Local Affinity Based Inversion of Filter Generators

O.A. Logachev
Information Security Institute,
Lomonosov University, Moscow
e-mail: logol@iisi.msu.ru

D.S. Nazarova
Computer Science Department,
Lomonosov University, Moscow
e-mail: dnazarova@gmail.com

Abstract

We propose a novel efficient cryptanalytic technique allowing an adversary to recover an initial state of filter generator given its output sequence. The technique is applicable to filter generators possessing local affinity property.

Keywords: Boolean function,filter generator, local affinity property.

1 Introduction

A filter generator is secure is there is no efficient algorithm to recover it's unknown initial state (the key) by given output sequence. The security is determined by cryptanalytic properties of automaton mapping induced by filter generator. It is known investigations of symmetric functions as filtering functions. But filter generator with symmetric function has a property which we call "local affinity property" (l.a.p.).

We propose a novel efficient algorithm to recover the initial state for any filter generator with "local affinity property". Some classes of Boolean functions which correspond to filter generators with local affinity property we distinguished too.

2 Preliminaries

For any positive integer n let $V_n = \mathbb{F}_2$ be the linear space of all vectors $\mathbf{x} = (x_0, \ldots, x_{n-1})^T$ over the finite field $\mathbb{F}_2 = GF(2)$. The Hamming weight of a vector $\mathbf{x} \in V_n$ is the number of its nonzero entries. We fixing the notation for two vectors in V_n:

$$\mathbf{0} = (0, 0, \ldots, 0)^T, \ \mathbf{1} = (1, 1, \ldots, 1)^T$$

and notation for vectors of canonical basis of V_n

$$\mathbf{e}_0 = (1, 0, \ldots, 0)^T, \ldots \mathbf{e}_{n-1} = (0, 0, \ldots, 1)^T.$$

Let $\oplus$ be an addition modulo 2 or bit-wise exclusive-or. For a vector $\mathbf{x} = (x_0, \ldots, x_{n-1})$ and $0 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant n-i$ be definition put vector-fragment $(\mathbf{x})_{i,j} = (x_i, x_{i+1}, \ldots, x_{i+j-1})^T$.

The Walsh Transform of f is an integer valued function $W_f : V_n \to [-2^n, 2^n]$ defined by

$$W_f(\mathbf{u}) = \sum_{\mathbf{x} \in V_n} (-1)^f(\mathbf{x}) \oplus \langle \mathbf{u}, \mathbf{x} \rangle$$

where $\langle \mathbf{u}, \mathbf{x} \rangle = u_0 x_0 \oplus \ldots \oplus u_{n-1} x_{n-1}$. The nonlinearity of Boolean function f can be quantified through the Walsh Transform:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{u \in V_n} |W_f(\mathbf{u})|$$

A Boolean function over V_n is a mapping $V_n \to \mathbb{F}_2$. The set of all mappings from V_n into V_m we denoting by $\mathcal{F}_{n,m}$. Then for $m = 1$ we get $\mathcal{F}_{n,1} = \mathcal{F}$, the set of all Boolean functions on V_n. The value of a Boolean function $f \in \mathcal{F}_n$ on a vector $\mathbf{x} \in V_n$ we shell denote by

$$f(\mathbf{x}) = f\left(x_0 \mathbf{e}_0 \oplus \ldots \oplus x_{n-1} \mathbf{e}_{n-1}\right) = f\left(x_0, \ldots, x_{n-1}\right).$$

To describe an attack we need of two cryptographic primitives. First, we present the filter generator based on a linear feedback shift register and on a filtering Boolean function. Let LFSR(χ, f) (Figure 1) be the filter generator with a primitive connection polynomial $\chi(\lambda) = \lambda^n \oplus \chi_1 \lambda^{n-1} \oplus \ldots \oplus \chi_{n-1}\lambda \oplus 1$ ($\chi_0 = \chi_n = 1$) and a filtering function f on V_n. A linear feedback shift register produces a vector $\mathbf{x} = (x_0, x_1, \ldots, x_{N+n-1})$, $N \leqslant 2^n + n - 1$, satisfying the linear recurrence relation

$$x_i = \chi_1 x_{i-1} \oplus \ldots \oplus \chi_{n-1} x_{i-(n-1)} \oplus \chi_n x_{i-n}, \tag{2.1}$$

for $i = n, n+1, \ldots, N+n-2$. The vector $(\mathbf{x})_{i,n} = (x_i, \ldots, x_{i+n-1})^T$ in V_n is called a state of the filter generator. The first state $(\mathbf{x})_{0,n} = (x_0, \ldots, x_{n-1})^T$ is initially loaded into

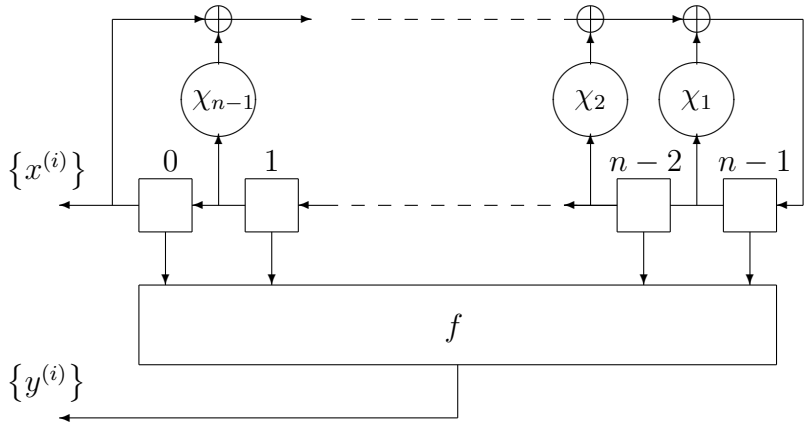

Figure 1.

the filter generator. This state is called the initial state or initial vector. It is clear that $(\mathbf{x})_{i+1,n} = U(\mathbf{x})_{i,n}$ with

$$U = \begin{bmatrix} 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \\ 1 & \chi_{n-1} & \cdots & \chi_1 & 1 \end{bmatrix}.$$

Let $\mathbf{y} = (y_0, \dots, y_{N-1})^T$ be an output vector of LFSR(χ, f) such that

$$y_i = f(x_i, \dots, x_{i+n-1}) = f\left(U^i(x_0, \dots, x_n - 1)^T, \right), \ i = 0, 1, \dots, N-1. \tag{2.2}$$

Secondly, we present shift register with filtering function f on V_n denoted by SR(f) (Figure 2).

If input vector of SR(f) is $\mathbf{x} = (x_0, \dots, x_{N+n-2})^T$ with recurrence relation (2.1) then SR(f) have output vector $\mathbf{y} = (y_0, \dots, y_{N-1})^T$ of the form (2.2).

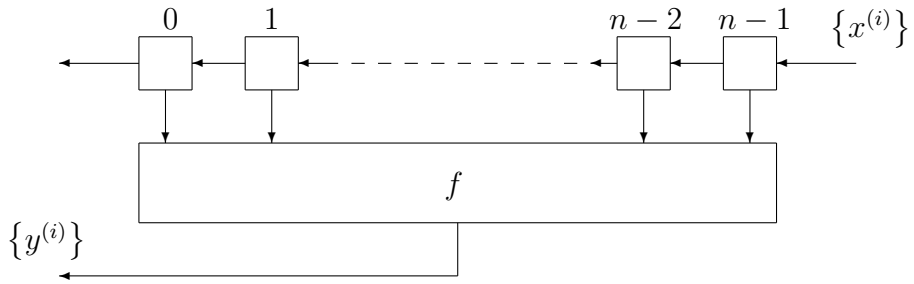

Figure 2.

For any positive integer N by definition, put

$$f_N^*(\mathbf{x}) = f_N^*(x_0, x_1, \ldots, x_{N+n-2}) = (f(x_0, \ldots, x_{n-1}), \ldots, f(x_{m-1}, \ldots, x_{N+n-1}))^T \quad (2.3)$$

for any vector $\mathbf{x} = (x_0, x_1, \ldots, x_{N+n-2})^T \in V_{N+n-1}$.

3 Local affinities of Boolean functions

Let A be a $k \times m$ - matrix over $\mathbb{F}_2$ with $\mathrm{rank}A = k,\ 1 \leqslant k \leqslant m$, and let B be $l \times (m+n-1)$ - matrix over $\mathbb{F}_2$ with $\mathrm{rank}B = l,\ 1 \leqslant l \leqslant m+n-1$. For vectors $\mathbf{a} \in V_m, \mathbf{b} \in V_{m+n-1}$ such that $\mathrm{rank}[A|\mathbf{a}] = k, \mathrm{rank}[B|\mathbf{b}] = l$ we will denote $\mathfrak{A} = (A, \mathbf{a}$ and $\mathfrak{B} = (B, \mathbf{b})$.

Definition 3.1. *A couple $\mathfrak{A} = (A, \mathbf{a})$ is called a local affinity of a span $(m, m+n-1)$ and of a cardinality $\left(2^{m-k}, 2^{m+n-l-1}\right)$.*

For any positive integers m, n let denote by $\mathrm{Prop}(m, n)$ the set of all local affinities of a span $(m, m+n-1)$.

Definition 3.2. *The Boolean function f in $\mathcal{F}_n$ is called the function with local affinity $(\mathfrak{A}, \mathfrak{B}) \in Prop(m, n)$ if for any $\mathbf{x} \in V_{m+n-1}, \mathbf{y} \in V_m$ such that $\mathbf{y} = f_m^*(\mathbf{x})$ and $A\mathbf{y} \oplus \mathbf{a} = \mathbf{0}$ the following condition holds: $B\mathbf{x} \oplus \mathbf{b} = \mathbf{0}$.*

4 General model of a local affinity based inversion

Suppose that a connection polynomial χ and a filtering function f with local affinity $(\mathfrak{A}, \mathfrak{B}) \in \mathrm{Prop}(m, n)$ are public knowledge. Also suppose we know outside vector $\mathbf{y} = (y_0, \ldots, y_{N-1})^T \in V_N$ of a filter generator $\mathrm{LFSR}(\chi, f)$. We concentrate on finding the vector $\mathbf{x} = (x_0, \ldots, x_{N+n-1})^T \in V_{N+n-1}$ such that $\mathbf{y} = f_N^*(\mathbf{x})$ and the recurrence relation (2.1) holds (i.e. the initial state of filter generator).

Recall that under recurrence relation (2.1) components $x_i, i = 0, 1, \ldots, N+n-1$ of the vector $\mathbf{x}$ expressed as linear functions $\xi_i, i = 0, 1, \ldots, N+n-1$ in n variables $x_0, x_1, \ldots, x_{n-1}$:

$$x_i = \xi_i(x_0, \ldots, x_{n-1}),\ i = 0, 1, \ldots, N+n-1. \tag{4.1}$$

Let $(\mathbf{y})_{s,m}, s = 0, 1, \ldots, N-m$ be the vector fragments of the vector $\mathbf{y} \in V_N$ and let $(\mathbf{x})_{s,m+n-1}, s = 0, 1, \ldots, N-m$ be the vector fragments of vector $\mathbf{x} \in V_{N+n-1}$. Look through consequently vector fragments $(\mathbf{y})_{s,m}, s = 0, 1, \ldots, N-m$ and check $A(\mathbf{y})_{s,m} \oplus \mathbf{a} = \mathbf{0}$. If this equation holds then under our assumptions of local affinity $(\mathfrak{A}, \mathfrak{B})$ of a function f we have $\mathfrak{B}(\mathbf{y})_{s,m+n-1} \oplus \mathbf{b} = \mathbf{0}$. Last equation with condition (4.1) give us l linear equations with respect of an initial state of $\mathrm{LFSR}(\chi, f)$ (i.e. $(\mathbf{x})_{0,n} = (x_0, \ldots, x_{n-1})^T$). Note that if $m+n \ll N$ and $2^k \ll N$ we can hope to cover initial uniquely by given linear equations.

5 Examples of a local affinity based inversion

5A Majority functions ([1],[2])

Let n be an odd positive integer. Suppose that a filtering function f of $\mathrm{LFSR}(\chi, f)$ is the majority function defined as follows

$$f(\mathbf{x}) = \begin{cases} 0, \mathrm{wt}(\mathbf{x}) \leqslant \frac{n-1}{2}; \\ 1, \mathrm{wt}(\mathbf{x}) \geqslant \frac{n+1}{2}. \end{cases} \tag{5.1}$$

The function (5.1) is a symmetric balanced function with $N_f = 2^{n-1} - \binom{n-1}{\frac{n-1}{2}}$ and algebraic immunity equals to $\lceil \frac{n}{2} \rceil = \frac{n+1}{2}$. Since $W_f(\mathbf{e}_0) = \ldots = W_f(\mathbf{e}_{n-1}) = \binom{n-1}{\frac{n-1}{2}}$, the function (5.1) is not a resilient function.

Now we describe some local affinities of functions defined by (5.1).

Lemma 5.1. *Let n be an odd positive integer, $m = 2, k = l = 2$. Let f be the majority function in $\mathcal{F}_n$ defined above. Then f have local affinities $(\mathfrak{A}_1, \mathfrak{B}_1)$ such that*

$$\mathfrak{A}_1 = (A_1, \mathbf{a}_1) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right),$$
$$\mathfrak{B}_1 = (B_1, \mathbf{b}_1) = \left(\begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

and $(\mathfrak{A}_2, \mathfrak{B}_2)$ such that

$$\mathfrak{A}_2 = (A_2, \mathbf{a}_2) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right),$$
$$\mathfrak{B}_2 = (B_2, \mathbf{b}_2) = \left(\begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right)$$

Proof. Let for some vector fragment $(\mathbf{y})_{i,2}$ of output vector $\mathbf{y}$ of $\mathrm{SR}(f)$ the equation $A_1(\mathbf{y})_{i,2} = \mathbf{a}_1$ holds. Then $f(x_i, \dots, x_{i+n-1}) = 0,\ f(x_{i+1}, \dots, x_{i+n}) = 1$. By (5.1) we obtain

$$\mathrm{wt}\left((x_i, \dots, x_{i+n-1})^T\right) = (n-1)/2 \tag{5.2}$$

and

$$\mathrm{wt}\left((x_{i+1}, \dots, x_{i+n})^T\right) = (n+1)/2. \tag{5.3}$$

Combining (5.2), (5.3) we get $x_i = 0$ and $x_{i+n} = 1$, i.e. the equation $B_1(\mathbf{x})_{i,n+1} = \mathbf{b}_1$ holds. In the same way we can proof the second assertion of this Lemma. □

To evaluate an efficiency of an attack it is to be found of values of some parameters. In particular we have to find a probability of an appearance of the event $\{y_i \neq y_{i+1}\}$. The event $\{y_i \neq y_{i+1}\}$ is called an alternation. The following assertions are needed for the sequel.

Theorem 5.2. *Let n be any odd positive integer. Let $LFSR(\chi, f)$ be a filter generator with a primitive connection polynomial χ of degree n and filtering function f in $\mathcal{F}_n$ of the form (5.1).*

Then the appearance number of events $\{y_i \neq y_{i+1}\}$ in output vector $\mathbf{y} = (y_0, \dots, y_{2^n-2}, y_{2^n-1})^T, y_0 = y_{2^n-1}$ is equal to $\binom{n-1}{\frac{n-1}{2}}$.

Proof. Note that under the condition of this Theorem for any output vector vector $\mathbf{y}' = (y'_0, \ldots, y'_{N-1})^T$, $N > 2^n - 1$ we have $\mathbf{y}'_i = y'_{i+2^n-1}$, $i = 0, 1, \ldots, N_2^n$. Hence an output vector $\mathbf{y} = (y_0, \ldots, y_{2^n-2}, y_{2^n-1})^T$, $y_0 = y_{2^n-1}$ contains all possible alterations of LFSR(χ, f). The proper input vector $\mathbf{x} = (x_0, \ldots, x_{2^n+n-1})^T$ contains a vector fragment equals to v for each $v \in V_n \setminus \{\mathbf{0}\}$.

By definition, put

$$V_{n,t} = \{\mathbf{x} \in V_n \mid \mathrm{wt}(\mathbf{x}) = t\},$$

$t = 0, 1, \ldots, n$. Consider the partition of the above set of the form

$$V_{n,t} = V_{n,t}^{(0)} \cup V_{n,t}^{(1)},$$

where $V_{n,t}^{(\varepsilon)} = \{\mathbf{x} \in V_n \mid \mathrm{wt}(\mathbf{x}) = t,\ x_1 = \varepsilon\},\ \varepsilon = 0, 1,\ t \neq 0, n$. It is obvious that for $t \neq 0, n$ we have

$$\#V_{n,t}^{(0)} = \binom{n-1}{t},\ \#V_{n,t}^{(1)} = \binom{n-1}{t-1}.$$

The alternation $(y_i, y_{i+1})^T = (0, 1)^T$ takes place at an output vector $\mathbf{y}$ of LFSR(χ, f) iff

$$(\mathbf{x})_{i,n} = (x_i, \ldots, x_{i+n-1})^T \in V_{n,\frac{n-1}{n}}^{(0)}$$

and

$$(\mathbf{x})_{i+1,n} = (x_{i+1}, \ldots, x_{i+n})^T \in V_{n,\frac{n+1}{n}},$$

i.e. $x_{i+n} = 1$. The alternation $(y_i, y_{i+1})^T = (1, 0)^T$ takes place in an output vector $\mathbf{y}$ of LFSR(χ, f) iff

$$(\mathbf{x})_{i,n} = (x_i, \ldots, x_{i+n-1})^T \in V_{n,\frac{n-1}{n}}^{(1)}$$

and

$$(\mathbf{x})_{i+1,n} = (x_{i+1}, \ldots, x_{i+n})^T \in V_{n,\frac{n-1}{n}},$$

i.e. $x_{i+n} = 0$.

Note that if $v \in V_{n,\frac{n-1}{n}}^{(0)}$ then $v \oplus 1 \in V_{n,\frac{n+1}{n}}^{(1)}$. By definition, put

$$O_n = \left\{(\mathbf{v}, \mathbf{v} \oplus \mathbf{1}) \mid \mathbf{v} \in V_{n,\frac{n-1}{n}}^{(0)}\right\}.$$

Let a couple $\left((x_i, \ldots, x_{i+n-1})^T, (x_j, \ldots, x_{j+n-1})^T\right)$ be from O_n. For an above couple using (2.1) we get

$$x_{i+n} \oplus x_{j+n} = \chi_1 x_{i+n-1} \oplus \ldots \oplus \chi_{n-1} x_{i+1} \oplus \chi_n x_i \oplus \chi_1 x_{j+n-1} \oplus \ldots \oplus \chi_{n-1} x_{j+1} \oplus \chi_n x_j = \chi_1 \oplus \ldots \oplus \chi_n.$$

Since a polynomial χ of degree n is primitive we have

$$x_{i+n} \oplus x_{j+n} = 0.$$

This means that:

- if $x_{i+n} = x_{j+n} = 1$, then $(\mathbf{x})_{i+1,n} \in V_{n,\frac{n+1}{n}}$; $(\mathbf{x})_{j+1,n} \in V_{n,\frac{n+1}{n}}$, i.e. we have the alternation $(y_i, y_{i+1})^T = (0,1)^T$;
- if $x_{i+n} = x_{j+n} = 0$, then $(\mathbf{x})_{i+1,n} \in V_{n,\frac{n-1}{n}}$; $(\mathbf{x})_{j+1,n} \in V_{n,\frac{n-1}{n}}$, i.e. we have the alternation $(y_i, y_{i+1})^T = (1,0)^T$.

Since only couple of the set O_n as fragments of input vector $\mathbf{x} = (x_0, x_1, \ldots, x_{2^n-2}, x_{2^n-1}, \ldots, x_{2^n+n-3}), x_{2^n-1} = x_0, \ldots, x_{2^n+n-3} = x_{n-1}$, generate alternations and takes place at the vector $\mathbf{x}$ once we get $r_n = \binom{n-1}{\frac{n-1}{2}}$. □

Let us assume that probability of alternation at output vector $\mathbf{y}$ is equals to $\binom{n-1}{\frac{n-1}{2}}/(2^n-1)$. Each alternation generates two linear equations with respect to initial state bits. Then the appearance of linear equation probability we can put $p_n = 2\binom{n-1}{\frac{n-1}{2}}/(2^n-1)$. By the relation $\binom{2\nu}{\nu} \sim 2^{2\nu}/\sqrt{\pi\nu}$ ([3]) we get $p_n \sim \sqrt{\frac{2}{\pi(n-1)}}$.

Consider now the complexity of the method. Let as above $\mathbf{y} = (y_0, \ldots, y_{N-1})^T \in V_N$ be an output vector and let $\mathbf{x} = (x_0, \ldots, x_{N+n-2})^T \in V_{N+n-1}$ be a proper input vector of LFSR(χ, f)

First step (precomputation). Each component $x_i, i = 0, 1, \ldots, N+n-2$ of the input vector $\mathbf{x}$ is a value of some linear function at $\mathcal{F}_n$ on the initial vector $(\mathbf{x})_{0,n} = \mathbf{v}$. These functions are:

$$\begin{aligned}
&x_0 = \xi_0(\mathbf{v}) = (\mathbf{e}_0, \mathbf{v}) = (\mathbf{c}_0, \mathbf{v}),\\
&x_1 = \xi_1(\mathbf{v}) = (\mathbf{e}_1, \mathbf{v}) = (\mathbf{c}_1, \mathbf{v}),\\
&\vdots\\
&x_{n-1} = \xi_{n-1}(\mathbf{v}) = (\mathbf{e}_{n-1}, \mathbf{v}) = (\mathbf{c}_{n-1}, \mathbf{v}),\\
&x_n = \xi_n(\mathbf{v}) = (\mathbf{e}_{n-1}, U\mathbf{v}) = (U^T\mathbf{e}_{n-1}, \mathbf{v}) = (\mathbf{c}_n, \mathbf{v}),\\
&x_{n+1} = \xi_{n+1}(\mathbf{v}) = (\mathbf{e}_{n-1}, U^2\mathbf{v}) = ((U^2)^T\mathbf{e}_{n-1}, \mathbf{v}) = (\mathbf{c}_{n+1}, \mathbf{x}),\\
&\vdots\\
&x_{n-1+j} = \xi_{n-1+j}(\mathbf{v}) = (\mathbf{e}_{n-1}, U^j\mathbf{v}) = ((U^j)^T\mathbf{e}_{n-1}, \mathbf{v}) = (\mathbf{c}_{n-1+j}, \mathbf{x}),\\
&\vdots\\
&x_{N-1} = \xi_{N-1}(\mathbf{v}) = (\mathbf{e}_{n-1}, U^{N-n}\mathbf{v}) = ((U^{N-n})^T\mathbf{e}_{n-1}, \mathbf{v}) = (\mathbf{c}_{N-1}, \mathbf{v}).
\end{aligned} \tag{5.4}$$

Relationship (5.4) mean that a running time of the first step is about $O(Nn^2)$, where $N = N(n)$.

Second step (generating of linear equations). The average number τ of linear equations corresponding to alterations of output vector $\mathbf{y}$ is equals to

$$\tau = \tau_n(N) = p_n N = 2N \binom{n-1}{\frac{n-1}{2}} \Big/ (2^n - 1). \tag{5.5}$$

Let us consider such a system of linear equations

$$B\mathbf{v} = \mathbf{b}, \tag{5.6}$$

where

$$B = \begin{bmatrix} b_{0\,0} & b_{0\,1} & \dots & b_{0\,n-1} \\ b_{1\,0} & b_{1\,1} & \dots & b_{1\,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{\tau-1\,0} & b_{\tau-1\,1} & \dots & b_{\tau-1\,n-1} \end{bmatrix}, \tag{5.7}$$

$\mathbf{v} \in V_n, \mathbf{b} \in V_n$. It is clear, that $\mathrm{rank}B = \mathrm{rank}[B|b]$ and the solution set of (5.5) includes an unknown initial vector $\mathbf{v} = (\mathbf{x})_{0,n}$ of LFSR(χ, f).

Now we introduce the following concept. Let entries $b_{i\,j}, i, j = 0, 1, \dots, n-1$ of matrix (5.6) be mutually independent random $\{0, 1\}$ - variables with a common uniform distribution. Denote the rank of a random matrix B as $\rho_n(\tau)$. In the sequel we shell deal with a useful statement.

Theorem 5.3. *([4]) Let s and r be given integer numbers such that $s \geqslant 0, s + r \geqslant 0$. If $n \to \infty$ and $\tau = n + r$, then*

$$P\left\{\rho_n(\tau) = n - s\right\} \to 2^{-s(r+s)} \prod_{i=s+1}^{\infty} \left(1 - \frac{1}{2^i}\right) \prod_{i=1}^{r+s} \left(1 - \frac{1}{2^i}\right)^{-1},$$

where the last multiplier we put 1 when $r + s = 0$.

From Theorem 5.3 it follows that $\rho_n(\tau)$ has a threshold property:

(i) if $\tau/n \to \alpha, 0 \leqslant \alpha < 1$, then $P\left\{\rho_n(\tau) = \tau\right\} \to 1$;

(ii) if $\tau/n \to \alpha,\ \alpha > 1$, then $P\left\{\rho_n(\tau) = n\right\} \to 1$.

Using (5.5) and Stirling's formula ([3]) we get a behavior of τ/n as $n \to \infty$:

$$\lim_{n\to\infty} \tau/n = \lim_{n\to\infty} \frac{2\binom{n-1}{\frac{n-1}{2}}N}{(2^n-1)n} = \lim_{n\to\infty} \frac{2(n-1)!N}{\left(\frac{n-1}{2}\right)!\left(\frac{n-1}{2}\right)!n(2^n-1)} =$$

$$= \lim_{n\to\infty} \frac{2\sqrt{2\pi(n-1)}(n-1)^{n-1}e^{-(n-1)}N}{\left(\sqrt{2\pi\left(\frac{n-1}{2}\right)}\right)^2\left(\left(\frac{n-1}{2}^{\frac{n-1}{2}}\right)\right)^2\left(e^{-\frac{n-1}{2}}\right)^2 n(2^n-1)} =$$

$$= \lim_{n\to\infty} \frac{2\sqrt{2\pi(n-1)}N}{\pi(n-1)\left(\frac{1}{2}\right)^{n-1} n(2^n-1)} = \lim_{n\to\infty} \sqrt{\frac{2}{\pi}}\frac{N}{n^{3/2}} \quad (5.8)$$

From (5.8) it follows that we can get $\tau/n \to \alpha, \alpha > 1$ with $N = O(n^{3/2})$. This means if $N = O(n^{3/2})$ and $\tau/n > 1$ the equation $\rho_\tau(n) = n$ holds with probability close to 1 and system (5.6) has a single solution. It will be $\mathbf{v} = (\mathbf{x})_{0,n}$, i.e. initial state of LFSR(χ, f).

Third step (converting initial state). To cover an initial state of LFSR(χ, f) we must find a solution of system (5.6). It's complexity is $O(n^w)$ where $w = \log_2(7) \approx 2.807$ corresponds to Strassen's exponent, which is the most efficient known method for Gaussian eliminations.

Table 1 shows complexities of several steps of method. Thus the method presented

	Complexity
1 step	$O(Nn^2) = O(n^{7/2}), N = O(n^{3/2})$
2 step	$O(n^{3/2})$
3 step	$O(n^w)$

Table 1.

above has polynomial complexity at about $O(n^{7/2})$ with success probability close to 1.

5B Symmetric Boolean Functions ([5],[6])

Definition 5.4. *A Boolean function $f \in \mathcal{F}_n$ is said to be symmetric if equations*

$$f(x_1, x_2, x_3, \ldots, x_n) = f(x_2, x_1, x_3, \ldots, x_n) = f(x_2, x_3, \ldots, x_n, x_1)$$

hold for any $\mathbf{x} = (x_1, \ldots, x_n)^T \in V_n$

Lemma 5.5. *Let f be any different from constant symmetric Boolean function at $\mathcal{F}_n$. Let $m = 2, k = 2, l = 1$. Then f have local affinities $(\mathfrak{A}'_1, \mathfrak{B}'_1)$ where*

$$\begin{aligned} \mathfrak{A}'_1 &= (A'_1, \mathbf{a}'_1) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right), \\ \mathfrak{B}'_1 &= (B'_1, \mathbf{b}'_1) = ((1, 0, \ldots, 0, 1), (1)) \end{aligned} \tag{5.9}$$

and $(\mathfrak{A}'_2, \mathfrak{B}'_2)$ where

$$\begin{aligned} \mathfrak{A}'_2 &= (A'_2, \mathbf{a}'_2) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right), \\ \mathfrak{B}'_2 &= (B'_2, \mathbf{b}'_2) = ((1, 0, \ldots, 0, 1), (1)) \end{aligned} \tag{5.10}$$

Proof. Suppose a fragment $(\mathbf{y})_{i,2}$ of the output vector $\mathbf{y}$ satisfies equality $A'_1(\mathbf{y})_{i,2} = \mathbf{a}'_1$, i.e. $(\mathbf{y})_{i,2} = (0, 1)^T$. Then $f(x_i, \ldots, x_{i+n-1}) = 0, f(x_{i+1}, \ldots, x_{i+n}) = 1$ where $(\mathbf{x})_{i,n} \in V_{n,s}, (\mathbf{x})_{i+1,n} \in V_{n,t}$ and $|s - t| = 1$. It is clear that $|s - t| = |x_i - x_{i+n}| = 1$. Thus we get $x_i \neq x_{i+n}$, i.e. $x_i \oplus x_{i+n} = 1$. Consequently $B'_1(\mathbf{x})_{i,n+1} = \mathbf{b}'_1$. It can be shown in the same that second assertion of the lemma holds. □

Definition 5.6 ([5])**.** *Let n be an odd positive integer and $f \in \mathcal{F}_n$ be a symmetric function. We say that f is trivial balanced function if $f(\mathbf{x} \oplus \mathbf{1}) = f(\mathbf{1}) \oplus 1$ for any $\mathbf{x} = (x_1, \ldots, x_n)^T \in V_n$.*

Lemma 5.7. *Let $n = 2k+1, k > 0$. Let $LFSR(\chi, f)$ be a filter generator with a primitive connection polynomial χ of degree n and a symmetric primitive balanced filtering function f at $\mathcal{F}_n$.*

Then the appearance number r_n of events $\{y_i \neq y_{i+1}\}$in output vector $\mathbf{y} = (y_0, \ldots, y_{2^n-2}, y_{2^n-1})^T, y_0 = y_{2^n-1}$ satisfies the inequality

$$r_n \geqslant \binom{n-1}{\frac{n-1}{2}}.$$

Proof. The proof follows from Theorem 5.2. □

Under the conditions of Lemma 5.7 we have

$$Pr\{y_i \neq y_{i+1}\} \geqslant \binom{n-1}{\frac{n-1}{2}} \Big/ (2^n - 1).$$

Since each alternation in this case generates only one linear equation the appearance of linear equation probability satisfies the inequality

$$p_n \geqslant \binom{n-1}{\frac{n-1}{2}} \Big/ (2^n - 1).$$

5C Rotation symmetric functions ([7],[8], [9], [10])

Definition 5.8. *Let n be positive integer and $f \in \mathcal{F}_n$. We say that f is rotation symmetric function if*

$$f(x_1, x_2, \ldots, x_n) = f(x_2, \ldots, x_n, x_1)$$

for any $\mathbf{x} = (x_1, \ldots, x_n)^T \in V_n$.

Note that every symmetric function is a rotation symmetric function.

Lemma 5.9. *Let f be any different from constant rotation symmetric function at $\mathcal{F}_n$. Let $m = 2, k = 2, l = 1$. Then f have local affinities $(\mathfrak{A}'_1, \mathfrak{B}'_1)$ and $(\mathfrak{A}'_2, \mathfrak{B}'_2)$ of the form (5.9), (5.10) accordingly.*

Proof. It can be shown in the usual way that is in Lemma 5.5. □

Lemma 5.10. *Let $n = 2k+1, k > 0$. Let LFSR(χ, f) be a filter generator with a primitive connection polynomial χ of degree n and a rotation symmetric primitive balanced filtering function f at $\mathcal{F}_n$.*

Then the appearance number r_n of events $\{y_i \neq y_{i+1}\}$ in output vector $\mathbf{y} = (y_0, \ldots, y_{2^n-2}, y_{2^n-1})^T, y_0 = y_{2^n-1}$ satisfies the inequality

$$r_n \geqslant \binom{n-1}{\frac{n-1}{2}}.$$

Proof. The proof follows from Theorem 5.2. □

5D "Minimal advantage" functions

Let $n = 2p + 1$. A filtering function $f \in \mathcal{F}_n$ of LFSR(χ, f) is said to be a "minimal advantage" function if it satisfies conditions

$$f(\mathbf{x}) = f(\mathbf{x^1}, \mathbf{x^2}) = \begin{cases} 1, \mathrm{wt}(\mathbf{x^1}) \geqslant \mathrm{wt}(\mathbf{x^2}); \\ 0, \mathrm{wt}(\mathbf{x^1}) < \mathrm{wt}(\mathbf{x^2}); \end{cases} \tag{5.11}$$

where $\mathbf{x} = (\mathbf{x^1}, \mathbf{x^2}) \in V_n, \mathbf{x^1} = (x_0, \ldots, x_{p-1})^T \in V_p, \mathbf{x^2} = (x_p, \ldots, x_{n-1})^T \in V_{p+1}$.

Proposition 5.11. *A Boolean function f of the form (5.11) is balanced.*

Proof. The proof is by direct calculation. □

Lemma 5.12. *Let $n = 2p+1, m = 2, k = 2, l = 1$. The "minimal advantage" function $f \in \mathcal{F}_n$ have local affinity $(\mathfrak{A}'', \mathfrak{B}'')$, where*

$$\mathfrak{A}'' = (A'', a'') = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right),$$
$$\mathfrak{B}'' = (B'', b'') = (0, \ldots, 0, 1, 0, \ldots, 0), (1)) = (\mathbf{e}_p, (1)).$$

Proof. Let $\mathbf{y} = (y_0, \ldots, y_{m-1})^T \in V_m$ be an output vector and $\mathbf{x} = (x_0, \ldots, x_{m+n-2})^T \in V_{m+n-1}$ be a proper input vector of $\mathrm{SR}(f)$. Suppose that $(\mathbf{y})_{i,2} = (0,1)^T$ for some $i = 0, 1, \ldots, m+n-3$. Then $f(x_0, \ldots, x_{p-1}, x_p, \ldots, x_{n-1}) = 0$ and $f(x_1, \ldots, x_p, x_{p+1}, \ldots, x_n) = 1$. By (5.11), it follows that

$$\begin{aligned} \mathrm{wt}(x_0, \ldots, x_{p-1}) &< \mathrm{wt}(x_p, \ldots, x_{n-1}), \\ \mathrm{wt}(x_1, \ldots, x_p) &\geqslant \mathrm{wt}(x_{p+1}, \ldots, x_n). \end{aligned} \tag{5.12}$$

If $x_p = 0$ it is such a chain of inequalities holds

$$\mathrm{wt}((x_1, \ldots, x_p)^T) \leqslant \mathrm{wt}((x_0, \ldots, x_{p-1})^T) < \mathrm{wt}((x_p, \ldots, x_{n-1})^T) \leqslant \mathrm{wt}((x_{p+1}, \ldots, x_n)^T).$$

This contradiction of second inequality of (5.12) proves the Lemma.

□

5E Finite automata ([11], [12])

Problem of finite automata analysis often involve restoring a proper input sequence by known output sequence ([13], [14], [15], [16], [17], [18], [19]). Obviously these problems have cryptography aspects. In this subsection we present a class of Boolean functions with local affinity property which permits to restore input sequences of an automaton $\mathrm{SR}(f)$.

Let $f \in func$ be a function linearly dependent of x_{n-1}, i.e.

$$f(x_0, \ldots, x_{n-2}, x_{n-1}) = f'(x_0, \ldots, x_{n-2}) \oplus x_{n-1}. \tag{5.13}$$

By [19], it follows that f is a perfectly balanced function. Consequently $\#(f_m^*)^{-1}(\mathbf{y}) = 2^{n-1}$ for any m and for every $\mathbf{y} \in V_m$. For an output vector $\mathbf{y} \in V_m$ of an automation $\mathrm{SR}(f)$ denote by

$$M_{\mathbf{y}}(f) = \begin{bmatrix} \mathbf{x^1} \\ \mathbf{x^2} \\ \vdots \\ \mathbf{x^{2^{n-1}}} \end{bmatrix} = \begin{bmatrix} x_0^1 & x_1^1 & \ldots & x_{m+n-2}^1 \\ x_0^2 & x_1^2 & \ldots & x_{m+n-2}^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{2^{n-1}} & x_1^{2^{n-1}} & \ldots & x_{m+n-2}^{2^{n-1}} \end{bmatrix} \tag{5.14}$$

— a $2^{n-1} \times (m+n-1)$-matrix which contains proper input vectors $x^1, \ldots, x^{2^{n-1}} \in (f_m^*)^{-1}(\mathbf{y})$ as rows. Consider a following set of Boolean functions.

Definition 5.13. *By D_n denote a subset of $\mathcal{F}_n$ which contains only Boolean functions of the form (5.13) with a property: for any $f \in D_n$ where exists $m = m(f)$ and $\mathbf{y} = \mathbf{y}(f) \in V_m$ such that*

$$\begin{aligned} &x_m^1 = x_m^2 = \ldots = x_m^{2^{n-1}} \\ &x_{m+1}^1 = x_{m+1}^2 = \ldots = x_{m+1}^{2^{n-1}} \\ &\vdots \\ &x_{m+n-2}^1 = x_{m+n-2}^2 = \ldots = x_{m+n-2}^{2^{n-1}}, \end{aligned}$$

at (5.14).

It is clear that Boolean function f has local affinity property $(\mathfrak{A}, \mathfrak{B})$, where $\mathfrak{A} = (A, \mathbf{a}), \mathfrak{B} = (B, \mathbf{b})$ with $B = E_k, \mathbf{b} = \mathbf{b}(\mathbf{y}) \in V_k$. Note that k in this case is not bounded.

Example 5.14. *Let $n = 3$ and $f(x_0, x_1, x_2) = x_0 x_1 \oplus x_2$. Suppose that $y_0 = (0,1,0,1)^T \in V_4$ is an output vector of SR(f). Then*

$$M_{y_0}(f) = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}, \tag{5.15}$$

By (5.15) so, that a function f have a local affinity property $(\mathfrak{A}, \mathfrak{B})$ where

$$\begin{aligned} \mathfrak{A} = (A, \mathbf{a}) &= \left(E_4, (0,1,0,1)^T\right), \\ \mathfrak{B} = (b, \mathbf{b}) &= \left(E_2, (0,1)^T\right). \end{aligned}$$

Let m' be any positive integer and let $\mathbf{y}'$ be any vector at $V_{m'}$. Consider a vector $(\mathbf{y_0}, \mathbf{y}') \in V_{m+m'}$ as an output vector of SR(f). It can be shown that f have a local affinity property $(\overline{\mathfrak{A}}, \overline{\mathfrak{B}})$ where

$$\begin{aligned} \overline{\mathfrak{A}} = (\overline{A}, \overline{\mathbf{a}}) &= \left(E_4, (0,1,0,1)^T\right), \\ \overline{\mathfrak{B}} = (\overline{B}, \overline{\mathbf{b}}) &= \left(E_{2+m'}, ((0,1), \mathbf{b}(\mathbf{y}'))^T\right), \end{aligned}$$

$\mathbf{b}(\mathbf{y}') \in V_{m'}$. *In other words, if an output vector $\mathbf{y} \in V_N$ of SR(f) such that $(\mathbf{y})_{i,4} = \mathbf{y_0}$, then a fragment $(\mathbf{x})_{i+4,N-i-2}$ of input vector $\mathbf{x} \in V_{N+2}$ we get uniquely.*

References

[1] M. Lobanov. Tight bound between nonlinearity and algebraic immunity. http://eprint.iacr.org/2005/441.

[2] D.K. Dalai, S. Maitra, S. Sarcar. Basic Theory in Constraction of Boolean Functions with Maximum Possible Algebraic Immunity. http://eprint.iacr.org/2005/229.

[3] W. Feller. An Introdaction to Probability Theory and Application. Volume 1. Wiley, New York, 1970.

[4] V. Kolchin. Random Mappings. Optimization Software inc., New York, 1986.

[5] A. Canteaut, M. Videau. Symmetric Boolean function. IEEE Transaction on Information Theory IT-51 (2005), no. 8, pp. 2791-2811.

[6] A. Braeken, B. Preneel. On the algebraic immunity of symmetric Boolean function. Indocrypt 2005, LNCS 3348, Springer-Verlag, 2004, pp. 120-135.

[7] D.K. Dalai, S. Maitra, P. Stanica. Results on Rotation Symmetric Bent Functions. http://eprint.iacr.org/2005/118.

[8] P. Ke, Z. Chang, Q. Wen. Results on Rotation Symmetric Boolean Functions. http://eprint.iacr.org/2005/130.

[9] A. Maximov. Classes of Plateaud Rotation Symmetric Boolean Functions under Transformation of Walsh Spectra. http://eprint.iacr.org/2004/354.

[10] S. Kavut, S. Maitra, P. Sarkar, M. D. Yucel. Enumeration of 9-variable Rotation Symmetric Boolean Functions having Nonlinearity $>$ 240. http://eprint.iacr.org/2006/249.

[11] B. Trakhtenbrot, Y. Barzdin. Finite automata (behavior and syntesis). Moscow, Nauka, 1970 (in Russian).

[12] V. Kudrjavtsev, S. Aleshin, A. Podkolzin. Introduction to automata theory. Moscow, Nauka, 1985 (in Russian).

[13] D.A. Huffman. Canonical forms for information-lossless finite-state logical mashines. IRE Trans. Circuit Th., 6, Spec. Suppl, 1959, pp. 41-59.

[14] D.A. Huffman. Notes on information-lossless finite-state automata. Nuovo cimento, 13, suppl. 2, 1959, pp. 397-405.

[15] S. Even. On information-lossless automata of finite order. IEEE Trans. Electronic Comput., 14, 1965, 4, pp. 561-569.

[16] A. Kurmit. Finite order automata without information loss. Riga, Zinatne, 1972 (in Russian).

[17] O. Logachev, A. Sal'nikov, V. Jaschenko. Boolean Functions in Coding Theory and Cryptology. MCCME, Moscow, 2004 (in Russian).

[18] O. Logachev, G. Proskurin, V. Jaschenko. Local inversion of an automata by means of automata. Diskr. Mat., v. 7, no. 2, 1995, pp. 19-33 (in Russian).

[19] S. Sumarokov. Functions of zero defect and invertability of some class of coders. Obozrenie prom. i prikl. mat., 1994, no. 1, pp. 33-55 (in Russian).