Formation of Pseudo-Random Sequences of Maximum Period of Transformation of Elliptic Curves

Alexandr Kuznetsov[1], Dmitriy Prokopovych-Tkachenko[2], Alexey Smirnov[3]
[1] *Professor in the Department of Information Technology Security of Kharkiv National University of Radioelectronic, Kharkiv, Ukraine,*
[2]*Ukrainian Academy of Customs, Dnipropetrovsk, Ukraine,*
[3]*Professor in the Department of Software, Kirovohrad National Technical University, Kirovohrad, Ukraine*

ABSTRACT

It is considered methods of forming pseudo-random sequences for cryptographic of applications, in particular for domestic mechanisms to ensure security of information systems and technologies. We investigate the properties of pseudo-random sequences generator using the changes in the group of points of elliptic curves [according to the standard NIST SP 800-90], there are some disadvantages of test generator with respect to the properties of the formed sequences and their statistical visibility with uniformly distributed sequences. It is developed an improved method by introducing additional recurrent conversion, which allows you to create sequences of pseudo-random numbers maximum period.

Keywords: *Pseudo-Random Sequences, Elliptic Curves*

I. INTRODUCTION

The analysis and comparative studies have shown that the most effective in terms of indivisibility of molded sequences with realization of stochastic process is a method of forming pseudo-random numbers, which are based on the use of modular transformations or changes in the group of points of an elliptic curve [1-3]. The most promising are generators of pseudo-random sequences (PRS), which are built using transformations under points of an elliptic curve.

At the same time, as shown in the work [4-5] carried out studies, the main drawback of the known method of forming the PRS using transformations on elliptic curves (according to the standard NIST SP 800-90) is that it does not allow to form a sequence of pseudo-random numbers maximum period that significantly reduces its efficiency and limits the possibilities for practical use**.** Indeed applied scalar point multiplication operation of an elliptic curve and coordinates reflection of obtaining point for formation of pseudo-random numbers does not provide the maximum amount of molded sequences [4-5].

In this paper, tasked to develop a method of forming of sequences of pseudo-random numbers is due to the additional driving recursive transformation in conjunction with the use of transforms under points of elliptic curve will generate a maximum period of PRS, increasing its efficiency and expand opportunities for use in practice.

II. A KNOWN METHOD OF FORMATION OF PSEUDO-RANDOM SEQUENCES (PRS) ON THE ELLIPTIC CURVES

A method of formation of PRS, using transformations on the elliptic curves that suggested in the recommendations NIST SP 800-90, is based on the use of two scalar products of points of an elliptic curve and mapping of corresponding x-coordinates of received results into non-zero integer values [3].

The first scalar product on a fixed point P is performed in order to form the intermediate phase s_i, and it is cyclically changed at each iteration during the functioning of the corresponding generator. So the value of state s_i depends on the value of the previous state s_{i-1} (at the previous iteration) and the value of fixed point P:

$$s_i = \varphi(x(s_{i-1}P)), \quad (1)$$

where $x(A)$ – is the x-coordinate of the point A, $\varphi(x)$ – field elements mapping function into non-zero integer numbers.

An initial value of the parameter s_0 is formed with the use of initialization procedure, that includes insertion of a secret key (Key), which sets the initial entropy, and inserted key hashing with the forming of received results to the specified length of the bits. The received value *Seed* initiates the initial value of the parameter: $s_0 = \text{Seed}$.

The second scalar product on a fixed point Q is performed in order to form an intermediate state r_i . This scalar product sets the value of generated pseudo-random bits after the corresponding conversion. The value of parameter r_i depends on the first scalar product of parameter s_i and the value of fixed point Q :

$$r_i = \varphi(x(s_i Q)) . \quad (2)$$

The value r_i is initial for forming of pseudo-random bits. These bits are formed by reading of the block with the least significant bits of number r_i .

PRS is formed by a concatenation of read-in bits of generated numbers r_i .

The values of fixed points are set as constants. They are not changed during the forming of PRS.

The structure chart of PRS generator with the use of conversions on the elliptic curves in accordance with the recommendations of the standard NIST SP 800-90 is shown in a Fig. 1.

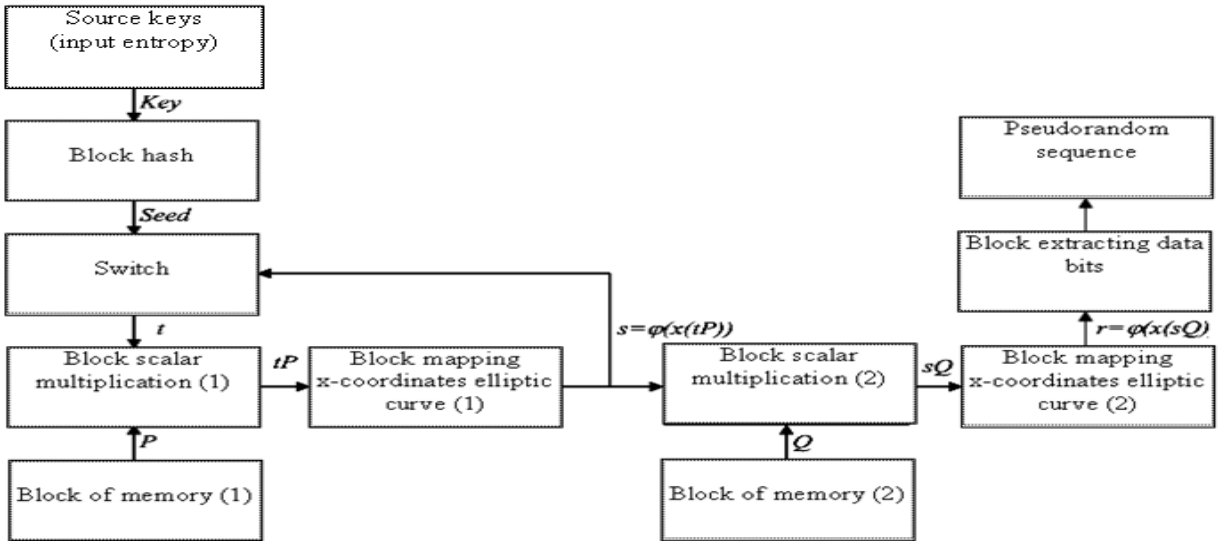

Fig. 1. The structure chart of PRS generator with the use of conversions on the elliptic curves (according to the recommendations of the standard NIST SP 800-90)

This method of PRS forming applies conversion in a cluster of points of an elliptic curve in order to form intermediate states s_i and r_i . The back action, or in the other words forming of s_{i-1} by the known s_i and/or forming of s_i by the known r_i is connected with a solution of a difficult theoretical task of discrete logarithm in a cluster of points of an elliptic curve.

Generator's intermediate states formation chart is represented in a Fig. 2.

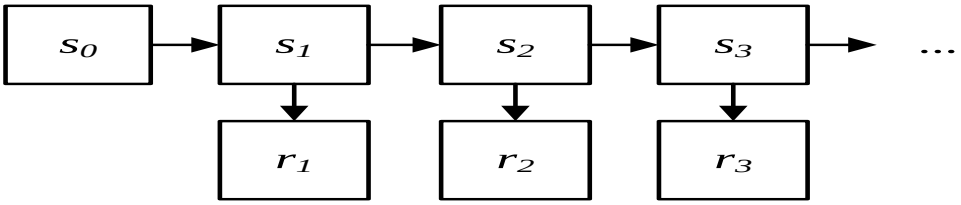

Fig. 2. Generator's intermediate states formation chart

As it is seen from the Fig. 2, the sequence of states $\dots s_{i-1}, s_i, \dots s_{i+1} \dots$ forms from the initial value $s_0 = \text{Seed}$, which in turn forms from secret key (Key), data. Each following value s_i depends on previous value of s_{i-1}, and forms by the instrumentality of elliptic curve's basic point scalar multiplication according to formula (1).

Some bits of PRS is formed by reading bit of sequence of numbers $\dots r_{i-1}, r_i, r_{i+1}, \dots$, i.e. by reading data from the result of another scalar multiplication of the base point on the value of states $\dots s_{i-1}, s_i, \dots s_{i+1} \dots$ according to the formula 2.

Since the secret Key, which sets the results for forming sequences after certain transformations determines the initial value of the parameter s_0, relevant sustainability of considered generator is based on the reduction of the problem of secrete key data recovery solutions to well-known and highly complicated mathematical task of discrete logarithm in the group of points of an elliptic curve. Besides fragments PRS also linked by scalar multiplication of elliptic curve points, i.e. to recover any piece of PRS by any other known fragment to solve the problem of discrete logarithm in an elliptic curve group.

The paper [4-5] studied the properties of periodic reporting generator PRS, including a comparison of the obtained lengths of the periods of sequences with maximum period that can be obtained for given length of keys and groups of points of an elliptic curve.

For maximum period of molded PRS take the meaning [4-5]:

$$L_{max} = \min(L_{max}(K), L_{max}(S), k), \tag{3}$$

where::

$$L_{max}(K) = 2^{l_K} - 1,$$

l_K – the length of secret key (bits);

$$L_{max}(S) = 2^{l_S} - 1,$$

$l_S = \log_2(\text{Seed})$ – bit length of meaning Seed;

k – order of point P of elliptic curve.

The generated sequences will reach the maximal period, when the elements of the sequence:

$$r_0, r_1, \dots, r_{i-1}, r_i, \dots r_{i+1}, \dots, r_{L-1}, r_0, r_1, \dots, \tag{4}$$

will possess each:

$$\min(2^{l_K} - 1, 2^{l_S} - 1, k)$$

non-zero value.

Practically it means, that the field elements mapping function $\varphi(x)$ into non-zero integer numbers at each i iteration for each generated point $s_{i-1}P$ is to generate unique integer number. But it is impossible. The order m of the group H_{EC} of the elliptic curves' points, which are used in cryptographic additions in cases, provided by the recommendations of standard NIST SP 800-90, is limited by the form:

$$p + 1 - 2\sqrt{p} \le m \le p + 1 + 2\sqrt{p},$$

where p is the order of simple Galois field GF (p) over which the elliptic curve is considered.

So the cases, when the order of cluster of points can be higher than the order of Galois field, can emerge. Practically it means that for some elements of the group H_{EC}, for example the function $\varphi(x)$ will return identical value for points P_i i P_j, $P_i \ne P_j$.

In this case the use of elliptic curves' arithmetic in the generator of pseudorandom numbers will mean the equality of states' values $s_i = s_j$ for some $i \ne j$, where:

$$s_i = \varphi(x(s_{i-1}P)) = \varphi(x(P_i))$$

and

$$s_j = \varphi(x(s_{j-1}P)) = \varphi(x(P_j)),$$

and $|i - j| < L_{max}$.

So the value of real periods L of generated consequences of states (4) will be lower than maximal period (3). But in this context we should consider the existence of negations for each element of the group H_{EC}. It means that for each point $P_i(x_i, y_i) \in H_{EC}$ exists the point $-P_i(x_i, -y_i) \in H_{EC}$, and its x-coordinate coincides with the point $P_i(x_i, y_i)$, and y-coordinate is inverse to corresponding y-coordinate of the point $P_i(x_i, y_i)$ relative to the operation of the addition in the Galois field $GF(p)$ arithmetic. The points of zero y-coordinate (the points of type $P_i(x_i, 0) = -P_i(x_i, 0) \in H_{EC}$) are the exceptions. In this case the mapping function $\varphi(x)$ of x-coordinate of the point P into non-zero integer numbers will return identical values, like in cases $P = P_i(x_i, y_i)$ and $P = -P_i(x_i, -y_i)$,so we will have the next case:

$$\varphi(x(P_i(x_i, y_i))) = \varphi(x(-P_i(x_i, -y_i))),$$

And equality correspondingly:

$$s_i = \varphi(x(P_i(x_i, y_i))) = \varphi(x(-P_i(x_i, -y_i))) = s_j.$$

Practically in means that according to the rule of PRC generating with the use of arithmetic of elliptic curves, that is described in the recommendations of the standard NIST SP 800-90 , the maximal periods of sequences will not be reached. Furthermore the experimental studies [4, 5] show that real periods will be lower than maximal.

III. DEVELOPMENT OF IMPROVED METHOD OF PRS GENERATING OF THE MAXIMAL PERIOD WITH THE USE OF TRANSFORMATIONS ON ELLIPTIC CURVES

The task of providing maximal period of generated PRS is solved by the additional recurrence transformations into the generator.

A structure chart of an improved PRS generator with the use of transformations on the elliptic curves is shown in a Fig. 3.

The first scalar multiplication on a fixed point P, like in the generator, that meets the recommendations of NIST SP 800-90, is performed in order to form an intermediate state S_i. And it is cyclically updated at each iteration during the functioning of the corresponding generator. But there is a fundamental difference. It is a forming process of this intermediate state. The improved method proposes to use a recurrence transformation, which initiates by a secret key insertion (Key), in order to provide a maximal period of sequences $\ldots s_{i-1}, s_i, \ldots s_{i+1} \ldots$

So every next state value S_i depends not only on the previous state value s_{i-1} (at previous iteration) and on the value of a fixed point P, but also it depends on the result of recurrence transformation ($LRR(y)$):

$$s_i = \varphi(x((s_{i-1} + LRR(y))P)),$$

where $x(A)$ is x-coordinate of the point A, $\varphi(x)$ is a mapping function of the field elements into non-zero integer numbers.

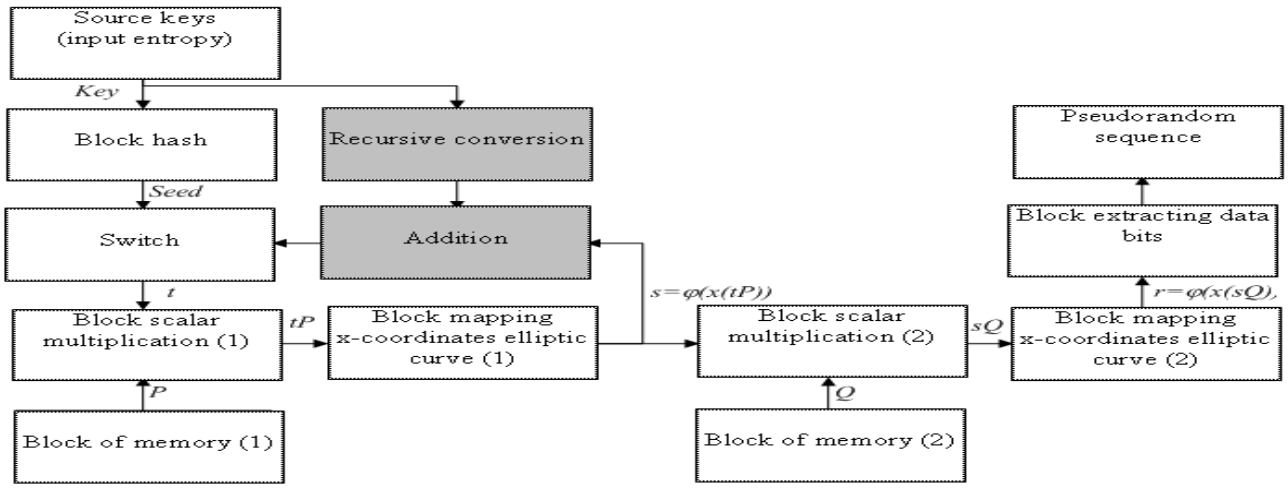

Fig. 3. A structure chart of the improved PRS generator with the use of transformations on the elliptic curve

A recurrence transformation can be built in different ways. The simplest way is the use of a circuit of linear recurrence registers (LRR) with a feedback (Fig. 4). The taps of the chain are set by coefficients of polynomial with binary coefficients

$$g(x) = g_0 + g_1 x + g_2 x^2 + ... + b_m x^m .$$

If the polynomial $g(x)$ is primitive over Galois field $GF(2^m)$, so the sequence, which is formed by LRR with the corresponding logic of a feedback, has a maximal period $2^m - 1$. The secret key value (Key), that initiates the work of $LRR(y)$, is written down into LRR as an initial value of the register.

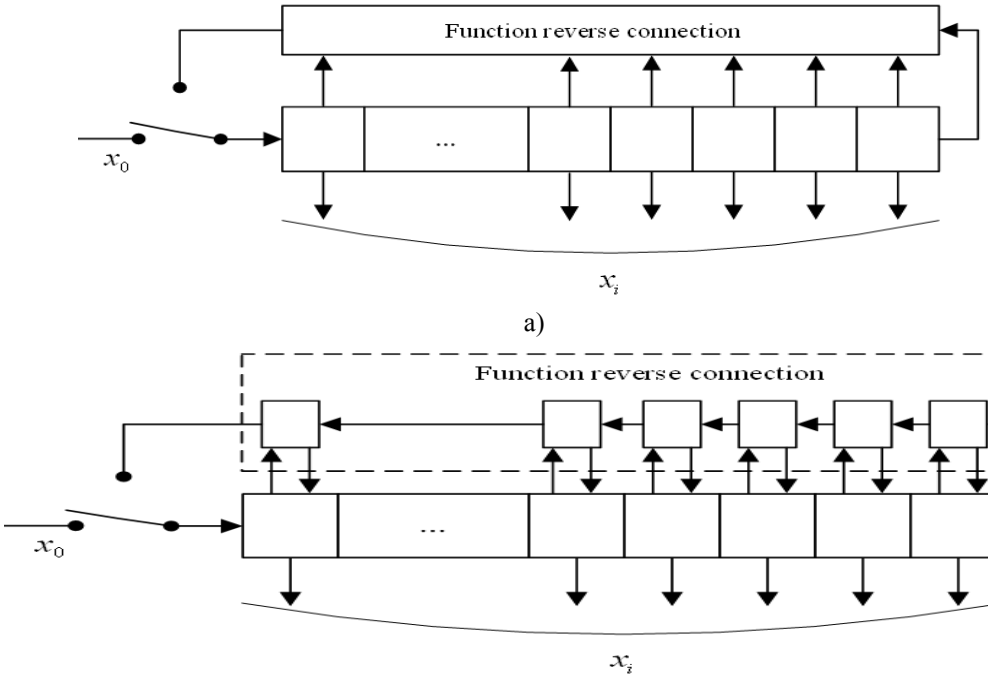

Fig. 4. A structure chart of a block of recurrence transformations with the use of LRR in Fibonacci configuration (a) and Galois configuration (b)

Devices represented at the chart №4 have the following principle of operation.

First of all initialization procedure is held. During this procedure the key of the devices is in a lower position; the initial value y_0, which is equal to the value of a secret key $y_0 = Key$, is put down into a shift register. Then the key switches on an upper position, that is mean that nothing goes to a shift register. During the work of the block the information, kept in a shift register, shifts to the right for one cell. And in the feedback circuit a value of feedback function goes to the first cell. So at i time interval the value of y_i is kept in a shift register and this value of y_i is read as a value of the function $L(y_i)$.

The feedback function provides the generating of PRS of the maximal period; it also sets a concrete look of a commutation of a feedback circuit.

According to the charts of the devices at the Fig. 4, at each step only the value of the last left cell is changed in the linear register under the Fibonacci configuration.

In the linear register under the Galois configuration at each step the values of all cells, which take part in a generating of the value of feedback function, are changed.

The main point of the improved method of PRS generating is that the key sequence is represented as a vector x_0, which initializes an initial value of an argument of a scalar product function of a point of elliptic curve $f(x) = x \cdot P$, where P is a point of the elliptic curve, that belongs to a cluster of points EC_n of multiple of N, and the initial value of y_0 of recurrence transformation $L(y)$, which is implemented for example with the help of linear recurrence registers with a feedback.

The next value x_i of an argument of a function $f(x)$ is calculated with the help of recurrence transformation (which is implemented for example with the help of linear recurrence registers with a feedback), with the help of devices of the scalar multiplication x_{i-1} on a fixed point P:

$$P'_i = (x_{i-1} + L(y_{i-1})) \cdot P,$$

and transformation $\varphi(P'_i)$ coordinates of the received point $P'_i \in EC_n$ with the help of the corresponding devices (for example x_i can be equal to the value of the coordinates of the point P'_i), so

$$x_i = \varphi(P'_i) = \varphi(f(x_{i-1} + L(y_{i-1}))) = \varphi((x_{i-1} + L(y_{i-1})) \cdot P).$$

The received values of x_i are represented as an argument of a function of scalar product of an elliptic curve point

$$f'(x) = x \cdot Q,$$

where Q is a point of an elliptic point, which belongs to a cluster of points EC_n of multiple of N.

Parent elements of sequence pseudorandom numbers forms by reading the meaning of scalar product function with the aid of corresponding devices, that is required sequence of length bit m will be the sequence:

$$b_0 \quad b_1 \quad b_2 \quad \dots \quad b_i \quad \dots \quad b_{m-1}, \; i = \overline{0,(m-1)},$$

where b_i – is a lower bit of number z_i,

$$z_i = \varphi(f'(x_i)) = \varphi(x_i \cdot Q).$$

The problem calculus of function $f(x)^{-1}$, which is inverse to the elliptic curve's point scalar product function $f(x) = x \cdot P$, that is calculation of some sense of x_{i-1} when x_i is known, is nagging theoretical-complicated problem of taking the discrete logarithm in cluster of points of elliptic curve. Conformably the problem of calculation the function $f'(x)^{-1}$, which is inverse to the elliptic curve's point scalar product function $f'(x) = x \cdot Q$, that is calculation of some sense of x_i when z_i is known, , is nagging theoretical-complicated problem of taking the discrete logarithm in cluster of points of elliptic curve. The effective logarithms of calculation discrete logarithms for basis points of large-scale order for resolution of this problem are rested unknown for today. That's why this way of formation of sequence of pseudorandom numbers is cryptographically resistant. Formally, the formation of PRS when the linear recurrent registers are used (indicated as LRR) could be shown in such a way.

Secret key: Key;

Constants: P, Q – points EC of the multiple of n;

Initial condition: $x_0 = Key, y_0 = Key$;

Cycle function:

$$\varphi(f(x + LRR(y))) = \varphi((x + LRR(y))P),$$

$$LRR(y = \{u_1, u_2, \dots, u_m\}) : u_i = -\sum_j a_j u_{i-j} + u_i$$

where: $\{u_1, u_2, \dots, u_m\}$ – is the condition of LRR, $\{a_1, a_2, \dots, a_m\}$ – are the coefficients, which specify the function of inverse liaison of LRR, $\varphi(P'_i)$ – transformation of coordinates of point $P'_i \in EC_n$ (f.e. reading of sense of one of the points's P'_i coordintaes).

Formed PRS:

$$(b_0, b_1, \dots, b_i, \dots)$$

where b_i – the less meaningful bit (the bit of twoness) number z_i,

$$z_i = \varphi(f'(\varphi((x_{i-1} + LRR(y_{i-1}))P))) = \varphi(\varphi((x_{i-1} + LRR(y_{i-1}))P)Q),$$

$$y_i = LRR(y_{i-1}).$$

To analyze periodical properties of enhanced generator PRS, let us consider the structure chart, which is shown at the Fig. 3.

The initial value of parameter S_0, as it is in the generator, which corresponds to the recommendations of NIST SP 800-90, forms with the use of initialization procedure, which includes the enter of secret key (Key), which defines the initial entropy (ambiguity), and hashing of the key entered with formatting of received result to concrete length of bits. Received sense Seed initiate the starting value of the parameter: $s_0 = Seed$.

The second scalar multiplication on a fixed point Q is performed in order to form an intermediate state r_i, which after the corresponding transformation set the value of the generated pseudorandom bits. Every next value of the state s_i depends on the results of an implementation of a recurrence transformation $LRR(y)$, which provides a maximal period of generated sequences, so the value of parameter r_i, that depends on the parameter S_i and the value of the fixed point Q: $r_i = \varphi(x(s_i Q))$, will depend on the results of results of an implementation of a recurrence transformation $LRR(y)$, so the generated sequence of states $\dots r_{i-1}, r_i, r_{i+1}, \dots$ will have a maximal period.

The received value r_i is an initial for generating of pseudorandom bits, which are generated by reading of block from the least significant bits of generated numbers r_i. PRS is generated by concatenation of read-in bits of generated numbers r_i. The values of fixed points are defined as constants and during PRS generating they don't change.

So the periodic features of states of the improved generator are defined by the periodic features of an additional recurrence transformation $LRR(y)$.

On the Fig. 5 we see an original sequence $LRR(y)$, indicated by $\dots y_{i-1}, y_i, \dots y_{i+1} \dots$ We sketch the influence of periodicity of this sequence on periodicity of sequences $\dots s_{i-1}, s_i, \dots s_{i+1} \dots$ and $\dots r_{i-1}, r_i, r_{i+1}, \dots$.

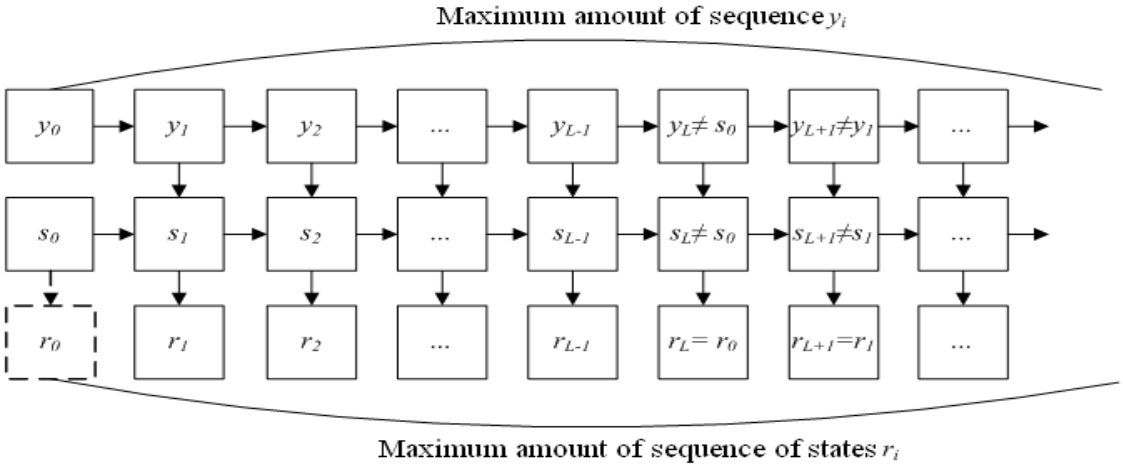

Fig. 5. The chart of forming of state sequences of the generator with maximal period

The periodic features of sequences $\dots s_{i-1}, s_i, \dots s_{i+1} \dots$ and $\dots r_{i-1}, r_i, r_{i+1}, \dots$ depends on features of sequences $\dots y_{i-1}, y_i, \dots y_{i+1} \dots$, so the use of recurrence transformation $LRR(y)$ with the maximal period of the original sequences provides the maximal period of the original sequence.

The additional recurrence transformations, which are implemented with the help of linear recurrence registers with feedbacks, help to form sequences of pseudorandom numbers of maximal period. It helps to increase the efficiency and widen the practical use.

IV. CONCLUSIONS

During the research of PRS generator on the elliptic curves, which is described in a standard NIST SP 800-90, we found out further shortcomings: a cyclic function of the generator, that provides the maximal period of the generated PRS of the inner states and the corresponding points of the elliptic curves, is not defined; the forming of PRS bits from the sequence of the elliptic curve points by a sample of a block with the least significant bits and its concatenation doesn't meet the requirements of the statistical discrepancy with uniformly separated sequence. So the PRS generator on the elliptic curves (NIST SP 800-90) doesn't meet the requirements sufficiently.

The improved method of forming PRS of the maximal period with the use of transformations on elliptic curves was elaborated during the research. This method unlike the others helps to generate sequences of pseudorandom numbers of the maximal period and it increases the efficiency and widens the practical use.

The elaborated method is based on the bringing of a task of a secret key finding to the solving of a difficult theoretical task of a discrete logarithm in a cluster of points; it also helps to form PRS with a maximal period.

An introduced method of forming of PRS with maximal period with the use of transformations on elliptic curves removes the uncovered drawbacks of the generator described in the standard NIST SP 800-90: it was proposed to use linear recurrence transformations, which help to form a maximal period of sequences of inner states and corresponding points of an elliptic curve; forming of an original PRS by reading of one the least significant bit from coordinates of elliptic curve points meets the requirements of a statistical safety.

So the introduced method of PRS forming meets modern requirements and can be used in order to improve different safety mechanisms for an information security of telecommunications networks and systems. Prospective course of a further research are the argumentation of practical recommendations concerning a realization of the introduced PRS and the ways of its use in different mechanisms of an information security of telecommunications networks and systems.

REFERENCES

[1] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography – CRC Press, 1997. – 794 p.
[2] Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag, 829 p.
[3] Elaine Barker and John Kelsey, Recommendation for random number generation using deterministic random bit generators, National Institute of Standards and Technology, January 2012, 124 p. http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf
[4] L.S.Soroka, O.O.Kuznetsov, D.I.Prokopovych-Tkachenko. The features of the generators of pseudorandom sequences on the elliptic curves. // the bulletin of Ukrainian Academy of Customs. Edition "Technics", №1 (47), 2012. – p. 5-15.
[5] L.S.Soroka, O.O.Kuznetsov, D.I.Prokopovych-Tkachenko. The research of the generators of pseudorandom sequences on the elliptic curves // An implementation of information technologies for training and activities of law-enforcement agencies: theses of reports from theoretical and practical conference of Academy of internal military forces of Ministry of internal affairs of Ukraine, March 21-22, 2012. – H.: Academy of internal military forces of Ministry of internal affairs of Ukraine. – 2012. – p. 47 – 49.

AUTHORS NAMES

Alexandr Kuznetsov. Graduated from Kharkiv Military University with a degree in "Automated Control Systems" in 1996. Doctor of Technical Sciences. Professor. Kharkov National University of Radio Electronics, Kharkov, Ukraine. Field of interest: information security and routing issues.

Dmitriy Prokopovych-Tkachenko*. Graduated from Kharkov Higher Military Command School of Engineeringwith a degree in "Automated Control Systems". Graduate student. Ukrainian Academy of Customs, Dnipropetrovsk, Ukraine. Field of interest: information security and routing issues.*

Alexey Smirnov*. Graduated from Kharkiv Military University with a degree in "Automated Control Systems" in 1999. Candidate of Technical Sciences (PhD). Professor of Department of Software of Kirovohrad National Technical University, Ukraine. Field of interest: information security and routing issues.*