

and discussed. Section V concludes the paper.

II. THE ANALYZED GENERATOR

We analyze the LCT attack on a noised pseudorandom sequence generator involving a primitive known as The Binary Rate Multiplier (BRM). BRM consists of 2 linear feedback shift registers (LFSRs). One of them, the clocking LFSR (LFSR_s), determines the clocking sequence for the clocked LFSR (LFSR_u), see Fig. 1.

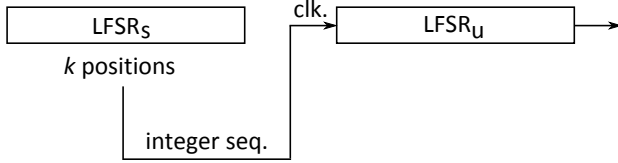


Fig. 1. The BRM primitive

The BRM operates as follows (Fig. 2): Without clocking by LFSR_s, the register LFSR_u produces the binary sequence u_n . At the clock pulse i of LFSR_s, the bits from k positions of LFSR_s determine the integer s_i that represents the number of bits from the sequence u_n that are going to be discarded. The integers s_i , $i = 1, 2, \dots$ make the sequence s_n . The process of discarding bits in this way is called *non-uniform decimation* of the sequence u_n . The maximum value of the integer s_i determines the maximum number of bits from the sequence u_n that can be discarded at a time. The binary sequence z_n is the output sequence of the whole BRM.

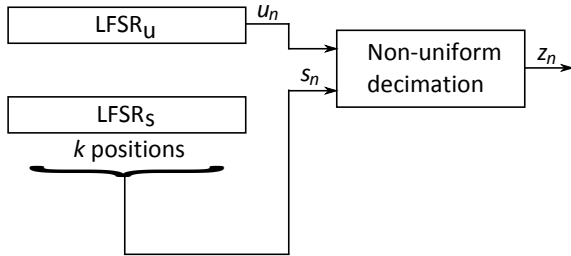


Fig. 2. Operation of the BRM

The BRM primitive has become popular in the design of stream ciphers since it can be shown [2] that the produced sequence z_n has extremely long period and high linear complexity preserving at the same time good statistical properties of a single LFSR.

III. THE NEW LCT ATTACK

In this section, we give details of the new LCT-based attack against a noised BRM. The general description and remarks about LCT have been exposed in the Introduction. To design an LCT attack against BRM, we have to determine which part of the BRM key (which consists of the initial states of LFSR_s and LFSR_u, as usual) is to be guessed. It is shown in [5] that assigning a linear system to a BRM when the initial state of LFSR_s is guessed is easy. Then the unknowns in the

system are the bits of the output sequence of LFSR_u without decimation together with the bits of the initial state of the same LFSR and the right-hand side of any equation in the system is the corresponding bit of the intercepted sequence. In our new LCT attack on a noised BRM, we use the same approach. We guess the initial state of LFSR_s and make a system of linear equations in the unknowns of the initial state of LFSR_u and the unknown bits of the output sequence of LFSR_u without decimation. The main point of our attack is the algorithm that eliminates the influence of the bits of the intercepted sequence complemented by noise.

Example 1

Suppose the BRM from Fig. 1 uses 4-bit LFSRs and the primitive feedback polynomials of LFSR_s and LFSR_u are $f_s(x) = 1 + x + x^4$ and $f_u(x) = 1 + x^3 + x^4$, respectively. Let the number of output taps of LFSR_s be $k = 2$ and the tap positions are the first and the second (from the left). Let the initial states of LFSR_s and LFSR_u be 1010 and 0110, respectively. Then the clocking sequence for LFSR_u (i.e. the integer sequence s_n) is 31021002333... and the output sequence of the BRM is 11010110111...

Let the cryptanalyst's guess of the initial state of LFSR_s be right, i.e. 1010. In the LCT attack against the generator without noise, the so-called *decimation sequence* is generated, containing the symbol '2' in the positions of the unknown bits. Each symbol '2' will correspond to a new variable in the system of equations assigned to the generator. In this case, the decimation sequence will be 2222 | 22212102212011220222122212221... The symbol | delimits the variables of the initial state of the clocked register LFSR_u from the rest of the variables. The variables to the left from the symbol | are given in the order x_4, x_3, x_2, x_1 , whereas the variables to the right from the symbol | are given in the increased order of indexing, i.e. x_5, x_6 , etc. Then the system of linear equations assigned to the given BRM is:

$$\begin{aligned} x_3 + x_4 + x_5 &= 0 \\ x_2 + x_3 + x_6 &= 0 \\ x_1 + x_2 + x_7 &= 0 \\ x_1 + x_5 &= 1 \\ x_5 + x_6 + x_8 &= 0 \\ &\vdots \end{aligned}$$

□

The new ciphertext-only attack against a BRM is described below:

1. Guess the initial state of the LFSR_s.
2. Set up a system of equations assigned to such a BRM without involving the intercepted bits. Such a system is homogeneous and always consistent.
3. Set up a system of equations involving only the equations containing the intercepted bits.
4. Join the obtained systems and check the consistency of the joint system. The following cases are possible:
 - 4.1 There is no noise and the right initial state of LFSR_s was guessed - the joint system will be consistent and