THE NUMBER OF OUTPUT SEQUENCES OF A BINARY SEQUENCE GENERATOR

Jovan Dj. Golić

Institute of Applied Mathematics and Electronics, Belgrade
School of Electrical Engineering, University of Belgrade,
Yugoslavia

Abstract: In this paper, a number of output sequences is proposed as a characteristic of binary sequence generators for cryptographic applications. Sufficient conditions for a variable-memory binary sequence generator to produce maximum possible number of output sequences are derived.

I. INTRODUCTION

An important characteristic of every binary sequence generator (BSG) for cryptographic or spread-spectrum applications is the number of output sequences it can produce for all the permitted initial states. A natural requirement is that different initial states give rise to different output sequences. For almost all the BSG's known in the cryptographic literature, this property has not been analyzed.

In this paper, we analyze the number of output sequences of a recently proposed [1] nonlinear BSG consisting of three linear feedback shift registers (LFSR's) and a variable memory (MEM-BSG). It is shown in [1] that MEM-BSG is suitable for generating fast binary sequences of large period and linear complexity and with good correlation properties. A number of output sequences of a well-known nonlinear BSG [2] with two LFSR's and a multiplexer (MUX-BSG) is also determined.

II. MEM-BSG

In this section we provide a short description of a MEM-BSG [1], shown in Fig. 1.

D.W. Davies (Ed.): Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp. 160-167, 1991.

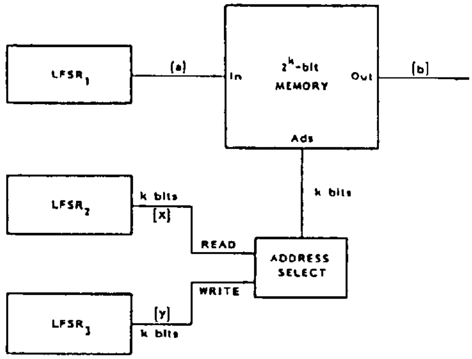

Fig. 1. Variable-memory binary sequence generator (MEM-BSG).

$LFSR_i$ of length m_i has a primitive characteristic polynomial $f_i(x)$, $i=1,2,3$. All the LFSR's are clocked by the same clock and have nonnull initial states, thus generating maximum-length pseudonoise (PN) sequences of periods $P_i=2^{m_i}-1$, $i=1,2,3$, respectively. The initial content of the 2^k bit memory is arbitrary. The read and write addresses are the binary k-tuples taken from any k stages of $LFSR_2$ and $LFSR_3$, respectively, whereas the binary output of $LFSR_1$ is used to load the memory. At any time $t=0,1,2,...$ the following two operations are carried out. First, the output bit $b(t)$ is read out of the memory location addressed by the read address $X(t)$. Second, the output bit $a(t)$ of $LFSR_1$ is written into the memory location addressed by the write address $Y(t)$. The BSG just described will be referred to as a MEM-BSG. It implements a time-varying nonlinear function of the phase shifts of a maximum-length sequence.

The output sequences of a MEM-BSG need not be periodic, because of the initial memory content. To make them periodic and independent of the initial memory content, in all that follows we assume $t=P_3$ is the initial time, that is, we set $t-P_3 \rightarrow t$.

III. ANALYSIS

In order to establish large enough lower bounds on the linear complexity and period of the output sequences of a MEM-BSG, it was assumed in [1] that

$$1 \leq k < \min\{m_2, m_3\}, \tag{1}$$

$$2^{m_3}-1 \leq m_1, \tag{2}$$

that m_1, m_2, and m_3 are pairwise coprime, and that the k address stages of $LFSR_2$ are equidistant if $3 \leq k \leq m_2-2$. Hovever, our objective here is to obtain the sufficient conditions, as general as possible, for a MEM-BSG to generate the maximum possible number of output sequences, for all the nonnull initial states of the LFSR's. To this end, instead of the four conditions given above, we shall here maintain only the first two, (1) and (2), generalize the third one, and drop the fourth one.

We start from a suitable expression for the MEM-BSG output sequence [b], derived in [1]:

$$b(t) = \sum_{s=0}^{P_3-1} C_s(t)\, V_s(t), \qquad t=0,1,2,\ldots \tag{3}$$

where

$$C_s(t) = \begin{cases} 1, & t-s=0 \bmod P_3 \\ 0, & t-s\neq 0 \bmod P_3 \end{cases}, \qquad s=0,1,\ldots, P_3-1 \tag{4}$$

$$V_s(t) = a(t-\Phi_s(X_t)), \quad t=0,1,2,\ldots, \qquad s=0,1,\ldots, P_3-1, \tag{5}$$

X_t, $t=0,1,2,\ldots$, is the read address sequence, of period P_2, taking values in the set $\underset{\sim}{K} = \{0,1\}^k$, and for each $s=0,1,\ldots, P_3-1$, $\Phi_s(\underset{\sim}{j})$, $\underset{\sim}{j}\epsilon\underset{\sim}{K}$, is an injective mapping $\underset{\sim}{K} \rightarrow \{1, \ldots, P_3\}$ which is defined in [1] in terms of the write address sequence. This definition is not needed here, but only the fact that

$$P_3 = \mathrm{lcm}\ \{M_{\underset{\sim}{j}} : \underset{\sim}{j}\epsilon\underset{\sim}{K}\} \tag{6}$$

where for each $\underset{\sim}{j}\epsilon\underset{\sim}{K}$, $M_{\underset{\sim}{j}}$ denotes the period of the periodic extension sequence $\Phi_t(\underset{\sim}{j})=\Phi_{t \bmod P_3}(\underset{\sim}{j})$, $t=0,1,2,\ldots$. Note that (3) actually means that [b] consists of P_3 interleaved sequences $[V_s(P_3t+s)]$, $s=0,1,\ldots,$

P_3-1, which are the decimated versions of $[V_s(t+s)]$, $s=0,1,\ldots, P_3-1$.

We now state and prove a theorem that gives the sufficient conditions for a MEM-BSG to produce the maximum possible number of output sequences.

Theorem: If the conditions (1) and (2) are satisfied and

$$\gcd(m_1, m_2) \neq m_1 \tag{7}$$

$$\gcd\left(P_2, \frac{P_1}{\gcd(P_1, P_2)}\right) = 1 \tag{8}$$

$$\gcd(P_3, P_1P_2) = 1, \tag{9}$$

then the MEM-BSG generates $P_1P_2P_3$ different output sequences, for all the nonnull initial states of $LFSR_i$, $i=1,2,3$.

Proof: First note that (1) and (2) imply that $m_2, m_3 \geq 2$ and $m_1 \geq 3$. Since each $LFSR_i$ generates cyclic shifts of the corresponding maximum-length sequence, the set of all the output sequences of the MEM-BSG is determined by:

$$b_{ijn}(t) = \sum_{s=0}^{P_3-1} C_s(t)\, a_0(t+i-\Phi^0_{s+n}(X^0_{t+j})), \quad t=0,1,2,\ldots \tag{10}$$

for $i=0,\ldots, P_1-1$, $j=0,\ldots, P_2-1$, $n=0,\ldots, P_3-1$, where the sequences $[a_0(t)]$, $[X^0_t]$, and $[\Phi^0_t(\underset{\sim}{j})]$, $\underset{\sim}{j}\in\underset{\sim}{K}$, correspond to arbitrarily chosen initial states of $LFSR_i$, $i=1,2,3$, respectively. We should prove that $b_{ijn}(t)=b_{i'j'n'}(t)$, $t=0,1,2,\ldots$, which is equivalent to

$$a_0(P_3t+s+i-\Phi^0_{s+n}(X^0_{P_3t+s+j})) = a_0(P_3t+s+i'-\Phi^0_{s+n'}(X^0_{P_3t+s+j'})),$$
$$s=0,\ldots, P_3-1, \quad t=0,1,2,\ldots \tag{11}$$

implies that $(i',j',n')=(i,j,n)$, for all admitted (i,j,n) and (i',j',n'). Since the periods of the sequences $[X^0_t]$ and $[a_0(t)]$ are P_2 and P_1, respectively, the periods of $[a_0(t+s+i-\Phi^0_{s+n}(X^0_{t+s+j}))]$ and

$[a_0(t+s+i'-\phi^0_{s+n'}(X^0_{t+s+j'}))]$ both divide P_1P_2, for each $s=0,\ldots,P_3-1$. In view of (9) it then follows that (11) involves a proper decimation by P_3 of the corresponding sequences. Employing the fact that a proper decimation is an one-to-one correspondence (see [2], for example), we obtain that (11) is equivalent to

$$a_0(t+s+i-\phi^0_{s+n}(X^0_{t+s+j})) = a_0(t+s+i'-\phi^0_{s+n'}(X^0_{t+s+j'})),$$
$$s=0,\ldots,P_3-1,\ t=0,1,2,\ldots\ . \tag{12}$$

Further, setting $t \to P_2t+r$, (12) becomes

$$a_0(P_2t+r+s+i-\phi^0_{s+n}(X^0_{r+s+j})) = a_0(P_2t+r+s+i'-\phi^0_{s+n'}(X^0_{r+s+j'})),$$
$$r=0,\ldots,P_2-1,\quad s=0,\ldots,P_3-1,\quad t=0,1,2,\ldots, \tag{13}$$

because $[X^0_t]$ has period P_2. In (13) we deal with a decimation by P_2 of the corresponding cyclic shifts of $[a^0_t]$. This decimation need not be proper. Nevertheless, on the condition (7), the decimation does not change the linear complexity [2, Lemma 2.2.8], and, hence, is an one-to-one correspondence of all the cyclic shifts of $[a_0(t)]$. Accordingly, (13) is equivalent to

$$[i - \phi^0_{s+n}(X^0_{r+s+j}) = i' - \phi^0_{s+n'}(X^0_{r+s+j'})] \bmod P_1,$$
$$r=0,\ldots,P_2-1,\quad s=0,\ldots,P_3-1. \tag{14}$$

Considering the periodicity of the sequences $[X^0_t]$ and $[\phi^0_t(\underset{\sim}{j})]$, $\underset{\sim}{j}\in\underset{\sim}{K}$, (14) reduces to

$$[\phi^0_{(s+n-n')\bmod P_3}(X^0_{(r+j-j')\bmod P_2}) = \phi^0_s(X^0_r)+i'-i] \bmod P_1,$$
$$r=0,\ldots,P_2-1,\quad s=0,\ldots,P_3-1. \tag{15}$$

With the notation $P_1'=P_1/\gcd(P_1,(i'-i)\bmod P_1)$, (15) gives rise to

$$[\phi^0_{(s+(n-n')P_1')\bmod P_3}(X^0_{(r+(j-j')P_1')\bmod P_2}) =$$

$$= \phi_s^0(X_r^0)+\mathrm{lcm}(P_1,(i'-i)\bmod P_1) = \phi_s^0(X_r^0)] \bmod P_1,$$

$$r=0,\ldots,P_2-1,\quad s=0,\ldots,P_3-1, \tag{16}$$

i.e.,

$$[\phi^0_{(s+(n-n')P_1't)\bmod P_3}(X^0_{(r+(j-j')P_1't)\bmod P_2}) = \phi_s^0(X_r^0)] \bmod P_1,$$

$$r=0,\ldots,P_2-1,\quad s=0,\ldots,P_3-1,\quad t=0,1,2,\ldots\ . \tag{17}$$

Setting $t=P_2$, (17) becomes

$$[\phi^0_{(s+(n-n')P_1'P_2)\bmod P_3}(X_r^0) = \phi_s^0(X_r^0)] \bmod P_1,$$

$$r=0,\ldots,P_2-1,\quad s=0,\ldots,P_3-1, \tag{18}$$

i.e.,

$$[\phi^0_{(s+(n-n')P_1'P_2)\bmod P_3}(\underset{\sim}{j}) = \phi_s^0(\underset{\sim}{j}),\quad \underset{\sim}{j}\in K,\quad s=0,\ldots,P_3-1, \tag{19}$$

where in (19), instead of the equality modulo P_1, we have the ordinary equality, because (2) implies that $1\leq\phi_s^0(\underset{\sim}{j})\leq P_3\leq m_1<2^{m_1}-1=P_1$, for any $m_1\geq3$, $\underset{\sim}{j}\in \underset{\sim}{K}$, and $s=0,\ldots,P_3-1$. Further, recalling that the period of $[\phi_t^0(\underset{\sim}{j})]$ denoted by $\underset{\sim}{M_j}$ satisfies $\underset{\sim}{M_j}|P_3$, for each $\underset{\sim}{j}\in \underset{\sim}{K}$, from (19) we obtain

$$\underset{\sim}{M_j}|[(n-n')P_1'P_2]\bmod P_3,\quad \underset{\sim}{j}\in \underset{\sim}{K}, \tag{20}$$

which in view of (6) leads to

$$P_3|[(n-n')\frac{P_1P_2}{\gcd(P_1,(i'-i)\bmod P_1)}]\bmod P_3, \tag{21}$$

i.e.,

$$[(n-n')\frac{P_1P_2}{\gcd(P_1,(i'-i)\bmod P_1)}]\bmod P_3 = 0. \tag{22}$$

Finally, (9) and (22) imply that $n'=n$.

Having proved that (11) results in $n'=n$, we now turn back to (15). With $n'=n$ it becomes

$$[\phi_s^0(X^0_{(r+(j-j'))\bmod P_2}) = \phi_s^0(X_r^0)+i'-i] \bmod P_1,$$
$$r=0,\ldots, P_2-1,\quad s=0,\ldots, P_3-1, \tag{23}$$

which yields

$$[\phi_s^0(X^0_{(r+(j-j'))\bmod P_2}) = \phi_s^0(X_r^0)+i'-i] \bmod P,$$
$$r=0,\ldots, P_2-1,\quad s=0,\ldots, P_3-1, \tag{24}$$

where $P=P_1/\gcd(P_1,P_2)$. In a similar way as (15) implies (16), (24) implies

$$[\phi_s^0(X^0_{(r+(j-j')P')\bmod P_2}) = \phi_s^0(X_r^0)] \bmod P,$$
$$r=0,\ldots, P_2-1,\quad s=0,\ldots, P_3-1, \tag{25}$$

where $P'=P/\gcd(P, (i'-i)\bmod P)$. On the other hand, from (7) we obtain

$$P = \frac{P_1}{\gcd(P_1,P_2)} = \frac{2^{m_1}-1}{2^{\gcd(m_1,m_2)}-1} \geq \frac{2^{m_1}-1}{2^{m_1/2}-1} =$$
$$2^{m_1/2}+1 > m_1 \quad ,m_1\geq 3, \tag{26}$$

which together with (2) yields $1\leq\phi_s^0(\underset{\sim}{j})\leq P_3\leq m_1<P$, $m_1\geq 3$, for each $\underset{\sim}{j}\in\underset{\sim}{K}$ and $s=0,\ldots, P_3-1$. Consequently, (25) remains true if the modulo P equality is replaced by the ordinary one. For each $s=0,\ldots, P_3-1$, the period of $[\phi_s^0(X_t^0)]$ is P_2 since $\phi_s^0(\underset{\sim}{j})$, $\underset{\sim}{j}\in\underset{\sim}{K}$, is an injection. Therefore, from (25) it follows that

$$P_2 \,|\, [(j-j')\frac{P}{\gcd(P,(i'-i)\bmod P)}]\bmod P_2, \tag{27}$$

i.e.,

$$[(j-j')\frac{P}{\gcd(P,(i'-i)\bmod P)}]\bmod P_2 = 0, \tag{28}$$

which in view of (8) results in $j'=j$.

Now we turn to (23). With $j'=j$ it reduces to $[i'=i]\bmod P_1$, that is, to $i'=i$. We have thus proved that from (11) it follows that $(i',j',n')=(i,j,n)$, for all admitted (i,j,n) and (i',j',n'). Q.E.D.

Note that the case $\gcd(m_1, m_2)=1$, which was considered in [1], is a special case of (7) and (8), meaning that the theorem remains true if (7) and (8) are replaced by $\gcd(m_1, m_2)=1$.

Finally, we analyze a well-known BSG [2] with two LFSR's and a multiplexer (MUX-BSG). Consider a MUX-BSG obtained from a MEM-BSG by substituting a k-bit address multiplexer for a 2^k-bit memory and $LFSR_3$. The multiplexer k-bit address is generated in the same way as the read address in the MEM-BSG, while the 2^k multiplexer inputs are taken from any 2^k stages of $LFSR_1$. It is shown in [1] that there is a strong connection between the MEM-BSG and the so-defined MUX-BSG. Accordingly, in a similar way one can prove that on the conditions (7) and (8) the MUX-BSG generates P_1P_2 different output sequences for all the nonnull initial states of $LFSR_1$ and $LFSR_2$. This fact was not revealed in [2].

IV. CONCLUSION

As a characteristic of binary sequence generators (BSG's) for cryptographic applications, the number of output sequences they can generate for all the permitted initial states is proposed. A natural cryptographic criterion is that this number be maximum possible. It is shown that this property can be analyzed for some types of the BSG's. It is proved that under certain conditions the recently defined MEM-BSG [1] and the well-known MUX-BSG [2] both produce maximum possible number of output sequences.

V. REFERENCES

[1] Jovan Dj. Golić, Miodrag M. Mihaljević, "Minimal linear equivalent analysis of a variable-memory binary sequence generator" IEEE Trans. Inform. Theory, vol. IT-36, pp. 190-192, Jan. 1990.

[2] S.M.Jennings, "A special class of binary sequences", Ph.D. thesis, Westfield College, London University, 1980.