Общероссийский математический портал

D. M. Dygin, I. V. Lavrikov, G. B. Marshalko, V. I. Rudskoy,
D. I. Trifonov, V. A. Shishkin, О новом российском стандарте шиф-
рования, *Матем. вопр. криптогр.*, 2015, том 6, выпуск 2, 29–34

DOI: <https://doi.org/10.4213/mvk142>

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: 52.23.180.231

26 апреля 2023 г., 13:41:04

УДК: 519.719.2

On a new Russian Encryption Standard

**D. M. Dygin, I. V. Lavrikov, G. B. Marshalko, V. I. Rudskoy,
D. I. Trifonov, V. A. Shishkin**

Technical committee for standardization (TC 26), Moscow

Получено 16.IX.2014

We give a brief analysis for the current demands in standardized encryption algorithms and present a draft of a new block cipher which in the nearest future would “keep company with GOST 28147-89” in a new Russian encryption standard.

Key words: GOST 28147-89, block cipher, encryption standard

О новом российском стандарте шифрования

**Д. М. Дыгин, И. В. Лавриков, Г. Б. Маршалко, В. И. Рудской,
Д. И. Трифонов, В. А. Шишкин**

Технический комитет по стандартизации (ТК 26), Москва

Аннотация. Мы приводим обзор современных требований к стандартизированным алгоритмам шифрования и описание нового блочного шифра, который в ближайшее время будет принят в качестве российского стандарта шифрования наряду с ГОСТ 28147-89.

Ключевые слова: ГОСТ 28147-89, блочные шифры, стандарты шифрования

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 6, no. 2, pp. 29–34 (Russian).

© 2015 D. M. Dygin, I. V. Lavrikov, G. B. Marshalko, V. I. Rudskoy, D. I. Trifonov, V. A. Shishkin

1. Present and future

The present state-of-the-art in practical information security is highlighted by the extreme diversity of possible applications of cryptographic mechanisms: from restricted environments (like RFID-tags and smart cards) to protection of broadband Internet data channels. Each of the possible application areas impose specific requirements on implementation specifications of cryptographic mechanisms, which sometime contradict with the desired cryptographic features.

The question is: whether we should try to make an all-in-one “Swiss army knife” which would actually be a compromise between implementation and cryptographic requirements, or develop a set of primitives, each for the possible application area.

The risk of the first approach is a possibly narrow security margin of a cryptographic primitive. Adoption of the second approach implies that we should maintain a reasonable diversity of cryptographic primitives, but shouldn’t make it too large.

GOST 28147-89 [1] is the only cipher standardized in the Russian Federation now. It was published in the end of 80’s and since that time is widely used all over the world. It has been thoroughly studied by Russian and foreign cryptanalysts and has proven its cryptographic strength.

The only theoretical attacks for the full version of GOST 28147-89 were published a few years ago [2, 3]. They do not threaten the security of the cipher since the obtained time complexity for these attacks is considered greater than enough for providing security in foreseeable future, and data complexity exceed the maximum amount of data that could be encrypted by a block cipher [4]. It’s worth to mention that by a simple change of the key schedule these attacks could be made inapplicable [5].

At the same time, as it was shown by Poschmann et al. in [1], GOST 28147-89 is an extremely lightweight-friendly cipher and has the complexity of hardware implementation comparable with the complexities of implementations of algorithms with significantly shorter key lengths.

However from a point of view of encrypting large amounts of data 64-bit block length is insufficient. So, despite the fact that GOST 28147-89 is secure and has efficient implementation, there is a need for a new block cipher with larger block length. In this article we present a new Russian draft encryption standard with 128-bit block length and 256-bit key length, which in the nearest future would be also standardized in the Russian Federation (see also [6]).

New algorithm is based on well known and stabilized principles following current state-of-the-art in block cipher design strategies. Our main concern was to build software oriented cipher with as large security margin as possible.

2. Description of a draft encryption standard

2.1. Definitions and notation

In the article the following notations are used:

V_n	the set of all binary strings of length n , where n is a natural number (sub-strings numbering goes from the right to the left starting from zero);
$A\ B$	a concatenation of strings $A, B \in V^*$, i.e. a string from the set $V_{ A + B }$, where the left substring is equal to A , and the right string is equal to B ;
$\oplus$	bit-wise addition modulo 2;
Z_m	the set $\{0, 1, \dots, m-1\}$;
P	a finite field $GF(2)[x]/g(x)$, where $g(x) = x^8 + x^7 + x^6 + x + 1 \in GF(2)[x]$ (each element $b_0 + b_1 \cdot \theta + \dots + b_7 \cdot \theta^7 \in P$, where θ denotes a residue class modulo $g(x)$ containing x) may be represented as integer number $b_0 + b_1 \cdot 2 + \dots + b_7 \cdot 2^7 \in Z_{2^8}$, $b_i \in \{0, 1\}$, $i = 0, 1, \dots, 7$;
$\mathcal{V}_n : Z_{2^n} \rightarrow V_n$	a bijective mapping, which transforms each element $z = z_0 + 2 \cdot z_1 + \dots + 2^{n-1} \cdot z_{n-1}$ ($z_j \in \{0, 1\}$, $j = 0, 1, \dots, n-1$) of Z_{2^n} into its binary representation, i.e. the following equation holds: $\mathcal{V}_n(z) = z_{n-1} \ \dots \ z_1 \ z_0$;
$\mathcal{I}_n : V_n \rightarrow Z_{2^n}$	an inverse mapping to $\mathcal{V}_n$, i.e. $\mathcal{I}_n = \mathcal{V}_n^{-1}$;
$\Delta : V_8 \rightarrow P$	a bijective mapping, which transforms a binary string from V_8 into an element of the field P as follows: the string $b_7 \ b_6 \ \dots \ b_0$ ($b_i \in V_1$, $i = 0, 1, \dots, 7$) is transformed into the element $b_0 + b_1 \cdot \theta + \dots + b_7 \cdot \theta^7 \in P$;
$\nabla : P \rightarrow V_8$	an inverse mapping to Δ , i.e. $\nabla = \Delta^{-1}$;
$\Phi\Psi$	a composition of mappings, where Ψ is the first to operate.

2.2. Parameters

2.2..1 Nonlinear bijective mapping

The nonlinear mapping of the algorithm is represented by the substitution $\pi = \mathcal{V}_8 \pi' \mathcal{I}_8 : V_8 \rightarrow V_8$, where $\pi' : Z_{2^8} \rightarrow Z_{2^8}$ is presented below as $\pi' = (\pi'(0), \pi'(1), \dots, \pi'(255))$:

$\pi' = (252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250, 218, 35, 197, 4, 77, 233, 119, 240, 219, 147, 46, 153, 186, 23, 54, 241, 187, 20, 205, 95, 193, 249, 24, 101, 90, 226, 92, 239, 33, 129, 28, 60, 66, 139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143, 160, 6, 11, 237, 152, 127, 212, 211, 31, 235, 52, 44, 81, 234, 200, 72, 171, 242, 42, 104, 162, 253, 58, 206, 204, 181, 112, 14, 86, 8, 12, 118, 18, 191, 114, 19, 71, 156, 183, 93, 135, 21, 161, 150, 41, 16, 123, 154, 199, 243, 145, 120, 111, 157, 158, 178, 177, 50, 117, 25, 61, 255, 53, 138, 126, 109, 84, 198, 128, 195, 189, 13, 87, 223, 245, 36, 169, 62, 168, 67, 201, 215, 121, 214, 246, 124, 34, 185, 3, 224, 15, 236, 222, 122, 148, 176, 188, 220, 232, 40, 80, 78, 51, 10, 74, 167, 151, 96, 115, 30, 0, 98, 68, 26, 184, 56, 130, 100, 159, 38, 65, 173, 69, 70, 146, 39, 94, 85, 47, 140, 163, 165, 125, 105, 213, 149, 59, 7, 88, 179, 64, 134, 172, 29, 247, 48, 55, 107, 228, 136, 217, 231, 137, 225, 27, 131, 73, 76, 63, 248, 254, 141, 83, 170, 144, 202, 216, 133, 97, 32, 113, 103, 164, 45, 43, 9, 91, 203, 155, 37, 208, 190, 229, 108, 82, 89, 166, 116, 210, 230, 244, 180, 192, 209, 102, 175, 194, 57, 75, 99, 182).$

2.2..2 Linear mapping

The linear mapping is denoted by $l : V_8^{16} \rightarrow V_8$ and is defined as:

$$l(a_{15}, \dots, a_0) = \nabla(148 \cdot \Delta(a_{15}) + 32 \cdot \Delta(a_{14}) + 133 \cdot \Delta(a_{13}) + 16 \cdot \Delta(a_{12}) + \\ + 194 \cdot \Delta(a_{11}) + 192 \cdot \Delta(a_{10}) + 1 \cdot \Delta(a_9) + 251 \cdot \Delta(a_8) + 1 \cdot \Delta(a_7) + 192 \cdot \Delta(a_6) + 194 \cdot \\ \Delta(a_5) + 16 \cdot \Delta(a_4) + 133 \cdot \Delta(a_3) + 32 \cdot \Delta(a_2) + 148 \cdot \Delta(a_1) + 1 \cdot \Delta(a_0))$$

for all $a_i \in V_8, i = 0, 1, \dots, 15$, with addition and multiplication in the field P .

2.2..3 Transformations

Transformations involved in encryption/decryption processes are described as follows:

$$X[k] : V_{128} \rightarrow V_{128}, \quad X[k](a) = k \oplus a, \quad k, a \in V_{128};$$

$$S : V_{128} \rightarrow V_{128}, \quad S(a) = S(a_{15} \parallel \dots \parallel a_0) = \pi(a_{15}) \parallel \dots \parallel \pi(a_0),$$

where $a = a_{15} \parallel \dots \parallel a_0 \in V_{128}, a_i \in V_8, i = 0, 1, \dots, 15$;

$S^{-1} : V_{128} \rightarrow V_{128}$, an inverse transformation for S , which may be evaluated, for example, as follows:
 $S^{-1}(a) = S^{-1}(a_{15} \parallel \dots \parallel a_0) = \pi^{-1}(a_{15}) \parallel \dots \parallel \pi^{-1}(a_0)$,
 where $a = a_{15} \parallel \dots \parallel a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, 1, \dots, 15$,
 π^{-1} – an inverse substitution for π ;
 $R : V_{128} \rightarrow V_{128}$, $R(a) = R(a_{15} \parallel \dots \parallel a_0) = l(a_{15}, \dots, a_0) \parallel a_{15} \parallel \dots \parallel a_1$,
 where $a = a_{15} \parallel \dots \parallel a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, 1, \dots, 15$;
 $L : V_{128} \rightarrow V_{128}$, $L(a) = R^{16}(a)$;
 $R^{-1} : V_{128} \rightarrow V_{128}$, an inverse transformation for R , which may be evaluated,
 for example, as follows: $R^{-1}(a) = R^{-1}(a_{15} \parallel \dots \parallel a_0) =$
 $= a_{14} \parallel a_{13} \parallel \dots \parallel a_0 \parallel l(a_{14}, a_{13}, \dots, a_0, a_{15})$,
 where $a = a_{15} \parallel \dots \parallel a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, 1, \dots, 15$;
 $L^{-1} : V_{128} \rightarrow V_{128}$, $L^{-1}(a) = (R^{-1})^{16}(a)$;
 $F[C] : V_{128}^2 \rightarrow V_{128}^2$, $F[C](a_1, a_0) = (LSX[C](a_1) \oplus a_0, a_1)$, where $C \in V_{128}$,
 $a_0, a_1 \in V_{128}$.

2.3. Key schedule

The round constants $C_i \in V_{128}$, $i = 1, 2, \dots, 32$, defined as

$$C_i = L(V_{128}(i)), \quad i = 1, 2, \dots, 32,$$

are used in the key schedule.

The round keys $K_i \in V_{128}$, $i = 1, 2, \dots, 10$, are derived from a master-key $K \in V_{256}$ as follows:

$$K_1 \parallel K_2 = K;$$

$$(K_{2i+1}, K_{2i+2}) = F[C_{8(i-1)+8}] \dots F[C_{8(i-1)+1}](K_{2i-1}, K_{2i}), \quad i = 1, 2, 3, 4.$$

2.4. Encryption algorithm

A 128-bit plain text $a \in V_{128}$ is encrypted as follows:

$$E_{K_1, \dots, K_{10}}(a) = X[K_{10}]LSX[K_9] \dots LSX[K_2]LSX[K_1](a).$$

2.5. Decryption algorithm

A 128-bit cipher text $b \in V_{128}$ is decrypted as follows

$$D_{K_1, \dots, K_{10}}(b) = X[K_1]S^{-1}L^{-1}X[K_2] \dots S^{-1}L^{-1}X[K_9]S^{-1}L^{-1}X[K_{10}](b).$$

References

- [1] *GOST 28147-89. Information Processing Systems. Cryptographic Protection. Cryptographic Transformation Algorithm* (in Russian).
- [1] Poschmann A., Ling S., Wang H., “256 bit standardized Crypto for 650 GE – GOST Revisited”, *CHES*, Lect. Notes Comput. Sci., **6225**, 2010, 219–233.
- [2] Isobe T., “A single-key attack on the full GOST block cipher”, *FSE 2011*, Lect. Notes Comput. Sci., **6733**, 290–305.
- [3] Dinur I., Dunkelman O., Shamir A., *Improved attacks on full GOST*, Cryptology ePrint Archive, Report 2011/558, 2011, <http://eprint.iacr.org/2011/558>.
- [4] *ISO/IEC JTC 1/SC 27 Standing Document 12 (SD12) on the Assessment of cryptographic algorithms and key lengths* <http://www.jtc1sc27.din.de/sbe/SD12>.
- [5] Dygin D.M., Dmukh A.A., Marshalko G.B., “A lightweight-friendly modification of GOST block cipher”, *Математические вопросы криптографии*, **5:2**, 47–55.
- [6] Shishkin V.A., “Design principles of a prospective block cipher with 128 bit block length”, Presentation at RusCrypto’2013 (in Russian <http://www.ruscrypto.ru/resource/summary/rc2013>).