D. A. Burov, B. A. Pogorelov, An attack on 6 rounds of Khazad, *Mat. Vopr. Kriptogr.*, 2016, Volume 7, Issue 2, 35–46

DOI: https://doi.org/10.4213/mvk181

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2016 Т. 7 № 2 С. 35–46

УДК 519.719.2

An attack on 6 rounds of Khazad

D. A. Burov [1] **, B. A. Pogorelov** [2]

[1] *TVP Laboratories, Moscow*
[2] *Academy of Cryptography of the Russian Federation, Moscow*

Получено 02.III.2015

Abstract. We suggest new attacks on the 64-bit block cipher Khazad. These attacks use some structural properties of its round function. As a result we find 14 new classes of weak keys for 5 and 6 rounds of Khazad. Particularly we show that Khazad has 7 classes of weak keys for 5 and 6 rounds such that the cardinality of each class is 2^{64}. The time complexity of weak keys recovering is 2^{35} S-box lookups for 5 rounds and 2^{43} S-box lookups for 6 rounds. The corresponding data complexity is 2^{32} chosen plaintexts.

Keywords: block cipher, Khazad, invariant subspaces, reducible linear transformation

Атака на 6 раундов Khazad

Д. А. Буров [1] **, Б. А. Погорелов** [2]

[1] *Лаборатории ТВП, Москва*
[2] *Академия криптографии Российской Федерации, Москва*

Аннотация. Рассматриваются новые атаки на 64-битовую блочную шифрсистему Khazad, использующие структурные свойства его раундовой функции. Найдено 14 новых классов слабых ключей для 5 и 6 раундов Khazad. В частности, показано, что имеется 7 классов слабых ключей для 5 и 6 раундов Khazad, каждый из которых содержит 2^{64} ключей. Нахождение слабого ключа в случае 5 раундов использует 2^{35} обращений к S-боксу, а в случае 6 раундов 2^{43} обращений и 2^{32} подобранных открытых текстов.

Ключевые слова: блочная шифрсистема, Khazad, инвариантные пространства, разложимое линейное преобразование

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 2, pp. 35–46 (Russian)

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 its finalist.

We represent the field $GF\left(2^8\right)$ as $GF\left(2\right)\left[x\right] / \, p(x)$, where $p\left(x\right) = x^8 \oplus x^4 \oplus x^3 \oplus x^2 \oplus 1$ is a primitive polynomial over $GF(2)$. A polynomial $a\left(x\right) = a_0 \oplus a_1 x \oplus \ldots \oplus a_7 x^7 \in GF\left(2\right)\left[x\right]$, where $a_i \in GF\left(2\right)$ for all $i \in \left\{0, \ldots, 7\right\}$, is denoted by a numerical value $\sum_{i=0}^{7} a_i 2^i$, and written in decimal notation. Let $V_m(2^d)$ be an m-dimensional subspace over the finite field $GF(2^d)$, $m, d \in \mathbb{N}$. Denote by V_n any subspace $V_n(2)$, $n \in \mathbb{N}$. Further a 64-bit cipher state is represented as a vector in $V_8(2^8)$.

Round function f_k consists of three transformations: $\widetilde{s}$, h, v_k.

Function $\widetilde{s} : V_8\left(2^8\right) \to V_8\left(2^8\right)$ consists of a parallel of application of a nonlinear involution substitution box $s : GF\left(2^8\right) \to GF(2^8)$:

$$\widetilde{s} : \left(a_0, \ldots, a_7\right) \mapsto \left(a_0^s, \ldots, a_7^s\right),$$

where $a_i \in GF\left(2^8\right)$ for all $i \in \left\{0, \ldots, 7\right\}$.

The diffusion layer realizes a multiplication by the matrix $h = \|\|h_{i,j}\|\| \in GL_8(2^8)$:

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

The linear transformation h is an involution.

The key addition $v_k : V_8\left(2^8\right) \to V_8\left(2^8\right)$ is a bitwise addition of a key vector $k \in V_8\left(2^8\right)$:

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

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

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

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

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

A round function is given by the formula

$$f_k : \alpha \mapsto \alpha^{v_k \widetilde{s} h}.$$

The full encryption function for r iteration is defined as

$$g_{k_0,\ldots,k_r} = f_{k_0} \cdot \ldots \cdot f_{k_{r-2}} v_{k_{r-1}} \widetilde{s} v_{k_r}.$$

2. Previous results on Khazad

Several attacks were applied on Khazad in a single-key model. An integral attack on 4 rounds of Khazad was proposed in [1]. The attack requires 2^9 chosen plaintexts and has time complexity 2^{91}. In [2] Biryukov finds a class of 2^{64} weak keys for which 5 rounds of Khazad may be broken with 2^{43} S-box lookups using 2^{38} chosen plaintexts. An attack on 5 rounds of Khazad was proposed by Muller [5]. This attack requires 2^{64} known plaintexts and have the time complexity 2^{91}. In [10] an attack on 6 rounds of Khazad was presented. The data complexity is 2^{64} chosen plaintexts and the time complexity was not estimated.

In [3] an attack on 7 rounds of Khazad in the related-key model and an attack on 8 rounds in the chosen-key model were presented.

Note that single-key attacks are more powerful than related-key and chosen-key attacks.

3. Structural properties of Khazad round function

In this section we investigate some properties of Khazad round function. These properties are consequences of the linear transformation h reducibility. Note that the transformation h is an optimal diffusion transformation. Invariant subspaces under $\widetilde{s}$ and h are described in Proposition 1.

Let G be a group generated by the linear transformation h and the group $\{v_\alpha \,|\, \alpha \in V_{64}\}$. The choice of S-box should take into account the properties of the group G. Otherwise a round function may be approximated by imprimitive transformations [7], [8] or isometric transformations [6], [9]. Also a round function may preserve some subspaces [4]. This fact is used to attack Khazad.

Proposition 1. *The following subspaces are invariant under* $\widetilde{s}$ *and* h :

$$W^{(1)} = \left\{(a,a,b,b,e,e,d,d) \mid a,b,e,d \in GF\left(2^8\right)\right\},$$

$$W^{(2)} = \left\{(a,b,a,b,e,d,e,d) \mid a,b,e,d \in GF\left(2^8\right)\right\},$$

$$W^{(3)} = \left\{(a,b,b,a,e,d,d,e) \mid a,b,e,d \in GF\left(2^8\right)\right\},$$

$$W^{(4)} = \left\{(a,b,e,d,a,b,e,d) \mid a,b,e,d \in GF\left(2^8\right)\right\},$$

$$W^{(5)} = \left\{(a,b,e,d,b,a,d,e) \mid a,b,e,d \in GF\left(2^8\right)\right\},$$

$$W^{(6)} = \left\{(a,b,e,d,e,d,a,b) \mid a,b,e,d \in GF\left(2^8\right)\right\},$$

$$W^{(7)} = \left\{(a,b,e,d,d,e,b,a) \mid a,b,e,d \in GF\left(2^8\right)\right\},$$

$$U^{(1)} = \left\{(a,a,a,a,b,b,b,b) \mid a,b \in GF\left(2^8\right)\right\},$$

$$U^{(2)} = \left\{(a,a,b,b,a,a,b,b) \mid a,b \in GF\left(2^8\right)\right\},$$

$$U^{(3)} = \left\{(a,a,b,b,b,b,a,a) \mid a,b \in GF\left(2^8\right)\right\},$$

$$U^{(4)} = \left\{(a,b,a,b,a,b,a,b) \mid a,b \in GF\left(2^8\right)\right\},$$

$$U^{(5)} = \left\{(a,b,a,b,b,a,b,a) \mid a,b \in GF\left(2^8\right)\right\},$$

$$U^{(6)} = \left\{(a,b,b,a,a,b,b,a) \mid a,b \in GF\left(2^8\right)\right\},$$

$$U^{(7)} = \left\{(a,b,b,a,b,a,a,b) \mid a,b \in GF\left(2^8\right)\right\},$$

$$Z^{(1)} = \left\{(a,a,a,a,a,a,a,a) \mid a \in GF\left(2^8\right)\right\}.$$

Proof. The proof is straightforward. □

Further we assume $W \in \{W^{(i)}, U^{(i)}, Z^{(1)} | i \in \{1,\ldots,7\}\}$. The existence of $\widetilde{s}h$-invariant subspaces may be a potential weakness of a block cipher. Only transformation v_k doesn't possess this invariance. However $W^{v_k} = W$ if $k \in W$.

4. An attack on 5 rounds of Khazad

In this section we describe new classes of weak keys for 5 rounds.

From the key schedule it follows that there are exactly $|W|^2$ encryption keys such that round keys k_1, k_2 belong to the subspace W. We have $k_0 \in W \oplus c_2$, $k_3 \in W \oplus c_3$ because $k_2 = k_1{}^{\widetilde{s}hv_{c_2}} \oplus k_0 \in W$, $k_1, k_2 \in W$ and $W^{\widetilde{s}h} = W$. Hence,

$$\left(W \oplus c_2\right)^{f_{k_0} f_{k_1} f_{k_2} v_{k_3}} = W \oplus c_3.$$

For any set $X \subset V_8(2^8)$ and for each $i \in \{0, \dots, 7\}$ we define a multiset

$$X_i = \{a \in GF(2^8) \,|\, (x_0, \dots, x_{i-1}, a, x_{i+1}, \dots, x_7) \in X\}.$$

In this context a multiset is a set where a value is allowed to appear several times. For each multiset X_i, $i \in \{0, \dots, 7\}$, we define vectors $\mu\left(X_i\right) = \left(\mu_a\left(X_i\right) | a \in GF\left(2^8\right)\right)$ and $\nu\left(X_i\right) = \left(n_0(X_i), n_1(X_i), \dots, n_{2^8}(X_i)\right)$, where

$$\mu_a\left(X_i\right) = \left|\{x \in X_i \mid x = a\}\right|, \quad n_j(X_i) = \left|\left\{a \in GF\left(2^8\right) \mid \mu_a\left(X_i\right) = j\right\}\right|.$$

Suppose $A = (W \oplus c_3)^{\widetilde{s}h} = \{\alpha_i = (a_{i,0}, \dots, a_{i,7}) \mid i \in \{0, \dots, |W| - 1\}\}$.

It is evident that a vector $\mu\left(A_i\right)$ coincides up to permutation with a vector $\mu\left(\left(A^{v_{k_4}\widetilde{s}v_{k_5}}\right)_i\right)$ for all $i \in \{0, \dots, 7\}$, k_4, $k_5 \in V_8\left(2^8\right)$. Using computer calculations we find that $\mu_a\left(A_i\right) \neq \mu_b\left(A_i\right)$ for all $i \in \{0, \dots, 7\}$ and $a, b \in GF\left(2^8\right)$ such that $a \neq b$. Hence $\mu_x\left(A_i\right) = \mu_a\left(B_i\right)$ if and only if $\left(x \oplus k_{4,i}\right)^s \oplus k_{5,i} = a$.

Algorithm 1.

Input: vectors $\mu\left(A_i\right)$ for all $i \in \{0, \dots, 7\}$, set $B = \{\alpha^{g_{k_0, \dots, k_5}} \,|\, \alpha \in W \oplus c_2\}$.

Output: keys k_4, k_5.

Step 1. For all $i \in \{0, \dots, 7\}$ do steps 2–4.

Step 2. Choose arbitrary $a, b \in GF\left(2^8\right)$ such that $a \neq b$.

Step 3. Find $x, y \in GF(2^8)$ such that $\mu_a\left(B_i\right) = \mu_x(A_i)$, $\mu_b\left(B_i\right) = \mu_y(A_i)$.

Step 4. Find $k_{4,i}$, $k_{5,i} \in GF\left(2^8\right)$ satisfying the following system of equations

$$\begin{cases} \left(x \oplus k_{4,i}\right)^s \oplus k_{5,i} = a, \\ \left(y \oplus k_{4,i}\right)^s \oplus k_{5,i} = b. \end{cases} \tag{1}$$

If the system (1) has more than one solution, then we can choose $c \in GF\left(2^8\right)$, $c \notin \{a, b\}$, and z such that $\mu_c(B_i) = \mu_z(A_i)$. Further we can add a new equation to system (1) to discard wrong keys.

The time complexity of this method equals to the time complexity of computing vectors $\mu(A_i)$ for all $i \in \{0, \ldots, 7\}$. This time complexity is $8 \cdot |W|$ S-box lookups. The data complexity is $|W|$ chosen plaintexts. Hence,

1) if $W \in \left\{W^{(i)} \mid i \in \{1, \ldots, 7\}\right\}$, then the time complexity is 2^{35} S-box lookups, the data complexity is 2^{32} chosen plaintext and there are 2^{64} weak keys;

2) if $W \in \left\{U^{(i)} \mid i \in \{1, \ldots 7\}\right\}$, then the time complexity is 2^{19} S-box lookups, the data complexity is 2^{16} chosen plaintexts and there are 2^{32} weak keys;

3) if $W = Z^{(1)}$, then the time complexity is 2^{11} S-box lookups, the data complexity is 2^8 chosen plaintexts and there are 2^{16} weak keys.

If $W \in \left\{W^{(i)} \mid i \in \{1, \ldots, 7\}\right\}$, then the time complexity and the data complexity of this method are smaller than the time complexity and the data complexity of the method presented in [2]. Moreover, we have 7 classes of weak keys instead of 1 class of weak keys in [2].

5. Membership tests for weak keys

In this section we present membership tests for weak keys of section 4. Membership tests are attacks designed not to recover the unknown key, but to determine if the key is a member of a set of weak keys. Notice that there is no membership test for weak keys in [2].

In this section we suppose that $W \in \left\{W^{(1)}, U^{(1)}\right\}$ for simplicity. For other subspaces from Proposition 1 similar results are true up to indices.

Proposition 2. *Assume* $i \in \{0, 1, 2, 3\}$. *If* $W = W^{(1)}$, *then*

$$A_{2i} = A_{2i+1}. \tag{2}$$

If $W = U^{(1)}$, *then*

$$A_0 = A_1 = A_2 = A_3, \tag{3}$$

$$A_4 = A_5 = A_6 = A_7. \tag{4}$$

Proof. Let φ, φ' be transformations from $V_4(2^8)$ to $GF(2^8)$. By definition, put $\varphi : (a, b, e, d) \mapsto x$, $\varphi' : (a, b, e, d) \mapsto x'$, where

$$\begin{aligned} x = {} & (a \oplus c_{3,0})^s h_{0,2i} \oplus (a \oplus c_{3,1})^s h_{1,2i} \oplus (b \oplus c_{3,2})^s h_{2,2i} \oplus (b \oplus c_{3,3})^s h_{3,2i} \oplus \\ & \oplus (e \oplus c_{3,4})^s h_{4,2i} \oplus (e \oplus c_{3,5})^s h_{5,2i} \oplus (d \oplus c_{3,6})^s h_{6,2i} \oplus (d \oplus c_{3,7})^s h_{7,2i}, \\ x' = {} & (a \oplus c_{3,0})^s h_{0,2i+1} \oplus (a \oplus c_{3,1})^s h_{1,2i+1} \oplus (b \oplus c_{3,2})^s h_{2,2i+1} \oplus \\ & \oplus (b \oplus c_{3,3})^s h_{3,2i+1} \oplus (e \oplus c_{3,4})^s h_{4,2i+1} \oplus (e \oplus c_{3,5})^s h_{5,2i+1} \oplus \\ & \oplus (d \oplus c_{3,6})^s h_{6,2i+1} \oplus (d \oplus c_{3,7})^s h_{7,2i+1}. \end{aligned}$$

From the definitions of A_{2i} and A_{2i+1} it follows that

$$(V_4(2^8))^{\varphi} = A_{2i}, \quad (V_4(2^8))^{\varphi'} = A_{2i+1}.$$

Note that for all $j \in \{0, 1, 2, 3\}$ we have $h_{2j,2i} = h_{2j+1,2i+1}$. Hence for all vectors $(a, b, e, d) \in V_4(2^8)$ we have

$$(a, b, e, d)^{\varphi} = (a \oplus c_{3,0} \oplus c_{3,1}, b \oplus c_{3,2} \oplus c_{3,3}, e \oplus c_{3,4} \oplus c_{3,4}, d \oplus c_{3,6} \oplus c_{3,7})^{\varphi'}.$$

So, we prove equality (2). Equalities (3) and (4) may be proved similarly. □

From Proposition 2 the next corollary follows.

Corollary. *For all* $i \in \{0, 1, 2, 3\}$, k_4, $k_5 \in V_8(2^8)$ *we have*

$$\nu\Big(\big(A^{v_{k_4} \widetilde{s} v_{k_5}}\big)_{2i}\Big) = \nu\Big(\big(A^{v_{k_4} \widetilde{s} v_{k_5}}\big)_{2i+1}\Big).$$

Based on this corollary we present an algorithm for identification of weak keys.

Algorithm 2.

Input: set $B = \{\alpha^{g_{k_0,\ldots,k_5}} \mid \alpha \in W^{(1)} \oplus c_2\}$.

Output: inconclusive (key is weak with large probability) or no (key is not weak).

Step 1. For all $i \in \{0, 1, 2, 3\}$ check

$$\nu\left(B_{2i}\right) = \nu\left(B_{2i+1}\right). \tag{5}$$

Step 2. If (5) is not satisfied for some $i \in \{0, 1, 2, 3\}$, then output: “key is not weak”, otherwise output “inconclusive”.

The time complexity of algorithm 2 is 2^{35} S-box lookups. If algorithm 2 gives us an inconclusive answer, then the key is weak with large probability.

Vectors $\nu\,(A_i)$ may be computed for Khazad easily. Therefore algorithm 2 may be improved.

Algorithm 3.

Input: set $B = \{\alpha^{g_{k_0,\dots,k_5}}\,|\,\alpha \in W \oplus c_2\}$, vectors $\nu\,(A_i)$ for all $i \in \{0,\dots,7\}$.

Output: inconclusive (key is weak with large probability) or no (key is not weak).

Step 1. For all $i \in \{0,\dots,7\}$ compute vectors $\nu(B_i)$.

Step 2. If there is $i \in \{0,\dots,7\}$ such that $\nu\,(B_i) \neq \nu\,(A_i)$, then output: “key is not weak”, otherwise output “inconclusive”.

The time complexity of algorithm 3 is 2^{35} S-box lookups. If algorithm 3 gives us an inconclusive answer, then the key is weak with probability larger than in algorithm 2.

6. An attack on 6 rounds of Khazad

In this section we describe an attack on 6 rounds of Khazad. This attack is similar to the attack of section 4.

The attack uses the property of the set $A = (W \oplus c_3)^{\widetilde{s}h}$.

The next result was obtained by computer computation.

Proposition 3. *Assume that* $W \in \{W^{(i)}\,|\,i \in \{1,\dots,7\}\}$. *For all* $a,b\in GF(2^8)$, $j\in\{0,\dots,7\}$ *we have*

$$\mu_a(A_j) \equiv \mu_b(A_j) \mod 2\,. \tag{6}$$

Note that Proposition 3 is not true for $W \in \{U^{(i)},\ Z^{(1)}\,|\,i \in \{1,\dots,7\}\}$.

Suppose

$$C = A^{v_{k_4}\widetilde{s}hv_{k_5}} = \{\gamma_i = (x_{i,0}, x_{i,1}, \dots, x_{i,7})\,|\,i \in \{0,\dots,2^{32}-1\}\}.$$

Proposition 4. *For all* $j \in \{0,\dots,2^{32}-1\}$ *we have*

$$\sum_{i=0}^{2^{32}-1} x_{i,j} = 0, \tag{7}$$

Proof. It is clear that equality (7) doesn't depend on k_5.

Suppose

$$Y = A^{v_{k_4}\widetilde{s}} = \{(y_{i,0}, y_{i,1}, \dots, y_{i,7}) \mid i \in \{0, \dots, 2^{32}-1\}\}.$$

The sum (7) may be represented in the form

$$\sum_{j=0}^{2^{32}-1} x_{i,j} = \sum_{i=0}^{2^{32}-1}\sum_{t=0}^{7} y_{i,t}\, h_{t,j} = \sum_{t=0}^{7} h_{t,j} \sum_{i=0}^{2^{32}-1} y_{i,t}.$$

From Proposition 3 it follows that the sum $\sum_{i=0}^{2^{32}-1} y_{i,t}$ is equal to 0 for all $t \in \{0, \dots, 7\}$. □

Suppose

$$D = \{\alpha^{g_{k_0,\dots,k_6}} \mid \alpha \in W \oplus c_2\} = \{\delta_i = (d_{i,7}, \dots, d_{i,0}), i \in \{0, \dots, 2^{32}-1\}\}.$$

Using Proposition 4 we present the algorithm 4 for recovering the key k_6 for 6 rounds of Khazad.

Algorithm 4.

Input: the set D.

Output: the set of possible keys k_6 containing the true key.

Step 1. For all $i \in \{0, \dots, 7\}$ do the following steps.

Step 2. For all $k_{6,i} \in GF(2^8)$ check

$$\sum_{j=0}^{2^{32}-1} (d_{j,i} \oplus k_{6,i})^{s^{-1}} = 0. \tag{8}$$

Step 3. If (8) is not satisfied, then $k_{6,i}$ is wrong, otherwise $k_{6,i}$ is a possible variant for the true key byte.

Algorithm 4 doesn't discard 2^8 keys on average. The data complexity of algorithm 4 is 2^{32} chosen plaintexts and the time complexity is 2^{43} S-box lookups, the probability of discarding the true key is equal to 0.

7. Chosen ciphertext attacks

In this section we show that chosen ciphertext attacks may be applied similarly to the above-stated chosen plaintext attacks.

Suppose $W \in \{W^{(i)}, U^{(i)}, Z^{(1)} \,|\, i \in \{1,\dots,7\}\}$. In the same way we have $k_6 \in W \oplus c_6$, $k_3 \in W \oplus c_5$, if $k_4, k_5 \in W$, and $k_5 \in W \oplus c_5$, $k_2 \in W \oplus c_4$, if $k_3, k_4 \in W$. There are exactly $|W|^2$ encryption keys such that $k_4, k_5 \in W$. There are exactly $|W|^2$ encryption keys such that $k_3, k_4 \in W$. Using chosen ciphertext $W \oplus c_5$ instead of chosen plaintext $W \oplus c_2$ we can apply attacks similar to attacks in sections 4, 5. Using computer computations we find that Proposition 3 is also true for sets $(W \oplus c_5)^{\widetilde{s}}$ where $W \in \{W^{(i)} \,|\, i \in \{1,\dots,7\}\}$. Therefore using chosen ciphertext $W \oplus c_6$ instead of chosen plaintext $W \oplus c_2$ we can apply attacks similar to attacks in sections 6.

Hence for 5 rounds of Khazad we have:

> there are 7 classes of weak keys with cardinality 2^{64}, the time complexity is 2^{35} S-box lookups, the data complexity is 2^{32} chosen ciphertexts;
>
> there are 7 classes of weak keys with cardinality 2^{32}, the time complexity is 2^{19} S-box lookups, the data complexity is 2^{16} chosen ciphertexts;
>
> there is 1 class of weak keys with cardinality 2^{16}, the time complexity is 2^{11} S-box lookups, the data complexity is 2^{8} chosen ciphertexts.

For 6 rounds of Khazad there are 7 classes of weak keys, cardinality of each of them is 2^{64}. The time complexity is 2^{43} S-box lookups, the data complexity is 2^{32} chosen ciphertexts.

8. Comparison of weak keys

In this section we compare the described classes of weak keys for 5 rounds with a class of weak keys from [2]. We briefly describe the idea of the method used in [2]. The encryption function of 5 rounds of Khazad may be represented in the form

$$g_{k_0,\dots,k_5} = v_{k_0} \widetilde{s}\, v_{k_1'}\, h\, \widetilde{s}\, h\, v_{k_2} \widetilde{s}\, v_{k_3'}\, h \widetilde{s}\, h\, v_{k_4}\, \widetilde{s}\, v_{k_5},$$

where $k_1' = k_1^h$, $k_3' = k_3^h$. Suppose $k_2 = k_3'$. Since $\widetilde{s}$, h are involutions, the transformation $h\, \widetilde{s}\, h\, v_{k_2}\, \widetilde{s}\, v_{k_3'}\, h\, \widetilde{s}\, h$ is an involution. This property is useful to apply slide attack for 5 rounds of Khazad. So the method of [2] uses property $k_2 = k_3^h$. It is clear that k_2, k_3 belong to the same coset over subspace W.

On the other hand, for our weak keys we have $k_2 \in W$, $k_3 \in W \oplus c_3$, $c_3 \notin W$ (chosen plaintext) and $k_3 \in W$, $k_2 \in W \oplus c_4$, $c_3 \notin W$ (chosen ciphertext).

Therefore our sets of weak keys for 5 rounds don't intersect with the set from [2].

9. Conclusions

In this paper we have investigated structural properties of the round function of Khazad. As a result we found 14 new classes of weak keys for 5 and 6 rounds. The cardinality of each class is 2^{64}. For recovering weak keys from 7 of 14 classes we need 2^{32} chosen plaintexts. The time complexity is 2^{35} S-box lookups for 5 rounds and 2^{45} S-box lookups for 6 rounds. For recovering weak keys from other 7 classes we need 2^{32} chosen ciphertexts. The time complexity is the same. Moreover, we find subclasses of these classes of weak keys such that to recover weak keys from these subclasses smaller data and number of operations are required.

References

[1] Barreto P. S. L. M., Rijmen V., "The Khazad legacy-level block cipher". In: "*Proceedings of First Open NESSIE Workshop*", Leuven: KU Leuven, 2000, https://www.cosic.esat.kuleuven.be/nessie/workshop/ submissions.html.

[2] Biryukov A., "Analysis of involutional ciphers: Khazad and Anubis". In: "*Fast Software Encryption*", FSE 2003, Lect. Notes Comput. Sci., **2887**, 2003, 45–53.

[3] Birukov A., Nikolic I., "Automatic search for related-key differential characteristics in byte-oriented block ciphers: Application to AES, Camellia, Khazad and others". In: "*Advances in Cryptology–EUROCRYPT 2010*", Lect. Notes Comput. Sci., **6110**, 2010, 322–344.

[4] Leander G., Abdelraheem M. A., Alkhzaimi H., Zenner E., "A cryptanalysis of PRINT cipher: The invariant subspace attack". In: "*Advances in Cryptology–EUROCRYPT 2011*", Lect. Notes Comput. Sci., **6841**, 2011, 206–221.

[5] Muller F., "A new attack against Khazad". In: "*Advances in Cryptology–ASIACRYPT 2003*", Lect. Notes Comput. Sci., **2894**, 2003, 347–358.

[6] Pogorelov B. A., *Fundamentals of the Theory of Permutation Groups. Part* 1. *General Aspects*, Moscow, 1986 (in Russian), 316 pp.

[7] Pogorelov B. A., Pudovkina M. A., "On the distance from permutations to imprimitive groups for a fixed system of imprimitivity", *Diskretnaya Matematika*, **26**:1 (2014), 103–117 (in Russian); Engl. transl., *Discrete Math. Appl.*, **24**:2 (2014), 95–108.

[8] Pogorelov B. A., Pudovkina M. A., “Factor structures of transformations”, *Математические вопросы криптографии* (*Math. Aspects Cryptogr.*), **3**:3 (2012), 81–104. (In Russian)

[9] Pogorelov B. A., Pudovkina M. A., “Combinatorical characterization of XL-layers”, *Математические вопросы криптографии* (*Math. Aspects Cryptogr.*), **4**:3 (2013), 99–129. (In Russian.)

[10] Yonglong T., “New Cryptanalysis on 6-round Khazad”, *Adv. Inf. Sci. Serv. Sci.*, **5**:1 (2013), 94–103.