UDC 004.42

# PROPERTIES OF ENCODING FLOW KEYS

B.L. Shramchenko, Ph.D., S.Sc.W.
*Kyiv National University of Technology and Design*

Keywords: shift feedback with linear feedback, Fibonacci configuration, Galois configuration, bit sequence period, stream encryption keys.

As is known [1], mechatronic information systems include a component related to information security. Therefore, the issues of development and research of information security tools are directly related to the range of issues studied in mechatronics.

In the present work, new properties of bit sequences at the output of pseudo-random sequence generators having a Fibonacci or Galois configuration are presented. The use of these properties opens up new possibilities in the development of streaming encryption.

The traditional means used in the construction of stream key generators are shift registers with linear feedback (SRLF). The most widespread to date are two types of SRLF: Fibonacci configuration and Galois configuration. In the first, the transformation of the states of the r-bit register in the transition from the current clock to the next occurs according to the expressions

$$a_{r-1}^{t+1} = \sum_{i=1}^{r} c_i a_{r-i}^{t}, \quad (1) \text{ (feedback)},$$

$$\forall i \mid 1 < i \le r, = a_{r-i}^{t+1} a_{r-i+1}^{t}, (2) \text{ (offset)}.$$

In the given expressions - the state of the cell *s* in clock t, takes the value 0 or 1. The sum is calculated modulo 2. The feedback coefficients (taps) also take the value 0 or 1. Therefore, the output signal of the register in time step *t* is determined as follows $a_0^t = a_1^{t-1} = \ldots = a_{r-1}^{t-r+1} = \sum_{i=1}^{r} c_i a_{r-i}^{t-r}$.

And since $a_i^{t-r} = a_0^{t-r+i}$,

the following recurrent relation takes place $a_0^t = \sum_{i=1}^{r} c_i a_0^{t-i}$.

The following relations are fulfilled for the second configuration

$$a_{r-1}^{t-r+1} = g_1 a_0^{t-r},$$
$$a_{r-2}^{t-r+2} = g_2 a_0^{t-r+1} \oplus a_{r-1}^{t-r+1},$$
$$a_{r-3}^{t-r+3} = g_3 a_0^{t-r+2} \oplus a_{r-2}^{t-r+2},$$
$$\cdots$$
$$a_1^{t-1} = g_{r-1} a_0^{t-2} \oplus a_2^{t-2},$$
$$a_0^t = g_r a_0^{t-1} \oplus a_1^{t-1}.$$

In the given system of equations the coefficient (taps) $g_i$ can be equal to 0 or 1.

Summarizing the equations of the last system we obtain

$$a_0^t = = \sum_{i=1}^{r} g_{r-i+1} a_0^{t-i}.$$

Whence we are convinced that under the condition $c_i = g_{r-i+1}$, $i = 1, \ldots, r$ (3) both configurations form cyclic sequences at the output, which satisfy the common recurrent relation.

In order for the Galois register to output the same sequence as the Fibonacci register, except for the correspondence between the taps, there must be a correspondence between the initial states of the registers. Determine the initial state $(b_{r-1}, b_{r-2},\ldots, b_0)$ of the Galois register at the given initial state $(a_{r-1}, a_{r-2},\ldots, a_0)$ of the Fibonacci register, which is the first $r$ members of the sequence at the output.

Obviously, $b_0 = a_0$

as the first member of the sequence at the output.

Next, from equation $b_1 \oplus g_1 a_0 = a_1$ we obtain

$$b_1 = g_1 a_0 \oplus a_1.$$

Using the ratio $b_1 \oplus g_1 a_0 = a_1$, we have

$$b_2 = g_2 a_0 \oplus g_1 a_1 \oplus a_2.$$

Continuing similarly, for any $i < r$ we can write

$$b_i = g_i a_0 \oplus g_{i-1} a_1 \oplus \ldots \oplus g_1 a_{i-1} \oplus a_i..$$

We now compare the behavior of two Fibonacci registers: $RF$ with taps $c_1, c_2, \ldots, c_r$ and $RF^1$ with taps $c_1^1, c_2^1, \ldots, c_r^1$, in which taps satisfy the relation $c_i = c_{r-i+1}^1$, $i = 1, \ldots, r-1$ (4). Let, in time step $t$ $(t > r)$ the state of the register $RF$ - $(a_{r-1}^t, a_{r-2}^t, \ldots, a_0^t)$, and $RF^1$ - $RF^1$ – $(a_0^t, a_1^t, \ldots, a_{r-1}^t)$. Then in the next $r$ time steps on the outputs of the registers are formed mutually inverse sequences (for each element the next in one sequence is equal to the previous one for this element in another sequence). To show that the mutual inversion of states in some time step $t$ under condition (4) results in complete mutual inversion of sequences at the output of registers, it suffices to show that the element at the output of the $RF$ register in time step $t + r$ is equal to the element at the $RF^1$ register output at time step t- 1.$RFa_{r-1}^t a_{r-2}^t a_0^t) RFa_0^t a_1^t a_{r-1}^t)$

For the register $RF$ we have

$$a_0^{t+r} = a_{r-1}^{t+1} = \sum_{i=1}^{r} c_i a_{i-1}^t.$$

The state of the $RF^1$ register in time step $t$ - $1$ has the form $(a_1^t, a_2^t, \ldots, a_{r-1}^t, x)$ where $x$ is the signal at the output. Therefore, for this register there is a relation

$$a_0^t = \sum_{i=1}^{r-1} c_{r-i+1}^1 a_{i-1}^t \oplus .x$$

Taking into account that $c_1 \equiv 1$, and the fact that the sum is taken by module 2, we can write

$$x = \sum_{i=1}^{r} c_i a_{i-1}^t,$$

that is, the signal at the output of the register $RF^1$ in the time step $t-1$ coincides with the signal at the output of the register $RF$ in the time step $t + r$.

Thus, the proposed method for determining the initial state of the Galois register, equivalent to the given Fibonacci register, it is shown that the inversion of taps in the Fibonacci registers follows the inversion of the output signals used as stream keys.

References

1. Егоров О.Д. Конструирование мехатронных модулей: Учебник. / О.Д. Егоров, Ю.В. Подураев**.** - М.: ИЦ МГТУ "СТАНКИН", 2004. – 360 с.