THE METHOD BASED ON BINARY MC(s,r) UNDER ADDITIVE DISTORTIONS FOR ESTIMATING THE MODEL PARAMETERS OF GEFFE'S GENERATOR

A. I. Piatlitski
Research Institute for Applied Problems of Mathematics and Informatics
Minsk, BELARUS
e-mail: piatlitski@bsu.by

Abstract

Statistical estimators for the parameters of the binary Markov chain with partial connections under additive distortions are presented. Using these estimators, we recover the model parameters of Geffe's generator by its output sequence.

1 Introduction

Cryptographic generators play an important role in information security. Many cryptographic generators use linear feedback shift registers (LFSRs) as building blocks [1]. One of the ways of combining LFSRs gives Geffe's generator [1]. This generator consists of three LFSRs connected as shown in Figure 1.

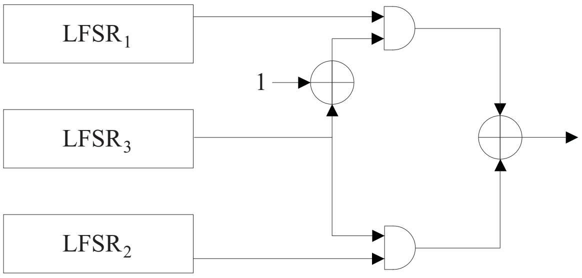

Figure 1: The scheme of Geffe's generator

If x_t^1, x_t^2, x_t^3 are output bits of LFSR$_1$, LFSR$_2$, and LFSR$_3$, respectively, then output signal of the generator at the moment t is

$$y_t = \overline{x_t^3} x_t^1 \oplus x_t^3 x_t^2 = x_t^1 \oplus x_t^3 (x_t^1 \oplus x_t^2). \tag{1}$$

Suppose that the three LFSRs have distinct primitive characteristic polynomials of degree s_1, s_2, and s_3, respectively. The generator would then have [1] linear complexity $(s_1 + s_2)s_3 + s_1$ and period $lcm(2^{s_1} - 1, 2^{s_2} - 1, 2^{s_3} - 1)$. Thus, Geffe's generator has attractive properties (period, linear complexity).

In this paper, we present a new method based on the binary Markov chain with partial connections under additive distortions for estimating the model parameters of Geffe's generator.

2 The Markov chain with partial connections

Let $A = \{0, 1, \ldots, N-1\}$ be a finite set; $J_i^k = (j_i, j_{i+1}, \ldots, j_k) \in A^{k-i+1}$ be a subsequence of $k-i+1$ indices, $k \geq i$; $\{x_t\}$ be a homogeneous and ergodic Markov chain of the s-th order with the state space A, the transition probabilities

$$p_{J_1^{s+1}} = \mathbf{P}\{x_{t+s} = j_{s+1} | x_{t+s-1} = j_s, \ldots, x_t = j_1\},\ J_1^{s+1} \in A^{s+1},\ t \in \mathbb{N}.$$

Definition 1. *The Markov chain $\{x_t\}$ is called the Markov chain of the s-th order with r partial connections and is denoted by $MC(s, r)$ [2] if*

$$p_{J_1^{s+1}} = p_{j_1,\ldots,j_s,j_{s+1}} = q_{j_{m_1^0},\ldots,j_{m_r^0},j_{s+1}},\ J_1^{s+1} \in A^{s+1}, \tag{2}$$

where $r \in \{1, 2, \ldots, s\}$ is the number of connections; $M_r^0 = (m_1^0, \ldots, m_r^0) \in \mathrm{M}$ is the integer-valued vector with r order components $1 = m_1^0 < m_2^0 < \ldots < m_r^0 \leq s$, called the pattern, M is the set of all such vectors; $Q = \left(q_{J_1^{r+1}}\right)_{J_1^{r+1} \in A^{r+1}}$ is the stochastic matrix.

Relationship (2) means that the transition probability of the process $\{x_t\}$ to the state j_{s+1} depends not on all s preceding states $j_1, \ldots, j_s$ but only on r selected states $j_{m_1^0}, \ldots, j_{m_r^0}$. Thus, the transition matrix for the MC(s, r) is completely determined by $N^r(N-1)$ parameters, instead of $N^s(N-1)$ parameters. The Markov chain with partial connections is the stochastic generalization of LFSR [1], where the length of LFSR is the order s, the number of the nonzero coefficients of the characteristic polynomial is the number of connections r, the indexes of the nonzero coefficients is the pattern M_r^0.

Introduce the notation: $X_1^n = (x_1, x_2, \ldots, x_n) \in A^n$ is the realization of the MC(s, r) of the length $n > s$; $F\left(J_i^{i+s-1}; M_r\right) = (j_{i+m_1-1}, j_{i+m_2-1}, \ldots, j_{i+m_r-1})$ is the selector of the r-th order for some pattern $M_r \in \mathrm{M}$, $J_i^{i+s-1} \in A^s$, $i \in \mathbb{N}$; $\delta_{J_1^k, I_1^k} = \prod_{l=1}^k \delta_{j_l, i_l}$ is the Kronecker symbol for J_1^k, $I_1^k \in A^k$, $k \in \mathbb{N}$;

$$\nu_{J_1^{r+1}}(X_1^n; M_r) = \sum\nolimits_{t=1}^{n-s} \delta_{F\left(X_t^{t+s-1}; M_r\right), J_1^r} \delta_{x_{t+s}, j_{r+1}},\ J_1^{r+1} \in A^{r+1},$$

are the frequency statistics; $\mu_{J_1^{r+1}}(M_r) = \mathbf{P}\{F\left(X_t^{t+s-1}; M_r\right) = J_1^r, x_{t+s} = j_{r+1}\}$ is the probability distribution of the $(r+1)$-tuple; $\hat{\mu}_{J_1^{r+1}}(M_r) = \nu_{J_1^{r+1}}(X_1^n; M_r)/(n-s)$ is the frequency estimator for the probability $\mu_{J_1^{r+1}}(M_r)$; the point instead of any index means summation on all possible values of this index.

The consistent estimators for the parameters Q, M_r^0 [2] are

$$\hat{Q} = (\hat{q}_{J_1^{r+1}})_{J_1^{r+1} \in A^{r+1}},\ \hat{q}_{J_1^{r+1}} = \hat{\mu}_{J_1^{r+1}}(M_r^0)/\hat{\mu}_{J_1^r \cdot}(M_r^0), \tag{3}$$

$$\hat{M}_r = \arg\min\nolimits_{M_r \in \mathrm{M}} \hat{H}(M_r), \tag{4}$$

where $\hat{H}(M_r) = -\sum_{J_1^{r+1} \in A^{r+1}} \hat{\mu}_{J_1^{r+1}}(M_r) \ln\left(\hat{\mu}_{J_1^{r+1}}(M_r)/\hat{\mu}_{J_1^r \cdot}(M_r)\right)$.

The consistent estimators for the parameters s, r using the Bayesian Information Criterion [2] are defined by the minimization:

$$BIC(\hat{s}, \hat{r}) \rightarrow \min\nolimits_{s_- \leq \hat{s} \leq s_+,\, r_- \leq \hat{r} \leq r_+}, \tag{5}$$

where $BIC(s, r) = n\hat{H}(\hat{M}_r) + (\sum\limits_{J_1^r \in A^r} |D_{J_1^r}| - N^r)\frac{\ln n}{2}$, $D_{J_1^r} = \{j_{r+1} \in A : \hat{\mu}_{J_1^{r+1}}(\hat{M}_r) > 0\}$.

Definition 2. *The binary Markov chain of the s-th order with r partial connections under additive distortions [3] is defined by the equation*

$$y_t = x_t \oplus \xi_t,\ t \in \mathbb{N}, \tag{6}$$

where $x_t \in A = \{0,1\}$ is the nonobservable binary MC(s,r), $\xi_t \in A$ is the nonobservable sequence of independent and identically distributed binary random variables, $\mathbf{P}\{\xi_t = 0\} = 1 - \mathbf{P}\{\xi_t = 1\} = p > 0.5$; $\{x_t\}$ and $\{\xi_t\}$ are independent.

Introduce the notation: $Y_1^n = (y_1, y_2, \ldots, y_n) \in A^n$ is the realization of the model (6) of the length $n > s$; $b_{K_1^{r+1}}(M_r) = \mathbf{P}\{F\big(Y_t^{t+s-1}; M_r\big) = K_1^r, y_{t+s} = k_{r+1}\}$ is the probability distribution of the $(r{+}1)$-tuple for the model (6); $\tilde{b}_{K_1^{r+1}}(M_r) = \nu_{K_1^{r+1}}(Y_1^n; M_r)/(n{-}s)$ is the frequency estimator for the probability $b_{K_1^{r+1}}(M_r)$; $w(\cdot)$ is the Hamming weight. Further, let us assume that the parameter p is known.

The consistent estimator for the probability $\mu_{J_1^{r+1}}(M_r)$, found by Y_1^n, [2] is

$$\tilde{\mu}_{J_1^{r+1}}(M_r) = \left(\frac{p}{2p-1}\right)^{r+1} \sum\nolimits_{K_1^{r+1} \in A^{r+1}} \tilde{b}_{K_1^{r+1}}(M_r) \left(\frac{p-1}{p}\right)^{w(J_1^{r+1} \oplus K_1^{r+1})}.$$

By the “plug-in” approach the consistent estimators $\tilde{Q}$, $\tilde{M}_r$, $\tilde{r}$, $\tilde{s}$ for the parameters Q, M_r^0, r, s can be computed by the estimators $\tilde{\mu}_{J_1^{r+1}}(M_r)$, $J_1^{r+1} \in A^{r+1}$, and formulas (3)–(5).

For estimation of the nonobservable realization X_1^n we use the Viterbi algorithm:

$$\tilde{X}_{n-s+1}^n = \arg\max\nolimits_{J_1^s \in A^s} \gamma_{J_1^s}(n-s+1),$$

$$\tilde{x}_t = \arg\max\nolimits_{j \in A} q_{F(j, \tilde{X}_{t+1}^{t+s-1}; M_r^0), \tilde{x}_{t+s}} \gamma_{j, \tilde{X}_{t+1}^{t+s-1}}(t),\ t = n-s, n-s-1, \ldots, 1, \tag{7}$$

where $\gamma_{J_2^{s+1}}(t{+}1) = p\left(\frac{1-p}{p}\right)^{k_{t+s} \oplus j_{s+1}} \max\limits_{j_1 \in A} q_{F(J_1^s; M_r^0), j_{s+1}} \gamma_{J_1^s}(t)$, $\gamma_{J_1^s}(1) = \frac{p^s}{2^s}\left(\frac{1-p}{p}\right)^{w\left(J_1^s \oplus K_1^s\right)}$.

3 Estimation of the parameters of Geffe’s generator

The algorithm based on the model (6) for estimating the parameters of Geffe’s generator by its output sequence consists of the following steps.

Step 1 is finding of the characteristic polynomials of LFSR$_1$, LFSR$_2$. The weakness of Geffe’s generator comes from the fact [4] that the coincidence probability between the output signal y_t and the output bits x_t^1 equals to

$$\mathbf{P}\left\{y_t = x_t^1\right\} = \mathbf{P}\left\{x_t^3 = 0\right\} + \mathbf{P}\left\{x_t^3 = 1\right\} \mathbf{P}\left\{x_t^2 = x_t^1\right\} = 0.75. \tag{8}$$

The coincidence probability between y_t and x_t^2 can be estimated similarly. From equations (1), (8), we have the output signal of Geffe’s generator can be described by the model (6) with the parameter $p = 0.75$. Thus, using the observable output sequence of this generator and the estimators for the parameters of the model (6), we find the characteristic polynomials of LFSR$_1$, LFSR$_2$.

Step 2 is recovery of the output bits of LFSR$_1$, LFSR$_2$. Since the characteristic polynomials of LFSR$_1$, LFSR$_2$ are known, then the sequences $\{x_t^1\}$, $\{x_t^2\}$ can be recovered by the linear syndrome algorithm [4] or formula (7).

Step 3 is finding of the characteristic polynomial of LFSR$_3$. Define

$$\bar{x}_t^3 = \begin{cases} i, & \text{if } x_t^1 \neq x_t^2,\ y_t = x_t^{i+1},\ i \in \{0,1\}, \\ \eta_t, & \text{if } x_t^1 = x_t^2,\ \eta_t \in \{0,1\} \text{ is i.i.d. random variables, } \mathbf{P}\{\eta_t = 0\} = 1/2. \end{cases}$$

Since, as can be easily seen,

$$\mathbf{P}\left\{x_t^3 = \bar{x}_t^3\right\} = 1 - \mathbf{P}\left\{x_t^3 \neq \bar{x}_t^3\right\} = 1 - \mathbf{P}\left\{x_t^1 = x_t^2\right\} \mathbf{P}\left\{x_t^3 \neq \eta_t\right\} = 0.75,$$

we have the sequence $\{\bar{x}_t^3\}$ can be described by the model (6) with the parameter $p = 0.75$. Thus, using the estimators for the parameters of the model (6), we find the characteristic polynomial of LFSR$_3$.

Step 4 is recovery of the output bits of LFSR$_3$. Taking into account the sequence $\{\bar{x}_t^3\}$ and the knowledge of the characteristic polynomial for LFSR$_3$, the sequence $\{x_t^3\}$ can be fully recovered by the linear syndrome algorithm [4] or formula (7).

Thus, despite having high period and moderately high linear complexity, Geffe's generator succumbs to attack, as described above.

4 Acknowledgments

This research was supported by Research grant No. F09M-042 from the Belarusian Republican Foundation for Fundamental Research.

References

[1] Kharin Yu.S. et al. (2003) *Mathematical and computer bases of cryptology*. New knowledge, Minsk. (in Russian).

[2] Kharin Yu.S., Piatlitski A.I. (2007) A Markov chain of order s with r partial connections and statistical inference on its parameters. *Discrete Mathematics and Applications*. Vol. **17**, pp. 295-317.

[3] Piatlitski A.I., Kharin Yu.S. (2008) Statistical analysis of binary Markov chain with partial connections under additive distortions. *Proc. of the National Academy of Sciences of Belarus, Ser. Phys.-Math. Sci.* No. **4**, pp. 30-36. (in Russian).

[4] Zeng K. et al. (1991) An improved linear syndrome algorithm in cryptanalysis with applications. *Lecture Notes In Computer Science*. Vol. **537**, pp. 34-47.