Tatra Mt. Math. Publ. **47** (2010), 99–113
DOI: 10.2478/v10127-010-0033-6

TATRA MOUNTAINS
Mathematical Publications

RESULTS OF UKRAINIAN NATIONAL PUBLIC CRYPTOGRAPHIC COMPETITION

Roman Oliynykov — Ivan Gorbenko — Viktor Dolgov –
– Viktor Ruzhentsev

ABSTRACT. Five symmetric block ciphers were proposed to Ukrainian national public cryptographic competition. Developers used different methods for achieving security and performance of the algorithms. An overview of proposed symmetric block ciphers and results of their security analysis is given in this paper.

Introduction

Ukrainian national public cryptographic competition was announced [1] in 2006 by State Service of Special Communication and Information Security of Ukraine. General aim of the competition is selection of the symmetric block cipher which can be a prototype of the national standard of Ukraine instead of GOST 28147–89 [2]. Cipher, proposed to the competition, should satisfy the following main requirements [1]:

- an algorithm must support block size and key length of 128, 256 and 512 bits;
- a cipher should be protected from all known cryptanalytical methods and should have enough security margin to be secure in the future;
- a proposed solution must not have any trapdoor and should not be suspected to have one;
- software implementation of the proposed cipher should be fast at least as GOST 28147–89.

Five algorithms were proposed to the competition:

- “Kalyna” (JSC “Institute of Information Technologies”, Kharkov) [3];
- “Mukhomor” (Kharkov National University of Radioelectronics) [4];

2010 Mathematics Subject Classification: 94–00, 94A60, 68P25.
Keywords: symmetric block cipher, Ukrainian national public cryptographic competition, Kalyna, ADE, Labyrinth, Mukhmor.

– “ADE” (Kozhedub Air Force University, Kiev/Kharkov) [5];
– “Labyrinth” (JSC “Cryptomach”, Kharkov);
– “RSB” (National Aviation University, Kiev).

Developers of the algorithms used different constructions and took into account the experience of AES [6], NESSIE [7] and CryptRec [8] cryptographic competitions, so proposed ciphers used rather well-known elements, but vary in security and speed characteristics.

After initial analysis, it was shown that “RSB” has a lack for encryption/decryption speed, potentially poor statistical properties (respectively, potential vulnerabilities to differential and linear cryptanalysis), so it was excluded from consideration. Other four algorithms were allowed for further analysis of cryptographic strength and implementation characteristics.

1. Symmetric block cipher “Kalyna”

1.1. Description of the cipher

“Kalyna” is Rijndael-based [9] algorithm and supports block sizes and key lengths up to 512 bits. Number of rounds depends on block size and is equal to 10, 14 or 30 (block size is 128, 256 and 512 bits, respectively.) with key-controlled pre- and post-whitening. The length of the key can be equal or greater than the block size.

“Kalyna” can be presented as the following transformations:

$$\mathrm{Kalyna}_{K_M} = \chi_{K_{N_r+1}} \circ \gamma \circ \prod_{i=1}^{N_r/2} \big(\sigma_{K2i} \circ \theta \circ \pi \circ \gamma \circ \chi_{K_{2i-1}} \circ \theta \circ \pi \circ \gamma\big) \circ \sigma_{K_0},$$

where

σ_{K_i} – XorRoundKey(State, K_i-)—XORing with a round key K_i;
χ_{K_i} – AddRoundKey(State, K_i)—modulo 2^{32} addition with a round key K_i;
π – ShiftRows(State)—byte permutation (shifting) on the cipher state;
γ – Kalyna_S_boxes(State)—S-box layer;
θ – MixColumns(State)—linear transformation layer (MDS matrix multiplication);
K_i – round key;
K_M – encryption/decryption key;
N_r – number of full rounds (without the last simplified one).

Key schedule of “Kalyna” uses round transformations operations and can be presented as follows:

$$\mathrm{KeySched}_{K_M}^{C_i} = \sigma_{K_M} \circ \theta \circ \pi \circ \gamma \circ \chi_{\overline{K_M}} \circ \theta \circ \pi \circ \gamma \circ \sigma_{K_M},$$

where
C_i – key schedule constant;
K_M – encryption/decryption key;
$\overline{K}_M$ – bitwise inversion of encryption/decryption key.

Key schedule constant C_i is used as a plaintext, which is encrypted by K_M key. From derived value of $KS_{K_M}^{C_i}$ several round keys can be obtained by simple byte permutation (shifting). Number of round keys obtained by the same value of $KS_{K_M}^{C_i}$ depends on block size and key length. It is used several values of C_i to generate all round keys (from 3 constants and key states, resp. for 128/128 mode up to 8 constants for 512/512).

Main differences between "Kalyna" and Rijndael are the following:

- larger range of supported block sizes and key lengths;
- increased number of rounds (taking into account keying pre- and post--whitening);
- eight random generated S-boxes, filtered according to DC, LC and degree of Boolean polynomial criteria (instead of the single Rijndael S-box with inverse element in GF(2^8));
- round key is added using XOR and modulo 2^{32} sum operations (depending on the round);
- linear transformation is an 8×8 MDS matrix (instead od 4×4 MDS in Rijndael);
- a new key schedule based on round transformations operations.

1.2. Design rationale of "Kalyna"

General requirement to "Kalyna" is to have very high level of cryptographic security providing acceptable implementation characteristics. Modifications of Rijndael construction decreased the speed of the cipher (approximately to $\sim$ 85 % of AES on software implementations), complicated hardware and software implementations (especially on smart-cards), but protected algorithm from potential weaknesses of AES/Rijndael (like algebraic analysis [10], related-key cryptanalysis [11]) and provided very good security margin, especially for the block length and key size of 512 bits.

S-boxes for "Kalyna" were selected from the set of randomly generated permutations (random sequences for generation were taken from hardware-based generator). Selection criteria include the following limitations: the maximum value of non-trivial XOR difference transformation probability is 2^{-5} (comparing to 2^{-6} of the Rijndael S-box), the maximum absolute value of linear approximation probability bias is 2^{-3} (2^{-4} of the Rijndael S-box), and the degree of the Boolean polynomial expressing the output bits through the input bits is 7. It should be noticed, that such selection criteria allowed preventing description of S-boxes and the whole cipher by overdefined system of equations of the 2nd degree [10], preserving good resistance to differential, linear and other statistical methods of cryptanalysis.

Modulo 2^{32} round key addition improves strength of the cipher to DC, LC etc., and gives additional protection from algebraic analysis. Although the modular addition can be described by a system of the 2nd degree, it is non-linear in GF(2) and adds new variables (unknowns) to the system, which significantly complicates solution of the system even on 2 round (very reduced) version of the cipher.

Increased size of MDS matrix provides better propagation properties, so the strength to the most of cryptanalytical methods. Increased size also requires additional memory for precomputed tables. For the fast implementation (eight S-boxes and 8×8 MDS) it is needed 8×2 kB $= 16$ kBytes of tables.

A new key schedule, proposed in “Kalyna”, provides strength to known attacks, good statistical and non-linear properties and high complexity of obtaining encryption key from one or several round keys [12].

1.3. Strength and security margins of “Kalyna”

Through using modulo 2^{32} key addition, “Kalyna” is not a Markov cipher [13]. So, the conventional method of strength estimation to DC cannot be directly applied.

The conventional method is based on the calculation of the sum of the active S-boxes number in every round during encryption process. Having this value and the maximal probability of S-box difference transformation, it is possible to estimate upper bound of the maximal probability of non-trivial differential characteristic for Markov ciphers.

“Kalyna” involves modulo 2^{32} key addition. This operation is non-linear over GF(2) and can change the number of active bytes (for a difference calculated modulo 2). Moreover, the probability of such transformation depends on the input data, so the probability of the whole characteristic also depends on the input data. This, conventional methods cannot be applied to “Kalyna”.

Correct results can be obtained using the following theorem.

Theorem (by A. N. Alekseychuk, L. V. Kovalchuk [15]). *For symmetric block cipher “Kalyna” the maximal probability* EDP(Ω) *of differential characteristic* ω *is upper bounded by the value*

$$\mathrm{EDP}(\Omega) \leq \left(\triangle^{S}_{\max}\right)^{(N_r/2)B_M+1},$$

where

N_r – *number of rounds in "Kalyna" (without last simplified round);*
B_M – *branch number of the "Kalyna" MDS matrix*
($B_M = 9$ for 8×8 MDS);
$\triangle^S_{\max}$ – *maximal non-trivial difference transformation probability*
on "Kalyna" S-box $\left(\triangle^S_{\max} = p_{D_{\max}} = 2^{-5}\right)$.

Proof. (Simplified version of the proof given in [15].) Let us take into account two consecutive rounds (number i and $i+1$) of "Kalyna" located between AddRoundKey() operation, and let ω_i and ω_{i+1} be the difference (bitwise modulo 2) at the input and output of the first of these rounds, respectively.

Let us define the number of active bytes (Hamming weight) in these differences as $wt(\omega_i)$ and $wt(\omega_{i+1})$. During round transformation, application of Kalyna_S_Boxes(), ShiftRows() and XorRoundKey() does not change the number of active in the difference, this value can be changed only on MixColumns().

According to the definition of branch number B_M for MDS matrix, we have

$$wt(\omega_i) + wt(\omega_{i+1}) \geq B_M \quad \text{for} \quad wt(\omega_i)1 > 0.$$

We may have strict equality when all active bytes are located at the input of one MDS matrix of "Kalyna" and inequality in other situation (MixColumns of 128-bit "Kalyna" uses 2 MDS matrices, 256-bit variant uses 4 matrices, and 512-bit variant has 8 MDS matrix multiplication).

So, the number of active S-boxes at the ith and $(i+1)$th rounds will be $wt(\omega_i)$ and $wt(\omega_{i+1})$, respectively, and for these two consecutive rounds number of active S-boxes is

$$wt(\omega_i) + wt(\omega_{i+1}) \geq B_M.$$

Thereby, the number of active S-boxes is at least B_M.

AddRoundKey() may change the number of active bytes between these couples of rounds. But modulo 2^{32} addition is a bijective operation, and if the input difference is non-zero, then the output difference will also have non-zero bytes ($wt(\omega_i) > 0$ for any couple of rounds).

In "Kalyna" we have $N_r/2$ such couples of rounds partitioned by AddRoundKey() operation. Besides these rounds, we have the first round, which has at least one active S-box (non-zero difference comes to the first round).

Thereby, the number of active S-boxes for the whole cipher is at least

$$(N_r/2)B_M + 1.$$

Assuming as usual for DC, that transformations on all S-boxes are performed independently, we have upper bound for value for differential characteristic probability

$$\mathrm{EDP}(\Omega) \leq (\triangle^S_{\max})^{(N_r/2)B_M+1}.$$

For 128-bit, 256-bit and 512-bit variants of "Kalyna" we have:

$$\mathrm{EDP}_{128}(\Omega) \leq 2^{-230}, \qquad \mathrm{EDP}_{256}(\Omega) \leq 2^{-320}, \qquad \mathrm{EDP}_{512}(\Omega) \leq 2^{-680}.$$

So, "Kalyna" is protected from differential attacks.

This theorem gives us an upper bound of probability only, not a strict value. It is more difficult to estimate strict security margins of "Kalyna" to differential cryptanalysis. From the proof of theorem it follows that 2 consecutive rounds between AddRoundKeys have at least B_M active S-boxes. So, 4 rounds will have at least $2 \cdot B_M = 18$ active S-boxes, etc. But we do not take into account that we have two or more MDS matrices, and at most cases modulo 2^{32} key addition will not decrease the number of active S-boxes. Therefore, 18 active S-boxes for 4 rounds is the lowest estimation which can have rather simple theoretical proof.

From the theorem we can calculate that it can be enough 6 rounds (of 11) to cross the threshold of 2^{-128} for 128-bit "Kalyna", but really secure number of rounds is less. Analogous results we have for 256-bit and 512-bit variants.

Similar to differential cryptanalysis results were got for linear cryptanalysis, truncated and impossible differentials, integral cryptanalysis, interpolation and boomerang attacks [14]. It was shown the impossibility of application of related keys, slide and other types of analysis to "Kalyna" [12], [14], [15].

"Kalyna" key schedule supposes non-bijective generation of round keys. This property increases the strength to various methods of cryptanalysis oriented on obtaining round keys only. Having good key agility and simple implementation (both in software and hardware) with protection from additional attacks, this key schedule allows potential collisions in round keys (different encryption keys might generate the same sequence of round keys).

We can estimate the probability of such event by application of differential cryptanalysis methods. Application of the best possible characteristics gives us the following: for the two distinct random encryption keys

$$K_M^{(1)} \neq K_M^{(2)}$$

the collision probability in all keys states $KS_{K_M}^{C_i}$ (getting all round keys equal) is upper bounded by the probability

$$p_{\mathrm{char}} \leq \left(\triangle_{\max}^{S}\right)^{B_M \cdot t},$$

where t is the number of key states [12]. This value does not take into account full differentials (each differential can cover several characteristics), so real collision probability can be higher. But having only 2-round transformation in the key schedule, we can suppose that the number of characteristics forming necessary differential is sufficiently small and it does not improve this probability greatly.

For "Kalyna" with 128-bit block and 128-bit encryption key we have

$$p_{\mathrm{char}} \leq (2^{-5})^{9 \cdot 3} = 2^{-135},$$

which is negligible small.

Thus, "Kalyna" is resisted to known methods of cryptanalysis and has a good security margin. □

2. Symmetric block cipher "Mukhomor"

2.1. Description of the cipher

"Mukhomor" is built using extended Lai-Massey scheme, like in FOX ciphers family [16]. According to requirements of competition, algorithm supports block sizes and key lengths of 128, 256 and 512 bits. Number of rounds depends on block size and is equal to 11, 13 or 18, respectively.

Cipher consists of initial whitening, application of round transformations and final whitening. Round transformation of "Mukhomor" is given at Figure 1.

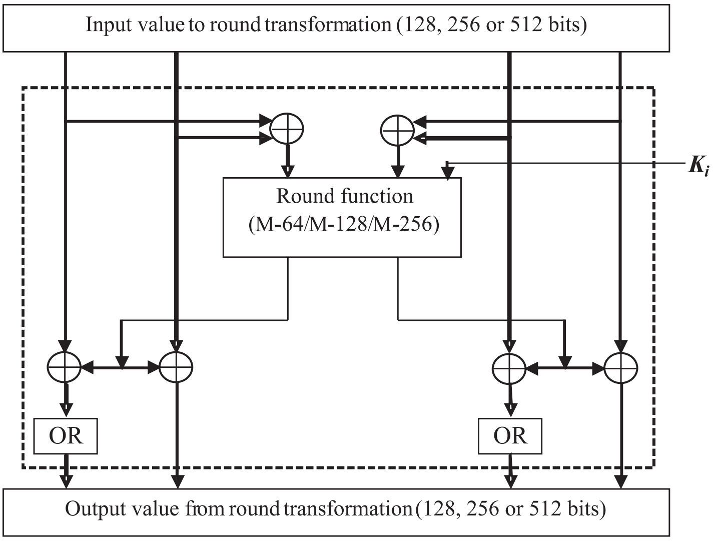
Input value to round transformation (128, 256 or 512 bits)
K_i
Round function
(M-64/M-128/M-256)
OR
OR
Output value from round transformation (128, 256 or 512 bits)

FIGURE 1. Round transformation of "Mukhomor".

After application of output values of round function to input quarters, the first and the third one are processed by OR transformation. Like in FOX ciphers family, OR uses one round of Feistel transformation with identity as a round function.

Construction of the round function used this transformation depends on block size of the cipher. Round function of "Mukhomor" for block size of 128 bits is given on the following page at Figure 2.

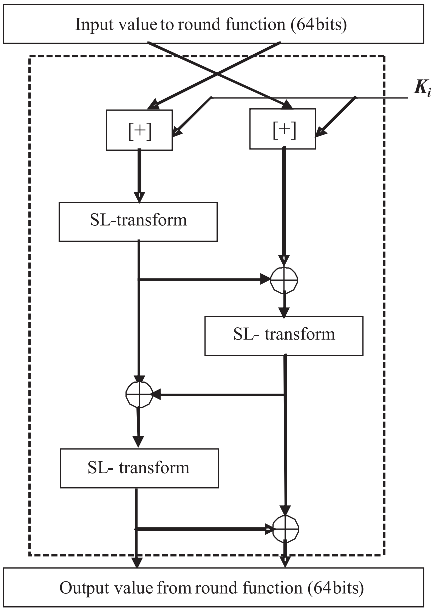
Input value to round function (64bits)
K_i
[+]
[+]
SL-transform
SL- transform
SL- transform
Output value from round function (64bits)

Figure 2. Round function M-64 of "Mukhomor".

Like in "Kalyna", it is used modulo 2^{32} key addition, but in every round. After 3-time application of SL-transformation, resulting value is transmitted to the output of round function.

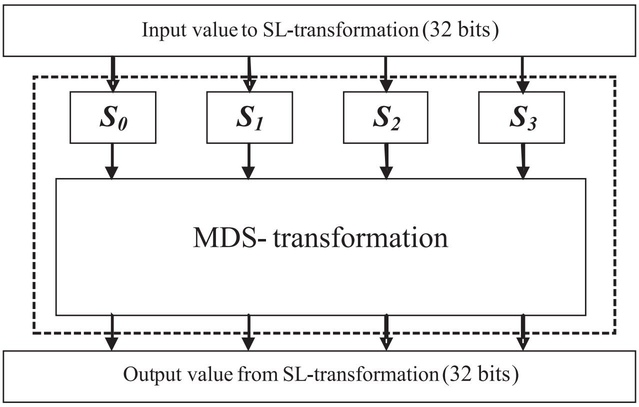
Input value to SL-transformation (32 bits)
S_0
S_1
S_2
S_3
MDS- transformation
Output value from SL-transformation (32 bits)

Figure 3. SL-transformation of "Mukhomor".

Structure of SL-transformation is given at Figure 3. SL-transformation of "Mukhomor" uses four different S-boxes with the same requirements, as for "Kalyna" (for similarity of these ciphers, all four S-boxes of "Mukhomor" were taken from “Kalyna” specification). MDS-transformation of “Mukhomor” has size 4×4 bytes, and taken from Rijndael.

Key schedule of “Mukhomor” uses the same principles as “Kalyna”. Some constant is encrypted by several parallel round functions using 2 rounds with byte permutation after the first one, and encryption key is applied as a round key. Key schedules of “Mukhomor” and “Kalyna” have equal properties from the security and implementation points of view.

2.2. Design rationale of “Mukhomor”

The aim of “Mukhomor” construction was to develop a modern fast cipher with acceptable level of security, which protects cipher from all known cryptanalytical attacks, but does not have a large security margin. Lay-Massey scheme is efficient and easy for implementation. Required number of rounds was estimated by strength to differential and linear cryptanalysis of simplified version of “Mukhomor” (without taking into account modulo 2^{32} addition with a round key, what makes “Mukhomor” a non-Markov cipher). Round function and SL-transformation was designed for good non-linear and propagation properties and efficient implementation on 32-bit platforms. Other elements of the algorithm, including key schedule, use the same principles (have the same properties), as “Kalyna”.

2.3. Strength of “Mukhomor”

Many cryptanalytical methods were considered concerning “Mukhomor”. It was shown strength of the cipher to differential and linear cryptanalysis, truncated and impossible differentials, integral cryptanalysis, interpolation and boomerang attacks, slide and other types of analysis [17].

So, “Mukhomor” is invulnerable to known method of cryptanalysis, and its implementations have high performance.

3. Symmetric block cipher “Labyrinth”

3.1. Description of the cipher

“Labyrinth” is a 16-round Feistel algorithm with initial and final whitening, supporting block sizes and key lengths of 128, 256 and 512 bits. Initial whitening consists of modulo key addition (modulo respective to the block size), an S-box layer and a byte permutation layer. Final whitening also involves byte permutation (another variant), a layer of inverse S-boxes and modulo key subtraction (like in initial whitening, modulo respective to the block size). Structure of round function of “Labyrinth” is given at Figure 4. Like in Camellia [19], it consists of round key addition (modulo respective to the half of block size), S-boxes and MDS matrix multiplication. Size of the MDS matrix is also chosen as 8×8 bytes.

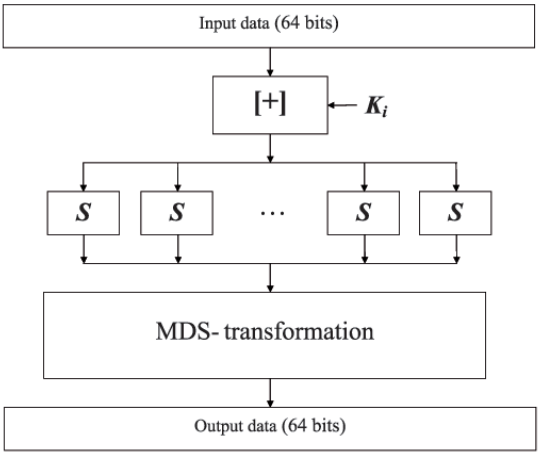

FIGURE 4. Round function of "Labyrinth" for 128-bit block size.

Key schedule of "Labyrinth" generates round keys by involving round function transformation. The first round keys are equal to corresponding parts of the encryption key (with respect to the key length of the cipher). For generation additional round keys, the encryption key is taken as a plaintext and is processed by several rounds of Feister transformation with "Labyrinth" round function, like in the CS-Cipher [21]. Instead of constants at the key schedule of CS-Cipher, a sum of encryption key parts is used as a round key in this procedure. After each application this sum is modified by modulo addition with some constant and XORing with another one. Round keys for the first 8 rounds are obtained by this method, last rounds uses the same keys in different sequence.

3.2. Design rationale of "Labyrinth"

According to developer's documents sent to the competition committee, the cipher is optimized for compact implementation of different platforms, having appropriate level of cryptographic security. Its speed is approximately equal to ~ 75 % of AES with software implementation on x86 platform. Full specification and supporting documents of "Labyrinth" is not published at scientific journals yet, so we give brief extraction here.

Initial and final whitening is intended to increase the number of active S-boxes on the first/last round and prevent nR-attacks of differential cryptanalysis. Like in Rijndael, "Labyrinth" uses the same S-box for all transformations, and also implements exponentiation in GF(2^8). Linear transformation layer requires maximal branch number property and uses MDS matrix multiplication. It is also optimized for compact implementation. Key schedule algorithm has non-linear properties and generates unique round keys.

3.3. Strength of "Labyrinth"

Developer of the cipher shows application of differential, linear cryptanalysis, truncated and impossible differentials, boomerang, linear sums, high order differentials and integral attack to modified version of "Labyrinth". Proof of strength to cryptanalytical attacks was made for "Labyrinth"-like cipher, where all modulo addition or subtraction operations are changed to XOR. Modified version became a Markov cipher, without taking into account that modulo operations can essentially change number of active bytes after every such operation. We can notice that in many cases such approach gives right estimations, but it is not a strict proof of original cipher properties.

In [19] it was shown, that such modified version of "Labyrinth" can be described with an overdefined system of 16800 equations of the 2nd degree with 1664 variables, like AES/Rijndael [10]. As modulo 2^{64}, 2^{128}, etc. addition can be described by the system of the 2nd degree, the whole cipher also can be described by the system of overdefined equations of the 2nd degree.

4. Symmetric block cipher "ADE"

4.1. Description of the cipher

"ADE" is another one Rijndael-based symmetric block cipher, proposed to the competition. It supports block sizes and key lengths of 128, 192, 256, 320, 512 bits (more values than required) and can be scaled more with a step of 32 bits.

Encryption of "ADE" (variant for 128 bits) can be presented as a set of transformations:

$$\mathrm{ADE}_{K_0} = \sigma_{K_{10}} \circ \pi_{K_{10}} \circ \gamma_{K_{10}} \circ \sigma_{K_9} \circ \prod_{i=0}^{8} \left(\theta_{K_i} \circ \pi_{K_i} \circ \gamma_{K_i} \circ \theta_{K_i}\right),$$

where

σ_{K_j} – AddRoundKey(State,RoundKey)—XORing with a round key K_i;

π_{K_j} – ShiftRows(State, RoundKey)—round key dependent shift on the cipher state;

γ_{K_j} – ByteSub(State, RoundKey)—layer of round key dependent S-boxes;

θ_{K_i} – MixColumn(State, RoundKey)—multiplication by round key dependent MDS matrix;

K_i – round key.

It should be noticed that all operations (ShiftRows, MixColumn and S-boxes in ByteSub) are key dependent and differ from round to round.

S-box transformation $b = S(a)$ for ADE can be expressed via formula

$$b = M \cdot (a \cdot \gamma)^{-1} + \beta,$$

where

M, β – corresponding binary matrix and vector form AES specification (multiplicative inverse also maps 0 onto itself),

γ – a byte from the current round key (if this byte is equal to zero, γ is set to a fixed non-zero constant).

ShiftRows takes 2-bit pairs from the byte of the current round key and uses every couple of bits as a shifting value for corresponding row. Thus, each row is shifted independently.

Like in AES, MixColumn implements multiplication of the current state column to the generator matrix of linear forward error correction code. Matrix can be of different size and has the following form:

$$M' = \begin{pmatrix} S & S^2 & S^3 & \cdots & S^{4i} \\ S^2 & S^4 & S^6 & \cdots & S^{8i} \\ S^3 & S^6 & S^9 & \cdots & S^{12i} \\ \cdots & \cdots & \cdots & \cdots & \\ S^{4i} & S^{8i} & S^{12i} & \cdots & S^{16i} \end{pmatrix},$$

where

s – a byte from the current round key (if this byte is equal to zero or one, s is set to fixed constant),

i – processor-dependent constant for cipher optimization to different platforms.

Key schedule of “ADE” is equal to such operation in AES/Rijndael.

If the cipher is implemented with a set of precomputed tables, ADE runs as fast as AES does, but tables must be computed before the encryption and require large amount of memory (potential problem for implementation of the cipher on smart-cards).

4.2. Design rationale of “ADE”

From authors’ statement, their aim was to protect cipher from algebraic analysis preserving all other excellent properties of AES/Rijndael. Key dependent operations make cipher invulnerable to potential weaknesses of AES and essentially improve cipher’s propagation properties. Other design solutions are based on Rijndael development document [9].

4.3. Strength of “ADE”

For “ADE” it was shown [5] strength to differential and linear cryptanalysis, truncated differential, square, interpolation and related-key attack. Authors prove that it is much harder to build overdefined system of equation for “ADE” than for AES, and such a system will be less sparse. Statistical properties of reduced round “ADE” are better than properties of AES with the same number of rounds.

But great number of key-dependent operations makes cipher potentially vulnerable to key schedule attacks or leads to existence of weak keys classes. Independent analysis has shown that key-dependent ShiftRows() operation can do synchronous shift of all rows to the same number of bytes. In [20] it was shown that such a synchronous shift was kept at all rounds of encryption for some set of keys. In this case each subpart of encrypted plaintext is processed independently. For example, on some set of keys 128-bit block “ADE” behaves like 4 independent ciphers with 32-block length.

Thus, “ADE” is protected from well-known cryptanalytical attacks, has excellent statistical properties, but has rather large classes of weak encryption keys, which application leads to very serious worsening of cryptographic properties of the cipher.

Conclusions

Ukrainian national public cryptographic competition for selection of algorithm-prototype for a national standard of symmetric block cipher of Ukraine was announced in 2006. Proposed ciphers accepted for participation in the competition became available for researchers in 2007.

Further analysis has shown that cipher “RBS” has potential weaknesses for statistical methods of cryptanalysis and a lack of encryption/decryption speed. Another candidate “ADE” has classes of weak encryption keys.

It was not shown existence of effective attacks against “Labyrinth”. But this cipher can be described by overdefined system equation of the 2nd degree, like AES. For original cipher there is no full formal proof of strength to known methods of cryptanalysis.

Algorithm “Mukhomor” is proven to be resistant to known cryptanalytical methods. Its implementations have high performance, but the cipher does not have large security margins.

Symmetric block cipher “Kalyna” was designed to be an algorithm with high level of security. It has a full proof of strength of known methods of cryptanalysis, does not have any potential weak points and has very good security margins for protection from attacks in the future. It also has sufficient performance of implementations.

On final decision of the competition committee “Kalyna” was selected as a symmetric block cipher which was allowed to be used for protection of non--government information. Existing standard GOST 28147–89 also continues to be used in Ukraine.

REFERENCES

[1] STATE SERVICE OF SPECIAL COMMUNICATION AND INFORMATION SECURITY OF UKRAINE.: *Statement about Public Competition of Cryptographic Algorithms.* State Service of Special Communication and Information Security of Ukraine, 2006. (In Ukrainian) `http://www.dstszi.gov.ua/dstszi/control/ru/publish/article;jsessionid =F88A950B67D1FC50BA7C7CB669238287?art_id=48387&cat_id=42056`.

[2] *GOST 28147–89. State Standard of the Soviet Union. Information Processing Systems. Cryptographic Security. Algorithm of Cryptographic Transformation.* 1990 (In Russian)

[3] OLIYNYKOV, R. V.—GORBENKO, I. D.— DOLGOV, V. I.—RUZHENTSEV, V. I.: *Symmetric block cipher “Kalyna”*, Applied Radio Electronics **6** (2007), 46–63. (In Ukrainian)

[4] OLIYNYKOV, R. V.—GORBENKO, I. D.—DOLGOV, V. I.—RUZHENTSEV, V. I.––BONDARENKO, M. F.: *Symmetric block cipher “Mukhomor”*, Applied Radio Electronics **6** (2007), 147–157. (In Ukrainian)

[5] KUZNETSOV, O. O. ET AL.: *Symmetric block cipher “ADE”*, Applied Radio Electronics **6** (2007), 241–249. (In Ukrainian)

[6] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, USA: *Announcing Development of a Federal Information Processing Standard for Advanced Encryption Standard*, 1997, `http://csrc.nist.gov/archive/aes/pre-round1/aes_9701.txt`.

[7] NEW EUROPEAN SCHEMES FOR SIGNATURE, INTEGRITY, AND ENCRYPTION: *Call for Cryptographic Primitives, Information Societies Technology (IST) Program of the European Commission*, 2000, `https://www.cosic.esat.kuleuven.be/nessie/call`.

[8] MINISTRY OF ECONOMY, TRADE AND INDUSTRY OF JAPAN: *Cryptography Research and Evaluation Committees*, 2000, `http://www.cryptrec.org`.

[9] DAEMEN, J.—RIJMEN, V.: *AES proposal: Rijndael*, AES Conference, Ventura, California, 1998, pp. 4–45, `http://www.nist.gov/aes`.

[10] COURTOIS, N. T.—PIEPRZYK, J.: *Cryptanalysis of block ciphers with ovedefined systems of equations,* in: Advances in Cryptology—ASIACRYPT ’02 8th Internat. Conf. on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, 2002 (Y. Zheng, ed.), Lect. Notes Comput. Sci., Vol. 2501, Springer-Verlag, Berlin, 2002, pp. 267–287.

[11] BIRYUKOV, A.—KHOVRATOVICH, D.: *Related-key cryptanalysis of the full AES-192 and AES 256,* in: Advances in Cryptology—ASIACRYPT ’09, 15th Internat. Conf. on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, 2009 (M. Matsui, ed.), Lecture Notes Comput. Sci., Vol. 5912, Springer-Verlag, Berlin, 2009, pp. 1–18.

[12] OLIYNYKOV, R. V.— RUZHENTSEV, V. I.: *Analysis of the key schedule properties of symmetric block cipher "Kalyna"*, in: Proc. of the Internat. Scientific Conf. Information Security at Information and Telecommunication Networks, Kiev, 2009, pp. 79–84. (In Russian)

[13] LAI, X.—MASSEY, J. L.—MARPHY, S.: *Markov ciphers and differential cryptanalysis,* in: Advanced in Cryptology—Eurocrypt '91, Brighton, UK, 1991, Lect. Notes Comput. Sci., Vol. 547, Springer-Verlag, Berlin, 1991, pp. 17–38.

[14] OLIYNYKOV, R. V.—GORBENKO, I. D.— DOLGOV, V. I.—RUZHENTSEV, V. I.: *Cryptographic strength of the symmetric block cipher "Kalyna"*, Applied Radio Electronics **6** (2007), 64–78. (In Ukrainian)

[15] ALEKSEYCHUK, A. N.—KOVALCHUK, L. V.—SKRYNNIK, A. S.: *Practical strength estimation of the block cipher "Kalyna" to differential, linear cryptanalysis and algebraic attacks based on homomorphism,* Applied Radio Electronics **7** (2008), 203–209. (In Ukrainian)

[16] JUNOD, P.—VAUDENAY, S.: *FOX Specifications. Version 1.2,* MediaCrypt AG, Switerland, 2005, `http://infoscience.epfl.ch/getfile.py?docid=12283&name=JV05&format=pdf&version=1`.

[17] OLIYNYKOV, R. V.—GORBENKO, I. D.—DOLGOV, V. I.—RUZHENTSEV, V. I.: *Cryptographic strength of the symmetric block cipher "Mukhomor"*, Applied Radioelectronics **6** (2007), 158–175. (In Ukrainian)

[18] AOKI, K.—ICHIKAWA, T. ET AL.: *Specification of Camellia—a 128-bit Block Cipher.* NTT, MEC, Japan, 2000, `http://140.127.40.45/crypto/Spec_camellia.pdf`.

[19] OLIYNYKOV, R. V.—KAZIMIROV, O. V.: *Alegebraic analysis of modified version of symmetric block cipher "Labyrinth"*, in: Proc. of the 12th Internat. Scientific Conf. "Information Security at Information and Telecommunication Networks", Kiev, 2009, pp. 39–45. (In Russian)

[20] OLIYNYKOV, R. V.—MIHAILENKO, M. S.—NEBYVAILOV, O. B.: *Results of cryptanalysis of symmetric block cipher "ADE"*, Applied Radio Electronics **7** (2008), 210–215. (In Russian)

[21] STERN, J.—VAUDENAY, S.: *CS-Cipher*, in: 5th Internat. Workshop on Fast Software Encryption—FSE '98, Paris, France, 1998 (S. Vaudenay, ed.), Lect. Notes Comput. Sci., Vol. 1372, Springer-Verlag, Berlin, 1998, pp. 189–204.

Received September 25, 2009

Kharkov National University
of Radioelectronics
Ukraine JSC Institute
of Information Technologies
Bakulina str. 12
61166–Kharkov
UKRAINE

E-mail: roliynykov@gmail.com
gorbenkoi@iit.kharkov.ua
dolgovvi@mail.ru
vityazik@rambler.ru