативой выступают способы формирования ключей посредством передачи информации по каналам электросвязи, которая, возможно, становится известной нарушителю. Поиск известных оценок информационной эффективности для некоторых способов открытого ключевого согласования двух законных корреспондентов представлял решение сложных теоретико-информационных задач. Результаты же решения подобных задач для более сложных условий, связанных с введением третьего корреспондента и открытым формированием теперь уже сетевого ключа, до настоящего времени не известны. **Цель исследования:** строго доказательный поиск потенциальных оценок информационной эффективности открытого сетевого формирования ключей. **Результаты:** произведена постановка задачи оценки информационной эффективности открытого ключевого согласования сети и определены условия, обеспечивающие ее решение. В рамках первого результата предложены модели нарушителя и сетевой канальной связности трех законных корреспондентов. Последняя модель представляет совокупность широковещательного канала, связывающего корреспондентов, и канала перехвата нарушителя. Обмен информацией основан на предложенных моделях случайного кодера и детерминированного декодера посредством разработанного асимптотического метода формирования ключа. В целях достижения второго результата представлена система показателей качества и требований, отличающаяся от известных определением «информационной» скорости формирования сетевого ключа. Введен термин ключевой пропускной способности сети, определяющий асимптотическую информационную эффективность формирования ключа. Представленные строгое доказательство теоремы о ключевой пропускной способности и обоснование ее граничных значений определяют формирование окончательных условий, обеспечивающих решение теоретико-информационной задачи оценки эффективности открытого формирования сетевого ключа.

Ключевые слова — сеть связи, законные корреспонденты, нарушитель, сетевой ключ, широковещательный канал связи, канал перехвата, случайный кодер и детерминированный декодер, совместная информация, асимптотический метод формирования сетевого ключа, показатели качества и требования к сетевому ключу, скорость формирования сетевого ключа, теорема о ключевой пропускной способности сети связи минимального объема, оценка ключевой пропускной способности.

Цитирование: Синюк А. Д., Остроумов О. А. Теорема о ключевой пропускной способности сети связи. *Информационно-управляющие системы*, 2018, № 5, с. 79–87. doi:10.31799/1684-8853-2018-5-79-87

Citation: Sinjuk A. D., Ostroumov O. A. Theorem about key capacity of a communication network. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 5, pp. 79–87. doi:10.31799/1684-8853-2018-5-79-87

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию. Рукописи не возвращаются.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.