Table 2

Experimental evaluation of total mixing and nonlinearity characteristics

k	Round t of total mixing	Round t of nonlinearity
1	30	33
3	18	20
5	16	18

6. Conclusion

Advanced characteristics of RKG based on MAG are shown both with and without the use of LCG. In the first case, the structural properties of the permutation states of RKG are guaranteed by the LCG parameters. In the second case, they are justified experimentally. The computational complexity of the round key generation method is low, which can be explained by uncomplicated implementation of MAG and LCG.

The presented method of key schedule generation can be used in many iterated block ciphers, in particular, the method is recommended for wide-block algorithm KB-256.

REFERENCES

1. *Fomichev V. M.* Metody diskretnoi matematiki v kriptologii [Methods of Discrete Mathematics in Cryptology]. Moscow, Dialog-MEPHI, 2012. 424 p. (in Russian)
2. *Koreneva A. M. and Fomichev V. M.* The mixing properties of modified additive generators. J. Appl. Industr. Math., 2017, vol. 11, no. 2, pp. 215–226.
3. *Knuth D. E.* The Art of Computer Programming. Vol. 2. Seminumerical Algorithms. Third ed. Reading, Massachusetts, Addison-Wesley, 1997. xiv+762 p.
4. *Fomichev V. M. and Melnikov D. A.* Kriptograficheskie metody zashchity informatsii. Ch. 1. Matematicheskie aspekty [Cryptographic Methods of Information Protection. P. 1. Mathematical Aspects]. Moscow, Urait Publ., 2016. 209 p. (in Russian)
5. *Fomichev V. M. and Koreneva A. M.* Encryption performance and security of certain wide block ciphers. J. Comput. Virol. Hack. Tech., 2020, vol. 16, pp. 197–216.

УДК 519.17 DOI 10.17223/2226308X/15/19

THE DIFFERENCE RELATIONS AND IMPOSSIBLE DIFFERENTIALS CONSTRUCTION FOR THE KB-256 ALGORITHM

V. M. Fomichev, A. V. Kurochkin, A. B. Chukno

In this paper, new results of the analysis of the KB 256-3 block cipher algorithm are outlined. We set up a difference relation with probability 1 for the six-round algorithm under study and propose a key recovery method using this difference relation for the nine-round KB 256-3 algorithm. We construct an impossible differential for the full-round algorithm.

Keywords: *differential cryptanalysis, impossible differentials.*

1. Introduction

The existence of a difference relation for a block cipher algorithm may indicate the possibility of developing efficient key recovering methods. We show that difference relations discovered for a block cipher algorithm can be efficiently used for key recovery computation (as compared to exhaustive key search) for the nine-round KB 256-3 algorithm. The existence of an impossible differential for a block cipher algorithm enables cryptanalysts to recover information about encrypted blocks.

2. Description of the KB 256-3 encryption algorithm

The KB 256-3 encryption algorithm, based on the generalized Feistel network, was proposed in [1, 2]. Next, the algorithm description is provided.

We introduce notations as follows:

— $\boxplus$ — the addition modulo 2^{32};
— $\oplus$ — the XOR of two binary strings of the same length;
— V_n — a set of binary strings of length $n \in \mathbb{N}$, where $V = \{0, 1\}$;
— $K = (K_0, K_1, \ldots, K_7)$, where $K_j \in V_{32}$, $j = 0, \ldots, 7$, — an encryption key;
— $Q_i = (q_{0.i}, q_{1.i}, q_{2.i})$, where $q_{0.i}, q_{1.i}, q_{2.i} \in V_{32}$, $i = 1, \ldots, 16$, — round keys, derived from the encryption key.

Encryption of a 256-bit block $X = (X_0, X_1, X_2, \ldots, X_7)$, where $X_j^0 \in V_{32}$, $j = 0, \ldots, 7$, with an encryption key K can be performed by applying 16-round functions R, in sequence. Each of these functions depends on three 32-bit round keys (q_0^i, q_1^i, q_2^i), $i = 1, \ldots, 16$ (i.e., each round of encryption uses three round keys). We denote the round transformation of the KB 256-3 encryption algorithm by $R : V_{256} \times V_{96} \to V_{256}$.

As a result, after the round $i \in \{1, \ldots, 16\}$, the block $X \in V_{256}$ encrypted with the key K can be written as

$$R(\ldots R(R(X^0, Q_1), Q_2)), \ldots, Q_i) = X^i = (X_0^i, X_1^i, \ldots, X_7^i).$$

We introduce the additional notation:

$$F(X, K) = R(\ldots R(R(X, Q_1), Q_2)), \ldots, Q_{16}).$$

3. Round transformation

We define a round transformation. We use notations as follows:

1) $\Sigma(A_0, A_1, \ldots, A_7) = A_1 \boxplus A_3 \boxplus A_4 \boxplus A_6 \boxplus A_7$, where $A_i \in V_{32}$, $i = 0, \ldots, 7$;
2) $f(a_0, a_1, \ldots, a_7) = T(s_0(a_0), s_1(a_1), \ldots, s_7(a_7))$, where 4-bit permutations $s_0, s_1, \ldots, s_7$ are taken from [3], T is the left cyclic shift of a 32-bit string by 19 positions, $a_i \in V_4$, $i = 0, \ldots, 7$.

Hence, the round transformation can be written as

$$R\,(A, (b_0, b_1, b_2)) =$$
$$= (A_1, A_2 \oplus f(\Sigma(A) \boxplus b_0), A_3, A_4, A_5 \oplus f(\Sigma(A) \boxplus b_1), A_6, A_7, A_0 \oplus f(\Sigma(A) \boxplus b_2)).$$

4. Round key sequence

To construct a sequence q_j based on the key $K = (K_0, K_1, \ldots, K_7)$, $K_j \in V_{32}$, $j = 0, \ldots, 7$, we use the non-linear shift register with $\alpha \in V_{32}$ as a parameter. The initial state of the register is:

$$q_1 = K_0,\ q_2 = K_1,\ q_3 = K_2,\ q_4 = K_3,\ q_5 = K_4,\ q_6 = K_5,\ q_7 = K_6;$$
$$q_i = T_1\,[q_{i-1} \boxplus q_{i-3} \boxplus q_{i-5} \boxplus q_{i-7}] \boxplus K_7 \boxplus (i-7)\alpha,$$

where $i \in \{8, \ldots, 123\}$ and T_1 is a left cyclic shift of a string from V_{32}.

5. Difference relation

We define the difference relation for the algorithm under study. Let $X^0, \underline{X}^0$ be plaintexts:

$$X^0 = \left(X_0^0, X_1^0, X_2^0, X_3^0, X_4^0, X_5^0, X_6^0, X_7^0\right),$$
$$\underline{X}^0 = \left(X_0^0, X_1^0 \oplus 2^{31}, X_2^0, X_3^0, X_4^0, X_5^0, X_6^0 \oplus 2^{31}, X_7^0\right).$$

It is evident that $X^0 \oplus \underline{X}^0 = (0, 2^{31}, 0, 0, 0, 0, 2^{31}, 0)$. For plaintexts X^0 и $\underline{X}^0$ and any round keys $Q_1, Q_2, \ldots, Q_6 \in V_{96}$ the following equations hold:

$$R(\ldots R(X^0, Q_1), \ldots, Q_i) \oplus R(\ldots R(\underline{X}^0, Q_1), \ldots, Q_i) = C_i,$$

where $i = 1, \ldots, 6$ and constant $C_1, C_2, \ldots, C_6$ are

$$C_1 = (2^{31}, 0, 0, 0, 0, 2^{31}, 0, 0); \quad C_2 = (0, 0, 0, 0, 2^{31}, 0, 0, 2^{31}); \quad C_3 = (0, 0, 0, 2^{31}, 0, 0, 2^{31}, 0);$$
$$C_4 = (0, 0, 2^{31}, 0, 0, 2^{31}, 0, 0); \quad C_5 = (0, 2^{31}, 0, 0, 2^{31}, 0, 0, 0); \quad C_6 = (2^{31}, 0, 0, 2^{31}, 0, 0, 0, 0).$$

Thus, the difference relation with probability 1 for the six-round algorithm is provided.

6. Difference relation attack on 9 rounds

We consider the truncated KB-256 algorithm which comprises 9 encryption rounds. The algorithm structure besides the number of rounds is similar to that of the original algorithm.

Let X^0 and $\underline{X}^0$ be plaintexts such that $X^0 \oplus \underline{X}^0 = C_0$. The encrypted plaintexts $X^9, \underline{X}^9$ are known to the cryptanalyst.

It is also known that $X^6 \oplus \underline{X}^6 = (2^{31}, 0, 0, 2^{31}, 0, 0, 0, 0)$. Due to the algorithm functioning principles, the following equations hold:

$$X_4^6 = X_2^8; \quad X_7^6 = X_5^8.$$

The equations are easy to verify.

Next, we demonstrate how round keys q_1^9, q_2^9 can be recovered. For ease, we denote $a = q_1^9$, $b = q_2^9$. The cryptanalyst derives:

$$\begin{aligned} Y_1 &= X_1^9 \oplus f(X_0^9 \boxplus X_2^9 \boxplus X_3^9 \boxplus X_5^9 \boxplus X_6^9 \boxplus a); \\ Y_2 &= \underline{X}_1^9 \oplus f(\underline{X}_0^9 \boxplus \underline{X}_2^9 \boxplus \underline{X}_3^9 \boxplus \underline{X}_5^9 \boxplus \underline{X}_6^9 \boxplus a). \end{aligned} \tag{1}$$

The Y_1, Y_2 values potentially coincide X_2^8 and $\underline{X}_2^8$ respectively. It is known that $X_2^8 = \underline{X}_2^8$. So for the key a the following equation holds: $Y_1 = Y_2$.

The b key can be recovered in the same way. Generally, it is possible that for several a values equations 1 hold. In this section, we study the KB-256 algorithm properties without delving into the key recovery algorithm. Therefore, for ease, we assume that having a single a, the equations 1 hold. Obviously, recovering a round key allows recovering the key within approximately 2^{224} operations. By operation we assume encryption of a block using KB-256.

7. Finding an impossible differential for the KB-256-3 algorithm

In this section, we prove that an impossible differential exists for the KB-256 algorithm. We assume that an impossible differential for the encryption algorithm $E : V_n \times V_k \to V_n$ is the pair $D_1, D_2 \in V_n$ such that for any key $K \in V_k$ and for any $X, \underline{X} \in V_n$ such that $X \oplus \underline{X} = D_1$ the inequality holds:

$$E_K(X) \oplus E_K(\underline{X}) \neq D_2.$$

If an impossible differential exists, in some cases, it is possible to design an effective attack on block algorithms [4]. In general, this property enables a cryptanalyst to gain some information about the plaintext from the ciphertext.

We demonstrate that there exists an impossible differential D_1, D_2 for the KB-256 algorithm, where

$$D_1 = (0, 2^{31}, 0, 0, 0, 0, 2^{31}, 0), \quad D_2 = (2^{31}, 0, 0, 2^{31}, 0, 0, 0, 0).$$

By verification, a cryptanalyst can make sure that the text pair $X, \underline{X}$ such that $X \oplus \underline{X} = (0, 2^{31}, 0, 0, 0, 0, 2^{31}, 0)$, after 8 rounds, becomes the pair $X^8, \underline{X^8}$ such that $X^8 \oplus \underline{X^8} = (t_1, t_2, 0, t_3, t_4, 0, t_5, t_6)$ for some non-zero vectors $t_1, t_2, t_3, t_4, t_5, t_6 \in V_{32}$. We note that $t_1, t_2, t_3, t_4, t_5, t_6$ depend on each pair $X, \underline{X}$.

In Table 1, the differences between texts after each of 8 rounds are presented.

Table 1

Round no.	Difference
1	$(2^{31}, 0, 0, 0, 0, 2^{31}, 0, 0)$
2	$(0, 0, 0, 0, 2^{31}, 0, 0, 2^{31})$
3	$(0, 0, 0, 2^{31}, 0, 0, 2^{31}, 0)$
4	$(0, 0, 2^{31}, 0, 0, 2^{31}, 0, 0)$
5	$(0, 2^{31}, 0, 0, 2^{31}, 0, 0, 0)$
6	$(2^{31}, 0, 0, 0, 0, 2^{31}, 0, 0)$
7	$(0, \circ, 2^{31}, 0, \circ, 0, 0, \circ)$
8	$(t_1, t_2, 0, t_3, t_4, 0, t_5, t_6)$

By $\circ$ we denote non-zero differences. By verification, the cryptanalyst can make sure that the pair $Y^{16}, \underline{Y^{16}}$ such that $Y^{16} \oplus \underline{Y^{16}} = (2^{31}, 0, 0, 2^{31}, 0, 0, 0, 0)$ after 8 reverse rounds, becomes the pair $Y^8, \underline{Y^8}$ such that $Y^8 \oplus \underline{Y^8} = (t'_1, t'_2, t'_3, t'_4, 0, t'_5, t'_6, 0)$ for some non-zero vectors $t'_1, t'_2, t'_3, t'_4, t'_5, t'_6 \in V_{32}$. We note that $t'_1, t'_2, t'_3, t'_4, t'_5, t'_6$ depend on each pair $Y^{16}, \underline{Y^{16}}$.

In Table 2, the differences between texts after each of 8 rounds are presented in reverse order.

Table 2

Round no.	Difference
15	$(0, 2^{31}, 0, 0, 2^{31}, 0, 0, 0)$
14	$(0, 0, 2^{31}, 0, 0, 2^{31}, 0, 0)$
13	$(0, 0, 0, 2^{31}, 0, 0, 2^{31}, 0)$
12	$(0, 0, 0, 0, 2^{31}, 0, 0, 2^{31})$
11	$(2^{31}, 0, 0, 0, 0, 2^{31}, 0, 0)$
10	$(0, 2^{31}, 0, 0, 0, 0, 2^{31}, 0)$
9	$(\circ, 0, \circ, 0, 0, \circ, 0, 2^{31})$
8	$(t'_1, t'_2, t'_3, t'_4, 0, t'_5, t'_6, 0)$

An impossible differential exists if for text pairs $X, \underline{X}$ and $Y^{16}, \underline{Y^{16}}$ such that $X \oplus \underline{X} = (0, 2^{31}, 0, 0, 0, 0, 2^{31}, 0)$, $Y^{16} \oplus \underline{Y^{16}} = (2^{31}, 0, 0, 2^{31}, 0, 0, 0, 0)$, the sets $(t_1, t_2, 0, t_3, t_4, 0, t_5, t_6)$ and $(t'_1, t'_2, t'_3, t'_4, 0, t'_5, t'_6, 0)$ never coincide. As a result, since we have $t'_5 \neq 0$, we derive that an impossible differential exists.

8. Conclusion

In this paper, the KB-256 properties that may influence the overall cipher strength are provided. However, no key recovery method has been found more efficient than exhaustive key searching for the full-round algorithm.

REFERENCES

1. *Fomichev V. M., Koreneva A. M., Miftakhutdinova A. R., and Zadorozhny D. I.* Ocenki predelnoy proizvoditelnosti algoritmov blochnogo shifrovaniya [Evaluation of the maximum performance of block encryption algorithms]. Matematicheskie Voprosy Kriptografii, 2019, vol. 10, no. 2, pp. 181–191.
2. *Fomichev V. M. and Koreneva A. M.* Encryption performance and security of certain wide block ciphers. J. Comput. Virol. Hack. Tech., 2020, vol. 16, pp. 197–216.
3. GOST 34.12-2018. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry. [GOST 34.12-2018. Information Technology. Cryptographic data security. Block ciphers]. `https://docs.cntd.ru/document/1200161708`, 2018.
4. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. J. Cryptology, 2005, vol. 18, pp. 291–311.