SECURITY EVALUATION FOR SNOW 2.0-LIKE STREAM CIPHERS AGAINST CORRELATION ATTACKS OVER EXTENSION FIELDS

A. N. Alekseychuk[*], S. M. Koniushok[**], M. V. Poremskyi[***]

Institute of Special Communication and Information Security,
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»

[*]alex-dtn@ukr.net [**]3tooth@iszzi.kpi.ua [***]undermyclouds@gmail.com

Abstract: We propose a general method for security evaluation of SNOW 2.0-like ciphers against correlation attacks that are built similarly to known attacks on SNOW 2.0. Unlike previously known methods, the method we propose is targeted at security proof and allows obtaining lower bounds for efficiency of attacks from the class under consideration directly using parameters of stream cipher components similarly to techniques for security proofs of block ciphers against linear cryptanalysis.

The method proposed is based upon automata-theoretic approach to evaluation the imbalance of discrete functions. In particular, we obtain a matrix representation and upper bounds for imbalance of an arbitrary discrete function being realized by a sequence of finite automata. These results generalize a number of previously known statements on matrix (linear) representations for imbalance of functions having specified forms, and may be applied to security proofs for other stream ciphers against correlation attacks.

Application of this method to SNOW 2.0 and Strumok ciphers shows that any of the considered correlation attacks on them over the field of the order 256 has an average time complexity not less than $2^{146.20}$ and $2^{249.40}$ respectively, and requires not less than $2^{142.77}$ and, respectively, $2^{249.38}$ keystream symbols.

Key words: symmetric cryptography, stream cipher, correlation attack, system of noised linear equations, discrete Fourier transform, proof of security, SNOW 2.0, Strumok.

Introduction

The stream cipher SNOW 2.0 [1] was proposed in 2002 as an alternative of a previous (weaker) version SNOW. At the moment, this cipher is standardized [2] and is one of the fastest software oriented stream ciphers.

The most powerful of the known attacks on SNOW 2.0 are correlation attacks, the essence of which is to compile and to solve systems of noised linear equations, in particular, systems of equations over the fields of order larger than 2 [3 – 7]. Despite certain progress in this direction, there are some unsolved problems related to development of methods for security evaluation and security proof of SNOW 2.0-like stream ciphers against correlation attacks. At the moment, there are no methods that would allow proving security of the mentioned ciphers against known correlation attacks directly using parameters of their components. Besides, an attempt to extend the known methods for security evaluation of SNOW 2.0 against correlation attacks for some other stream ciphers (e.g. Strumok that was proposed as a candidate for a national standard of stream encryption [8]) encountered difficulties related to the scale of problems to be resolved to obtain the bounds. Unlike SNOW 2.0 that is built over the field of the order 2^{32}, the Strumok cipher is built over the field of the order 2^{64} that results in impossibility of practical application of certain algorithms [4, 5, 7] complexity of which increases from $2^{32} \div 2^{37}$ to 2^{64} bit operations.

In this paper, we present methods allowing practical evaluation and proving security of SNOW 2.0-like stream ciphers against a wide class of correlation attacks.

In Section 1, we adduce the definition of SNOW 2.0-like stream ciphers and of a number of related concepts. Note that Section 1 considers ciphers of a more general form than those proposed in [9]. In particular, we define binary ciphers that differ from previously defined (modular) ciphers [9] by replacement the addition modulo powers of 2 with coordinate-wise XOR operation of binary vectors. Binary ciphers may be regarded as simplified versions of the respective modular ciphers (that include SNOW 2.0 and Strumok), however their research is of independent interest. In particular, as shown in Section 3, there exist (quite practical) binary SNOW 2.0-like ciphers that are proved to be secure against known correlation attacks.

In Section 2, based upon [7], we describe a class of attacks considered in the following sections. Unlike [7], we use for description of these attacks (or rather, of the systems of noised equations solving of which presents the essence of the mentioned attacks) the trace function from a finite field into its sub-field. That enables obtaining a description that is more useful for further analysis, in particular, to set an analytical expression for the parameter that determines the efficiency of a correlation attack in terms of Fourier coefficients of noise distribution in the right-hand sides of the relevant system of equations.

The main result of Section 2 is Theorem 1 allowing to reduce the problem of obtaining lower bounds for the time complexity of a correlation attack from the specified class and also for the size of the keystream needed for its successful implementation to construction upper bounds for the maximum modules of Fourier coefficients of noise distribution in the right-hand sides of equations in a system not depending on a specific attack.

We also study the relation between efficiency of attacks over fields of order $2^{r'}$, where $r' > 1$, and ordinary binary attacks that are built over the field of two elements. We show that the transition from binary correlation attacks to attacks over fields of order $2^{r'}$ may increase efficiency of the former not more than $2^{r'}$ times.

In Section 3, we obtain lower bounds of the time and data complexities needed for successful implementation of correlation attacks on ordinary binary SNOW 2.0-like stream ciphers. Expressions for obtained bounds depend on parameters that are traditionally used for security evaluation of block ciphers against linear cryptanalysis:

the maximal elements of linear approximations tables of s-boxes and the branch number of the linear transform used in the encryption algorithm. Application of these bounds to binary versions of SNOW 2.0 and Strumok ciphers shows that any correlation attack (from the specified class) on them over the field of the order 256 has average time complexity not less than $2^{146.20}$ and $2^{249.40}$ respectively, and requires not less than $2^{142.77}$ and, respectively, $2^{249.38}$ keystream symbols.

Results extension of Section 3 for modular SNOW 2.0-like ciphers encountered difficulties associated with application in such ciphers the addition of binary integers modulo power of two. Methods developed to overcome these difficulties [4, 5, 7] require calculation of probability distributions of noise in the right-hand sides of systems of equations used in correlation attacks and appear to be inapplicable when the order of the field over which the cipher is defined is 2^{64} or more (e.g. for Strumok). Besides, these methods are focused on the construction of specific attacks and not on proof of security of SNOW 2.0-like ciphers, so their use for the purpose of proof of security, even in the case of SNOW 2.0 cipher, leads to a large amount of computations.

To overcome these drawbacks, we propose in Section 4 an automata-theoretic approach to construction upper bounds for imbalance of discrete functions being realized by sequences of finite automata. The source of this approach is the paper [10], where a matrix representation is obtained for the preimages' number of the output sequence of a finite automaton; however, in the case discussed below we deal not with the distribution of the number of preimages, but with Fourier coefficients of this distribution.

The main results of Section 4 are Theorems 5, 6 and 7, the first of which generalizes a series of separate results on matrix (or linear) representations of the imbalance of maps that are implemented by automata of special forms [4, 11], and the second and the third provide upper bounds of imbalance that can be used, in particular, for proof the security of ordinary modular SNOW 2.0-like ciphers against correlation attacks.

In Section 5, by means of Theorem 7 we obtain lower bounds for the time complexity and the size of the keystream needed for successful implementation correlation attacks on ordinary modular SNOW 2.0-like ciphers. Expressions for the obtained bounds depend on certain parameters of s-boxes that may be considered as modified elements of their linear approximations tables, and also on the branch number of the linear transform used in the encryption algorithm. Application of the obtained bounds to SNOW 2.0 and Strumok leads to the results that coincide with the results obtained for their binary versions: any correlation attack on the mentioned ciphers (from the specified class of attacks) over the field of the order 256 has an average time complexity not less than $2^{146.20}$ and $2^{249.40}$ respectively and requires not less than $2^{142.77}$ and, respectively, $2^{249.38}$ keystream symbols.

Note that certain results of this paper, in particular, those in Sections 2 and 4, are applicable not only to SNOW 2.0-like ciphers and can be used to solve other problems of the correlation cryptanalysis of symmetric encryption schemes.

1 SNOW 2.0-like stream ciphers

For any natural r, let us denote by V_r the set of binary vectors of the length r. Let us stipulate on this set the structure of the field F_{2^r} (of the order 2^r) agreed with the operation $\oplus$ of the coordinate-wise Boolean addition of binary vectors. Let us identify the elements of the set V_r with r-bit integers assuming that the number $x_1 + 2x_2 + \cdots + 2^{r-1}x_r$ corresponds to the vector $x = (x_1, x_2, \ldots, x_r) \in V_r$, and let us denote by $\overset{r}{+}$ the addition operation of these numbers modulo 2^r.

By definition, *the initial data for construction of the keystream generator of a SNOW 2.0-like stream cipher* are the following objects (Figure 1):

- a primitive polynomial $g(z) = z^n \oplus c_{n-1}z^{n-1} \oplus \ldots \oplus c_0$ over the field F_{2^r};
- a permutation $\sigma : V_r \to V_r$;
- a natural number $\mu \in \overline{1, n-2}$;
- a commutative group operation $*$ on the set V_r.

The keystream generator is a finite autonomous automaton with the set of states ${V_r}^n \times {V_r}^2$, the next state function

$$h((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = ((x_n, x_{n-1}, \ldots, x_1), x_\mu * v, \sigma(u)),$$

and the output function

$$f((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = x_0 \oplus (x_{n-1} * u) \oplus v,$$

where $x_0, \ldots, x_{n-1}, u, v \in V_r$, $x_n = c_{n-1}x_{n-1} \oplus \ldots \oplus c_0 x_0$. So, the keystream symbol γ_i at the time i is determined by the initial state $((x_{n-1}, x_{n-2}, \ldots, x_0), u_0, v_0)$ of the generator by means of the recurrent relations

$$\gamma_i = x_i \oplus (x_{i+n-1} * u_i) \oplus v_i, \tag{1}$$

$$u_{i+1} = x_{i+\mu} * v_i, \; v_{i+1} = \sigma(u_i) \tag{2}$$

valid for all $i = 0, 1, \ldots$.

Starting from Section 3, we consider only SNOW 2.0-like stream ciphers that satisfy the condition $* \in \{\oplus, \overset{r}{+}\}$. A cipher is called *binary*, if $* = \oplus$ and *modular*, if

$* = \overset{r}{+}$, where $r \geq 2$.

A SNOW 2.0-like cipher is called *ordinary,* if there exist integer numbers $p, t \geq 2$ such that $r = pt$, a basis B of the field F_{2^r} over the field F_{2^t}, permutations $s_i : F_{2^t} \to F_{2^t}$, $i \in \overline{0,\ p-1}$, and a reversible $p \times p$-matrix D over the field F_{2^t} such that if elements z and $\sigma(z)$ of the field F_{2^r} are identified with the vectors of their coordinates in the basis B the following equality holds:

$$\sigma(z) = (s_0(z_0), \ldots, s_{p-1}(z_{p-1}))D,\ z = (z_0, \ldots, z_{p-1}) \in F_{2^t}^{\,p}. \tag{3}$$

Usually, the permutations $s_i : F_{2^t} \to F_{2^t}$, $i \in \overline{0,\ p-1}$ are called *s-boxes* of the cipher under consideration.

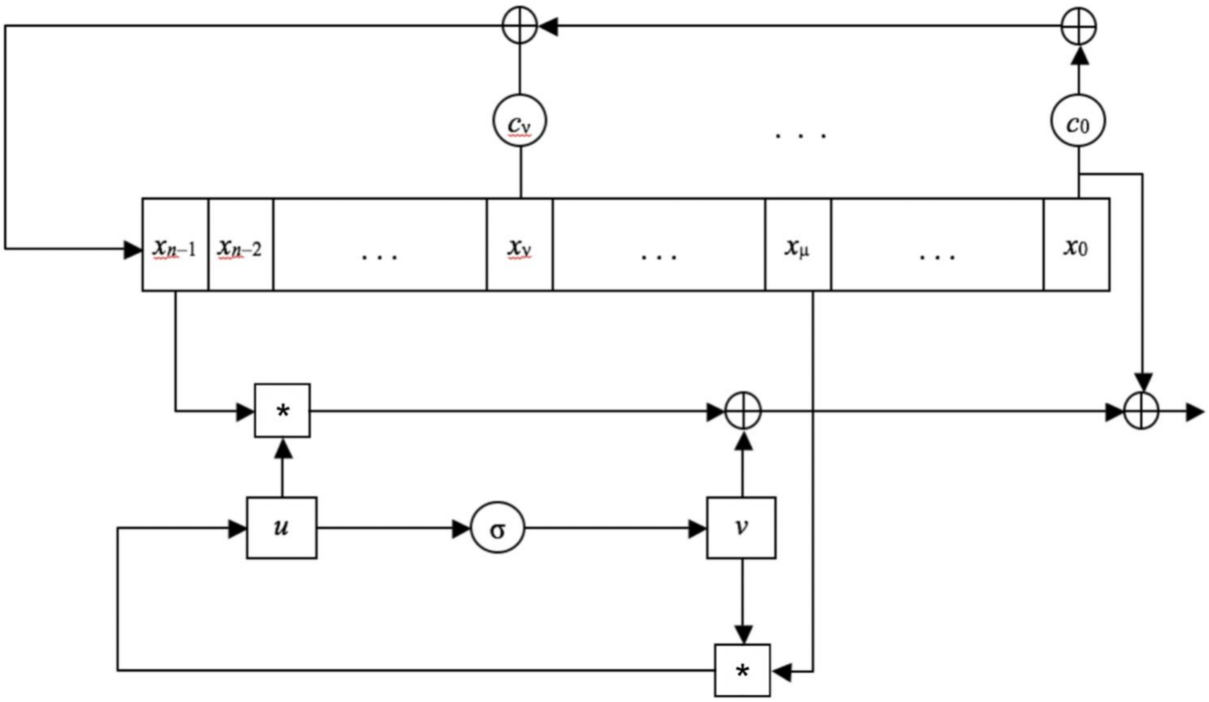

Figure 1. Scheme of the keystream generator for a SNOW 2.0-like stream cipher

Example 1. SNOW 2.0 [1] is an ordinary modular cipher with the parameters $t = 8$, $p = 4$ ($r = 32$). Here $n = 16$, $\mu = 5$, and the s-boxes s_i, $i \in \overline{0,\ p-1}$ and the matrix D are defined in the same way as in the round transform of Rijndael [12].

Example 2. The stream cipher Strumok [8] is an ordinary modular SNOW 2.0-like cipher with the parameters $t = 8$, $p = 8$ ($r = 64$). Here $n = 16$, $\mu = 13$, and the s-boxes s_i, $i \in \overline{0,\ p-1}$ and the matrix D are defined in the same way as for Kalyna block cipher [13, 14].

2 Correlation attacks on SNOW 2.0-like stream ciphers

2.1 Construction of systems of noised linear equations for correlation attacks. Practically all known correlation attacks on SNOW 2.0 [3 – 7] are based on the feature that the sum of keystream symbols in any successive times is a result of a symbol distortion in a linear recurring sequence over the field F_{2^r} by which one can directly recover the initial state of the LFSR in Figure 1. For an arbitrary SNOW 2.0-like stream cipher we obtain from (1), (2):

$$\gamma_i \oplus \gamma_{i+1} = x_i \oplus x_{i+1} \oplus x_{i+\mu} \oplus x_{i+n-1} \oplus x_{i+n} \oplus \xi_i\,,\ i = 0, 1, ..., \tag{4}$$

where

$$\xi_i = ((x_{i+n-1} * u_i) \oplus x_{i+n-1} \oplus \sigma(u_i)) \oplus$$

$$\oplus ((x_{i+n} * x_{i+\mu} * v_i) \oplus (x_{i+n} \oplus x_{i+\mu} \oplus v_i)),\ i = 0, 1, ... \tag{5}$$

Assuming that $x_{i+\mu}, x_{i+n-1}, x_{i+n}, u_i, v_i$ in (5) are independent random variables with uniform distribution on the set V_r and presenting the symbols $x_i, x_{i+1}, x_{i+\mu}, x_{i+n-1}, x_{i+n}$ of the linear recurring sequence through the initial state of the LFSR in Figure 1 we obtain the system (4) of noised linear equations over the field F_{2^r}, where distortions (i.e., the noisy symbols) are random variables (5).

Let us describe a method for construction of consequences for system (4) that are used further in correlation attacks on SNOW 2.0-like stream ciphers.

Let's write the first N equations of the system (4) in the form

$$b_i = A_i a \oplus \xi_i\,,\ i \in \overline{0, N-1}\,, \tag{6}$$

where $b_i = \gamma_i \oplus \gamma_{i+1}$, $A_i a = x_i \oplus x_{i+1} \oplus x_{i+\mu} \oplus x_{i+n-1} \oplus x_{i+n}$, A_i is a known row vector of the length n over the field F_{2^r}, and $a = (x_0, ..., x_{n-1})^T$ is the *target solution* of the system (4), i.e., the unknown column vector equal to the initial state of the LFSR in Figure 1 .

Let us fix an arbitrary (positive) divisor r' of the number r and let us denote by $\mathrm{Tr}^{2^r}_{2^{r'}}(z) = z \oplus z^{2^{r'}} \oplus \cdots \oplus z^{2^{r'(r''-1)}}$ the trace of the element $z \in F_{2^r}$ in the field $F_{2^{r'}}$, where $r'r'' = r$.

Let us recall (see e.g. [15], Definition 2.30) that the bases $\mathrm{B} = \{b_1, ..., b_{r''}\}$ and $\hat{\mathrm{B}} = \{\hat{b}_1, ..., \hat{b}_{r''}\}$ of the field F_{2^r} over the sub-field $F_{2^{r'}}$ are called *dual* if $\mathrm{Tr}^{2^r}_{2^{r'}}(b_i \hat{b}_j) = 1$ when $i = j$, $\mathrm{Tr}^{2^r}_{2^{r'}}(b_i \hat{b}_j) = 0$ if otherwise. It follows from this definition that the trace of the product of arbitrary elements from the field F_{2^r} coincides with the dot product of vectors of their coordinates in (any) dual bases.

To construct a consequence of the system (6) let us fix an element $c \in F_{2^r} \setminus \{0\}$ and a pair of dual bases B and $\hat{\mathrm{B}}$ of the field F_{2^r} over the sub-field $F_{2^{r'}}$. Observe that the equalities $\mathrm{Tr}_{2^{r'}}^{2^r}(cb_i) = \mathrm{Tr}_{2^{r'}}^{2^r}(A_i(ca)) \oplus \mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i)$, $i \in \overline{0, N-1}$ follow from equalities (6) and $\mathrm{Tr}_{2^{r'}}^{2^r}(A_i(ca))$ is the dot product over $F_{2^{r'}}$ of the vectors A_i' and a' that can be received by substitution of each coordinate of the vector A_i (respectively, of the vector ca) with its representation in the basis B (respectively, in the basis $\hat{\mathrm{B}}$). Whence the vector $a' \in F_{2^{r'}}{}^{nr''}$ coincides with the target solution of the following system of the noised linear equations:

$$A_i' x = b_i' = A_i' a' \oplus \eta_i, \; i \in \overline{0, N-1}, \tag{7}$$

where $b_i' = \mathrm{Tr}_{2^{r'}}^{2^r}(cb_i)$, $\eta_i = \mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i)$ for each $i \in \overline{0, N-1}$.

Thus, to recover the vector a from the system of equations (4) it is sufficient to construct for the previously chosen r' and c the system of equations (7) over the field $F_{2^{r'}}$, and to recover its target solution a' by one of the known methods. Knowing the vector a' and the basis $\hat{\mathrm{B}}$, it is easy to find the vector ca, and thus also the required vector a.

Note that all known correlation attacks on SNOW 2.0 are based upon solving the systems of noised equations having the mentioned form (however, without explicit utilization of the trace function) or consequences of such systems that are linear combinations of their separate equations. In particular, the papers [3, 4, 6] contain consideration of Boolean systems of noised linear equations ($r' = 1$) that are obtained from (4) by certain linear transforms over the field F_2, and the paper [7] contains consideration of similar systems of equations over the field of the order 2^8 ($r' = 8$). Besides, [5] proposes to use direct the system (4) over the field $F_{2^{32}}$ for construction a distinguishing attack on SNOW 2.0.

2.2 An algorithm for solving the obtained systems of noised linear equations. At the moment, there are a lot of fast (sub-exponential) algorithms for solving systems of noised linear equations over the field of two elements (see e.g. [7, 16 – 18]). Some of them allow natural generalizations for systems over finite fields or even over arbitrary finite rings [19].

Subsequently, we will assume that when carrying out a correlation attack on a SNOW 2.0-like cipher the algorithm proposed in [7] will be used to solve the system of equations (7).

The mentioned algorithm depends on parameters $k \geq 2$ (that is a power of two) and $l' \in \overline{1,l}$, where $l = nr''$, and consists of two stages.

At the first stage, Wagner's k-tree algorithm [20] is used to exclude the last $l - l'$ unknowns from the system (7). As a result, we obtain a new noised system of equations with l' unknowns over the field $F_{2^{r'}}$, each equation of which is the sum of certain k equations of the input system. At the second stage, the obtained system is solved by the maximum likelihood method with application of the fast Hadamard (or Walsh) transform. Thus, the mentioned algorithm allows to recover the first l' unknowns of the system of equations (7). Applying it $\lceil l/l' \rceil$ times to various sets of unknowns that do not intersect, we can find the required vector a'.

Observe that the distribution of distortions η_i in the right-hand sides of equations in (7) has the following form:

$$\mathbf{P}\{\eta_i = z\} \;=\; \sum_{x \in F_{2^r}:\ \mathrm{Tr}^{2^r}_{2^{r'}}(cx) = z} \mathbf{P}\{\xi_i = x\},\ z \in F_{2^{r'}}, \tag{8}$$

where the random variable ξ_i is defined by (5), $i \in \overline{0, N-1}$. Besides, the distortion in the right-hand side of each equation in the system that is obtained as a result of the first stage of the algorithm, is the sum of k independent random variables distributed by (8). So, the distribution of distortions in the right-hand sides of equations in the system obtained after the first stage, has the following form:

$$p_{c,r',k}(z) = \mathbf{P}\{\eta_1 \oplus \cdots \oplus \eta_k = z\},\ z \in F_{2^{r'}}. \tag{9}$$

Note also that these distortions are dependent random variables; however, in [7] the heuristic assumption about their independence is used (implicitly). Based on this assumption one can show [19, 21] that to recover the target solution of the system (7) with the error probability not more than $\delta \in (0, 1/2)$ at the second stage of the algorithm it is necessary to have not less than

$$m_{c,r'}(k,l') = \Delta_{c,r'}(k)^{-1}((1-\delta)l'r' - h(\delta))\ln 2$$

equations, where $h(\delta) = -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta)$,

$$\Delta_{c,r'}(k) = 2^{-r'} \sum_{z \in F_{2^{r'}}} (2^{r'} p_{c,r',k}(z) - 1)^2. \tag{10}$$

The following heuristic formula is used in [7] to evaluate the number of equations necessary for successful solving the system of equations at the second stage of the algorithm:

$$m_{c,r'}(k,l') = 2\Delta_{c,r'}(k)^{-1} l'r' \ln 2 . \tag{11}$$

According to [7], the average time complexity of the algorithm (provided an independent et random choice of the rows A_i', $i \in \overline{0, N-1}$) is equal to

$$T_{c,r'}(k,l') = (m_{c,r'}(k,l'))^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} + r'(m_{c,r'}(k,l') + r'l'2^{r'l'}) + 2^{r'(l'+1)} , \tag{12}$$

and the size of the keystream needed for the successful implementation of the algorithm is equal to

$$N = N_{c,r'}(k,l') = k 2^{\frac{r'(l-l')}{\theta}} (2l'r' \ln 2)^{\frac{1}{\theta}} \Delta_{c,r'}(k)^{-\frac{1}{\theta}} , \tag{13}$$

where $\theta = 1 + \log k$ and $m_{c,r'}(k,l')$ has the form (11). It is clear that to improve the efficiency of the algorithm the parameters k and l' should by chosen from the condition of the minimum value (12).

2.3 Expression of the parameter that characterizes efficiency of correlation attacks on SNOW 2.0-like stream ciphers. Below, the term “correlation attack” means one of the attacks described in Sections 2.1, 2.2. Let us recall that each such attack is determined by a divisor r' of the number r and by a non-zero element c of the field F_{2^r}, and consists in construction of the system (7) and its further solving with the algorithm from [7] that depends on the parameters $k \geq 2$ (that is a power of two) and $l' \in \overline{1, l}$, where $l = nr''$, $r'r'' = r$. The average time complexity of the attack is determined by the formula (12) and the data complexity of the attack – by the formula (13).

Both formulas contain the expression of the parameter $\Delta_{c,r'}(k)$ that on the basis of (9), (10) has the following form:

$$\Delta_{c,r'}(k) = 2^{-r'} \sum_{z \in F_{2^{r'}}} (2^{r'} \mathbf{P}\{\eta_1 \oplus \cdots \oplus \eta_k = z\} - 1)^2 , \tag{14}$$

where $\eta_i = \mathrm{Tr}^{2^r}_{2^{r'}}(c\xi_i)$, and the random variables ξ_i are defined by (5), $i \in \overline{1, k}$. Thus, to evaluate the efficiency of correlation attacks on SNOW 2.0-like stream ciphers or for the proof of security of these ciphers against the mentioned attacks it is necessary to be able to calculate (or to evaluate) values of the parameter (14) directly by the cipher components.

Let us obtain an expression of this parameter in terms of Fourier coefficients for the probability distributions of random variables (5).

Let us recall that the Fourier transform of an arbitrary distribution $(p(z): z \in F_{2^m})$ on the field F_{2^m} is defined by the formula

$$\hat{p}(u) = \sum_{z \in F_{2^m}} p(z)(-1)^{\mathrm{Tr}_2^{2^m}(uz)}, \; u \in F_{2^m},$$

where $\mathrm{Tr}_2^{2^m}(x) = x \oplus x^2 \oplus \cdots \oplus x^{2^{m-1}}$ is the absolute trace of $x \in F_{2^m}$. It follows from the Parseval's identity (see e.g. [22]) that

$$2^{-m} \sum_{z \in F_{2^m}} (2^m p(z) - 1)^2 = \sum_{u \in F_{2^m} \setminus \{0\}} |\, \hat{p}(u) \,|^2 . \tag{15}$$

Further, according to the Convolution Theorem [22] the Fourier transform for the distribution of the sum of independent random variables is equal to the product of the Fourier transforms of the summands' distributions. Whence, on the basis of (14), (15) with $m = r'$, $p(z) = \mathbf{P}\{\eta_1 \oplus \cdots \oplus \eta_k = z\}$, $z \in F_{2^{r'}}$ we obtain the equality

$$\Delta_{c,r'}(k) = \sum_{u \in F_{2^{r'}} \setminus \{0\}} |\, \varphi_c(u) \,|^{2k}, \tag{16}$$

where

$$\varphi_c(u) = \sum_{z \in F_{2^{r'}}} \mathbf{P}\{\eta_i = z\}(-1)^{\mathrm{Tr}_2^{2^{r'}}(uz)}, \; u \in F_{2^{r'}} \tag{17}$$

is the Fourier transform of the probability distribution of the random variable $\eta_i = \mathrm{Tr}_{2^{r'}}^{2^r}(c\xi_i)$.

Let us prove that

$$\varphi_c(u) = \hat{\pi}(uc), \; u \in F_{2^{r'}}, \tag{18}$$

where

$$\hat{\pi}(\alpha) = \sum_{x \in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha x)}, \; \alpha \in F_{2^r} \tag{19}$$

is the Fourier transform of the probability distribution of random variables (5).

Indeed, using (17), the condition $u \in F_{2^{r'}}$, and transitivity of the trace function (see e.g. [15], Theorem 2.26) we obtain that

$$\varphi_c(u) = \sum_{z\in F_{2^{r'}}} \mathbf{P}\{\mathrm{Tr}^{2^r}_{2^{r'}}(c\xi_i) = z\}(-1)^{\mathrm{Tr}^{2^{r'}}_2(uz)} = \sum_{z\in F_{2^{r'}}} \sum_{\substack{x\in F_{2^r}: \\ \mathrm{Tr}^{2^r}_{2^{r'}}(cx)=z}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}^{2^{r'}}_2(uz)} =$$

$$= \sum_{x\in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}^{2^{r'}}_2(u\mathrm{Tr}^{2^r}_{2^{r'}}(cx))} = \sum_{x\in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}^{2^{r'}}_2(\mathrm{Tr}^{2^r}_{2^{r'}}(ucx))} =$$

$$= \sum_{x\in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}^{2^r}_2(ucx)} = \hat{\pi}(uc)\,.$$

Thus, the equality (18) is true, and whence on the basis of (16) we obtain the following theorem.

Theorem 1. *The parameter (14) satisfies the equality*

$$\Delta_{c,r'}(k) = \sum_{u\in F_{2^{r'}}\setminus\{0\}} |\,\hat{\pi}(uc)\,|^{2k}\,, \tag{20}$$

where the value $\hat{\pi}(uc)$ *is defined by (19) with* $\alpha = uc$.

The obtained theorem allows us to evaluate the efficiency of correlation attacks on SNOW 2.0-like stream ciphers directly by the Fourier coefficients of the probability distribution of random variables (5) and forms the basis for the results set forth in the following Sections.

2.4 Efficiency comparison of correlation attacks over fields of various orders. Theorem 1 allows to get an answer to the question of how much more efficient (in terms of the average time complexity and data complexity) may be correlation attacks over fields of the order $2^{r'}$, where $r' \geq 2$, in comparison with traditional binary attacks on SNOW 2.0-like stream ciphers.

The following Theorem holds.

Theorem 2. *Let* $r'r'' = r$, *where* $r', r'' \in \mathbf{N}$, $c \in F_{2^r}\setminus\{0\}$, $k = 2^s$, *where* $s \in \mathbf{N}$, $l = nr''$ *and* $l' \in \overline{1,l}$. *Let us denote by* α^* *a non-zero element of the field* F_{2^r} *such that*

$$|\,\hat{\pi}(\alpha^*)\,| = \max_{\alpha\in F^r\setminus\{0\}} |\,\hat{\pi}(\alpha)\,|, \tag{21}$$

where $\hat{\pi}(\alpha)$ *is determined by (19). Then, for the parameters (12) and (13) the following inequalities hold:*

$$T_{c,r'}(k,l') \geq (2^{r'}-1)^{-1} T_{\alpha^*,1}(k,r'l'), \tag{22}$$

$$N_{c,r'}(k,l') \geq (2^{r'}-1)^{-1} N_{\alpha^*,1}(k,r'l') \tag{23}$$

Thus, any correlation attack over the field $F_{2^{r'}}$ (from the class of attacks being considered) is not more than $2^{r'}$ times more efficient (both with respect to the time and the data complexity) in comparison with the best correlation attack over the field F_2.

Proof. On the basis of Theorem 1 and formula (21) the following relation holds:

$$\Delta_{c,r'}(k) = \sum_{u\in F_{2^{r'}}\setminus\{0\}} |\,\hat{\pi}(uc)\,|^{2k} \leq (2^{r'}-1)\,|\,\hat{\pi}(\alpha^*)\,|^{2k} = (2^{r'}-1)\,\Delta_{\alpha^*,1}(k)\,.$$

Using (11), (12) we obtain that

$$T_{c,r'}(k,l') = (2\Delta_{c,r'}(k)^{-1} l'r' \ln 2)^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} +$$

$$+ r'(2\Delta_{c,r'}(k)^{-1} l'r' \ln 2 + r'l' 2^{r'l'}) + 2^{r'(l'+1)} \geq$$

$$\geq (2^{r'}-1)^{-\frac{1}{\theta}} (2\Delta_{\alpha^*,1}(k)^{-1} l'r' \ln 2)^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} +$$

$$+ r'(2^{r'}-1)^{-1}(2\Delta_{\alpha*,1}(k)^{-1} l'r' \ln 2 + r'l' 2^{r'l'}) + 2^{t'(l'+1)}.$$

Further, putting $l'' = r'l'$ and using equalities $r'l = r'nr'' = nr$, $r' \geq 1$ we obtain the following relations:

$$T_{c,r'}(k,l') \geq (2^{r'}-1)^{-1}(2\Delta_{\alpha^*,1}(k)^{-1} l'' \ln 2)^{\frac{1}{\theta}} k 2^{\frac{nr-l''}{\theta}} +$$

$$+ (2^{r'}-1)^{-1}(2\Delta_{\alpha*,1}(k)^{-1} l'' \ln 2 + l'' 2^{l''}) + 2^{l''+1} = (2^{r'}-1)^{-1} T_{\alpha^*,1}(k,l'').$$

So, the inequality (22) is. The inequality (23) may be proved similarly.

Theorem is proved.

Example 3. In [7] a correlation attack over the field F_{2^8} on SNOW 2.0 is suggested that has the average time complexity $2^{164.15}$, requires approximately $2^{163.59}$

keystream symbols, and is significantly faster than the previously known binary attack which time complexity is $2^{212.38}$ [6].

Along with that, on the basis of Theorem 2 there exists a binary correlation attack on SNOW 2.0 that has the average time complexity not more than $2^8 \cdot 2^{164.15} = 2^{172.15}$ and requires not more than $2^8 \cdot 2^{163.59} = 2^{171.59}$ keystream symbols, and the parameters of this attack (the vector α^* and the numbers k and l') can be determined directly by the parameters of the input attack over the field F_{2^8} (see formulas (21), (22)).

The provided example shows that the gain in terms of time complexity of the attack from [7] compared to the attack described in [6] is achieved not so much by application of the field of larger order (F_{2^8} instead of F_2) but to a larger extent as a result of a successful choice of the system of noised linear equations for the attack, and also of application of a more efficient algorithm for solving this system.

In general, according to Theorem 2, transition from binary correlation attacks to attacks over fields of the order $2^{r'}$ can increase the efficiency of the former not more than $2^{r'}$ times.

3 Security evaluation for binary SNOW 2.0-like ciphers against correlation attacks

Let us consider a binary SNOW 2.0-like cipher that is obtained by replacement the operation $*$ in the scheme in Figure 1 by the operation $\oplus$. In this case, the random variable (5) has the form $\xi_i = u_i \oplus \sigma(u_i)$, where u_i is a random vector with the uniform distribution on the set V_r, $i = 0, 1, \ldots$.

Let's receive a condition that guarantees the security of this cipher against correlation attacks (we point out that the term "correlation attack" means solely one of the attacks described in Sections 2.1, 2.2).

By definition from [23] the permutation $\sigma : V_r \to V_r$ is called an *orthomorphism* if the map $u \mapsto u \oplus \sigma(u)$, $u \in V_r$ is also a permutation. A well-known example of an orthomorphism is the map implemented by a 2-round Feistel network:

$$\sigma(u_1, u_2) = (u_1 \oplus \varphi(u_2), u_2 \oplus \varphi(u_1 \oplus \varphi(u_2))),\ u_1, u_2 \in V_m,$$

where $r = 2m$, and φ is a permutation on the set V_m (see e.g. [23]).

Directly from the adduced definition we obtain the following result.

Theorem 3. *Let in the scheme in Figure 1 $* = \oplus$, and σ is an orthomorphism. Then the distortions (5) in the right-hand side of the system of equation (4) are uniformly distributed on the set V_r; so the respective SNOW 2.0-like cipher is secure against (described above) correlation attacks.*

Now we get an analytical expression and an upper bound of the parameter (14) for an arbitrary ordinary binary cipher (see definition in Section 1).

Let us assume that $r = pt$, where $p, t \in \mathbf{N}$, $p, t \geq 2$, and there exist a basis B of the field F_{2^r} over the sub-field F_{2^t}, permutations $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0, p-1}$, and a reversible $p \times p$ -matrix D over the field F_{2^t} such that (with identification the elements z and $\sigma(z)$ of the field F_{2^r} with the sets of their coordinates in the basis B) the equality (3) is satisfied.

Let us denote by $\hat{\mathrm{B}}$ the basis dual to the basis B. Similarly to the above, we will identify an arbitrary element $z \in F_{2^r}$ with the vector $(z_0, \dots, z_{p-1})$ of its coordinates in the basis B, and denote this vector with the same symbol $z = (z_0, \dots, z_{p-1})$. The symbol $\hat{z} = (\hat{z}_0, \dots, \hat{z}_{p-1})$ will denote the vector of coordinates of the element $z \in F_{2^r}$ in the basis $\hat{\mathrm{B}}$. In what follows we will omit the transposition symbol in formulas like Dz^T supposing (as usual) that the vector z is a column if it is written on the right of a matrix D.

For any $z = (z_0, \dots, z_{p-1}) \in F_{2^t}{}^p$ let us denote

$$\mathrm{supp}(z) = \{ j \in \overline{0, p-1} : z_j \neq 0 \},\ wt(z) = |\,\mathrm{supp}(z)\,|.$$

Let us recall (see e.g. [24]) that the branch number of the matrix D^T is defined by the formula

$$B(D^T) = \min\{ wt(z) + wt(zD^T) : z \in F_{2^t}{}^p \setminus \{0\} , \qquad (24)$$

and the elements of the linear approximations table of the s-box s_j by the formulas [25]

$$l_{s_j}(a_j, b_j) = \left(2^{-t} \sum_{u_j \in F_{2^t}} (-1)^{\mathrm{Tr}_2^{2^t}(u_j a_j \oplus s_j(u_j) b_j)} \right)^2, a_j, b_j \in F_{2^t},\ j \in \overline{0, p-1}. \qquad (25)$$

Note that in (25) the expression $\mathrm{Tr}_2^{2^t}(u_j a_j \oplus s_j(u_j) b_j)$ can be replaced by the Boolean dot product $u_j a_j \oplus s_j(u_j) b_j$, if we identify the elements u_j, $s_j(u_j)$ with the vectors of their coordinates in some basis of the field F_{2^t}, and the elements a_j, b_j with the vectors of their coordinates in the respective dual basis.

Let us prove a theorem that gives an expression and an upper bound of parameter (14) for an ordinary binary SNOW 2.0-like cipher in terms of parameters (24), (25).

Theorem 4. *We have*

$$\Delta_{c,r'}(k) \le (2^{r'}-1)\big(l_{\max}\big)^{\left\lceil \frac{B(D^T)}{2} \right\rceil k}, \tag{26}$$

where $l_{\max} = \max\{l_{s_j}(a_j, b_j) : a_j, b_j \in F_{2^t} \setminus \{0\}, j \in \overline{0, p-1}\}$.

Besides, if r' *is a divisor of* t, *then*

$$\Delta_{c,r'}(k) = \sum_{u \in F_{2^{r'}} \setminus\{0\}} l_{s_0}(u\hat{c}_0, u\hat{c}'_0)^k \cdots l_{s_{p-1}}(u\hat{c}_{p-1}, u\hat{c}'_{p-1})^k , \tag{27}$$

where $\hat{c} = (\hat{c}_0, \dots, \hat{c}_{p-1})$ *is the vector of coordinates of the element* $c \in F_{2^r}$ *in the basis* $\hat{\mathrm{B}}$, $(\hat{c}'_0, \dots, \hat{c}'_{p-1}) = \hat{c}D^T$.

Proof. Let us show that parameter (19) satisfies the following equality:

$$|\hat{\pi}(\alpha)|^2 = l_{s_0}(\hat{\alpha}_0, \hat{\alpha}'_0) \cdots l_{s_{p-1}}(\hat{\alpha}_{p-1}, \hat{\alpha}'_{p-1}), \tag{28}$$

where $\hat{\alpha}' = (\hat{\alpha}'_0, \dots,, \hat{\alpha}'_{p-1}) = (\hat{\alpha}_0, \dots, \hat{\alpha}_{p-1})D^T$.

Indeed, due to transitivity of the trace function and duality of the bases B and $\hat{\mathrm{B}}$ for any $x, \alpha \in F_{2^{pt}}$ the following equalities are true:

$$\mathrm{Tr}_2^{2^{pt}}(x\alpha) = \mathrm{Tr}_2^{2^t}(\mathrm{Tr}_{2^t}^{2^{pt}}(x\alpha)) = \mathrm{Tr}_2^{2^t}(x \cdot \hat{\alpha}),$$

where $x \cdot \hat{\alpha}$ is the dot product of the vectors $(x_0, \dots, x_{p-1})$ and $(\hat{\alpha}_0, \dots, \hat{\alpha}_{p-1})$ over the field F_{2^t} . So, from (19) and the equalities $\xi_i = u_i \oplus \sigma(u_i)$, $i = 0, 1, \dots$, we obtain that

$$\hat{\pi}(\alpha) = \sum_{x \in F_{2^t}{}^p} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^t}(x \cdot \hat{\alpha})} =$$

$$= 2^{-r} \sum_{x \in F_{2^t}{}^p} \sum_{\substack{u \in F_{2^t}{}^p: \\ u \oplus \sigma(u) = x}} (-1)^{\mathrm{Tr}_2^{2^t}(x \cdot \hat{\alpha})} = 2^{-r} \sum_{u \in F_{2^t}{}^p} (-1)^{\mathrm{Tr}_2^{2^t}((u \oplus \sigma(u)) \cdot \hat{\alpha})} .$$

Using formula (3) we get:

$$\hat{\pi}(\alpha) = 2^{-pt} \sum_{(u_0,\ldots,u_{p-1})\in F_{2^t}{}^p} (-1)^{\mathrm{Tr}_2^{2^t}(u\cdot\hat{\alpha} \oplus ((s_0(u_0),\ldots,s_{p-1}(u_{p-1}))D)\cdot\hat{\alpha})} =$$

$$= 2^{-pt} \sum_{(u_0,\ldots,u_{p-1})\in F_{2^t}{}^p} (-1)^{\mathrm{Tr}_2^{2^t}(u\cdot\hat{\alpha} \oplus (s_0(u_0),\ldots,s_{p-1}(u_{p-1}))\cdot(D\hat{\alpha}))} =$$

$$= 2^{-pt} \sum_{(u_0,\ldots,u_{p-1})\in F_{2^t}{}^p} (-1)^{\mathrm{Tr}_2^{2^t}(u\cdot\hat{\alpha} \oplus (s_0(u_0),\ldots,s_{p-1}(u_{p-1}))\cdot\hat{\alpha})} =$$

$$= \prod_{j=0}^{p-1} \left(2^{-t} \sum_{u_j \in F_{2^t}} (-1)^{\mathrm{Tr}_2^{2^t}(u_j\hat{\alpha}_j \oplus s_j(u_j)\hat{\alpha}'_j)} \right).$$

Taking the square of this expression we obtain (28).

Let us prove the inequality (26).

Let α be a non-zero element of the field F_{2^r} such that $|\hat{\pi}(\alpha)| = \max_{\beta\in F^r\setminus\{0\}} |\hat{\pi}(\beta)|$. It follows from Theorem 1 that $\Delta_{c,r'}(k) \le (2^{r'}-1)|\hat{\pi}(\alpha)|^{2k}$ and from (25), (28) we conclude that $|\hat{\pi}(\alpha)| = 0$ if there exists at least one $j \in \overline{0, p-1}$ such that $\hat{\alpha}_j = 0$, $\hat{\alpha}'_j \ne 0$ or $\hat{\alpha}_j \ne 0$, $\hat{\alpha}'_j = 0$. Thus, under condition $|\hat{\pi}(\alpha)| \ne 0$ the following equality holds: $\mathrm{supp}(\hat{\alpha}) = \mathrm{supp}(\hat{\alpha}D^T)$. Hence, on the basis of (28) and (24) we have

$$\Delta_{c,r'}(k) \le (2^{r'}-1)(l_{\max})^{\frac{wt(\hat{\alpha})}{2}k},\ 2wt(\hat{\alpha}) \ge B(D^T),$$

So, the inequality (26) is proved.

Now, assume that r' is a divisor of t. Substituting the expression in the right-hand side of (28) into (20) on the basis of the relation $F_{2^{r'}} \subseteq F_{2^t}$ we obtain the equality (27). This completeness the proof of Theorem.

The obtained theorem, along with relations (11) – (13), provides security evaluation of ordinary binary SNOW 2.0-like stream ciphers against correlation attacks by parameters (24) and (25) of their components. (Note that these parameters are traditionally used for security evaluation of block ciphers against linear cryptanalysis). Utilization, instead of the parameter $\Delta_{c,r'}(k)$, of its upper bound (26) in (11) – (13) enables to obtain lower bounds of the average time complexity and the size of the keystream needed for any of the (above-mentioned) correlation attacks over the field of the order $2^{r'}$ (see Algorithm 1 in Figure 2).

It also follows from Theorem 4 that to construct correlation attacks over the field F_{2^t} on ordinary binary SNOW 2.0-like ciphers it is possible to use only such elements $c \in F_{2^{pt}} \setminus \{0\}$ that satisfy the condition

$$\mathrm{supp}(\hat{c}) = \mathrm{supp}(\hat{c}D^T)\,. \tag{29}$$

In a practically important case $B(D^T) = p+1$ (when D is a MDS matrix; see e.g. [26]) according to Theorem 4 in [27] for each $l \ge \left\lceil \frac{B(D^T)}{2} \right\rceil$ there exist exactly

$$(2^t - 1)\binom{p}{l}\sum_{j=0}^{2l-(p+1)} (-1)^j \binom{2l-1}{j} 2^{t(2l-(p+1+j))}$$

of the mentioned elements c such that $wt(\hat{c}) = l$.

Example 4. Let us consider a binary version of SNOW 2.0 that differs from the original [1] by using of the operation $\oplus$ instead of $\overset{32}{+}$ in the scheme in Figure 1.

The parameters of this cipher have the following values: $t = 8$, $p = 4$, $n = 16$. The permutation σ has the form (3), where the s-boxes $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0, p-1}$ and the matrix D are defined in the same way as in the round transform of Rijndael (see Example 1). In particular, it is known that $l_{\max} = 2^{-6}$, $B(D^T) = p+1 = 5$ [12].

Using Algorithm 1, we obtain lower bounds of the parameters that determine the efficiency of correlation attacks over the field $F_{2^t} = F_{256}$ on the binary version of SNOW 2.0 (Table 1).

Table 1: Results obtained by Algorithm 1 for the binary version of SNOW 2.0 ($r' = t$)

k	$l*$	$\log T_{r'}(k, l*)$	$\log N_{r'}(k, l*)$
2	22	187.84	186.97
4	17	151.24	151.19
8	12	146.20	142.77
16	1	292.45	161.50

The obtained results mean that any of the (considered above) correlation attacks over the field of the order 256 on the binary version of the cipher has an average time complexity not less than $2^{146.20}$ and requires not less than $2^{142.77}$ keystream symbols.

(Note that the best of the known correlation attacks on SNOW 2.0 requires around $2^{163.59}$ keystream symbols and has an average time complexity $2^{164.15}$ [7]). Further increase of the value of k in Algorithm 1 leads to an increase of values of the parameters $T_{r'}(k, l^*)$, $N_{r'}(k, l^*)$.

```
Algorithm 1
Input:
  – integer numbers $n, p, t$;
  – s-boxes $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0, p-1}$;
  – a reversible $p \times p$-matrix $D$ over the field $F_{2^t}$.
  – a number $k \geq 2$ that is a power of two;
  – a divisor $r'$ of the number $r = pt$.
Processing:
  1. Calculate $\Delta_{r'}(k) = (2^{r'} - 1)(l_{\max})^{\left\lceil \frac{B(D^T)}{2} \right\rceil k}$ using formulas (24), (25).
  2. Put $r'' = pt(r')^{-1}$, $l = nr''$, $\theta = 1 + \log k$.
  3. For each $l' = 1, 2, ..., l-1$ calculate
         $m_{r'}(k) = 2(\Delta_{r'}(k))^{-1} l'r' \ln 2$,
         $T_{r'}(k, l') = (m_{r'}(k))^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} + r'(m_{r'}(k) + r'l'2^{r'l'}) + 2^{r'(l'+1)}$.
  4. Choose $l^* \in \overline{1, l-1}$ such that $T_{r'}(k, l^*) = \min\{T_{r'}(k, l') : l' \in \overline{1, l-1}\}$.
Output:
  – the number $l^*$ of $r'$-bit words (of the initial state of LFSR) that are recovered by the attack;
  – the average time complexity of the attack $T_{r'}(k, l^*)$;
  – the data complexity
         $N_{r'}(k, l^*) = k 2^{\frac{r'(l-l^*)}{\theta}} (2l^* r' \ln 2)^{\frac{1}{\theta}} (\Delta_{r'}(k))^{-\frac{1}{\theta}}$,
  needed for successful implementation of the attack.
```

Figure 2. The algorithm for security evaluation of ordinary binary SNOW 2.0-like ciphers against correlation attacks over the field of the order $2^{r'}$

Example 5. According to [8], the cipher Strumok uses the following parameters: $t=8$, $p=8$, $n=16$. The permutation σ has the form (3), where the s-boxes and the matrix D are defined in the same way as in Kalyna (see Example 2). In particular, it is known that $l_{\max}=9\cdot 2^{-8}$, $B(D^T)=p+1=9$ [14].

Using Algorithm 1 we obtain values of the parameters that determine the efficiency of correlation attacks over the field $F_{2^t}=F_{256}$ on the binary version of Strumok (Table 2).

Table 2: Results obtained by Algorithm 1 for the binary version of Strumok ($r'=t$)

k	$l*$	$\log T_{r'}(k,l*)$	$\log N_{r'}(k,l*)$
2	44	363.91	361.62
4	34	285.42	285.06
8	29	249.40	249.38
16	1	384.88	283.58

Further increase of the value of k in Algorithm 1 results in increase of values of the parameters $T_{r'}(k,l*)$, $N_{r'}(k,l*)$ in Table 2. So, any of (the considered above) correlation attacks over the field of the order 256 on the binary version of Strumok has an average time complexity not less than $2^{249.40}$ and requires not less than $2^{249.38}$ keystream symbols.

In general, the obtained results show that the binary versions of SNOW 2.0 and Strumok are practical secure against the considered correlation attacks under the condition that the keystream length for any fixed pair of key and initialization vector is limited by (e.g.) 2^{80}.

4 Upper bounds for imbalance of discrete functions realized by sequences of finite automata

Let U, X be finite sets, $h_i:U\times X\to U$, $f_i:U\times X\to V_t$, $i=0,1,\ldots$. For any $n\in\mathbf{N}$, set the functions $H_n:U\times X^n\to U$ and $F_n:U\times X^n\to V_t^n$, putting

$$H_n(u_0,x_0,\ldots,x_{n-1})=u_n,$$

$$F_n(u_0,x_0,\ldots,x_{n-1})=y_0,y_1,\ldots,y_{n-1}, \tag{30}$$

where the elements $u_1,u_2,\ldots$, $y_0,y_1,\ldots$ are calculated using recurrence relations $u_{i+1}=h_i(u_i,x_i)$, $y_i=f_i(u_i,x_i)$, $i=0,1,\ldots$.

If $h_i=h$, $f_i=f$ for each $i=0,1,\ldots$, then $F_n(u_0,x_0,\ldots,x_{n-1})$ is the output sequence generated in accordance to the initial state u_0 and the input sequence $x_0,\ldots,x_{n-1}$ of the automaton (X,U,V_t,h,f) (with the input alphabet X, the set of states U and the output alphabet V_t) and $H_n(u_0, x_0, ..., x_{n-1})$ is the state of this automaton at time n.

By definition, a *function* $F : X^n \to V_t^n$ *is realized by a sequence of automata* (X, U, V_t, h_i, f_i), $i = \overline{0, n-1}$ if there exists an element $u_0 \in U$ such that $F(x_0, ..., x_{n-1}) = F_n(u_0, x_0, ..., x_{n-1})$ for each $(x_0, ..., x_{n-1}) \in X^n$.

Let $\alpha = (\alpha_0, \alpha_1, ...)$ be a sequence of binary vectors, $\alpha_i \in V_t$, $i = 0, 1, \ldots$. For any $n \in \mathbf{N}$, let us denote $\alpha^{(n)} = (\alpha_0, \alpha_1, ..., \alpha_{n-1})$ and set the function $F_n\alpha^{(n)}$ that takes each point $(u_0, x_0, ..., x_{n-1})$ to the Boolean dot product of the vectors $F_n(u_0, x_0, ..., x_{n-1})$ and $\alpha^{(n)}$. The *imbalance* of this function at a fixed value of $u_0 \in U$ is determined as follows:

$$l_\alpha^{(n)}(u_0) = \frac{1}{|X|^n} \left| \sum_{(x_0, \ldots, x_{n-1}) \in X^n} (-1)^{F_n(u_0, x_0, \ldots, x_{n-1})\alpha^{(n)}} \right|. \qquad (31)$$

Let us obtain a matrix representation and upper bounds of the parameter (31). For any $u, u' \in U$, let us denote

$$l_\alpha^{(n)}(u, u') = \frac{1}{|X|^n} \sum_{\substack{(x_0, \ldots, x_{n-1}) \in X^n: \\ H_n(u, x_0, \ldots, x_{n-1}) = u'}} (-1)^{F_n(u, x_0, \ldots, x_{n-1})\alpha^{(n)}}. \qquad (32)$$

Let's enumerate (in arbitrary order) the elements of the set U, putting $U = \{u_0, u_1, \ldots, u_{M-1}\}$, where $M = |U|$, and take $M \times M$-matrices $A_{\alpha_i}^{(i)}$ with elements

$$A_{\alpha_i}^{(i)}(u, u') = \frac{1}{|X|} \sum_{x \in X:\, h_i(u, x) = u'} (-1)^{f_i(u, x)\alpha_i}, \quad u, u' \in U, \qquad (33)$$

where $f_i(u, x)\alpha_i$ denotes the Boolean dot product of the mentioned binary vectors of the length t, $i = 0, 1, \ldots$.

Theorem 5. *For any* $n \in \mathbf{N}$, *the following equality holds:*

$$l_\alpha^{(n)}(u, u') = (A_{\alpha_0}^{(0)} A_{\alpha_1}^{(1)} \cdots A_{\alpha_{n-1}}^{(n-1)})(u, u'), \; u, u' \in U; \qquad (34)$$

in other words, the parameter (32) coincides with the (u, u')*-th element of the product of matrices (33) over all* $i \in \overline{0, n-1}$. *Besides, the parameter (31) satisfies the following equality:*

$$l_{\alpha}^{(n)}(u_0) = \left|\mathbf{e}\, A_{\alpha_0}^{(0)} A_{\alpha_1}^{(1)} \cdots A_{\alpha_{n-1}}^{(n-1)}\, \mathbf{1}\right|, \tag{35}$$

where $\mathbf{e} = (1, 0, \dots, 0)$, $\mathbf{1} = (1, 1, \dots, 1)^T$.

Proof. Formula (34) can be proved by means of induction by n. For $n = 1$, it follows directly from the above definitions. For $n \geq 2$ it is sufficient to check the correctness of such equality:

$$l_{\alpha}^{(n)}(u, u') = \sum_{u'' \in U} l_{\alpha}^{(n-1)}(u, u'')\, A_{\alpha_{n-1}}^{(n-1)}(u'', u'),\ u, u' \in U. \tag{36}$$

Indeed, on the basis of (32), (33), and the definitions of the functions H_n, F_n, the following equalities hold:

$$\sum_{u'' \in U} l_{\alpha}^{(n-1)}(u, u'')\, A_{\alpha_{n-1}}^{(n-1)}(u'', u') =$$

$$= \frac{1}{|X|^n} \sum_{u'' \in U} \sum_{\substack{(x_0, \dots, x_{n-2}) \in X^{n-1}: \\ H_{n-1}(u, x_0, \dots, x_{n-2}) = u''}} (-1)^{F_{n-1}(u, x_0, \dots, x_{n-2})\alpha^{(n-1)}} \sum_{\substack{x_{n-1} \in X: \\ h_{n-1}(u'', x_{n-1}) = u'}} (-1)^{f_{n-1}(u'', x_{n-1})\alpha_{n-1}} =$$

$$= \frac{1}{|X|^n} \sum_{(x_0, \dots, x_{n-2}) \in X^{n-1}} (-1)^{F_{n-1}(u, x_0, \dots, x_{n-2})\alpha^{(n-1)}} \times$$

$$\times \sum_{\substack{x_{n-1} \in X: \\ h_{n-1}(H_{n-1}(u, x_0, \dots, x_{n-2}), x_{n-1}) = u'}} (-1)^{f_{n-1}(H_{n-1}(u, x_0, \dots, x_{n-2}), x_{n-1})\alpha_{n-1}} =$$

$$= \frac{1}{|X|^n} \sum_{\substack{(x_0, \dots, x_{n-2}) \in X^{n-1},\ x_{n-1} \in X: \\ H_n(u, x_0, \dots, x_{n-1}) = u'}} (-1)^{F_{n-1}(u, x_0, \dots, x_{n-2})\alpha^{(n-1)} \oplus f_{n-1}(H_{n-1}(u, x_0, \dots, x_{n-2}), x_{n-1})\alpha_{n-1}} =$$

$$= \frac{1}{|X|^n} \sum_{\substack{(x_0, \dots, x_{n-1}) \in X^n: \\ H_n(u, x_0, \dots, x_{n-1}) = u'}} (-1)^{F_n(u, x_0, \dots, x_{n-1})\alpha^{(n)}} = l_{\alpha}^{(n)}(u, u').$$

So, the equality (36) is proved. Finally, the correctness of (35) follows from (34) and the equality $l_{\alpha}^{(n)}(u_0) = \left|\sum_{u' \in U} l_{\alpha}^{(n)}(u_0, u')\right|$.

Thus, Theorem is completely proved.

Note that Theorem 5 generalizes a number of separate results on matrix (or linear) representations for the parameters of the form (31) for functions realized by finite automata of special form [4, 11]. This theorem allows us to obtain upper bounds of the parameter (31) that can be used, in particular, for security proofs of ordinary modular SNOW 2.0-like ciphers against correlation attacks.

Let us introduce some additional notation. For any vector $x=(x_1,...,x_n)$ with real coordinates let us denote

$$\| x\|_1 = |x_1| + \cdots + |x_n|, \ \| x\|_\infty = \max\{|x_i| : i \in \overline{1,n}\}.$$

Let us set in a usual way the sup-norm of a real $n\times n$-matrix A, putting $\| A\|_\infty = \sup\{\| Ax\|_\infty : \| x\|_\infty = 1\}$, where supremum is taken over all real vectors $x=(x_1,...,x_n)^T$ such that $\| x\|_\infty = 1$. It is not difficult to check that

$$\| A\|_\infty = \max\{\| A_1\|_1, \| A_2\|_1, \dots, \| A_n\|_1\}, \tag{37}$$

where $A_1, A_2, \dots, A_n$ are rows of the matrix A. Besides, for any real $n\times n$-matrices A and B, the following inequality holds:

$$\| AB\|_\infty \le \| A\|_\infty \| B\|_\infty . \tag{38}$$

Theorem 6. *The parameter (31) satisfies the following inequality*

$$l_\alpha^{(n)}(u_0) \le \left\| A_{\alpha_0}^{(0)} \right\|_\infty \left\| A_{\alpha_1}^{(1)} \right\|_\infty \cdots \left\| A_{\alpha_{n-2}}^{(n-2)} \right\|_\infty \left\| A_{\alpha_{n-1}}^{(n-1)} \mathbf{1} \right\|_\infty , \tag{39}$$

where

$$\left\| A_{\alpha_i}^{(i)} \right\|_\infty = \max_{u\in U} \left\{ \frac{1}{|X|} \sum_{u'\in U} \left| \sum_{x\in X:\, h_i(u,\, x)=u'} (-1)^{f_i(u,x)\alpha_i} \right| \right\}, \ i \in \overline{0, n-2},$$

$$\left\| A_{\alpha_{n-1}}^{(n-1)} \mathbf{1} \right\|_\infty = \max_{u\in U} \left\{ \frac{1}{|X|} \left| \sum_{x\in X} (-1)^{f_{n-1}(u,x)\alpha_{n-1}} \right| \right\}.$$

Besides, the following inequality holds:

$$\max_{(\alpha_0,\dots,\alpha_{n-1})\ne(0,\dots,0)} \{ l_\alpha^{(n)}(u_0) \} \le \max_{i\in\overline{0,n-1}} \max_{\alpha_i \ne 0} \left\{ \left\| A_{\alpha_i}^{(i)} \mathbf{1} \right\|_\infty \right\}. \tag{40}$$

Proof. The inequality (39) follows directly from (35), (37), and (38).

Let us prove the inequality (40). Let’s denote by i the largest integer from 0 to $n-1$ such that $\alpha_i \neq 0$. As $\alpha_{i+1} = \ldots = \alpha_{n-1} = 0$, then on the basis of (33) $A^{(i+1)}_{\alpha_{i+1}} \cdots A^{(n-1)}_{\alpha_{n-1}} \mathbf{1} = \mathbf{1}$, whence from (35) we have $l^{(n)}_{\alpha}(u_0) = \left| \mathbf{e}\, A^{(0)}_{\alpha_0} A^{(1)}_{\alpha_1} \cdots A^{(i)}_{\alpha_i}\, \mathbf{1} \right|$. Thus,

$$l^{(n)}_{\alpha}(u_0) \leq \left\| A^{(0)}_{\alpha_0} \right\|_{\infty} \cdots \left\| A^{(i-1)}_{\alpha_{i-1}} \right\|_{\infty} \left\| A^{(i)}_{\alpha_i} \mathbf{1} \right\|_{\infty} \leq \left\| A^{(i)}_{\alpha_i} \mathbf{1} \right\|_{\infty}.$$

Theorem is proved.

As an example of application of Theorems 5 and 6, let us consider arbitrary tuples of permutations $s = (s_0, \ldots, s_{p-1})$ and vectors $\alpha = (\alpha_0, \ldots, \alpha_{p-1})$, $\beta = (\beta_0, \ldots, \beta_{p-1})$, where $s_i : V_t \to V_t$, $\alpha_i, \beta_i \in V_t$, $i \in \overline{0, p-1}$, and obtain an upper bound of the parameter

$$l_{\alpha,\beta}(s) = 2^{-2tp} \left| \sum_{x,y \in V_t{}^p} (-1)^{((x \overset{pt}{+} y) \oplus x)\alpha \oplus s(y)\beta} \right|, \tag{41}$$

where $x = (x_0, \ldots, x_{p-1})$, $y = (y_0, \ldots, y_{p-1})$, $s(y) = (s_0(y_0), \ldots, s_{p-1}(y_{p-1}))$, $x_i, y_i \in V_t$, $i \in \overline{0, p-1}$, and $x \overset{pt}{+} y$ denotes the sum modulo 2^{pt} of binary integers correspond to vectors x, y (hereinafter, any vector $x = (x_0, \ldots, x_{p-1}) \in V_t{}^p$ is identified with the integer whose least significant bit coincides with the leftmost coordinate of the vector x_0).

For any $a, b \in V_t$, $i \in \overline{0, p-1}$, let us define a 2×2-matrix $A^{(i)}_{a,b}$ with the elements

$$A^{(i)}_{a,b}(u,u') = 2^{-2t} \sum_{\substack{x_i, y_i \in V_t: \\ \mathrm{msb}(x_i + y_i + u) = u'}} (-1)^{(x_i \overset{t}{+} y_i \overset{t}{+} u)a \oplus x_i a \oplus s_i(y_i) b}, \quad u, u' \in \{0, 1\}, \tag{42}$$

where $\mathrm{msb}(x_i + y_i + u)$ is the most significant (i.e., the t-th) bit of the sum of integers corresponds to the mentioned binary vectors of the length t, and $x_i \overset{t}{+} y_i \overset{t}{+} u$ is the sum of these numbers modulo 2^t.

Theorem 7. *The parameter (41) satisfies the following equality*:

$$l_{\alpha,\beta}(s) = \left| (1, 0)\, A^{(0)}_{\alpha_0,\beta_0}\, A^{(1)}_{\alpha_1,\beta_1} \cdots A^{(p-1)}_{\alpha_{p-1},\beta_{p-1}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right|, \tag{43}$$

Besides, the following inequality holds:

$$l_{\alpha,\beta}(s) \le n_{\alpha_0,\beta_0}(s_0)\, n_{\alpha_1,\beta_1}(s_1) \cdots n_{\alpha_{p-1},\beta_{p-1}}(s_{p-1}), \tag{44}$$

where

$$n_{\alpha_i,\beta_i}(s_i) = \left\| A^{(i)}_{\alpha_i,\beta_i} \right\|_\infty =$$

$$= \max\{| A^{(i)}_{\alpha_i,\beta_i}(0,0) | + | A^{(i)}_{\alpha_i,\beta_i}(0,1) |, | A^{(i)}_{\alpha_i,\beta_i}(1,0) | + | A^{(i)}_{\alpha_i,\beta_i}(1,1) |\},\ i \in \overline{0, p-1}. \tag{45}$$

Proof. On the basis of Theorems 5 and 6, it is sufficient to check that the function $F(x,y) = ((x \overset{pt}{+} y) \oplus x, s(y))$, $x, y \in V_t{}^p$ (from the set $V_t{}^p \times V_t{}^p$ into itself) is realized by a sequence of finite automata (X, U, V_{2t}, h_i, f_i), where $X = V_{2t}$, $U = \{0,1\}$, and the functions h_i, f_i are defined as follows:

$$h_i(u,(x_i, y_i)) = \mathrm{msb}(u + x_i + y_i),\ u \in U,\ (x_i, y_i) \in X,$$

$$f_i(u,(x_i, y_i)) = ((u \overset{t}{+} x_i \overset{t}{+} y_i) \oplus x_i,\ s_i(y_i)),\ u \in U,\ (x_i, y_i) \in X,\ i \in \overline{0,\ p-1}.$$

Indeed, let us denote $z = (z_0, ..., z_{p-1}) = (x \overset{pt}{+} y) \oplus x$ and set

$$u_0 = 0,\ u_{i+1} = h_i(u_i, (x_i, y_i)),\ z_i' = (u_i \overset{t}{+} x_i \overset{t}{+} y_i) \oplus x_i,\ i \in \overline{0,\ p-1}.$$

Using induction by i, it is not difficult to check that $z_i = z_i'$ for each $i \in \overline{0,\ p-1}$. Whence, the function F coincides with (30) for the mentioned functions h_i, f_i, fixed value $u_0 = 0$, and $n = p$.

Thus, theorem is proved.

5 Application of the automata-theoretic approach to security evaluation of ordinary modular SNOW 2.0-like ciphers against correlation attacks

Let us consider an ordinary modular SNOW 2.0-like cipher that is obtained by replacement of the operation $*$ in the scheme in Figure 1 with the operation $\overset{r}{+}$ of addition of binary integers modulo 2^r, and the permutation σ is defined by (3). From (12), (13), the security of this cipher against correlation attacks over the field of the order $2^{r'}$, where r' divides r, depends on the parameter (14).

The following theorem sets an upper bound of this parameter.

Theorem 8. *For any ordinary modular SNOW 2.0-like cipher, the parameter (14) satisfies the following inequality:*

$$\Delta_{c,r'}(k) \le (2^{r'}-1)\left(n_{\max}\right)^{2k\left\lceil \frac{B(D^T)}{2} \right\rceil}, \qquad (46)$$

where

$$n_{\max} = \max\{n_{\alpha_i,\beta_i}(s_i) : (\alpha_i,\beta_i) \in V_t \times V_t \setminus \{(0,\,0)\}, i \in \overline{0,\,p-1}\},$$

$n_{\alpha_i,\beta_i}(s_i)$ *is defined by (45),* $i \in \overline{0,\,p-1}$*, and* $B(D^T)$ *is defined by (24).*

Proof. It follows from Theorem 1 that

$$\Delta_{c,r'}(k) \le (2^{r'}-1)\left(\max_{\alpha\in F_{2^r}\setminus\{0\}} |\hat{\pi}(\alpha)|\right)^{2k}, \qquad (47)$$

where $\hat{\pi}(\alpha)$ is the Fourier transform of the distribution of (5):

$$\hat{\pi}(\alpha) = \sum_{x\in F_{2^r}} \mathbf{P}\{\xi_i = x\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha x)},\ \alpha \in F_{2^r}\setminus\{0\}.$$

According to (5), the random variable ξ_i is the sum of two independent random variables:

$$\xi_{1,i} = (x_{i+n-1} \overset{r}{+} u_i) \oplus x_{i+n-1} \oplus \sigma(u_i)$$

and

$$\xi_{2,i} = (x_{i+n} \overset{r}{+} x_{i+\mu} \overset{r}{+} v_i) \oplus (x_{i+n} \oplus x_{i+\mu} \oplus v_i),$$

where $x_{i+\mu}, x_{i+n-1}, x_{i+n}, u_i, v_i$ are independent random variables with the uniform distribution on the set V_r. So, on the basis of the Convolution Theorem the Fourier transform of the distribution ξ_i are products of Fourier transforms of the distributions $\xi_{1,i}$ and $\xi_{2,i}$, i.e., $\hat{\pi}(\alpha) = \hat{\pi}_1(\alpha)\hat{\pi}_2(\alpha)$, where

$$\hat{\pi}_1(\alpha) = \sum_{z\in F_{2^r}} \mathbf{P}\{\xi_{1,i} = z\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha z)},\ \hat{\pi}_2(\alpha) = \sum_{z\in F_{2^r}} \mathbf{P}\{\xi_{2,i} = z\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha z)}.$$

Whence, we have

$$|\,\hat{\pi}(\alpha)\,| \le |\,\hat{\pi}_2(\alpha)\,| = \left| \sum_{z\in F_{2^r}} \mathbf{P}\{\xi_{2,i} = z\}(-1)^{\mathrm{Tr}_2^{2^r}(\alpha z)} \right| = 2^{-2r} \left| \sum_{x,y\in F_{2^r}} (-1)^{\mathrm{Tr}_2^{2^r}(((x\overset{r}{+}y)\oplus x\oplus\sigma(y))\alpha)} \right| .$$

Further, using the formula (3) and the pair of the dual bases B, $\hat{\mathrm{B}}$ of the field F_{2^r} over the sub-field F_{2^t} in the same way as in the proof of Theorem 4 we obtain that

$$\mathrm{Tr}_2^{2^r}(((x\overset{r}{+}y)\oplus x\oplus\sigma(y))\alpha) = \mathrm{Tr}_2^{2^t}(((x\overset{r}{+}y)\oplus x)\cdot\hat{\alpha}\oplus s(y)\cdot\hat{\beta}), \qquad (48)$$

where the elements $(x\overset{r}{+}y)\oplus x$ and $s(y)=(s_0(y_0),...,s_{p-1}(y_{p-1}))$ of the field F_{2^r} are identified with the vectors of their coordinates in the basis B, $\hat{\alpha}=(\hat{\alpha}_0,\dots,\hat{\alpha}_{p-1})$ is the vector of coordinates of α in the basis $\hat{\mathrm{B}}$, $\hat{\beta}=\hat{\alpha}D^T$, and the symbol $\bullet$ denotes the dot product of the vectors over the field F_{2^t}. Finally, the expression in the right-hand side of the equality (48) coincides with the Boolean dot product $((x\overset{r}{+}y)\oplus x)\hat{\alpha}\oplus s(y)\hat{\beta}$, if we identify the coordinates of the vectors $(x\overset{r}{+}y)\oplus x$ and $s(y)$ over the field F_{2^t} with the vectors of their coordinates in a certain basis of this field over the sub-field F_2 and the coordinates of the vectors $\hat{\alpha}$ and $\hat{\beta}$ with the vectors of their coordinates in the respective dual basis.

Thus, the following inequality is true:

$$|\,\hat{\pi}(\alpha)\,| \le 2^{-2tp} \left| \sum_{x,y\in {F_{2^t}}^p} (-1)^{((x\overset{pt}{+}y)\oplus x)\hat{\alpha}\oplus s(y)\hat{\beta}} \right| , \qquad (49)$$

where $\hat{\alpha}=(\hat{\alpha}_0,\dots,\hat{\alpha}_{p-1})\in {F_{2^t}}^p$, $\hat{\beta}=\hat{\alpha}D^T$, and $((x\overset{r}{+}y)\oplus x)\hat{\alpha}$ and $s(y)\hat{\beta}$ denotes the Boolean dot products of the mentioned binary vectors.

It follows from the obtained inequality and from Theorem 7 that

$$|\,\hat{\pi}(\alpha)\,| \le n_{\hat{\alpha}_0,\hat{\beta}_0}(s_0)\, n_{\hat{\alpha}_1,\hat{\beta}_1}(s_1)\cdots n_{\hat{\alpha}_{p-1},\hat{\beta}_{p-1}}(s_{p-1}) \le (n_{\max})^l ,$$

where $l = |\{i\in\overline{0,p-1} : (\hat{\alpha}_i,\hat{\beta}_i)\ne(0,0)\}|$.

Further, using the equality $\hat{\beta}=\hat{\alpha}D^T$ and formula (24) we obtain that $B(D^T) \le wt(\hat{\alpha}) + wt(\hat{\beta}) \le l + l = 2l$. So, for any $\alpha \in F_{2^r} \setminus \{0\}$ the following inequality holds: $|\hat{\pi}(\alpha)| \le (n_{\max})^{\left\lceil \frac{B(D^T)}{2} \right\rceil}$, whence, using (47) we obtain (46).

Theorem is proved.

This theorem, along with the equalities (11) – (13), provides security evaluation of ordinary modular SNOW 2.0-like stream ciphers against correlation attacks directly by the parameters of their components (see formulas (24), (42), and (45)). Utilization instead of the parameter $\Delta_{c,r'}(k)$ of its upper bound (46) in (11) – (13) enables to obtain lower bounds of the average time complexity and the size of the keystream needed for any of (the above-mentioned) correlation attacks over the field of the order $2^{r'}$ (see Algorithm 2 in Figure 3).

Note that for calculation of the parameter $n_{\max}$ at Step 1 of Algorithm 2 it is possible to use Algorithm 3 (see Figure 4), correctness of which follows directly from (42), (45). Application of the fast Hadamard transform (see e.g. [28], p. 217) at Step 2 of Algorithm 3 allows to reduce the time complexity of calculation of the value $n_{\max}$ to $O(pt2^{2t})$ operations instead of $O(p2^{4t})$ operations used in trivial algorithm based upon (42).

Example 6. We get lower bounds of parameters that determine the efficiency of correlation attacks over the field $F_{2^t} = F_{256}$ on SNOW 2.0.

Let us recall (see Example 1) that the parameters of this cipher have the following values: $t = 8$, $p = 4$, $n = 16$. The permutation σ has the form (3), where the permutations $s_i : F_{2^t} \to F_{2^t}$, $i \in \overline{0, p-1}$, and the matrix D are defined in the same way as for the round transform of Rijndaep; in particular, $B(D^T) = p + 1 = 5$.

Using Algorithm 4, we obtain that $n_{\max} = 2^{-3}$. So, $(n_{\max})^2 = 2^{-6} = l_{\max}$, where the value of $l_{\max}$ is given in Example 4. Whence, the results obtained by means of Algorithm 1 for the binary version of the cipher (see Table 1) coincide with the respective results obtained by means of Algorithm 2 for the original SNOW 2.0.

Thus, according to Table 1 any of (the considered above) correlation attacks over the field of the order 256 on SNOW 2.0 has the average time complexity not less than $2^{146.20}$ and requires not less than $2^{142.77}$ keystream symbols.

Example 7. Let us consider the cipher Strumok (Example 2), where the following parameters are used: $t = 8$, $p = 8$, $n = 16$. The permutation σ has the form (3), where the s-boxes and the matrix D are defined in the same way as for Kalyna block cipher. In particular, in Strumok four various permutations are used: π_0, π_1, π_2, π_3 (each of them is used twice); and $B(D^T) = p + 1 = 9$.

Table 3 gives values of the parameter $n_{\max}(\pi_i)$, $i \in \overline{0, 3}$, and also of the vectors a, b at which the maximum in the expression of this parameter is reached (see Step 4 of Algorithm 3). In accordance to Table 3, $(n_{\max})^2 = (3 \cdot 2^{-4})^2 = l_{\max}$, where the value of $l_{\max}$ was given in Example 5. So, the results obtained by means of Algorithm 1 for the binary version of Strumok (see Table 2) coincide with the respective results obtained by means of Algorithm 2 for the original encryption algorithm.

Algorithm 2

Input:

– integer numbers n, p, t;

– s-boxes $s_j : F_{2^t} \to F_{2^t}$, $j \in \overline{0,\ p-1}$;

– a reversible $p \times p$-matrix D over the field F_{2^t}.

– a number $k \geq 2$ that is a power of two;

– a divisor r' of the number $r = pt$.

Processing:

1. Calculate $\Delta_{r'}(k) = (2^{r'} - 1)\left(n_{\max}\right)^{2k\left\lceil \frac{B(D^T)}{2} \right\rceil}$, using (24), (42), and (45).
2. Set $r'' = r \cdot (r')^{-1}$, $l = nr''$, $\theta = 1 + \log k$.
3. For each $l' = 1, 2, ..., l-1$ calculate

$$m_{r'}(k) = 2(\Delta_{r'}(k))^{-1} l' r' \ln 2,$$

$$T_{r'}(k,l') = (m_{r'}(k))^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} + r'(m_{r'}(k) + r'l'2^{r'l'}) + 2^{r'(l'+1)}.$$

4. Choose $l^* \in \overline{1, l-1}$ such that $T_{r'}(k,l^*) = \min\{T_{r'}(k,l') : l' \in \overline{1, l-1}\}$.

Output:

– the number l^* of r'-bit words (of the initial state of LFSR) that are recovered by the attack;

– the average time complexity of the attack $T_{r'}(k,l^*)$;

– the data complexity

$$N_{r'}(k,l^*) = k 2^{\frac{r'(l-l^*)}{\theta}} (2l^* r' \ln 2)^{\frac{1}{\theta}} (\Delta_{r'}(k))^{-\frac{1}{\theta}},$$

needed for successful implementation of the attack.

Figure 3. The algorithm for security evaluation of ordinary modular SNOW 2.0-like ciphers against correlation attacks over the field of the order $2^{r'}$

Algorithm 3

Input: s-boxes $s_i : V_t \to V_t$, $i \in \overline{0,\ p-1}$.

Processing:

For each $i \in \overline{0,\ p-1}$ make the following calculations.

1. For each $u \in \{0, 1\}$:

– calculate the values

$$D_{u,u'}^{(i)}(x, y) = |\{(z_1, z_2) \in V_t \times V_t :$$

$$\mathrm{msb}(u + z_1 + z_2) = u',\ (u \overset{t}{+} z_1 \overset{t}{+} z_2) \oplus z_1 = x,\ \ s_i(z_2) = y\}|$$

for all $u' \in \{0, 1\}$, $x, y \in V_t$;

– calculate the values

$$A_{a,b}^{(i)}(u, u') = 2^{-2t} \sum_{(x,y)\in V_t \times V_t} D_{u,u'}^{(i)}(x, y)(-1)^{xa \oplus yb}$$

for all $u' \in \{0, 1\}$, $a, b \in V_t$ using fast Hadamard transform.

2. For of each pair $(a, b) \in V_t \times V_t \setminus \{(0, 0)\}$ calculate

$$n_{a,b}(s_i) = \max\{|\ A_{a,b}^{(i)}(0, 0)\,| + |\ A_{a,b}^{(i)}(0, 1)\,|,\ |\ A_{a,b}^{(i)}(1, 0)\,| + |\ A_{a,b}^{(i)}(1, 1)\,|\}\ .$$

3. Calculate

$$n_{\max}(s_i) = \max\{n_{a,b}(s_i) : (a, b) \in V_t \times V_t \setminus \{(0, 0)\}\}.$$

Output:

$$n_{\max} = \max_{i \in \overline{0,\, p-1}} \{n_{\max}(s_i)\}$$

Figure 4. Fast algorithm for calculation of the parameter $n_{\max}$

Table 3: Results obtained by Algorithm 4 for the s-boxes of Strumok

Permutations π used in Kalyna	$n_{\max}(\pi)$	a	b
π_0	$3 \cdot 2^{-4}$	1 = (0000 0001)	212 = (1101 0100)
π_1	$11 \cdot 2^{-6}$	1 = (0000 0001)	244 = (1111 0100)
π_2	$5 \cdot 2^{-5}$	1 = (0000 0001)	20 = (0001 0100)
π_3	$5 \cdot 2^{-5}$	1 = (0000 0001)	190 = (1011 1110)

Thus, any of (the considered above) correlation attacks over the field of the order 256 on Strumok has the average time complexity not less than $2^{249.40}$ and requires not less than $2^{249.38}$ keystream symbols.

In general, the obtained results show that the ciphers SNOW 2.0 and Strumok are practical secure against the considered correlation attacks on the condition that the keystream length for any fixed pair of key and initialization vector is limited by (e.g.) 2^{80}.

Summary

1. The paper proposes methods for security evaluation for SNOW 2.0-like stream ciphers against correlation attacks constructed similarly to the known attacks on SNOW 2.0 [3 – 7]. Each such attack is defined by a divisor r' of degree r of the field, over which the LFSR in Figure 3.1 is set, and by a non-zero element c of this field, and consists in construction of the system of equations (7) and its further solving by the algorithm from [7] that depends on the parameters $k \geq 2$ (that is a powers of two), and $l' \in \overline{1,l}$, where $l = nr''$, $r'r'' = r$. The average time complexity of an attack is determined by formula (12), and the size of the keystream needed for successful implementation of the attack is determined by formula (13).

2. Theorem 1 reduces the problem of obtaining lower bounds for the time complexity of any correlation attack from the specified class and also for the size of the keystream needed for successful implementation of the attack to construction of upper bounds for the maximum modules of Fourier coefficients of the noise distribution in the right-hand sides of equations in the system (4) not depending on a specific attack. Thus, the efficiency of correlation attacks on a SNOW 2.0-like stream cipher can be evaluated directly from Fourier coefficients of the distribution of random variable (5).

3. Any correlation attack over the field $F_{2^{r'}}$ (from the class of attacks being considered) is not more than $2^{r'}$ times efficient (both with respect to time and the data complexity) compared to the best correlation attack over the field F_2. So, a transition from binary correlation attacks to attacks over fields of order $2^{r'}$ may increase efficiency of the former not more than $2^{r'}$ times.

4. Theorem 4 provides security evaluation of ordinary binary SNOW 2.0-like stream ciphers against correlation attacks over the field of the order $2^{r'}$ directly by the parameters (24) and (25) of their components. Utilization instead of the parameter $\Delta_{c,r'}(k)$ of its upper bound (27) in formulas (11) – (13) enables to obtain lower bounds of the average time complexity and the size of the keystream needed for successful implementation of any of (the above-mentioned) correlation attacks.

5. Application of Theorem 4 to binary versions of SNOW 2.0 and Strumok shows that any correlation attack on them (from the specified class) over the field of the

order 256 has the average time complexity not less than $2^{146.20}$ and $2^{249.40}$ respectively and requires not less than $2^{142.77}$ and, respectively, $2^{249.38}$ keystream symbols that shows practical security of the mentioned binary ciphers against known correlation attacks on condition that the keystream length for any fixed pair of key and initialization vector is limited by (e.g.) 2^{80}.

6. Theorem 5 provides a matrix representation and upper bounds of imbalance for an arbitrary discrete function realized by a sequence of finite automata, and generalize a number of previously known statements on matrix (linear) representations for the imbalance of maps that are realized by finite automata of the special form [4, 11]. Theorems 6 and 7 give upper bounds of imbalance that may be used, in particular, for the proof of security of ordinary modular SNOW 2.0-like ciphers against correlation attacks.

7. Theorem 8 sets lower bounds of the time complexity and the size of the keystream needed for successful implementation correlation attacks on ordinary modular SNOW 2.0-like ciphers. Application of the obtained bounds to SNOW 2.0 and Strumok gives results that coincide with the results obtained for their binary versions: any correlation attack on the mentioned ciphers (from the specified class of attacks) over the field of the order 256 has the average time complexity not less than $2^{146.20}$ and $2^{249.40}$ respectively, and requires not less than $2^{142.77}$ and, respectively, $2^{249.38}$ keystream symbols. That shows the practical security of SNOW 2.0 and Strumok against known correlation attacks on condition that the keystream length for any pair of key and initialization vector is limited by (e.g.) 2^{80}.

References

1. P. Ekdahl and T. Johansson "A new version of the stream cipher SNOW", Selected Areas in Cryptography – SAC 2002, LNCS **2595**, pp. 47 – 61, Springer-Verlag, 2002.

2. ISO/IEC 18033-4: 2011(E). Information technology – Security techniques – Encryption algorithm – Part 4: Stream ciphers, 2011. – 92 p.

3. D. Watanabe, A. Biryukov, and C. de Cannière "A distinguishing attack of SNOW 2.0 with linear masking method", Selected Arreas in Cryptography – SAC 2003, LNCS **3006**, pp. 222 – 233, – Springer-Verlag, 2003.

4. K. Nyberg and J. Wallén "Improved linear distinguishers for SNOW 2.0", Fast Software Encryption – FSE 2006, LNCS **4047**, pp. 144 – 162, Springer-Verlag. 2006.

5. A. Maximov and Th. Johansson "Fast computation for large distribution and and its cryptographic application", Advanced in Cryptology – ASIACRYPT 2005, LNCS **3788**, pp. 313 – 332, Springer-Verlag, 2005.

6. J.-K. Lee, D.H. Lee, and S. Park "Cryptanalysis of SOSEMANUC and SNOW 2.0 using linear masks", Advanced in Cryptology – ASIACRYPT 2008, LNCS **5350**, pp. 524 – 538, Springer-Verlag, 2008.

7. B. Zhang, C. Xu, and W. Meier "Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0", Cryptology ePrint Archive, Report **2016/311**, http://eprint.iacr.org/2016/311.

8. I. Gorbenko, A. Kuznetsov, Yu. Gorbenko, A. Alekseychuk, and V. Timchenko "Strumok Keystream Generator", The 9th IEEE International Conference on Dependable Systems, Services and Technologies – DESSERT’2018, pp. 292 – 299, Kyiv, Ukraine, 24 – 27 May, 2018.

9. A.N. Alekseychuk "Sufficient condition for SNOW-2.0-like stream ciphers’ to be secure against some related key attacks", *Ukrainian Information Security Research Journal*, **18**, No. 4, pp. 261 – 268, 2016 [in Ukrainian].

10. A.E. Zhukov and V.P. Chistyakov "Matrix approach to the study of the number of preimages of the output sequence of a finite automaton", *Review of applied and industrial mathematics*, **1**, Issue 1, pp. 108 – 117, 1994 [in Russian].

11. J. Wallén "Linear approximation of addition modulo 2^n", Fast Software Encryption – FSE 2003, LNCS **2887**, pp. 261 – 273, Springer-Verlag, 2003.

12. J. Daemen and V. Rijmen "AES proposal: Rijndael", htpp://csrc.nist.gov/encription/aes/rijndael/ Rijndael.pdf.

13. R.V. Oliynykov, I.D. Gorbenko, O.V. Kazymyrov et al., "A New Encryption Standard of Ukraine: The Kalyna Block Cipher", Cryptology ePrint Archive, Report **2015/650**, http://eprint.iacr.org/2015/650.

14. A.N. Alekseychuk, L.V. Kovalchuk, A.S. Shevtsov, and S.V. Yakovliev "Cryptographic Properties of a New National Encryption Standard of Ukraine", *Cybernetics and Systems Analysis*, **52**, Issue 3, pp 351–364, 2016.

15. R. Lidl and H. Niederreiter "Finite Fields", Cambridge, U.K., Cambridge University Press, 1997, 755 p.

16. A. Blum, A. Kalai, and H. Wasserman "Noise-tolerant learning, the parity problem, and the statistical query model", *J. ACM*, **50**, No. 3, pp. 506 – 519, 2003.

17. A.N. Alekseychuk, "Sub-exponential algorithms for solving systems of linear Boolean equations with noised right-hand side", *Applied Radio Electronics: Sci. Journ*, **11**, No 2, pp. 128 – 136, 2012 [in Ukrainian].

18. S. Bogos, F. Tram′er and S. Vaudenay "On solving LPN using BKW and variants. Implementation and analysis", Cryptology ePrint Archive, Report **2015/049**, http://eprint.iacr.org/2015/049.

19. A.N. Alekseychuk, S.M. Ignatenko, and M.V. Poremskyi "Systems of linear equations corrupted by noise over arbitrary finite rings", *Mathematical and computer modelling. Series: Technical sciences: scientific journal*, Issue 15, pp. 150 – 155, 2017 [in Ukrainian].

20. D. Wagner "A generalized birthday problem", Advances in Cryptology – CRYPTO’02, Proceedings, LNCS **2442**, pp. 288 – 303, Springer-Verlag, 2002.

21. A.N. Alekseychuk and M.V. Poremskyi "Lover bounds for the data complexity of correlation attacks on stream ciphers over fields of order 2^r", *Ukrainian Information Security Research Journal*, **19**, No. 2, pp. 119 – 124, 2017 [in Ukrainian].

22. C. Carlet "Boolean functions for cryptography and error correcting codes", *In "Boolean Methods and Models*", Ed. by P. Hammer and Y. Crama, Cambridge, U.K., Cambridge University Press, 2006.

23. S. Vaudenay "On the Lai-Massey scheme", Advanced in Cryptology – ASIACRYPT 1999, LNCS **1716**, pp. 8 – 19, Springer-Verlag, 1999.

24. J. Daemen "Cipher and hash function design strategies based on linear and differential cryptanalysis", KU Leuven, Doctoral Dissertation, 1995.

25. F. Chabaud and S. Vaudenay "Links between differential and linear cryptanalysis", Advances in Cryptology – EUROCRYPT'94, Proceedings, LNCS 950, pp. 356 – 365, Springer-Verlag, 1995.

26. F.J. MacWilliams and N.J.A. Sloane "The theory of error correcting code*s*", Amsterdam, New York, North-Holland Publishing Company, 1977, 762 p.

27. M.M. Gluhov "On mixing linear transforms for block ciphers", *Mathematical Aspects of Cryptography*, **2**, No. 2, pp. 5 – 40, 2011 [in Russian].

28. O.A. Logachev, A.A. Salnikov, and V.V. Yashchenko "Boolean Functions in Coding Theory and Cryptography", American Mathematical Soc, 2012, 334 p.