Parallel generator of $q$-valued pseudorandom sequences based on arithmetic polynomials

Abstract. A new method for parallel generation of $q$-valued pseudorandom sequence based on the presentation of systems generating logical formulae by means of arithmetic polynomials is proposed. Fragment consisting of $k$-elements of $q$-valued pseudorandom sequence may be obtained by means of single computing of a single recursion numerical formula. It is mentioned that the method of the “arithmetization” of generation may be used and further developed in order to protect the encryption gears from cryptographic onset, resulting in the initiating of mass hardware failures.

Streszczenie. Zaproponowano metodę równoległej generacji $q$-wartościowych sekwencji pseudolosowych na podstawie przedstawienia generujących układów rekurencyjnych wzorców logicznych za pomocą wielomianów liczbowych. Fragment zawierający $k$-elementów $q$-wartościowych sekwencji pseudolosowej można uzyskać za pomocą jednokrotnego obliczania jednego ze wzorców liczbowych. Zwrócono uwagę na to, że propo- onowana metoda „arytmetyzacji” generowania takich sekwencji może w przyszłości być rozpowszechniona na przypadek zabezpeżenia urządzeń kryptograficznych przed kryptanalyczymi atakami, polegającymi na wywoływaniu masowych zaburzeń funkcjonowania ośrędu. (Równoległy generator $q$-wartościowych sekwencji pseudolosowych wykorzystujący wielomiany arytmetyczne)

Keywords: cryptographic protection of information, pseudo-random sequences, residue number system, modular arithmetic

Słowa kluczowe: Kryptograficzna ochrona informacji, sekwencje pseudolosowe, system resztkowy, arytmetyka modularna

Introduction

As we know, PRS over $\mathbb{GF}(q)$ is defined as $L=q^r-1$;

\[ s_{n+r} = p_{r-1}s_{n+r-1} + p_{r-2}s_{n+r-2} + \ldots + p_0s_n \pmod{q}, \]

where $p_j \in \mathbb{GF}(q)$, and $r$ is $P(z)$ polynomial order, $r \leq n$, and to the constructed according to it recurrent equation:

In general case $q$-LFSR consists of $D_j \ (j = 0, 1, \ldots, r - 1)$ cells and has the following initial fill: $s_0, s_1, \ldots, s_{r-1}$. Here the “cell” is the $[\log_2 q]$ parallel stage register ($\lfloor x \rfloor$ being the least integral number equal or more than $x$). After the first cycle $q$-LFSR has the following fill: $s_1, s_2, \ldots, s_r$. In general $q$-LFSR generates infinite $q$-valued PRS: $s_0, s_1, s_2, \ldots, s_{r-1}, \ldots$ [2].

In notation of linear algebra the next $q$-valued element of PRS $s_{n+r}$ is represented as a product:

\[
\begin{bmatrix}
  s_{n+r} \\
  s_{n+r-1} \\
  \vdots \\
  s_{n+2} \\
  s_{n+1}
\end{bmatrix}^T =
\begin{bmatrix}
  s_{n+r-1} \\
  s_{n+r-2} \\
  \vdots \\
  s_{n+1} \\
  s_{n}
\end{bmatrix}^T \begin{bmatrix}
  p_{r-1} & 1 & 0 & \ldots & 0 \\
  p_{r-2} & 0 & 1 & \ldots & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  p_1 & 0 & 0 & \ldots & 1 \\
  p_0 & 0 & 0 & \ldots & 0
\end{bmatrix}.
\]

In the Fig. 1 Structural diagram of the sequential $q$-LFSR functioning is shown.

As we know, PRS over $\mathbb{GF}(q)$ has a range of “useful” structural properties, including [2, 3]:

- number of symbols at the period of PRS or PRS period is defined as $L=q^r-1$;
- addition of elements in a PRS with elements of the same PRS period is equal to $q^r-1$, and to the constructed according to it recurrent equation:

\[
\begin{bmatrix}
  s_{n+r} \\
  s_{n+r-1} \\
  \vdots \\
  s_{n+2} \\
  s_{n+1}
\end{bmatrix}^T =
\begin{bmatrix}
  s_{n+r-1} \\
  s_{n+r-2} \\
  \vdots \\
  s_{n+1} \\
  s_{n}
\end{bmatrix}^T \begin{bmatrix}
  p_{r-1} & 1 & 0 & \ldots & 0 \\
  p_{r-2} & 0 & 1 & \ldots & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  p_1 & 0 & 0 & \ldots & 1 \\
  p_0 & 0 & 0 & \ldots & 0
\end{bmatrix}.
\]

In the Fig. 1 Structural diagram of the sequential $q$-LFSR functioning is shown.

As we know, PRS over $\mathbb{GF}(q)$ has a range of “useful” structural properties, including [2, 3]:

- number of symbols at the period of PRS or PRS period is defined as $L=q^r-1$;
- addition of elements in a PRS with elements of the same PRS period is equal to $q^r-1$, and to the constructed according to it recurrent equation:

\[
\begin{bmatrix}
  s_{n+r} \\
  s_{n+r-1} \\
  \vdots \\
  s_{n+2} \\
  s_{n+1}
\end{bmatrix}^T =
\begin{bmatrix}
  s_{n+r-1} \\
  s_{n+r-2} \\
  \vdots \\
  s_{n+1} \\
  s_{n}
\end{bmatrix}^T \begin{bmatrix}
  p_{r-1} & 1 & 0 & \ldots & 0 \\
  p_{r-2} & 0 & 1 & \ldots & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  p_1 & 0 & 0 & \ldots & 1 \\
  p_0 & 0 & 0 & \ldots & 0
\end{bmatrix}.
\]

In the Fig. 1 Structural diagram of the sequential $q$-LFSR functioning is shown.

As we know, PRS over $\mathbb{GF}(q)$ has a range of “useful” structural properties, including [2, 3]:

- number of symbols at the period of PRS or PRS period is defined as $L=q^r-1$;
- addition of elements in a PRS with elements of the same PRS period is equal to $q^r-1$, and to the constructed according to it recurrent equation:

\[
\begin{bmatrix}
  s_{n+r} \\
  s_{n+r-1} \\
  \vdots \\
  s_{n+2} \\
  s_{n+1}
\end{bmatrix}^T =
\begin{bmatrix}
  s_{n+r-1} \\
  s_{n+r-2} \\
  \vdots \\
  s_{n+1} \\
  s_{n}
\end{bmatrix}^T \begin{bmatrix}
  p_{r-1} & 1 & 0 & \ldots & 0 \\
  p_{r-2} & 0 & 1 & \ldots & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  p_1 & 0 & 0 & \ldots & 1 \\
  p_0 & 0 & 0 & \ldots & 0
\end{bmatrix}.
\]

In the Fig. 1 Structural diagram of the sequential $q$-LFSR functioning is shown.

As we know, PRS over $\mathbb{GF}(q)$ has a range of “useful” structural properties, including [2, 3]:

- number of symbols at the period of PRS or PRS period is defined as $L=q^r-1$;
- addition of elements in a PRS with elements of the same PRS period is equal to $q^r-1$, and to the constructed according to it recurrent equation:

\[
\begin{bmatrix}
  s_{n+r} \\
  s_{n+r-1} \\
  \vdots \\
  s_{n+2} \\
  s_{n+1}
\end{bmatrix}^T =
\begin{bmatrix}
  s_{n+r-1} \\
  s_{n+r-2} \\
  \vdots \\
  s_{n+1} \\
  s_{n}
\end{bmatrix}^T \begin{bmatrix}
  p_{r-1} & 1 & 0 & \ldots & 0 \\
  p_{r-2} & 0 & 1 & \ldots & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  p_1 & 0 & 0 & \ldots & 1 \\
  p_0 & 0 & 0 & \ldots & 0
\end{bmatrix}.
\]
Fig. 1. Structural diagram of the operation of the sequential $q$-LFSR in accordance with formula (1) $\oplus$ and $\odot$ — according to transaction of addition and multiplication of the $\mod q$.

the system (2) through the given initial condition:

$$s_{n+r} = p_{r-1}s_{n+r-1} + p_{r-2}s_{n+r-2} + \ldots + p_0s_n \quad (\mod q),$$
$$s_{n+r+1} = p_{r-1}(p_{r-1}s_{n+r-1} + p_{r-2}s_{n+r-2} + \ldots + p_0s_n) \oplus (n) \mod p_0s_n + p_{r-1}s_{n+r-1} + p_{r-2}s_{n+r-2} + \ldots + p_0s_n + 1 \quad (\mod q),$$
$$s_{n+2r} = p_{r-1}(p_{r-1}s_{n+2r-1} + p_{r-2}s_{n+2r-2} + \ldots + p_0s_n + 1) \oplus p_{r-2}(p_{r-1}s_{n+2r-1} + p_{r-2}s_{n+2r-2} + \ldots + p_0s_n) \oplus \ldots + p_0(p_{r-1}s_{n+2r-1} + p_{r-2}s_{n+2r-2} + \ldots + p_0s_n) \oplus \ldots \oplus p_0s_n \quad (\mod q).$$

Let represent the system (3) as the system $r$ MVFLA or of $r$-variables:

$$f_1(s_{n+r-1}, \ldots, s_n) = p_{r-1}s_{n+r-1} + p_{r-2}s_{n+r-2} + \ldots + p_0s_n \quad (\mod q),$$
$$f_2(s_{n+r-1}, \ldots, s_n) = \sum_{i=0}^{r-1} a_i s_n^{i+1} \quad (\mod q),$$
$$f_r(s_{n+r-1}, \ldots, s_n) = \sum_{i=0}^{r-1} a_i s_n^{i+1} \mod a_i + p_{r-2}s_{n+r-2} + \ldots + p_0s_n \mod 0, s_n \quad (\mod q).$$

Coefficients $a_i^{(j)} \in \{0, 1, \ldots, q-1\}$ are formed after reduction formulas (3). Structural diagram of the parallel operation of the generator in accordance with formula (4) has the form (see Fig. 2).

By analogy with [8] we may realize the MVFLA system (4) by calculation of some arithmetical polynomial.

To do that, let us coordinate MVFLA (4) system with the system of arithmetical polynomials (5). Then we get:

$$A_1(S) = \sum_{i=0}^{r-1} a_i s_n^{i+1},$$
$$A_2(S) = \sum_{i=0}^{r-1} a_2 s_n^{i+1},$$
$$A_r(S) = \sum_{i=0}^{r-1} a_r s_n^{i+1},$$

Let multiple the polynomials of the system (6) by weights $q_i$ ($i = 1, 2, \ldots, r$):

$$A_1^*(S) = q_1P_1(S) = \sum_{i=0}^{r-1} a_i s_n^{i+1},$$
$$A_2^*(S) = q_1P_2(S) = \sum_{i=0}^{r-1} a_2 s_n^{i+1},$$
$$A_r^*(S) = q_1P_r(S) = \sum_{i=0}^{r-1} a_r s_n^{i+1},$$

where $a_i^{(j)} = q_i^{(1)}a_i$ ($j = 1, 2, \ldots, r; i = 0, 1, \ldots, q_i^{(1)} - 1$).

Then we get:

$$D(S) = \sum_{i=0}^{r-1} a_i s_n^{i+1} \mod q_i^{(1)}$$

According to paper [8] the modular form of an arithmetical polynomials can be received:

$$M(S) = \sum_{i=0}^{r-1} a_i s_n^{i+1} \mod q_i^{(1)}$$

where

$$c_i = \sum_{j=0}^{r-1} a_i^{(j)} (i = 0, 1, \ldots, q_i^{(1)} - 1).$$

Let computing the values of the required MVFLA. To do that, we should represent the result of calculation of MVFLA in $q$-valued notation system and apply the masking operator $\Xi^l(M(S))$ [9]:

$$\Xi^l(M(S)) = \left[ \frac{M(S)}{q^t} \right] \quad (\mod q),$$

where $t$ is the required $q$-stage of the representation $M(S)$. Structural diagram of the parallel operation of the generator in accordance with formula (7) has the form (see Fig. 3).

Numerical example

Let examine the construction $q = 3$ LFSR, generating 3-digit PRS given by characteristic equation: $s_{k+3} = 2s_{k+2} + s_k \mod 3$ and initial fill: $s_0 = 0, s_1 = 1, s_2 = 2.$
The corresponding characteristic polynomial is represented as: \( P(z) = z^3 + 2z^2 + 1 \).

In this case the system of characteristic equations for the PRS section of three elements will be represented as follows:

\[
\begin{align*}
\{ f_3(s_2, s_1, s_0) &= 2s_2 \oplus s_0 \quad \text{(mod 3)}, \\
\{ f_4(s_2, s_1, s_0) &= 2s_2 \oplus s_1 \oplus 2s_0 \quad \text{(mod 3)}, \\
\{ f_5(s_2, s_1, s_0) &= s_0 \oplus 2s_1 \quad \text{(mod 3).}
\end{align*}
\]

Then let us represent the system of characteristic equations as the MVFLA system with right part of equalities, expressed by means of initial given conditions:

\[
\begin{align*}
\{ f_3(s_2, s_1, s_0) &= 2s_2 \oplus s_0 \quad \text{(mod 3),} \\
\{ f_4(s_2, s_1, s_0) &= s_2 \oplus s_1 \oplus 2s_0 \quad \text{(mod 3),} \\
\{ f_5(s_2, s_1, s_0) &= s_0 \oplus 2s_1 \quad \text{(mod 3).}
\end{align*}
\]

According to (6) we shall get the system of arithmatic polynomials as follows:

\[
\begin{align*}
\{ A_3(S) &= \frac{1}{4}(14s_2 - 6s_2^2 + 4s_0 - 39s_2s_0 + 21s_0s_2^2 + 15s_0^2s_2 - 9s_0^2s_2^2), \\
\{ A_4(S) &= \frac{1}{4}(8s_2 + 8s_1 + 42s_1s_2 - 30s_1s_2^2 - 30s_2s_1^2 + 18s_2^2s_1^2 + 28s_0 - 78s_0s_2 + 30s_0s_2^2 - 78s_0s_1 + 78s_0s_1s_2 + 30s_0s_1^2s_2 - 12s_0^2 + 42s_0^2s_2 - 18s_0^2s_2^2 + 42s_0^2s_1 - 72s_0^2s_1s_2 + 18s_0^2s_1s_2^2 - 18s_0^2s_1^2 + 18s_0^2s_1^2s_2^2), \\
\{ A_5(S) &= \frac{1}{4}(14s_1 - 6s_1^2 + 4s_0 - 39s_1s_0 + 21s_0s_1^2 + 15s_0^2s_1 - 9s_0^2s_1^2).
\end{align*}
\]

Let realize the system of arithmatical expressions as arithmatical polynomial:

\[
\begin{align*}
D(S) &= \frac{1}{4} (14s_2 - 6s_2^2 + 4s_0 - 39s_2s_0 + 21s_0s_2^2 + 15s_0^2s_2 - 9s_0^2s_2^2) + 3\left(\frac{1}{4}(8s_2 + 8s_1 + 42s_1s_2 - 30s_1s_2^2 - 30s_2s_1^2 + 18s_2^2s_1^2 + 28s_0 - 78s_0s_2 + 30s_0s_2^2 - 78s_0s_1 + 78s_0s_1s_2 + 30s_0s_1^2s_2 - 12s_0^2 + 42s_0^2s_2 - 18s_0^2s_2^2 + 42s_0^2s_1 - 72s_0^2s_1s_2 + 18s_0^2s_1s_2^2 - 18s_0^2s_1^2 + 18s_0^2s_1^2s_2^2)\right) + 3\left(\frac{1}{4}(14s_1 - 6s_1^2 + 4s_0 - 39s_1s_0 + 21s_0s_1^2 + 15s_0^2s_1 - 9s_0^2s_1^2)\right).
\end{align*}
\]
Modular polynomial form will be expressed as:

$$M(S) =$$

$$7s_0 \oplus 9s_2^2 \oplus 21s_1 \oplus 18s_0s_1 \oplus 9s_0^2s_1 \oplus 18s_0s_1^2$$
$$\oplus 20s_2 \oplus 15s_0s_2 \oplus 6s_2^2 \oplus 9s_1s_2 \oplus 9s_0s_1s_2$$
$$\oplus 9s_1^2s_2 \oplus 12s_2^3 \oplus 3s_0s_2^2 \oplus 18s_0^2s_2 \oplus 9s_1s_2^2 \pmod{27}.$$  

According to the given initial conditions we may obtain the following three-digit fragment of PRS:

\[
\begin{align*}
\text{step 1} & \quad s_3 = \Xi^0(19) = 1, \\
\text{step 2} & \quad s_4 = \Xi^1(19) = 0, \\
\text{step 3} & \quad s_5 = \Xi^2(19) = 2; \\
\text{step 5} & \quad s_{15} = \Xi^0(5) = 2, \\
\text{step 6} & \quad s_{16} = \Xi^1(5) = 1, \\
\text{step 7} & \quad s_{17} = \Xi^2(5) = 0; \\
\text{step 8} & \quad s_{18} = \Xi^0(4) = 1, \\
\text{step 9} & \quad s_{19} = \Xi^1(4) = 1, \\
\text{step 10} & \quad s_{20} = \Xi^2(4) = 0; \\
\text{step 11} & \quad s_{21} = \Xi^0(19) = 1, \\
\text{step 12} & \quad s_{22} = \Xi^1(19) = 0, \\
\text{step 13} & \quad s_{23} = \Xi^2(19) = 0; \\
\end{align*}
\]

Conclusion

Here is the representation of one of the possible non-standard methods of realization of parallel algorithm of generation of \(q\)-valued PRS, based on the arithmetical representation of MVFLA. The developed algorithm may be used for the realization of perspective high-performance cryptographic facilities for information protection.

The further direction of the research is the realization of the developed algorithm of generation of \(q\)-valued PRS using the redundant code redundant number system, which provide control over the errors while computing the PRS elements.

REFERENCES


Authors: prof. PhD, D.Sc. Oleg Finko; Ph.D. Dmitriy Samoylenko; PhD. Sergey Dichenko; PhD. Nikolay Eliseev, Institute of Computer Systems and Information Security of Kuban State Technological University, 350072, Krasnodar, Moskovskaya St., 2, Russia, email: ofinko@yandex.ru; ofinko@member.ams.org; Personal page: http://www.mathnet.ru/eng/person/40004