4. *Bernstein D. J.* ChaCha, a Variant of Salsa20. `https://cr.yp.to/chacha/chacha-20080128.pdf`. 2008.
5. *Aumasson J.-P., Meier W., Phan R. C.-W., and Henzen L.* The Hash Function BLAKE. `https://www.researchgate.net/publication/316806226_The_Hash_Function_BLAKE`. 2014.
6. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
7. *Lipmaa H., Wallen J., and Dumas P.* On the additive differential probability of exclusive-or // LNCS. 2004. V. 3017. P. 317–331.
8. *Mouha N., Kolomeec N., Akhtiamov D., et al.* Maximums of the additive differential probability of Exclusive-Or // IACR Trans. Symmetric Cryptology. 2021. No. 2. P. 292–313.
9. *Gligoroski D., Odegard R. S., Mihova M., et al.* Cryptographic hash function Edon-R // Proc. IWSCN. 2009. P. 1–9.

UDC 519.17 DOI 10.17223/2226308X/15/18

KEY SCHEDULE BASED ON A MODIFIED ADDITIVE GENERATOR[1]

V. M. Fomichev, D. A. Bobrovskiy, R. R. Sotov

A method of round key generation for iterated block ciphers based on a modified additive generator (MAG), and, in addition, on MAG and a linear congruent generator in a series circuit is proposed. The bijectivity of the generating transformation is demonstrated. Using the matrix-graph approach the number of iterations necessary for achieving enhanced cryptographic properties is experimentally evaluated. This number depends on the generator characteristics.

Keywords: *key scheduling algorithm, iterative block ciphers, matrix-graph approach, modified additive generator, mixing properties, nonlinearity.*

1. Introduction

The key schedule is an important component of any iterated block cipher. The first versions of key schedules (DES, GOST 28147-89) involved bit sampling from the cipher key which gives the cryptanalyst grounds for attacks such as differential analysis. In AES, the generation of round keys is more complex and requires a non-stationary recurrence relation over a set of binary vectors. The Kuznechik algorithm provides a complex key dependency using the Feistel network. The goal of key schedule algorithms is to combine a complex functional relationship between the bits of the cipher key and the round keys with a relatively low computational complexity of key generation.

This paper proposes a round key generator (RKG) based on a modified additive generator and, in addition, on MAG and a linear congruent generator (LCG) in a series circuit.

2. Additive generator

The additive generator (AG) is a shift register of length n with feedback $f(z_0, \ldots, z_{n-1})$ over the space of binary r-dimensional vectors, i.e., a register transformation φ of the set $V_{nr} = \{(z_0, \ldots, z_{n-1}) : z_0, \ldots, z_{n-1} \in V_r\}$:

$$\varphi(z_0, \ldots, z_{n-1}) = (z_1, \ldots, z_{n-1}, f(z_0, \ldots, z_{n-1})), \tag{1}$$

where the function $f\colon V_{nr} \to V_r$ is the shift register feedback function.

The AG feedback has the following form: $f(z_0, \ldots, z_{n-1}) = z_0 \boxplus z_2 \boxplus z_4 \boxplus z_6$, where $\boxplus$ is addition modulo 2^r, that is, f is bijective on the variable z_0, hence the transformation φ is also bijective [1]. It has insufficient mixing: the leading bits of all vectors depend only on the least significant ones. Therefore, a transformation φ^g of the modified AG is proposed, in which the vector value of the feedback is transformed by permutation g of the set V_r. The feedback of the MAG is denoted by f^g. It is proved that the transformation $\varphi^g(z_0, \ldots, z_{n-1})$ is bijective if and only if the function φ is bijective and g is a permutation [2].

The MAG is studied given $r = 32$, where the transformation $g(k)$ is a cyclic shift permutation of binary vectors by k bits towards the leading bits. Hence $\varphi^{g(k)}$ is a bijection of the set V_{nr}, and the feedback function has the form

$$f^{g(k)}(z_0, \ldots, z_{n-1}) = \mathrm{Int}_{32}(g(k)(\mathrm{Vec}_{32}(z_0 \boxplus z_2 \boxplus z_4 \boxplus z_6))), \tag{2}$$

where $\mathrm{Vec}_{32}\colon \mathbb{Z}_{2^{32}} \to V_{32}$ is a bijection that maps a number $X \in \mathbb{Z}_{2^{32}}$ to its binary representation, $\mathrm{Int}_{32} = \mathrm{Vec}_{32}^{-1}$ is the inverse function.

Given $t = 0, 1, 2, \ldots$, we denote:

- $g(k)$ — left cyclic shift by 1 bit ($k = 1$);
- $X_j^{(t)}$ — the state of the j-th MAG cell at t, $j = 0, 1, \ldots, 6$;
- $X^{(t)} = (X_0^{(t)}, X_1^{(t)}, \ldots, X_6^{(t)})$ — the state of the MAG at t;
- $X^{(0)}$ — the initial state of MAG.

The key of MAG is its initial state. From (1) and (2) we get:

$$X^{(t+1)} = (X_1^{(t)}, \ldots, X_6^{(t)}, g(k)(X_0^{(t)} \boxplus X_2^{(t)} \boxplus X_4^{(t)} \boxplus X_6^{(t)})). \tag{3}$$

A round key sequence is formed as an irregular sample from the sequence $\{X_0^{(t)}\}$, $t = 0, 1, 2, \ldots$

3. Cyclic structure of the MAG state digraph

To avoid repetitions in the sequence of round keys, short cycles of length less than 300 are undesirable in the cyclic transformation structure (this limit is determined by the required number of round keys in a number of block ciphers). The structure of the MAG state digraph was studied.

We denote by $\Gamma(\varphi^{g(k)})$ the $\varphi^{g(k)}$ transformation digraph, i.e., $\Gamma(\varphi^{g(k)}) = (V_{224}, E)$, where E is the set of arcs. The arc (z^i, z^j) exists if $\varphi^{g(k)}(z^i) = z^j$.

The digraph $\Gamma(\varphi^{g(k)})$ has one self-loop generated by the zero fill of MAG.

The cyclic structure of the digraph $\Gamma(\varphi^{g(k)})$ was studied given $k = 1$, $r = 4, 5, 6$ (as r increases, the computational complexity increases rapidly). Using an algorithm that generates a sequence of MAG states, 11 cycles at $r = 4$, more than 18 cycles at $r = 5$, and more than two cycles at $r = 6$ are found in the corresponding digraphs. In Table 1, the lengths of the found cycles are provided.

At $r = 32$, the lengths of the cycles are also experimentally evaluated. We assume 10^8 generated pseudorandom numbers as initial values. For each of the numbers assumed 1000 clock cycles of the generator are implemented (which is enough to generate all the round keys). It is obtained that the length of all cycles exceeds 1000, which excludes repetitions in the sequence of round keys.

The results of the experiment given $r = 32$ suggest that a randomly chosen state of MAG with a probability close to 1 belongs to a cycle of the length greater than 1000.

Table 1

Cycles lengths

Cycle number	Length, $r = 4$	Length, $r = 5$	Length, $r = 6$
1	234 711 845	16 871 058 994	837 124 439 025
2	17 076 802	13 808 636 426	117 617 876 965
3	15 925 876	1 965 696 526	
4	305 050	1 122 723 601	
5	208 004	233 097 005	
6	91 195	151 954 479	
7	67 889	65 351 609	
8	28 603	43 458 018	
9	11 552	41 627 677	
10	7 497	29 128 117	
11	1 142	14 671 598	
12		10 296 293	
13		1 134 118	
14		460 091	
15		212 519	
16		120 918	
17		62 980	
18		22 785	

4. Round keys generator using LCG

In a RKG based on the MAG and LCG series circuit, the key is the initial state of LCG and MAG. The recurrence of the LCG can be represented as

$$X_{n+1} = (aX_n + c) \bmod m, \quad n \geqslant 0,$$

where a is a multiplier, m is a modulus, c is a shift and X_0 is an initial value.

Recommended LCG parameters: $a = 1$, $m = 2^{32}$, c is an odd number, guaranteeing the full-cycle permutation of LCG [3].

The MAG+LCG automaton model's transition function is injective regarding the input variable, hence the period length of the sequence of GRK states is a multiple of the period length of LCG, that is a multiple of 2^{32} [4].

From (3) we get

$$X^{(t+1)} = (X_1^{(t)}, \ldots, X_6^{(t)}, g(k)(X_0^{(t)} \boxplus X_2^{(t)} \boxplus X_4^{(t)} \boxplus X_6^{(t)}) \boxplus (K_0 \boxplus c(t+1))),$$

where K_0 is the lowest 32 bits of the initial key, $c \in \mathbb{Z}_{2^{32}}$ is an odd number, $t = 1, 2, 3, \ldots$ is the sequence number of iteration of the RKG. Consequently, the period length of the sequence $\{X_0^{(t)}\}$ is guaranteed to be at least 2^{32}.

5. Mixing properties and nonlinearity

The RKG parameter k influences the key schedule properties of nonlinearity and mixing. These properties are evaluated using the local exponent of the mixing digraph for RKG state permutations (according to the matrix-graph approach [5]). After evaluation, the properties are determined experimentally.

The experiment results are presented here given different k. The least number of the RKG clock cycles is found after which each vector $\{X_0^{(t)}\}$ coordinate depends essentially and nonlinearly on each initial state bit. In Table 2, the results for $k = 1, 3, 5$ are provided.

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