Evaluation of the Maximum Productivity for Block Encryption Algorithms

Authors: V.M. Fomichev, **A.M. Koreneva**, D.I. Zadorozhniy, A.R. Miftahutdinova

Introduction

Block ciphers are used for encryption of **large volumes of data**.

The relevant task is to construct **high-performance block encryption algorithms** based on SP-networks, Feistel networks, on some of its generalizations, etc.

The main factors determining the encryption productivity:

- **size of data blocks,**
- **computational complexity of round implementation,**
- **number of encryption rounds.**

One of the important tasks is **to find compromise** between cryptographic strength and encryption productivity.

We propose <u>**a mathematical idea**</u> that allows **to increase** the encryption productivity, **to estimate** the number of rounds and **to compare** block algorithms from a particular class in terms of achieving a certain maximum productivity.

Block algorithms under research

We consider block algorithms based on ***R*(*n*,*r*,*m*)** class of autonomous shift register **of length *n*** with ***m* feedbacks** over the set V_r of all **binary vectors of length *r*** (further – ***R*-type** algorithms). For example, the class $R(2,r,1)$ is associated with original Feistel network; $R(n,r,1)$ – with GFN-1.

For simplicity, we imply that the register **feedbacks are the same** and implemented by the function $\boldsymbol{f(x_1,\ldots,x_r)}$ for $m>1$.

Denote by ***g* – round transformation** based on *R*-type register.

We research the productivity of *R*-type algorithms depending on the following characteristics:

- size of data blocks (the value of ***nr***)
- amount of feedbacks (the value of ***m***)
- value of exponent of mixing digraph $\Gamma(g)$

The exponent ($\exp\Gamma(g)$) – the smallest positive integer t such that $M(g)^t>0$, where $M(g)$ is an adjacency matrix associated with $\Gamma(g)$.

Theoretical evaluation of productivity (1)

Notation:

$\tau(f)$ – time (in *sec*) of calculating the value of the function $f(x_1,\ldots,x_r)$ (we assume that the time is the same regardless of the input);

$\pi(n,r,m,h)$ – productivity of h-round R-type algorithm (in *bits per second*);

$v(g,n,r,m)$ – maximum productivity of R-type algorithm with the round transformation g.

Proposition 1. If the time of implementation for the shift of blocks is substantially less than $\tau(f)$, then

$$\pi(n,r,m,h) \approx nr/hm\tau(f).$$

Proposition 2. The following is correct:

$$v(n,r,m,g) \approx nr/h_0m\tau(f),$$

where $h_0=\exp\Gamma(g)+\exp\Gamma(g^{-1}) - 1$.

Theoretical evaluation of productivity (2)

The mixing digraph $\Gamma(g)$ has nr vertices (in practical cases, at least 64 and can reach 1024 or more).

For large values of nr (for example, if $n \geq 8$ and $r \geq 32$) it is convenient to consider **the block mixing digraph $\Gamma_B(g)$** with n vertices ($2 \leq n \leq 32$ in our cases).

In accordance with the definition, $\mathbf{\exp\Gamma_B(g) \leq \exp\Gamma(g)}$ and these values are close in many cases.

Hence, the upper bound for the maximum encryption productivity of R-type algorithm:

$$\boldsymbol{v(n,r,m,g) \leq nr/h_b m\tau(f)},$$

where $h_b = \exp\Gamma_B(g) + \exp\Gamma_B(g^{-1}) - 1$.

Theoretical evaluation of productivity (3)

The maximum encryption productivity of *R*-type algorithms **depends on the characteristics** of the round transformation *g*.

So the relevant problem is to describe *R*-type shift registers in terms of achieving a certain maximum productivity.

Important tasks in this context are as follows:

- choice of the feedback function with the relatively **small value of $\tau(f)$**;
- determination of the **ratio of n and m**, such that the **value of $h_0 m$ is the least**.

Classes of algorithms under research (1)

We considered 5 classes of R-type algorithms:

***R*(8,32,3), *R*(15,32,5), *R*(16,32,5), *R*(30,32,9) and *R*(32,32,9).**

Further we use the following notation:

$R(8,32,3)$ – 256-3,
$R(15,32,5)$ – 480-5,
$R(16,32,5)$ – 512-5,
$R(30,32,9)$ – 960-9,
$R(32,32,9)$ – 1024-9.

The round transformation g should provide (in the context of our research) the following properties:

- bijectivity,
- nonlinearity of all the coordinate functions,
- the smallest (or close to) value of $\exp \Gamma(g)$.

Determination of functions

Round transformation g is the register transformation over the set V_{32*n} with the same feedback functions:

$$\boldsymbol{f(S, q_j) \boxplus X_k},$$

where $\boxplus$ – addition modulo 2^{32},

$\boldsymbol{S}$ **– sum modulo $\mathbf{2^{32}}$** of the some subblocks of the input block $X=(X_1,\ldots,X_n)$,

$\boldsymbol{X_k}$ – **subblock**, $k\in\{1,\ldots,n\}$,

$\boldsymbol{q_j}$ – **round key**, $\mathbf{1\leq \boldsymbol{j} \leq \boldsymbol{m}}$.

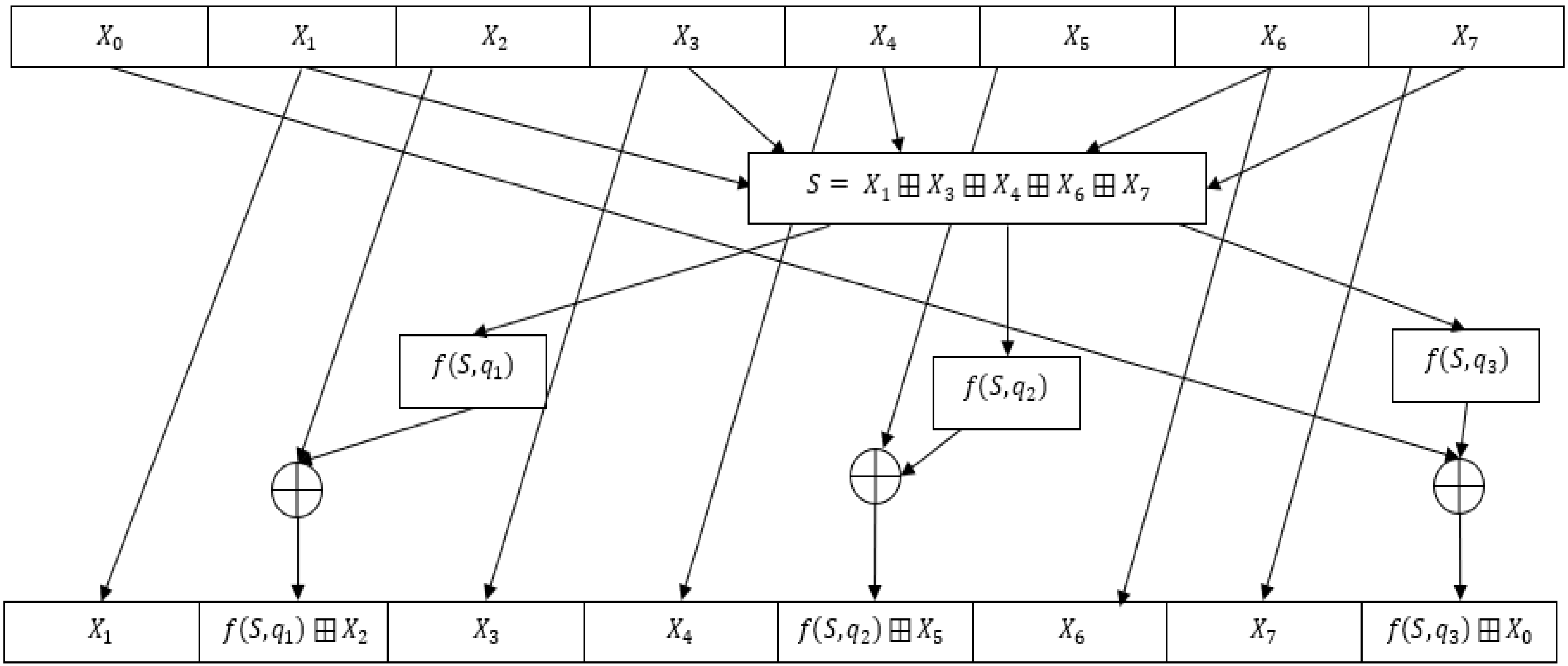
The function f is similar to the function of GOST 28147-89:

$$\boldsymbol{f(S, q_j)=T^{11}(sbox_{8,4}(S \boxplus q_j))}, \tag{1}$$

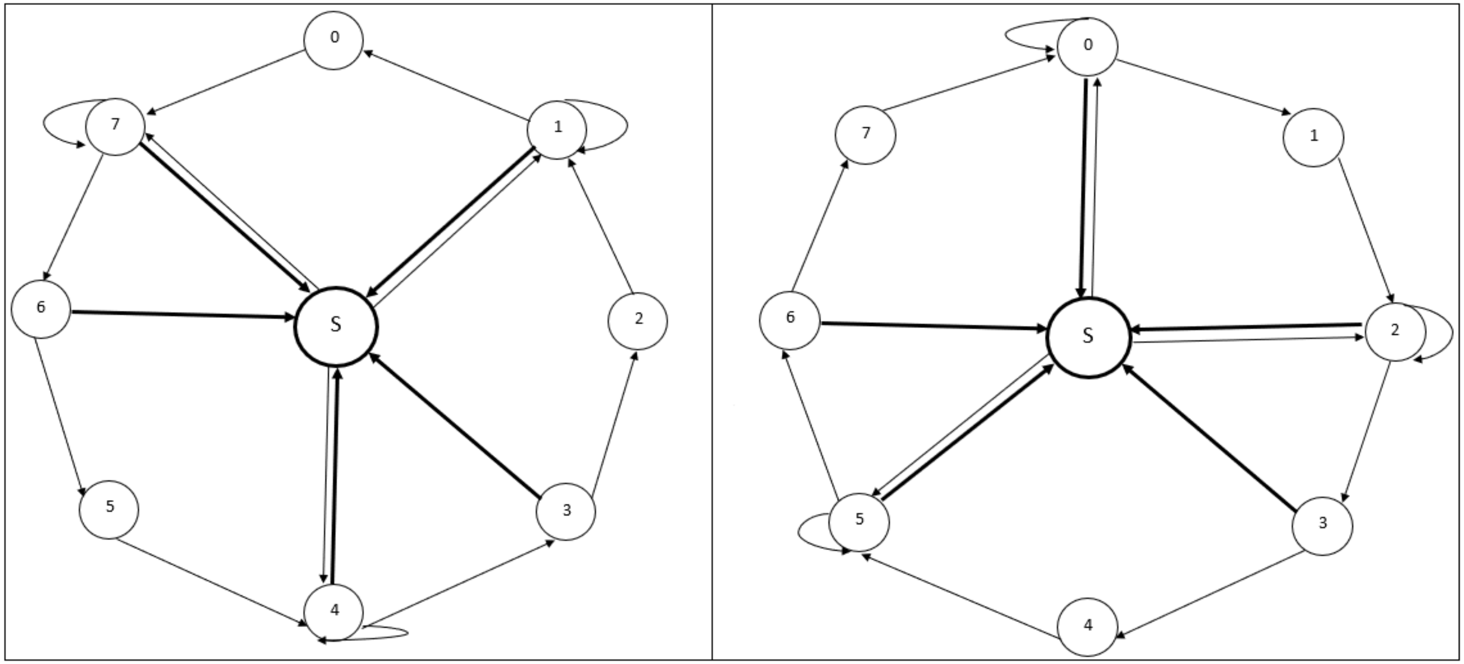
where $\boldsymbol{T^{11}}$ – 11-bit circular shift towards most significant bits,

$\boldsymbol{sbox_{8,4}}$ – 8 s-boxes of size 4x4 of GOST 28147-89.

Round of the 256-3 algorithm



Estimation the number of rounds by h_b



$\exp\Gamma_B(g) = 4$
$\exp\Gamma_B(g^{-1})=4$
$h_b= 7$

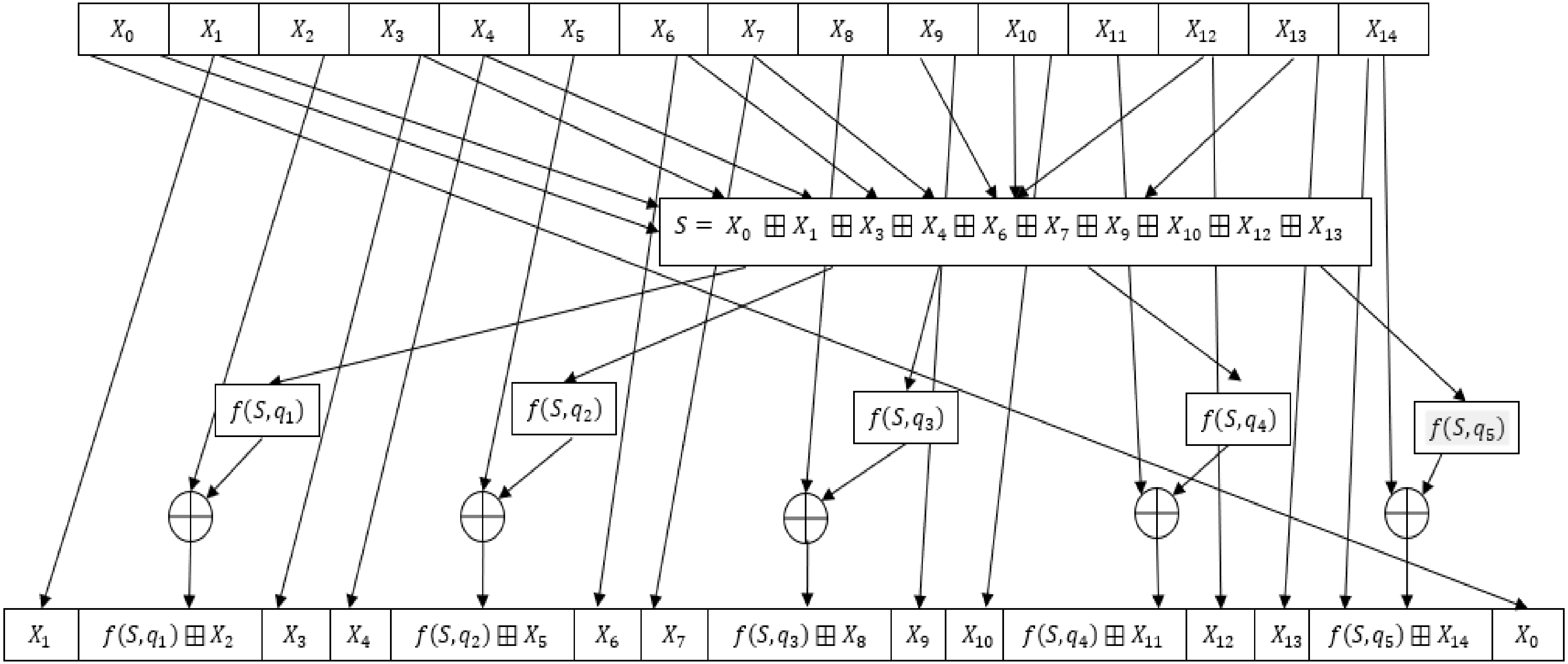
Block mixing digraphs $\Gamma_B(g)$ and $\Gamma_B(g^{-1})$ of the 256-3 algorithm

Bold arrows (i,S) indicate that the subblock X_i is used to calculate the sum S (mod 2^{32}) ; arrows (S,j) indicate that the sum S (mod 2^{32}) is used to calculate X_j , $0 \le i,j \le 7$.

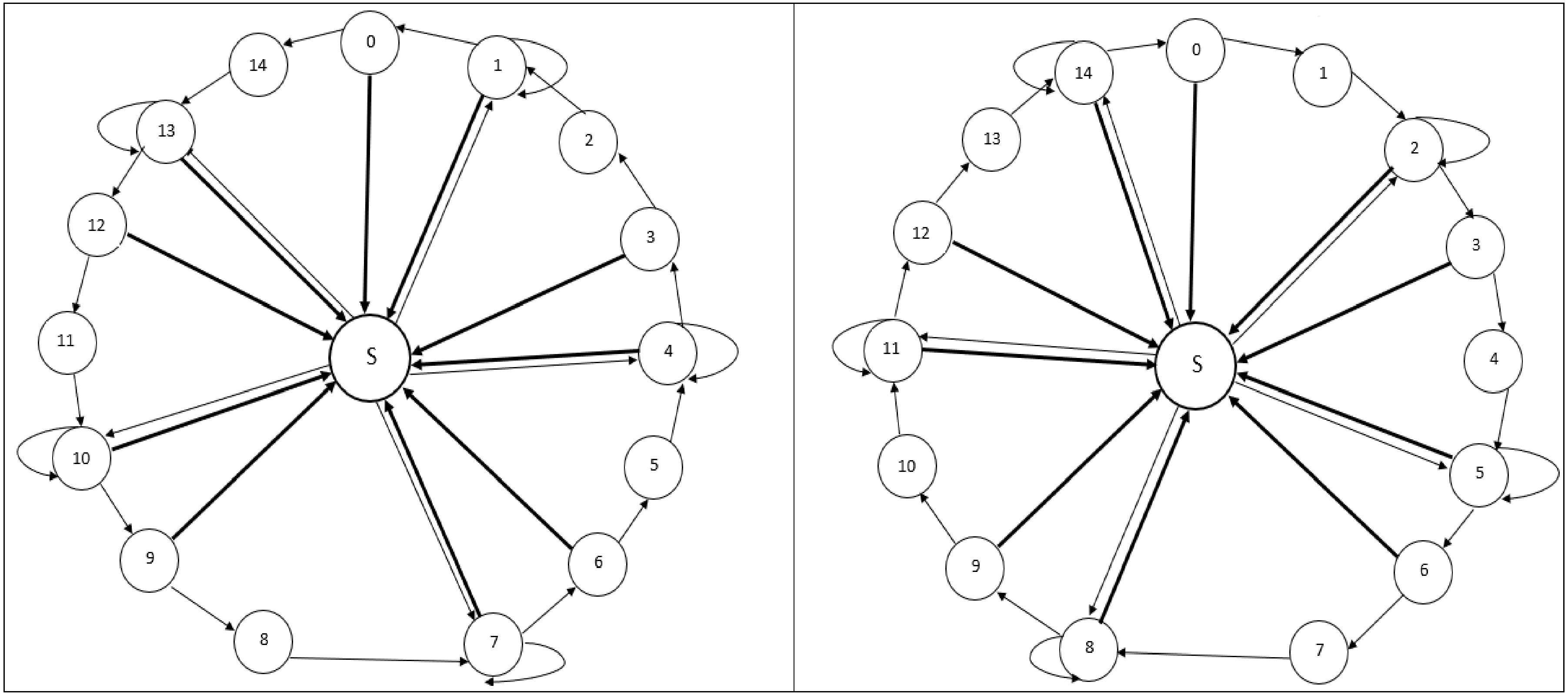
Thus, an **arc in block mixing digraph** is either a simple arrow (not bold), or a concatenation of the **bold** arrow with a simple arrow.

For example, the shortest path from 0 to 0 is the path (0,7,1,0) of length 3.

Round of the 480-5 algorithm



Estimation the number of rounds by h_b



Block mixing digraphs $\Gamma_B(g)$ and $\Gamma_B(g^{-1})$ of the 480-5 algorithm

$$\exp\Gamma_B(g) = \exp\Gamma_B(g^{-1}) = 5,$$

$$\boldsymbol{h_b = 9.}$$

Experimental evaluation of encryption productivity

Our assumptions:

- The evaluation of productivity is given in comparison with GOST 28147-89
- We use only ECB-mode for encryption of the same plaintext of length $T = 21120$ bytes
- The time $\tau(f)$ of computation of the value of the function $f(x_1,\dots,x_r)$ is estimated by the value of 0.001 seconds for each considered algorithm (256-3, 480-5, 512-5, 960-9, 1024-9)
- For all algorithms except GOST 28147-89, we assumed that each bit of the round key depends on all bits of the encryption key

Evaluation of productivity

Algorithm	Number of rounds, h_b	Theoretically gain in productivity, *number of times*	Practically gain in productivity, *number of times*
GOST 28147-89	17	1	1
256-3	7	3,238	3,635
480-5	7	3,643	4,008
512-5	9	3,022	3,444
960-9	9	3,148	3,522
1024-9	9	3,358	3,956

We obtain (experimentally) that the **encryption productivity is close to the maximum** when the number *m* of feedback functions is defined by the equation:

$$\boldsymbol{m = \lceil n/4 \rceil + 1.}$$

The 480-5 algorithm has the highest maximum productivity.

Conclusion

- We **proposed a characteristic** for estimation of the maximum performance of block encryption algorithms, that **can be used to determine the parameters** for *R*-type block encryption algorithms.
- We **determined the most productive algorithm** in the class under research: the algorithm based on the shift register of length 15 with 5 feedbacks over V_{32}.

The obtained estimations show that with increasing the input block size up to 1024 bits (the number of feedbacks of high-performance algorithms grows more slowly, reaching 9), **the maximum encryption performance grows, but slower than the block size.**

Thank you!

email: a.koreneva@securitycode.ru