Math-Net.Ru

Общероссийский математический портал

L. R. Ahmetzyanova, E. K. Alekseev, I. B. Oshkin, S. V. Smyshlyaev, L. A. Sonina,
О свойствах блочных алгоритмов шифрования Магма и Кузнечик в режиме
CTR с преобразованием ключа методом CryptoPro Key Meshing, *Матем. вопр.
криптогр.*, 2017, том 8, выпуск 2, 39–50

DOI: <https://doi.org/10.4213/mvk222>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и
согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.198.64.247

26 апреля 2023 г., 14:23:03

**On the properties of the CTR encryption mode of Magma
and Kuznyechik block ciphers with re-keying method
based on CryptoPro Key Meshing**

**L. R. Ahmetzyanova, E. K. Alekseev, I. B. Oshkin,
S. V. Smyshlyaev, L. A. Sonina**

CryptoPro LLC, Moscow

Получено 03.IV.2016

Abstract. Security bounds for the Magma cipher CTR encryption mode with the CryptoPro Key Meshing (CPKM) re-keying method are obtained for the standard security model and side channel information model. A modified re-keying method better than CPKM is proposed. Operational features of the Kuznyechik cipher CTR encryption mode for several re-keying methods are discussed.

The work was supported by the Russian Foundation of Basic Research, the project 16-01-00226 A.

Keywords: provable security, encryption mode, block cipher, GOST, re-keying

**О свойствах блочных алгоритмов шифрования Магма и Кузнечик
в режиме CTR с преобразованием ключа методом CryptoPro Key
Meshing**

**Л. Р. Ахметзянова, Е. К. Алексеев, И. Б. Ошкин, С. В. Смышляев,
Л. А. Сони́на**

ООО «Крипто-Про», Москва

Аннотация. Для шифра Магма с преобразованием ключа методом CryptoPro Key Meshing (CPKM) получены оценки стойкости в рамках стандартной модели и модели с информацией из побочных каналов. Предложена модификация алгоритма преобразования ключа, улучшенная по сравнению с CPKM. Обсуждаются эксплуатационные характеристики шифра Кузнечик в режиме CTR для нескольких методов преобразования ключа.

Работа выполнена при поддержке РФФИ, проект 16-01-00226 А.

Ключевые слова: доказуемая стойкость, режим шифрования, блочный шифр, ГОСТ, смена ключа

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 39–50 (Russian)

© Академия криптографии Российской Федерации, 2017 г.

1. Introduction

The effectiveness of many cryptanalytic methods (see, e.g. [6] and [7]) depends heavily on the amount of data (e.g., number of pairs of plaintext and ciphertext) obtained using one and the same key. The amount of data that may be securely processed with one key is called a key lifetime. The key lifetime should be limited in order to prevent the adversary to obtain any significant information, so there exists a necessity to use special encryption modes that assume a key transformation every time after a given amount of data was processed.

The introduction of new Magma and Kuznyechik block ciphers in Russia (see [1]) and their encryption modes (see [2]) makes it necessary to define some re-keying methods. The re-keying method for the GOST 28147-89 algorithm [8] was defined in [4] and is called CryptoPro Key Meshing. In [5] the combinatorial and probabilistic properties of this method were analyzed, but there is no analysis of its impact on cryptographic properties of the used encryption mode. In view of an opportunity to use this re-keying method (or methods based on it) with the new block ciphers, it is relevant to analyze the properties of encryption modes which include a re-keying method.

In developing a new re-keying method the operational differences between the Magma and Kuznyechik ciphers, such as block size and key extension complexity, should be taken into account. Therefore it is interesting to analyze the influence of the Kuznyechik's features with re-keying method on the efficiency of the extended encryption mode.

2. Notation

By V_n we denote a set of n -component bit strings where components are enumerated from left to right starting from zero. We denote by $M_{(i)}$ the i -th bit, $i \in \{0, \dots, n-1\}$, of the string $M \in V_n$. For $A \in V_n$ and $B \in V_m$ we denote by $A \parallel B$ a string $A_{(0)} \parallel \dots \parallel A_{(n-1)} \parallel B_{(0)} \parallel \dots \parallel B_{(m-1)} \in V_{n+m}$. Let $|M|$ be a bit length of the string M , and $|M|_8$ be a length of M in bytes.

For a finite set A we denote by $Perm(A)$ a set of all bijective mappings on A (permutations on A), and by $Func(A)$ a set of all mappings from A to A . A block cipher E (or just a cipher) is a set of permutations $\{E_K | K \in V_k\} \subseteq Perm(V_n)$, where K is a key. For $M \in V_{mn}$, $m \geq 1$, we denote by M_i , $0 \leq i \leq m-1$, a string $M_{(i \cdot n)} \parallel M_{(i \cdot n + 1)} \parallel \dots \parallel M_{(i \cdot n + n - 1)} \in V_n$ and call it the i -th block of the string M . Thus the string M is represented as $M = M_0 \parallel M_1 \parallel \dots \parallel M_{m-1}$. If $IV \in V_{n/2}$, then we assume that IV_i , $i \in \{0, 1, \dots, 2^{n/2} - 1\}$, is a string $IV \parallel i \in V_n$, implying without additional notations that IV is concatenated with $n/2$ -bit representation of the number i , defined according to [2].

We model an adversary by means of a probabilistic Turing machine. If an algorithm $\mathcal{A}$ with inputs $X_1, \dots, X_t$ returns Y as a result, we denote this as $\mathcal{A}(X_1, \dots, X_t) \Rightarrow Y$. A formula $s \in_{\mathcal{U}} S$ denote that a value s is chosen from a set S at random according to the uniform distribution. We denote by $\mathcal{A}(t, a, b, \dots)$ a set of adversaries whose computational resources (a sum of program size and average complexity) are not greater than t and the other parameters (e.g. a number of requests to oracles) are limited with values $a, b, \dots$ (the meaning of these parameters will be explained in each specific case). If $\mathcal{T}$ is a decisional problem where an adversary A should distinguish a bit b , then the advantage of this adversary for the problem $\mathcal{T}$ is

$$\mathbf{Adv}^{\mathcal{T}}(A) = \Pr[A \Rightarrow 1 | b = 1] - \Pr[A \Rightarrow 1 | b = 0].$$

3. Block cipher encryption modes

Block cipher is used as a basic function to construct some protocols. The challenge of confidentiality is solved with the use of block cipher in a special way, which is commonly referred to as “an encryption mode”.

In this paper we consider a CTR encryption mode, defined according to [2] (in the case where $s=n$): the result of the encryption of a message

$$M = M_0 || \dots || M_{m-1} || M_m, \quad M_0, \dots, M_{m-1} \in V_n, \quad M_m \in V_r,$$

is a string $IV || C_0 || \dots || C_{m-1} || C_m$, where $IV \in V_{n/2}$, $C_i = M_i \oplus E_K(IV_i)$ and $C_m = M_m \oplus E_K(IV_m)_{(0)} || \dots || E_K(IV_m)_{(r-1)}$. In addition, the strings IV are different for different messages processed with one key.

A periodical key transformation for long message processing is considered as an extension of the basic encryption mode. The CryptoPro Key Meshing re-keying method for the GOST 28147-89 algorithm [8] was defined in [4] in the following way:

$$K_0 = K, \quad K_{i+1} = E_{K_i}^{-1}(D_1) || E_{K_i}^{-1}(D_2) || E_{K_i}^{-1}(D_3) || E_{K_i}^{-1}(D_4), \quad i \geq 0,$$

where $D_1, D_2, D_3, D_4 \in V_{64}$ are pairwise different constants, K is an initial random key and $K_0, K_1, \dots$ are keys directly used for message processing.

We consider an incomplete version of the CPKM method, where only the key is changed. There is an additional rule for changing IV in the original CPKM method. For the Kuznyechik cipher we assume an algorithm that is similar to CPKM but uses two 128-bits constants instead of four, and we denote it by CPKM_{128} .

We denote by CTR-CPKM_l the CTR encryption mode that assumes the key transformation according to the CPKM method after every l processed blocks of message. The string which consists of message blocks processed by means of one key will be called “section”.

4. The target properties of the perspective re-keying method

The requirements for the re-keying method which are used in high-level cryptographic protocols may be divided into operational and cryptographic. The main operational requirements are:

1. Maximal efficiency in the case of short data processing — the first section should be processed using the initial key.
2. Efficiency — the data processing speed with the re-keying method should not differ significantly from the speed without it.

The cryptographic requirements are formulated as follows:

1. Common security — the use of the re-keying method should improve the security properties of the initial encryption scheme.
2. Security in the extended model — the complexity of one section key disclosure with side channels information should not differ significantly from cases where adversary additionally has the same information about keys of other sections.
3. Forward secrecy — the compromise of the key used in one section should not compromise the keys or data used in previous sections.

These requirements should be accounted during the development of re-keying methods with the new standardized block ciphers and their encryption modes.

In section 6 we give the security bounds for the CTR-CPKM_l encryption mode in the common model, i.e. we analyze whether the CPKM method satisfies the first requirement. A discussion on the CPKM method conformity with the second requirement may be found in section 7.

The re-keying methods which are similar to CPKM satisfy the first operational requirement. The second requirement is considered in section 9, where we present some results on the operational features of the Kuznyechik cipher in the CTR encryption mode with several re-keying methods.

5. Known models and security bounds

It is a common practice to bound the security of block ciphers in the PRF and PRP-CCA models (see, e.g. [3]), for clarity we call them problems.

Definition 5.1. A PRF (Pseudo Random Function) problem for a cipher $\{E_K : V_n \rightarrow V_n \mid K \in V_k\}$ is the following decisional problem. An adversary A has access to an oracle $\mathcal{O}^{\text{PRF}}$ which operates in the following way. Before starting the work the oracle $\mathcal{O}^{\text{PRF}}$ chooses $b \in_{\mathcal{U}} \{0, 1\}$. If $b = 0$, then $\mathcal{O}^{\text{PRF}}$ chooses a function $F \in_{\mathcal{U}} \text{Func}(V_n)$ and if $b = 1$, then it chooses a key $K \in_{\mathcal{U}} V_k$. The oracle $\mathcal{O}^{\text{PRF}}$ with input $M \in V_n$ returns either $F(M)$ (if $b = 0$) or $E_K(M)$ (if $b = 1$).

The advantage of the cipher E in the PRF problem with parameters t and q (q is a number of queries to the oracle $\mathcal{O}^{\text{PRF}}$) is

$$\text{Adv}_E^{\text{PRF}}(t, q) = \max_{A \in \mathcal{A}(t, q)} \text{Adv}_E^{\text{PRF}}(A).$$

Definition 5.2. A PRP-CCA (Pseudo Random Permutation in Chosen Ciphertext Attack) problem for a cipher $\{E_K : V_n \rightarrow V_n \mid K \in V_k\}$ is the following decisional problem. An adversary A has access to oracles $\mathcal{O}^{\text{PRP}}$ and $\mathcal{O}^{\text{PRP}^{-1}}$ which operate in the following way. Before starting the work the oracle $\mathcal{O}^{\text{PRP}}$ chooses $b \in_{\mathcal{U}} \{0, 1\}$. If $b = 0$, then $\mathcal{O}^{\text{PRP}}$ chooses a permutation $R \in_{\mathcal{U}} \text{Perm}(V_n)$, and if $b = 1$, then it chooses a key $K \in_{\mathcal{U}} V_k$. The oracle $\mathcal{O}^{\text{PRP}}$ with an input $M \in V_n$ returns either $R(M)$ (if $b = 0$) or $E_K(M)$ (if $b = 1$). The oracle $\mathcal{O}^{\text{PRP}^{-1}}$ takes the input string M and returns the result of the permutation that is the inverse of the function realized by the oracle $\mathcal{O}^{\text{PRP}}$.

The advantage of the cipher E in the PRP-CCA problem with parameters t and q_1, q_2 (q_1 is a number of queries to the oracle $\mathcal{O}^{\text{PRP}}$, q_2 is a number of queries to the oracle $\mathcal{O}^{\text{PRP}^{-1}}$) is

$$\text{Adv}_E^{\text{PRP-CCA}}(t, q_1, q_2) = \max_{A \in \mathcal{A}(t, q_1, q_2)} \text{Adv}_E^{\text{PRP-CCA}}(A).$$

If the block cipher has no specific methods to decrease the security, the values $\text{Adv}_E^{\text{PRF}}(t, q)$ and $\text{Adv}_E^{\text{PRP-CCA}}(t, q_1, q_2)$ may be bounded by the characteristics of general methods of solving these problems. For the PRF problem it is a method based on the birthday paradox, and for the PRP-CCA problem it is a brute force attack. So for such cipher E we assume the following approximations:

$$\text{Adv}_E^{\text{PRP-CCA}}(t, q) \approx \frac{t}{2^k}, \quad \text{Adv}_E^{\text{PRF}}(t, q) \approx \frac{t}{2^k} + \frac{q^2}{2^n}. \quad (1)$$

A standard model to bound the security of encryption modes is a LOR-CPA problem (see, e.g. [3]).

Definition 5.3. A LOR-CPA (Left Or Right in Chosen Plaintext Attack) problem for a $\mathcal{SE}$ encryption mode is the following decisional problem. An adversary A has access to an oracle $\mathcal{O}^{\text{LOR}}$ that operates in the following way. Before starting the work the oracle $\mathcal{O}^{\text{LOR}}$ chooses $b \in_{\mathcal{U}} \{0, 1\}$. The adversary A can make requests to the oracle $\mathcal{O}^{\text{LOR}}$, each of these requests is a pair of strings (M^0, M^1) , $|M^0| = |M^1|$. In response to the request (M^0, M^1) the oracle returns a string C that is a result of processing the string M^b according to the $\mathcal{SE}$ encryption mode.

The advantage of the $\mathcal{SE}$ mode in the LOR-CPA problem with parameters t, q, m (q is a number of queries to the oracle $\mathcal{O}^{\text{LOR}}$, m is a maximal amount of blocks that the messages in query can consist of) is

$$\text{Adv}_{\mathcal{SE}}^{\text{LOR-CPA}}(t, q, m) = \max_{A \in \mathcal{A}(t, q, m)} \text{Adv}_{\mathcal{SE}}^{\text{LOR-CPA}}(A).$$

Theorem 5.1 ([3]). *The following inequality holds*

$$\text{Adv}_{\text{CTR}}^{\text{LOR-CPA}}(t, q, m) \leq 2 \cdot \text{Adv}_E^{\text{PRF}}(t + q + nqm, qm).$$

6. Security bound of the CTR-CPKM encryption mode in the LOR-CPA model

The main element of the proof of the theorem on security of the CTR-CPKM $_l$ encryption mode is the introduction of an intermediate IND-KM $_{l,m}$ problem (where m is referred to the maximal number of sections), that is used to replace the CTR-CPKM $_l$ mode by the abstract CTR-RK $_l$ mode where a key is chosen at random for every new section.

Definition 6.1. An IND-KM $_{l,m}$ problem, where $l, m \in \mathbb{N}$, for a set of permutations $\mathcal{F} \subset \text{Perm}(V_n)$ is the following decisional problem. An adversary A has an access to an oracle $\mathcal{O}^{\text{IND-KM}_{l,m}}$, that stores an initially empty set $\mathcal{I}$. Before starting the work the oracle $\mathcal{O}^{\text{IND-KM}_{l,m}}$ chooses a bit $b \in_{\mathcal{U}} \{0, 1\}$ and a permutation $F \in_{\mathcal{U}} \mathcal{F}$. The first query of the adversary A is a number $j \in \{0, 1, \dots, m-1\}$. The oracle $\mathcal{O}^{\text{IND-KM}_{l,m}}$ returns a string $K' = F^{-1}(D_1) || F^{-1}(D_2) || F^{-1}(D_3) || F^{-1}(D_4)$ in response, if $b = 1$, and $K' \in_{\mathcal{U}} V_k$, if $b = 0$ (here D_1, D_2, D_3, D_4 are pairwise different constants). The subsequent queries of the adversary A to the oracle are empty strings. In response to each of these queries the oracle $\mathcal{O}^{\text{IND-KM}_{l,m}}$ operates as follows: chooses $IV \in_{\mathcal{U}} V_{\frac{n}{2}} \setminus \mathcal{I}$, adds the element IV to $\mathcal{I}$ and returns $IV || F(IV_{j:l}) || \dots || F(IV_{j:l+l-1})$.

We denote by $\mathbf{Adv}_{\mathcal{F}}^{\text{IND-KM}_{l,m}}(t, q)$ the following value:

$$\mathbf{Adv}_{\mathcal{F}}^{\text{IND-KM}_{l,m}}(t, q) = \max_{A \in \mathcal{A}(t, q)} \mathbf{Adv}_{\mathcal{F}}^{\text{IND-KM}_{l,m}}(A).$$

Lemma 6.1. *The following inequality holds*

$$\mathbf{Adv}_E^{\text{IND-KM}_{l,m}}(t, q) \leq 2 \cdot \mathbf{Adv}_E^{\text{PRP-CCA}}\left(t + q \cdot \frac{n}{2}, q \cdot l, 4\right) + \frac{8ql + 6}{2^n} + \left(\frac{4ql}{2^n}\right)^2.$$

The following final bound holds.

Theorem 6.1. *The following inequality holds for natural l, t, q, m if $k \in \{4n, 2n\}$:*

$$\begin{aligned} \mathbf{Adv}_{\text{CTR-CPKM}_l}^{\text{LOR-CPA}}(t, q, ml) &\leq 4m \cdot \mathbf{Adv}_E^{\text{PRP-CCA}}\left(t + mlq + q \cdot \frac{n}{2}, q \cdot l, \frac{k}{n}\right) + \\ &+ 2m \cdot \mathbf{Adv}_E^{\text{PRF}}(t + qml, ql) + 2m\delta, \end{aligned}$$

where

$$\delta = \begin{cases} \frac{8ql + 6}{2^n} + \left(\frac{4ql}{2^n}\right)^2, & \text{if } k = 4n, \\ \frac{4ql + 1}{2^n} + \left(\frac{2ql}{2^n}\right)^2, & \text{if } k = 2n. \end{cases}$$

Compare the security bounds of the CTR and CTR-CPKM_l modes in the LOR-CPA model. We assume that for the used cipher E the assumptions (1) hold. If these assumptions hold it may be shown that the obtained bounds for the CTR and CTR-CPKM_l modes are achievable. We also assume that $2^k \gg 2^n$, that holds for the Magma and Kuznyechik ciphers. For convenience we use the value ml instead of m in case of the CTR mode. So the amount of processed blocks is no more than qml . If $qml < 2^{n/2}$ and $t \ll 2^k$, then for the Magma cipher the following approximations hold:

$$\mathbf{Adv}_{\text{CTR}}^{\text{LOR-CPA}}(t, q, ml) \approx \frac{2m^2 q^2 l^2}{2^n} + \frac{t + q + nmql}{2^k} \approx m^2 \cdot \frac{2q^2 l^2}{2^n},$$

$$\mathbf{Adv}_{\text{CTR-CPKM}_l}^{\text{LOR-CPA}}(t, q, ml) \approx 2m \left(2 \cdot \frac{t + qml}{2^k} + \frac{q^2 l^2}{2^n} + \frac{t + qml}{2^k} + \delta \right) \approx m \cdot \frac{2q^2 l^2}{2^n}.$$

These relations indicate that the security estimate of the CTR-CPKM_l mode is improved in comparison with the security estimate of the basic CTR mode. The arguments and the final conclusions for the Kuznyechik cipher and the CPKM₁₂₈ re-keying method are similar to the Magma cipher.

7. Approaches to estimate the security for side channel information model

The use of each key should be limited in order to protect from methods using side channel information. We assume that during message processing such methods may give us some additional information about the used key that efficiently “narrows” a set of possible keys. The key lifetime limitation provides sufficiently large, i.e. secure, size of this set. Thus we can guarantee the required security for a single encrypted section. However keys of different sections are related, therefore there is a question on possibility to use information about the keys of different sections in order to find one of them.

The following statements explain a negative answer on the formulated question for a pair of adjacent keys. The structure of information about key obtained with some hypothetical method may be different. Below we consider an “extreme” case, when we obtain w bits of the key (on some fixed places) as a result of the method.

Let K_1 and K_2 are the keys used for two adjacent sections that are related by the equation $K_2 = \text{CPKM}(K_1)$, and there are w known bits for every key. Note that the complexity of searching the key K_1 or the key K_2 by the trivial brute force attack is $Q_0 = 2^{k-w}$. There is a reason to use information about two keys at the same time if the complexity of searching the key is much less than Q_0 .

Further we assume that amount of data processed with one key is sufficient. We assume that a key is found if a list that contains this key is constructed.

Proposition 7.1 (informal). *If there exists an adversary A who finds the key K_1 with complexity $Q_1 \ll Q_0$, then there exists an adversary B who finds a random key K with complexity $Q_1 \cdot 2^w \ll 2^k$ in a chosen plaintext attack (knowing w bits of a string $K' = \text{CPKM}(K)$).*

Define a KoR problem in order to state Proposition 7.2.

Definition 7.1. A KoR (Key Or Random) problem for a cipher E is the following decisional problem. An adversary A has access to an oracle $\mathcal{O}$ that operates in the following way. Before starting the work the oracle $\mathcal{O}$ chooses bit $b \in_{\mathcal{U}} \{0, 1\}$. If $b = 0$, then $\mathcal{O}$ chooses $R_1 \in_{\mathcal{U}} V_w$ and $R_2 \in_{\mathcal{U}} V_k$ and returns to the adversary a pair (R_1, R_2) . If $b = 1$, then it chooses a key $K \in_{\mathcal{U}} V_k$ and returns w fixed bits of the key on fixed places and a value $K' = \text{CPKM}(K)$.

Proposition 7.2 (informal). *If there exists an adversary A who finds the key K_2 with complexity $Q_1 \ll Q_0$, then there exists an adversary B who solves the KoR problem with complexity Q_1 and advantage*

$$1 - \frac{Q_1}{2^{n-w}}.$$

Thus the capability to use information about adjacent keys in the CPKM method results in the weakness of the used cipher, that makes it possible to find a key using bits of ciphertexts efficiently or to distinguish successfully a concatenation of ciphertext and some bits of the key from a random string. Therefore the method allows to consider adversaries who process each section separately of each other.

8. Open questions

Despite of the fact that the CPKM re-keying method improves the security of the CTR encryption mode, this re-keying method has the following properties:

- a key with equal n -bit blocks cannot be a result of the CPKM method;
- if there is a block of gamma that coincides with one of the constants used in the CPKM method then an adversary obtains a part of the key of the next section.

Consider the following method that doesn't have the second property (that may be regarded as disadvantage):

$$K' = \text{KM}_l(K) = E_K(\varphi(D_1)) || E_K(\varphi(D_2)) || E_K(\varphi(D_3)) || E_K(\varphi(D_4)),$$

where $\varphi : V_{64} \rightarrow V_{64}$, $\varphi(X_1 || X || X_2) = X_1 || 1 || X_2$ for $X_1 \in V_{32}$, $X_2 \in V_{31}$, $X \in V_1$ and $D_1, D_2, D_3, D_4 \in V_{64}$ are arbitrary constants such that values $\varphi(D_1), \varphi(D_2), \varphi(D_3), \varphi(D_4)$ are pairwise different. The message size should be less than $2^{n/2-1}$.

The given limitation on a value l , the use of the encryption instead of the decryption and the additional function φ guarantee that blocks encrypted using this method cannot coincide with blocks IV_i . This follows from the fact that for any IV_i the most significant bit of the second semiblock is 0 and the function φ set this value to 1.

A security bound of the CTR-KM mode is obtained in the same way as for the CTR-CPKM mode but there are several differences that support the KM method. The first difference is that in the final bound the value $\text{Adv}_E^{\text{PRP-CCA}}(\cdot, \cdot, \cdot)$ is replaced by $\text{Adv}_E^{\text{PRP-CPA}}(\cdot, \cdot)$. It is known (see, e.g. [3]) that $\text{Adv}_E^{\text{PRP-CPA}}(\cdot, \cdot) \leq \text{Adv}_E^{\text{PRP-CCA}}(\cdot, \cdot, \cdot)$, but the capabilities of adversaries in the PRP-CCA model is significantly greater then the capabilities in the PRP-CPA problem. If new methods that decrease a cipher security appear it is more likely that $\text{Adv}_E^{\text{PRP-CPA}}(\cdot, \cdot)$ will be strictly less than $\text{Adv}_E^{\text{PRP-CCA}}(\cdot, \cdot, \cdot)$. The second difference is that the value δ in Theorem 6.1 will decrease as the KM method doesn't allow to consider adversaries that use the second property described above in order to solve the $\text{IND-KM}_{l,m}$ problem.

Also the KM method has some operational advantages over CPKM. For some ciphers, particularly for Kuznyechik, encryption and decryption codes are very different. Therefore it is relevant to use encryption procedure instead of decryption one in the re-keying method in order not to increase the code size.

Note that the KM method has the first combinatorial property described above. This property was analyzed in detail in [5]. It could be regarded as disadvantage but as Theorem 6.1 shows this property doesn't influence on the security in the model with computationally limited adversary.

9. Influence of the Kuznyechik properties on efficiency of the CTR mode with re-keying method

The use of the re-keying method with any encryption mode decreases data processing speed. We analyze the correlation between encryption efficiency and value l , re-keying method and procedures related to this method. The IV transformation was not made. The measurement was made during the encryption of one long message in the CTR mode. The computer with the following characteristics was used: Intel Core i5-6500 CPU 3.20GHz, L1 D-Cache 32 KB x 4, L1 I-Cache 32 KB x 4, L2 Cache 256 KB x 4.

Speed of the encryption process in the CTR mode in the case where the re-keying method was not used is equal to 335 MB/s. In the tables below the speed is expressed in megabytes per second.

Table 1. A key is not changed, a repeated key extension is not made — slowing is explained by a repeated function call

l	1 KB	2 KB	4 KB	8 KB	16 KB	32 KB	64 KB
	320.8	322.5	324.2	325.4	326.5	329.4	330.0

Table 2. The key is not changed, but there is the repeated key extension

l	1 KB	2 KB	4 KB	8 KB	16 KB	32 KB	64 KB
	142.2	197.9	247.3	281.3	302.7	308.9	316.6

The Table 2 shows a contribution of the key extension to the complexity of the key transformation.

Table 3. The CPKM₁₂₈ re-keying method

l	1 KB	2 KB	4 KB	8 KB	16 KB	32 KB	64 KB
	132.7	186.1	233.4	266.9	287.6	300.0	306.0

Table 4. The KM re-keying method

l	1 KB	2 KB	4 KB	8 KB	16 KB	32 KB	64 KB
	134.2	192.9	242.6	277.3	300.0	308.6	315.6

10. Conclusion

Results obtained in this paper show that the use of the modified CPKM method (without changing of initialize vector) for the CTR mode improves the security properties of the initial encryption mode in the standard security model.

We propose approaches that allow to analyze the influence of the CPKM method on the security properties in the extended security model with additional side channel information. We show that the use of the CPKM method doesn't allow adversaries to use information about a key of one section in order to find a key of another section. Therefore the method allows to consider adversaries who process each section separately of each other. Also we propose a modified method and justify its advantages over the CPKM method. We obtain certain results about the operational features of the Kuznyechik cipher in the CTR encryption mode with several re-keying methods.

The authors are very grateful to Ekaterina Smyshlyaeva for her valuable comments and suggestions concerning the text of the article.

The full version of the current paper is available at [9].

References

- [1] *GOST R 34.12-2015. Information technology. Cryptographic protection of information. Block ciphers*, Moscow: Standartinform, 2015 (in Russian).
- [2] *GOST R 34.13-2015. Information technology. Cryptographic data security. Modes of operation for block ciphers*, Moscow: Standartinform, 2015 (in Russian).
- [3] Bellare M., Desai A., Joripii E., Rogaway P., "A concrete security treatment of symmetric encryption". In: "Proc. 38th Ann. Symp. Found. Comput. Sci. (FOCS '97)": IEEE, 1997, 394–403.
- [4] Popov V., Kurepkin I., Leontiev S., "Additional cryptographic algorithms for use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 algorithms". In: "IETF RFC 4357", 2006.
- [5] Mironkin V., "On some probabilistic characteristics of the "CryptoPro Key Meshing" method", *Problemy Inform. Bezopasnosti. Komp'uternye systemy*, № 4 (2015) (In Russian).
- [6] Matsui M., "Linear cryptanalysis method for DES cipher". In: "EUROCRYPT'93", Lect. Notes Comput. Sci., **765**, 1994, 386–397.
- [7] Biham E., Shamir A., "Differential cryptanalysis of DES-like cryptosystems". In: "CRYPTO'90", Lect. Notes Comput. Sci., **537**, 1990, 2–21.

- [8] *GOST 28147-89. Cryptographic Protection for Data Processing System, Gosudarstvennyi Standard of USSR*: Government Committee of the USSR for Standards, 1989 (In Russian).
- [9] Ahmetzyanova L. R., Alekseev E. K., Oshkin I. B., Smyshlyayev S. V., Sonina L. A., *On the properties of the CTR encryption mode of the Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing*, Cryptology ePrint Archive, Report 2016/628, <http://eprint.iacr.org/2016/628>.