Math-Net.Ru

Общероссийский математический портал

D. A. Burov, V. A. Pogorelov, Влияние приводимости линейного преобразования на выбор раундовых констант, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 2, 51–64

DOI: <https://doi.org/10.4213/mvk223>

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: 54.92.164.108

26 апреля 2023 г., 14:14:46

The influence of linear mapping reducibility on the choice of round constants

D. A. Burov¹, B. A. Pogorelov²

¹ TVP Laboratories, Moscow

² Academy of Cryptography of the Russian Federation, Moscow

Получено 19.III.2016

Abstract. The influence of reducibility of linear mappings on the security of block ciphers is studied. It is shown that the replacement of only two key schedule constants of Khazad block cipher leads to the appearance of weak key classes. We study invariant subspaces of the Kuznyechik linear mapping and demonstrate that there are no weak key schedule constants similar to Khazad. But the choice of other linear mappings constructed similarly to the original Kuznyechik mapping and choice of other constants may results in the appearance of weak keys.

Keywords: block cipher, Kuznyechik, Khazad, invariant subspace, reducible linear mapping, key schedule constants

Влияние приводимости линейного преобразования на выбор раундовых констант

Д. А. Буров¹, Б. А. Погорелов²

¹ Лаборатории ТВП, Москва

² Академия криптографии Российской Федерации, Москва

Аннотация. Исследуется влияние приводимости линейного преобразования на стойкость блочных шифрсистем. Показано, что при замене двух констант в алгоритме развертывания ключа шифра Khazad возникают классы слабых ключей. Изучаются также инвариантные подпространства линейного преобразования шифра Кузнечик; показано, что в отличие от шифра Khazad для него не существует слабых констант алгоритма развертывания ключа. Выбор другого линейного преобразования, аналогичного используемому в шифре Кузнечик, и других констант алгоритма развертывания ключа может привести к появлению слабых ключей.

Ключевые слова: блочный шифр, Кузнечик, Khazad, инвариантное подпространство, приводимое линейное преобразование, константы, алгоритм развертывания ключа

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 51–64 (Russian)

© Академия криптографии Российской Федерации, 2017 г.

1. Introduction

Development of differential and linear methods leads to the searching for new directions in the constructions of block ciphers, which are resistant to these methods. The main direction is using linear mappings with large branch number and s -boxes with good differential and linear properties. But a branch number describes diffusion property of linear mapping relatively to canonical basis only. Many linear mappings of block ciphers have reducible characteristic polynomial. Such mappings have nontrivial invariant subspaces, moreover, the group generated by linear mapping and the additive group of vector space is an imprimitive group. If a nonlinear mapping (s -boxes layer) does not diffuse systems of imprimitivity of this group, then block cipher may be vulnerable, for example, to homomorphism attack.

The question on the influence of the linear mapping reducibility on the security of block ciphers was raised in the paper [5]. Some papers published by B. A. Pogorelov and M. A. Pudovkina are devoted to this question [9–11]. In particular they study systems of imprimitivity and metrics which are invariant with respect to linear mapping and key addition transformations. Reducibility of linear mappings permits to construct attacks on some block ciphers: PRINT [7], [2], Robin, iSCREAM, Zorro [8], Midory [6]. But authors of these papers don't mention this fact. In [3] B. A. Pogorelov and D. A. Burov had used the reducibility of the Khazad linear mapping to find weak keys for six rounds of Khazad block cipher. Note that the linear mapping of Khazad is MDS, i. e. it has maximal branch number [4].

This paper is organized as follows. Section 2 is devoted to Khazad. We describe weak constants of the key schedule of Khazad. These weak constants satisfy conditions required by the authors of Khazad. Section 3 is devoted to the Russian standard Kuznyechik block cipher. We study invariants subspaces of the Kuznyechik linear mapping and show that the nonlinear mapping diffuses systems of imprimitivity efficiently.

2. Weak constants of Khazad

2.1. Description of Khazad

Khazad is an 8-round SP-network with 64-bit block length and 128-bit key length [1]. It was proposed by V. Rijmen and P. Barreto specially for the NESSIE project and was chosen as one of finalists.

We represent the field $GF(2^8)$ as $GF(2^8)[x]/p(x)$, where $p(x) = x^8 \oplus x^4 \oplus x^3 \oplus x^2 \oplus 1$ is a primitive polynomial over $GF(2)$. A polynomial $a(x) = a_0 \oplus a_1x \oplus \dots \oplus a_7x^7 \in GF(2)[x]$ is denoted by numerical value $\sum_{i=0}^7 a_i 2^i$, and written in decimal notation. Denote by $V_n(q)$ a vector space of dimension $n \in \mathbb{N}$ over the field $GF(q)$. Further 64-bit cipher state is represented as a vector in $V_8(2^8)$.

The nonlinear mapping $\tilde{s}: V_8(2^8) \rightarrow V_8(2^8)$ consists of the parallel application of a nonlinear involution substitution s-box $s \in S(GF(2^8))$:

$$\tilde{s}: (a_0, \dots, a_7) \mapsto (a_0^s, \dots, a_7^s),$$

where $a_i \in GF(2^8)$, $i = 0, \dots, 7$.

The linear mapping h is represented as multiplication by a matrix $\mathbf{h} = \|h_{i,j}\| \in GL_8(2^8)$:

$$\mathbf{h} = \begin{pmatrix} 1 & 3 & 4 & 5 & 6 & 8 & 11 & 7 \\ 3 & 1 & 5 & 4 & 8 & 6 & 7 & 11 \\ 4 & 5 & 1 & 3 & 11 & 7 & 6 & 8 \\ 5 & 4 & 3 & 1 & 7 & 11 & 8 & 6 \\ 6 & 8 & 11 & 7 & 1 & 3 & 4 & 5 \\ 8 & 6 & 7 & 11 & 3 & 1 & 5 & 4 \\ 11 & 7 & 6 & 8 & 4 & 5 & 1 & 3 \\ 7 & 11 & 8 & 6 & 5 & 4 & 3 & 1 \end{pmatrix}.$$

The key addition v_k is represented as addition of a round key $k \in V_8(2^8)$ to block $\alpha \in V_8(2^8)$:

$$v_k: \alpha \mapsto \alpha \oplus k.$$

Khazad round function f_k is represented as $f_k = v_k \tilde{s} h$. Here and in what follows mappings are composed left-to-right, i. e. $v_k \tilde{s} h: \alpha \mapsto h(\tilde{s}(v_k(\alpha)))$.

The key schedule expands the cipher key $k = (k_{-2}, k_{-1}) \in V_{16}(2^8)$ into a sequence of round keys $k_0, \dots, k_8$, where $k_i \in V_8(2^8)$, $i = 0, \dots, 8$. The round keys are computed by means of a Feistel iteration:

$$k_i = (k_{i-1})^{\tilde{s}h} \oplus c_i \oplus k_{i-2},$$

where $c_i = (c_{i,0}, \dots, c_{i,7})$ are defined as

$$c_{i,j} = (8i + j)^s, \quad i, j = 0, \dots, 7.$$

By $f_{k_0, \dots, k_r}$ we denote a product $f_{k_0} \dots f_{k_r}$ of round functions $f_{k_0}, \dots, f_{k_r}$, $r = 0, \dots, 8$. The full encryption function is defined as

$$g_k = f_{k_0, \dots, k_6} v_{k_7} \tilde{s} v_{k_8}.$$

2.2. Invariant subspaces of the Khazad linear mapping and weak constants of Khazad

The authors had described invariant subspaces of mappings $\tilde{s}$ and h in [3].

Proposition 1 ([3]). *The following subspaces are invariant with respect to mappings $\tilde{s}$ and h :*

- 1) $W^{(1)} = \{(a, a, b, b, e, e, d, d) | a, b, e, d \in GF(2^8)\},$
- 2) $W^{(2)} = \{(a, b, a, b, e, d, e, d) | a, b, e, d \in GF(2^8)\},$
- 3) $W^{(3)} = \{(a, b, b, a, e, d, d, e) | a, b, e, d \in GF(2^8)\},$
- 4) $W^{(4)} = \{(a, b, e, d, a, b, e, d) | a, b, e, d \in GF(2^8)\},$
- 5) $W^{(5)} = \{(a, b, e, d, b, a, d, e) | a, b, e, d \in GF(2^8)\},$
- 6) $W^{(6)} = \{(a, b, e, d, e, d, a, b) | a, b, e, d \in GF(2^8)\},$
- 7) $W^{(7)} = \{(a, b, e, d, d, e, b, a) | a, b, e, d \in GF(2^8)\},$
- 8) $U^{(1)} = \{(a, a, a, a, b, b, b, b) | a, b \in GF(2^8)\},$
- 9) $U^{(2)} = \{(a, a, b, b, a, a, b, b) | a, b \in GF(2^8)\},$
- 10) $U^{(3)} = \{(a, a, b, b, b, b, a, a) | a, b \in GF(2^8)\},$
- 11) $U^{(4)} = \{(a, b, a, b, a, b, a, b) | a, b \in GF(2^8)\},$
- 12) $U^{(5)} = \{(a, b, a, b, b, a, b, a) | a, b \in GF(2^8)\},$
- 13) $U^{(6)} = \{(a, b, b, a, a, b, b, a) | a, b \in GF(2^8)\},$
- 14) $U^{(7)} = \{(a, b, b, a, b, a, a, b) | a, b \in GF(2^8)\},$
- 15) $Z^{(1)} = \{(a, a, a, a, a, a, a, a) | a \in GF(2^8)\}.$

Further we assume $W \in \{W^{(i)} | i = 1, \dots, 7\}$. Suppose that round constants c_3, c_4 belong to W . Denote by g'_k the cipher function of Khazad with new constants c_3, c_4 . Note that these constants satisfy the requirements of the authors of Khazad: «Good round constants should not be equal for all bytes in a state, and also not equal for all bit positions in a byte. They should also be different in each round» [1]. Let $K(W)$ be the set of cipher keys such that round keys k_1, k_2, k_3, k_4 belong to W . At the same time round key k_5 belong to $W \oplus c_5$. Then we have

$$f_{k_0, \dots, k_5} : W \oplus c_2 \rightarrow (W \oplus c_5)^{\tilde{s}h}.$$

It is easy to show that $|K(W)| = |W|^2 = 2^{64}$.

Now we prove the property of the set $(W \oplus c_5)^{\widetilde{s}h}$ obtained in the paper [3] experimentally.

Теорема 2. Let $s_0, \dots, s_{m-1}$ be arbitrary permutations of vector space V_n , $3 \leq n \leq 2m$, $\zeta: V_{mn} \rightarrow V_n$,

$$\zeta: (\alpha_0, \dots, \alpha_{m-1}) \mapsto \sum_{i=0}^{m-1} \alpha_i \oplus \alpha_i^{s_i}.$$

Then for all $\alpha, \beta \in V_n$

$$|\alpha^{\zeta^{-1}}| \equiv |\beta^{\zeta^{-1}}| \pmod{2}.$$

Proof. Let the maps $\eta_i: V_n \rightarrow \mathbb{N}$ be given by

$$\eta_i: \alpha \mapsto |\{\gamma \in V_n \mid \gamma^{s_i} \oplus \gamma = \alpha\}|$$

for all $\alpha \in V_n$, $i = 0, \dots, m-1$. We obviously have for all $\alpha \in V_m$

$$|\alpha^{\zeta^{-1}}| = \sum_{\alpha_0, \dots, \alpha_{m-2} \in V_n} \alpha_0^{\eta_0} \cdot \alpha_1^{\eta_1} \cdots \alpha_{m-2}^{\eta_{m-2}} \cdot (\alpha_0 \oplus \alpha_1 \oplus \cdots \oplus \alpha_{m-2} \oplus \alpha)^{\eta_{m-1}}.$$

Let the maps $f_i: V_n \rightarrow GF(2)$ be given by $f_i: \alpha \mapsto \alpha^{\eta_i} \pmod{2}$ for all $\alpha \in V_n$, $i = 0, \dots, m-1$. Therefore,

$$|\alpha^{\zeta^{-1}}| \equiv \sum_{\alpha_0, \dots, \alpha_{m-2} \in V_n} f_0(\alpha_0) \cdots f_{m-2}(\alpha_{m-2}) \cdot f_{m-1}(\alpha_0 \oplus \cdots \oplus \alpha_{m-2} \oplus \alpha) \pmod{2}. \quad (1)$$

Let j denote an arbitrary element of the set $\{0, \dots, m-1\}$. Since $\sum_{\alpha \in V_n} \alpha^{\eta_j} = 2^n$, it follows that the function f_j has even weight. Let M_j be the multiset $[\alpha \oplus \alpha^{s_j} \mid \alpha \in V_n]$. Since $s_j \in S(V_n)$, it follows that $\sum_{\beta \in M_j} \beta = 0$. Therefore, we have

$$\sum_{\alpha \in N_{f_j}} \alpha = 0,$$

where $N_{f_j} = \{\alpha \in V_n \mid f_j(\alpha) = 1\}$. It is not hard to prove that

$$\begin{aligned} & \left\{ f: V_n \rightarrow GF(2) \mid \sum_{\alpha \in N_f} \alpha = 0, |N_f| \equiv 0 \pmod{2} \right\} = \\ & = \{f: V_n \rightarrow GF(2) \mid \deg f \leq n-2\}. \end{aligned} \quad (2)$$

Let $f_{\alpha,\beta}$ for any $\alpha, \beta \in V_n$ be map from $V_{n(m-1)}$ to $GF(2)$ such that

$$\begin{aligned} f_{\alpha,\beta}(\alpha_0, \dots, \alpha_{m-2}) &= f_0(\alpha_0) \dots f_{m-2}(\alpha_{m-2}) \cdot \\ &\cdot (f_{m-1}(\alpha_0 \oplus \dots \oplus \alpha_{m-2} \oplus \alpha) \oplus \\ &\oplus f_{m-1}(\alpha_0 \oplus \dots \oplus \alpha_{m-2} \oplus \beta)). \end{aligned}$$

To complete the proof it remains to note that $f_{\alpha,\beta}$ has even weight. Indeed, we have:

$$\begin{aligned} \deg f_{\alpha,\beta}(\alpha_0, \dots, \alpha_{m-2}) &\leq \\ &\leq \deg f_0(\alpha_0) + \dots + \deg f_{m-2}(\alpha_{m-2}) + \\ &+ \deg (f_{m-1}(\alpha_0 \oplus \dots \oplus \alpha_{m-2} \oplus \alpha) \oplus f_{m-1}(\alpha_0 \oplus \dots \oplus \alpha_{m-2} \oplus \beta)) \leq \\ &\leq (m-1) \cdot (n-2) + n - 3. \end{aligned}$$

Since $n \leq 2m$, it follows that $\deg f_{\alpha,\beta} < (m-1)n$ and $f_{\alpha,\beta}$ has even weight. This completes the proof. $\square$

Using theorem 2, we can prove the main property of the set $(W \oplus c_5)^{\bar{s}h}$. Let A be a subset of the vector space $V_8(2^8)$. Denote by $[A_i]$ the multiset of i -th coordinates of vectors from the set A , $i = 0, \dots, 7$. Let $\nu_a(A_i)$ be a frequency of an element $a \in GF(2^8)$ in multiset $[A_i]$.

Proposition 3. *Let W be an arbitrary subspace from the set $\{W^{(i)} \mid i = 1, \dots, 7\}$, T be equal to $(W \oplus \theta)^{\bar{s}h}$, θ be an arbitrary vector from $V_8(2^8)$. Then for all $a, b \in GF(2^8)$*

$$\nu_a(T_j) \equiv \nu_b(T_j) \pmod{2}, \quad j = 0, \dots, 7.$$

Proof. Without loss of generality it may be assumed that $W = W^{(1)}$. We have

$$\begin{aligned} [T_j] &= [(a \oplus t_0)^s h_{0,j} \oplus (a \oplus t_1)^s h_{1,j} \oplus \\ &\oplus (b \oplus t_2)^s h_{2,j} \oplus (b \oplus t_3)^s h_{3,j} \oplus \\ &\oplus (c \oplus t_4)^s h_{4,j} \oplus (c \oplus t_5)^s h_{5,j} \oplus \\ &\oplus (d \oplus t_6)^s h_{6,j} \oplus (d \oplus t_7)^s h_{7,j} \mid a, b, c, d \in GF(2^8)], \end{aligned} \quad (3)$$

where $\theta = (t_0, \dots, t_7)$. If we replace $(a \oplus t_0)^s h_{0,j}$ by y_0 , $(b \oplus t_2)^s h_{2,j}$ by y_1 , $(c \oplus t_4)^s h_{4,j}$ by y_2 , $(d \oplus t_6)^s h_{6,j}$ by y_3 in (3), we obtain

$$[T_j] = \left[\sum_{i=0}^3 y_i^{s_i} \oplus y_i \mid y_i \in GF(2^8), i = 0, \dots, 3 \right],$$

where $s_0, \dots, s_3 \in S(GF(2^8))$ are defined as follows:

$$\begin{aligned} s_0 : x &\mapsto ((xh_{0,j}^{-1})^{s^{-1}} \oplus t_0 \oplus t_1)^s h_{1,j}, & \forall x \in GF(2^8), \\ s_1 : x &\mapsto ((xh_{2,j}^{-1})^{s^{-1}} \oplus t_2 \oplus t_3)^s h_{3,j}, & \forall x \in GF(2^8), \\ s_2 : x &\mapsto ((xh_{4,j}^{-1})^{s^{-1}} \oplus t_4 \oplus t_5)^s h_{5,j}, & \forall x \in GF(2^8), \\ s_3 : x &\mapsto ((xh_{6,j}^{-1})^{s^{-1}} \oplus t_6 \oplus t_7)^s h_{7,j}, & \forall x \in GF(2^8). \end{aligned}$$

To conclude the proof, it remains to use Theorem 2. $\square$

Corollary 4. Let k_6, k_7 be arbitrary vectors from $V_8(2^8)$,

$$(W \oplus c_5)^{\tilde{s}h v_{k_6} \tilde{s}h v_{k_7}} = \{\gamma_i = (x_{i,0}, \dots, x_{i,7}) \mid i = 0, \dots, 2^{32}-1\}.$$

Then

$$\sum_{i=0}^{2^{32}-1} x_{i,j} = 0 \quad \text{for all } j = 0, \dots, 7. \quad (4)$$

Proof. Suppose that $(W \oplus c_5)^{\tilde{s}h}$ is equal to the set

$$\{\alpha_i = (a_{i,0}, \dots, a_{i,7}) \mid i = 0, \dots, 2^{32}-1\}.$$

The sum (4) may be represented as follows

$$\begin{aligned} \sum_{i=0}^{2^{32}-1} x_{i,j} &= \sum_{i=0}^{2^{32}-1} \left(\sum_{t=0}^7 (a_{i,t} \oplus k_{6,t})^s h_{t,j} \right) \oplus k_{7,i} \\ &= \sum_{t=0}^7 h_{t,j} \sum_{i=0}^{2^{32}-1} (a_{i,t} \oplus k_{6,t})^s. \end{aligned}$$

Using proposition 3, it is easy to prove that

$$\sum_{i=0}^{2^{32}-1} (a_{i,t} \oplus k_{6,t})^s = 0 \quad \text{for all } t = 0, \dots, 7. \quad \square$$

Using corollary 4, we show that cipher keys from $K(W)$ are weak for Khazad with two new constants c_3, c_4 . An attack on Khazad consists of three stages. The purpose of the first stage is recovering the round key k_8 .

Algorithm 1.

Input: THE SET $A = \{\alpha^{g'_k} \mid \alpha \in W \oplus c_2\} = \{(a_{j,0}, \dots, a_{j,7}) \mid j = 0, \dots, 2^{32}-1\}$,
WHERE $k \in K(W)$.

Output: THE SETS $B_i \subseteq V_8(2^8)$ CONTAINING POSSIBLE VARIANTS OF KEY BYTE $k_{8,i}$, $i = 0, \dots, 7$.

Step 1. FOR ALL $i = 0, \dots, 7$ DO THE NEXT STEP.

Step 2. FOR ALL $k_{8,i} \in GF(2^8)$ CHECK THE EQUALITY

$$\sum_{j=0}^{2^{32}-1} (a_{j,i} \oplus k_{8,i})^{s^{-1}} = 0. \quad (5)$$

IF EQUALITY (5) IS NOT TRUE, THEN $k_{8,i}$ IS WRONG. ELSE $k_{8,i}$ IS INCLUDED INTO B_i .

The set $B = B_0 \times \dots \times B_7$ is the set of possible variants of the round key k_8 . Let us suppose that the probability of satisfying the equality (5) for the wrong key byte $k_{8,i}$ is equal to 2^{-8} . Then the mean cardinality of the set B is equal to

$$\left(1 + \frac{255}{256}\right)^8,$$

i. e. after the first stage we have no more than 2^8 possible variants for the round key k_8 on the average. The time complexity of the first stage is equal to 2^{40} s-box lookups and $\oplus$ -operations, the data complexity is equal to 2^{32} chosen plaintexts.

On the second stage we find key k_7 . In order to do it, we use the idea of the attack on five rounds from the paper [3]. We have

$$f_{k_0, \dots, k_5} : W \oplus c_2 \rightarrow (W \oplus c_5)^{\tilde{s}h}.$$

It is clear that the vector

$$(\mu_a(W \oplus c_5)_i^{\tilde{s}h} \mid a \in GF(2^8)) \in \mathbb{Z}^{256}$$

differs from the vector

$$(\mu_a(W \oplus c_5)_i^{\tilde{s}h v_{k_6} \tilde{s}v_{k_7}} \mid a \in GF(2^8))$$

by some permutation. Using this fact, we can recover round keys k_6 and k_7 .

Algorithm 2.

Input: VECTORS $(\mu_a(W \oplus c_5)_i^{\tilde{s}h} \mid a \in GF(2^8))$, $i = 0, \dots, 7$, $B = (W \oplus c_2)^{g'_k}$,
WHERE $k \in K(W)$.

Output: ROUND KEYS k_6 , k_7 .

Step 1. FIND VECTORS $(\mu_a(B_i) | a \in GF(2^8)), i = 0, \dots, 7$.

Step 2. FOR ALL $i = 0, \dots, 7$ DO THE NEXT STEPS.

Step 2.1. CHOOSE TWO ARBITRARY DISTINCT ELEMENTS $a, b \in GF(2^8)$.

Step 2.2. FIND TWO ELEMENTS $x, y \in GF(2^8)$ SUCH THAT

$$\mu_x(R_i) = \mu_a((W \oplus c_5)_i^{\tilde{s}h}), \quad \mu_y((W \oplus c_5)_i^{\tilde{s}h}) = \mu_b(B_i).$$

Step 2.3. FIND $k_{4,i}, k_{5,i}$ AS SOLUTION OF THE SYSTEM OF EQUATIONS

$$\begin{cases} (x \oplus k_{4,i})^s \oplus k_{5,i} = a, \\ (y \oplus k_{4,i})^s \oplus k_{5,i} = b. \end{cases} \quad (6)$$

Using computation, we find that for all pairs $a, b \in GF(2^8), a \neq b, \mu_a(B_i)$ is not equal to $\mu_b(B_i), i = 0, \dots, 7$. Hence, there is only one pair x, y such that

$$\mu_a(B_i) = \mu_x((W \oplus c_5)_i^{\tilde{s}h}), \quad \mu_b(B_i) = \mu_y((W \oplus c_5)_i^{\tilde{s}h}).$$

It is clear that the complexity of finding solutions of system (6) is not larger than $6 \cdot 2^8$ s-box lookups and $\oplus$ -operations. Therefore, the complexity of the second stage is equal roughly to the complexity of obtaining vectors $(\mu_a(R_i) | a \in GF(2^8)), i = 0, \dots, 7$. It is equal to $8 \cdot 2^{32}$ s-box lookups approximately. After the second stage we have no more than 2^8 possible variants for the round keys k_6, k_7, k_8 on the average.

On the third stage, using one block of plaintext, we discard wrong variants of the cipher key.

We assume that the complexity of round encryption is larger than eight s-box lookups. The time complexity of this attack is 2^{40} round encryptions, the data complexity is 2^{32} chosen plaintext, the cardinality of the weak key set is 2^{64} .

3. Kuznyechik round function properties

In this section we study invariant subspaces of the Kuznyechik linear mapping and the diffusion properties of the nonlinear mapping $\tilde{s}$.

3.1. Description of Kuznyechik

Kuznyechik is a 9-round SP-network with 128-bit block length and 256-bit key length [12].

We represent the field $GF(2^8)$ as $GF(2^8)[x]/p(x)$, where $p(x) = x^8 \oplus x^7 \oplus x^6 \oplus x \oplus 1$ is an irreducible polynomial over $GF(2)$. A polynomial $a(x) = a_0 \oplus a_1 x \oplus \dots \oplus a_7 x^7 \in GF(2)[x]$ is denoted by numerical value $\sum_{i=0}^7 a_i 2^i$, and written in decimal notation. Further 128-bit cipher state is represented as a vector in $V_{16}(2^8)$.

The nonlinear mapping $\tilde{s}$ is presented as the application of the s-box $s \in GF(2^8)$ 16 times in parallel:

$$\tilde{s} : (a_0, \dots, a_{15}) \mapsto (a_0^s, \dots, a_{15}^s),$$

where $a_i \in GF(2^8)$, $i = 0, \dots, 15$.

The linear mapping h is presented as multiplication by (16×16) -matrix $\mathbf{h} = \mathbf{u}_t^{16} \in GL_{16}(2^8)$, where

$$\begin{aligned} t(x) = & x^{16} \oplus 148x^{15} \oplus 32x^{14} \oplus 133x^{13} \oplus 16x^{12} \oplus 194x^{11} \oplus 192x^{10} \oplus \\ & \oplus x^9 \oplus 251x^8 \oplus x^7 \oplus 192x^6 \oplus 194x^5 \oplus \\ & \oplus 16x^4 \oplus 133x^3 \oplus 32x^2 \oplus 148x \oplus 1, \end{aligned}$$

$\mathbf{u}_t$ is the companion matrix of the polynomial $t(x) \in GF(2^8)[x]$.

The Kuznyechik round function is presented as $f_k = v_k \tilde{s} h$, the encryption function is defined as $g_k = f_{k_1, \dots, k_9} v_{k_{10}}$.

The key schedule expands the cipher key $k = (k_1, k_2) \in V_{32}(2^8)$ into a sequence of round keys $k_1, \dots, k_{10} \in V_{16}(2^8)$. Round keys k_{2i+1}, k_{2i+2} are computed from round keys k_{2i-1}, k_{2i} by means of an 8 Feistel iterations with round function $e_\gamma : (\alpha, \beta) \mapsto (\beta, \alpha \oplus (\beta \oplus \gamma)^{\tilde{s}h})$, i. e.

$$(k_{2i+1}, k_{2i+2}) = (k_{2i-1}, k_{2i})^{e_{c_{8i+1}} \dots e_{c_{8i+8}}}, \quad i = 0, \dots, 4,$$

where $c_j \in V_{16}(2^8)$ are round constants of Kuznyechik, $j = 1, \dots, 32$.

3.2. Invariant subspaces of the Kuznyechik linear mapping

Using computations, we find that

$$\begin{aligned} t(x) = & (x \oplus 6)(x \oplus 12)(x \oplus 24)(x \oplus 48)(x \oplus 70)(x \oplus 75)(x \oplus 95) \cdot \\ & \cdot (x \oplus 103)(x \oplus 117)(x \oplus 140)(x \oplus 150)(x \oplus 196) \cdot \\ & \cdot (x \oplus 206)(x \oplus 210)(x \oplus 219)(x \oplus 239). \end{aligned}$$

Let us describe invariant subspaces of linear mapping h in the general case.

Let $\mathbf{h} = \mathbf{u}_t^m$ be $(m \times m)$ -matrix over $GF(2^d)$, $m, d \geq 2$,

$$t(x) = (x \oplus r_0)(x \oplus r_1) \dots (x \oplus r_{m-1}) \in GF(2^d)[x].$$

It is clear that the characteristic polynomial of $\mathbf{h}$ is equal to

$$\chi_h(x) = (x \oplus r_0^m)(x \oplus r_1^m) \dots (x \oplus r_{m-1}^m).$$

If $(i-j)m \nmid 2^d - 1$, $i, j = 0, \dots, m-1$, then

$$V_m(2^d) = W^{(0)} \dot{+} \dots \dot{+} W^{(m-1)}, \quad \alpha^h = \alpha \cdot r_i^m, \quad \forall \alpha \in W^{(i)}, \quad i = 0, \dots, m-1,$$

where $W^{(i)}$ are invariant subspaces of h , $\dim W^{(i)} = 1$.

In the next proposition we describe subspaces $W^{(i)}$, $i = 0, \dots, m-1$.

Proposition 5. Let $\mathbf{h} = \mathbf{u}_t^m$ be $(m \times m)$ -matrix over $GF(2^d)$,

$$t(x) = (x \oplus r_0)(x \oplus r_1) \cdots (x \oplus r_{m-1}) \in GF(2^d)[x],$$

$\dim W^{(i)} = 1$, $W^{(i)}$ are h -invariant subspaces, $(i-j)m \nmid 2^d - 1$, $i, j = 0, \dots, m-1$, $W^{(i)} < V_m(2^d)$. Then

$$W^{(i)} = \{(a, a r_i^{-1}, \dots, a r_i^{-(m-1)}) \mid a \in GF(2^d)\}, \quad i = 0, \dots, m-1. \quad (7)$$

Proof. Suppose vector $\alpha = (a_0, a_1, \dots, a_{m-1})$ belongs to the subspace $W^{(i)}$. Then on the one hand for appropriate $b \in GF(2^d)$ we have

$$\alpha \mathbf{u}_t = (b, a_0, a_1, \dots, a_{m-2}) \in W^{(i)}. \quad (8)$$

On the other hand, since α is an eigenvector of the matrix $\mathbf{u}_t$ and r_i is an eigenvalue associated with α , we have

$$\alpha \mathbf{u}_t = (a_0 r_i, a_1 r_i, \dots, a_{m-1} r_i). \quad (9)$$

Using (8), (9), we get

$$\begin{cases} b = a_0 r_i^{-1}, \\ a_0 = a_1 r_i^{-1}, \\ \dots \dots \\ a_{m-2} = a_{m-1} r_i^{-1}. \end{cases} \quad (10)$$

To conclude the proof, it remains to note that equality (7) follows from (10). $\square$

Let $W_j^{(i)}$ be a coset of $W^{(i)}$ in $V_m(2^d)$, $W_0^{(i)} = W$, $\alpha_{i,j} \in W_j^{(i)}$, $i = 0, \dots, m-1$, $j = 0, \dots, 2^{(m-1)d} - 1$. Using proposition 5, we conclude that the group $\langle V_m(2^d)^+, h \rangle$ is imprimitive and partition

$$\mathbf{W}^{(i)} = \{W_0^{(i)}, W_1^{(i)}, \dots, W_{2^{(m-1)d}-1}^{(i)}\}$$

is an imprimitive system, $i = 0, \dots, 2^{(m-1)d} - 1$. Properties of diffusion of imprimitive system $W^{(i)}$ by nonlinear map $\tilde{s} = (s_1, \dots, s_m)$ are characterized by $(2^{(m-1)d} \times 2^{(m-1)d})$ -matrix $c_{W^{(i)}}(\tilde{s}) = \|c_{\alpha_{i,j}, \alpha_{i,l}}^{W^{(i)}}(\tilde{s})\|$, where

$$c_{\alpha_{i,j}, \alpha_{i,l}}^{W^{(i)}}(\tilde{s}) = |\tilde{s}(W_j^{(i)}) \cap W_l^{(i)}|.$$

In the next proposition we describe matrix $c_{W^{(i)}}(\tilde{s})$ in terms of $s_1, \dots, s_m$.

Proposition 6. *Let $m \geq 2$, $d \geq 2$, and let $\mathbf{h} = \mathbf{u}_t^m$ be an $(m \times m)$ -matrix over $GF(2^d)$, $(i-j)m \nmid 2^d - 1$, $i, j = 0, \dots, m-1$, $W^{(0)}, \dots, W^{(m-1)}$ be h -invariant subspaces of $V_m(2^d)$, $\dim W^{(i)} = 1$, $i = 0, \dots, m-1$,*

$$\tilde{s} = (s_0, \dots, s_{m-1}) \in S(V_m(2^d)), \quad s_i \in S(GF(2^d)), \quad i = 0, \dots, m-1,$$

$$\alpha = (0, \alpha_1, \dots, \alpha_{m-1}) \in V_m(2^d), \quad \beta = (0, b_1, \dots, b_{m-1}) \in V_m(2^d).$$

Then the element $c_{\alpha, \beta}^{W^{(i)}}(\tilde{s})$ is equal to the number of solutions of system of equations

$$\begin{cases} (xr_i^{-1} \oplus a_1)^{s_1} \oplus x^{s_0} r_i^{-1} = b_1, \\ (xr_i^{-2} \oplus a_2)^{s_2} \oplus x^{s_0} r_i^{-2} = b_2, \\ \dots\dots\dots \\ (xr_i^{-(m-1)} \oplus a_{m-1})^{s_{m-1}} \oplus x^{s_0} r_i^{-(m-1)} = b_{m-1}. \end{cases} \quad (11)$$

Proof. Let

$$V_m(2^d) = \bigcup_{(c_1, c_2, \dots, c_{m-1}) \in V_{m-1}(2^d)} (W^{(i)} \oplus (0, c_1, \dots, c_{m-1}))$$

be the partition of space $V_m(2^d)$ by cosets of $W^{(i)}$ in $V_m(2^d)$.

It follows easily that the element $c_{\alpha, \beta}^{W^{(i)}}(\tilde{s}) = |(W^{(i)} \oplus \alpha)^{\tilde{s}} \cap (W^{(i)} \oplus \beta)|$ equals the number of solutions $\gamma, \delta \in W^{(i)}$ of equation

$$(\gamma \oplus \alpha)^{\tilde{s}} \oplus \beta = \delta. \quad (12)$$

By proposition 5, the equation (12) is equivalent to the following system of equations

$$\begin{cases} c_0^{s_0} = d_0, \\ (c_0 r_i^{-1} \oplus a_1)^{s_1} \oplus b_1 = d_0 r_i^{-1}, \\ \dots\dots\dots \\ (c_0 r_i^{-(m-1)} \oplus a_{m-1})^{s_{m-1}} \oplus b_{m-1} = d_0 r_i^{-(m-1)}. \end{cases}$$

This system of equations is equivalent to the system (11). This ends the proof. $\square$

Let us find an upper bound of the maximal element of matrix $c_{W^{(i)}}(\tilde{s})$. Let $n_{a, b, r_i}^{(j)}$ be a number of solutions $x \in GF(2^d)$ of the equation

$$(xr_i^{-j} \oplus a)^{s_j} \oplus b = x^{s_0} r_i^{-j}, \quad j = 1, \dots, m-1.$$

Then we have

$$c_{\alpha,\beta}^{W^{(i)}}(\tilde{s}) \leq \min_{j \in \{1, \dots, m-1\}} n_{a_j, b_j, r_i}^{(j)},$$

where $\alpha = (0, a_1, \dots, a_{m-1}), \beta = (0, b_1, \dots, b_{m-1}) \in V_m(2^d)$.

Suppose that vectors $\gamma = (0, c_1, \dots, c_{m-1}), \delta = (0, d_1, \dots, d_{m-1}) \in V_m(2^d)$ are such that

$$\max_{a, b \in GF(2^d)} n_{a, b, r_i}^{(j)} = n_{c_j, d_j, r_i}^{(j)}, \quad j = 1, \dots, m-1.$$

Then we have

$$\begin{aligned} \max_{\substack{\alpha = (0, a_1, \dots, a_{m-1}) \in V_m(2^d), \\ \beta = (0, b_1, \dots, b_{m-1}) \in V_m(2^d)}} c_{\alpha,\beta}^{W^{(i)}}(\tilde{s}) &\leq \max_{\alpha, \beta \in V_m(2^d)} \min_{j \in \{1, \dots, m-1\}} n_{a_j, b_j, r_i}^{(j)} = \\ &= \min_{j \in \{1, \dots, m-1\}} n_{c_j, d_j, r_i}^{(j)} = \min_{j \in \{1, \dots, m-1\}} \max_{a, b \in GF(2^d)} n_{a, b, r_i}^{(j)}. \end{aligned} \quad (13)$$

Using inequality (13), we can find upper bound for the maximal element of matrix $c_{W^{(i)}}(\tilde{s})$ for Kuznyechik nonlinear map $\tilde{s} \in S(V_{16}(2^8))$, $i = 0, \dots, 15$. Using computer computations, we have

$$c_{\max}^{W^{(i)}}(\tilde{s}) \leq 7, \quad i = 0, \dots, 15.$$

Therefore the nonlinear map $\tilde{s}$ diffuses imprimitivity systems $\mathbf{W}^{(i)}$ efficiently. Hence there are no weak constants of key schedule for Kuznyechik as opposed to Khazad.

Let us show that choice of other linear mapping and key schedule constants can make Kuznyechik be vulnerable similarly to Khazad. Suppose $t(x)$ is divisible by $(x \oplus 1) \in GF(2^8)[x]$. It is true, for example, for matrix

$$\mathbf{h}(r_i) = \mathbf{diag}(1, r_i, \dots, r_i^{15})^{-1} \cdot \mathbf{h} \cdot \mathbf{diag}(r_i, r_i^2, \dots, r_i^{16}),$$

where $r_i \in \{6, 12, 24, 48, 70, 75, 95, 103, 117, 140, 150, 196, 206, 210, 219, 239\}$. Indeed the subspace

$$W = \{(a, \dots, a) \mid a \in GF(2^8)\}$$

is invariant under $h(r_i)$ and $\tilde{s}$. Let $c_1, \dots, c_{32}$ belong to W . In this case for all cipher keys belonging to $W \times W$ the cipher function maps W to W . Therefore, there are $|W|^2 = 2^{16}$ weak keys. Note that $\mathbf{h}(r_i)$ is MDS matrix, i. e. its branch number is equal to 17. Moreover it is easy to show that $\mathbf{h}(r_i) = \mathbf{u}_i^{16}$, where

$$\begin{aligned} t'(x) &= (x \oplus r_i r_0) \cdots (x \oplus r_i r_{i-1}) \cdot \\ &\cdot (x \oplus 1) \cdot (x \oplus r_i r_{i+1}) \cdots (x \oplus r_i r_{15}). \end{aligned}$$

Hence, $\mathbf{h}$ is constructed similarly to $\mathbf{h}(r_i)$.

4. Conclusion

In this paper we show that reducibility of linear mapping may have an influence on the security of block cipher. In particular it is shown that substitution of two key schedule constants in Khazad cipher leads to the appearance of weak keys. Also we show that Kuznyechik doesn't have constants such that it is possible to change a linear mapping in Kuznyechik in such a way that it would have weak keys.

References

- [1] Barreto P., Rijmen V., "The Khazad Legacy-Level Block Cipher". In: "*First Open NESSIE Workshop. Submission to NESSIE*", 2000.
- [2] Bulygin S., Walter M., "Study of the invariant coset attack on PRINT cipher: more weak keys with practical key recovery", Cryptology ePrint Archive. Report 2012/085.
- [3] Burov D. A., Pogorelov B. A., "An attack on 6 rounds of Khazad", *Mathematical Aspects of Cryptography*, **2**:7 (2016), 35–46.
- [4] Daemen J., *Cipher and hash function design strategies based on linear and differential cryptanalysis*, Leuven, Belgium: K. U. Leuven, 1995, 252 pp.
- [5] D.STVL.9. *Ongoing Research Areas in Symmetric Cryptography*, 2008 IST-2002-507932. ECRYPT. European Network of Excellence in Cryptology.
- [6] Guo J., Jean J., Nikolic I., Qiao K., Sasaki Y., Meng Sim S., "Invariant subspace attack against full Midory64", Cryptology ePrint Archive. Report 2015/1189.
- [7] Leander G., Abdelraheem M., Alkhzaimi H., Zenner E., "A cryptanalysis of PRINT cipher: The invariant subspace attack". In: "*CRYPTO'11*", Lect. Notes Comput. Sci., **6841**, 2011, 206–221.
- [8] Leander G., Minaud B., Sonjom S., "A generic approach to invariant subspace attacks: cryptanalysis of Robin, iSCREAM and Zorro". In: "*EUROCRYPT'15*", Lect. Notes Comput. Sci., **9056**, 2015, 254–283.
- [9] Pogorelov B. A., Pudovkina M. A., "On the distance from permutations to imprimitive groups for a fixed system of imprimitivity", *Discrete Math. Appl.*, **24**:2 (2014), 95–108.
- [10] Pogorelov B. A., Pudovkina M. A., "Factor structures of transformations", *Mathematical Aspects of Cryptography*, **3**:3 (2012), 81–104 (in Russian).
- [11] Pogorelov B. A., Pudovkina M. A., "Combinatorial characterization of XL-layers", *Mathematical Aspects of Cryptography*, **4**:3 (2013), 99–129 (in Russian).
- [12] Shishkin V., Dygin D., Lavrikov I., Marshalko G., Rudskoy V., Trifonov D., "On a new Russian Encryption Standard", *Mathematical Aspects of Cryptography*, **6**:2 (2015), 29–34.