Hryhoriy Kravtsov, Director of Research-and-Implemention Company “BKP-consulting”, Kyiv, Ukraine, e-mail kga@bkp.liga-net.org

The task of integration of difference equation, that is unsolvable in the quadratures.

In 1969 J.L. Massey in his work [1] formulated a universal cryptographical attack on the generators of encoding sequence, which has a potential to replace any generator of cipher (code) by its shortest linear equivalent.

If a shift register with linear feedback has generated a cipher sequence with linear complexity L, then investigation of $2L$ bits of this sequence is enough.

By linear complexity (linear range, liner excursion) of sequence for enciphering we understand a length L of the shortest shift registry with linear feedback, which can create this sequence.

The results of Massey’s works have implementation in the Berlekamp-Massey algorithm [1]. This algorithm is a strong quality indicator for enciphering sequence.

But G.Vernam’s chipper, which has been known since 1926, is the only hope for absolute safety [2]. This cipher needs a random key. The basic characteristic of random key is its unpredictability.

The author of this article formulated the task of getting a mechanism of resistance to Berlekamp-Massey’s algorithm. During the investigation the author has learnt a wide class (large number) of elementary and special mathematical functions and has chosen on differential equation of Riccati.

It is known, that the differential equation of Riccati

$$\frac{dy}{dx} = P(x)y^2 + Q(x)y + R(x), \tag{1}$$

generally speaking, can not be integrated in quadratures (this equation can not be solved by the finite number of serial (step-by-step) integrations).

The equation (1) can be written in terms of sequences or arrays:

$$Y_i - Y_{i-1} + P_i Y_i^2 + Q_i Y_i = R_i,$$

where P, Q and R are known sequence, Y - is an unknown sequence.

We can find the Y by solving the next system of equations:

$$\begin{cases} y_1 - y_0 + p_1 y_1^2 + q_1 y_1 = r_1 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ y_i - y_{i-1} + p_i y_i^2 + q_i y_i = r_i \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ y_n - y_{n-1} + p_n y_n^2 + q_n y_n = r_n \end{cases} .$$

The common solving of this system is equivalent to solving of equation $f(y_n^k, y_0) = 0$, where $k = 2^n$. The last equation has the infinite number of roots, because the number of the variables is more than the number of equations.

For practical use let us rewrite (1) as

$$(Y_i - Y_{i-1} + P_i Y_i^2 + Q_i Y_i) \bmod p = R_i ,$$

Where P, Q - are known sequences (parameters);

p - Large prime number;

R - Galois field $GF(p)$,

Y - Unknown sequence.

Let us suppose, that a cryptanalyst knows the values of P, Q, R. If the sequence Y is a key sequence, then a cryptanalyst needs to solve the task of discrete integration of difference equation that does not have solutions in the quadratures.

Bibliography:

1. J.L. Massey, “Shift-Register synthesis and BCH decoding”, IEEE Trans. Inform. Theory, vol.IT-15, pp.122-127, Jan.1969
2. G.S. Vernam, “Cipher printing telegraph system for wire and radio telegraphic communication”, J.Amer.Inst.Elec.Eng., vol. 45, pp. 109-115, 1926
3. Dh.W.Diffie, M.E.Hellman. “New directions in cryptography”, IEEE Trans. Inform. Theory, vol.IT-22, pp.644-654, Nov.1976