ANALYSIS OF A NONLINEAR FEEDFORWARD LOGIC FOR BINARY SEQUENCE GENERATORS

J. Bernasconi and C.G. Günther
Brown Boveri Research Center
CH-5405 Baden, Switzerland

A new type of nonlinear feedforward logic for binary sequence generators is proposed, i.e. a logic that combines the stages of a linear feedback shift register (LFSR) in a nonlinear way. The sequences generated are analyzed with respect to their transient and ultimately periodic behavior. They are shown to have a balanced zero-one distribution, and a lower bound on their linear complexity is derived which grows exponentially with the length of the LFSR.

Binary sequences with good randomness properties play an important role in cipher systems [1]. Usually, such sequences are generated by a finite state machine and are therefore not truly random. A common measure for the unpredictability of a pseudorandom binary sequence is its linear complexity L, defined as the length of the shortest linear feedback shift register (LFSR) that can generate the sequence. A high linear complexity is an important necessary requirement for cryptographic applications, and corresponding generators therefore have to be nonlinear.

In the case of a nonlinear feedforward logic that combines the stages of a single LFSR, Key [2] has shown how the linear complexity can be determined. If the order of the feedforward function is larger than two, however, the procedure becomes very involved and in general only yields upper bounds. In this paper, we shall show that a lower bound on the linear complexity can be obtained if the feedforward function satisfies certain requirements.

A special type of logic that produces such feedforward functions is shown in Figure 1. It is applied to an ℓ-stage m-LFSR (i.e. an LFSR generating a sequence $\{u_t\}$ of maximal period $2^{\ell}-1$) and contains the following elements:

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 161-166, 1986.

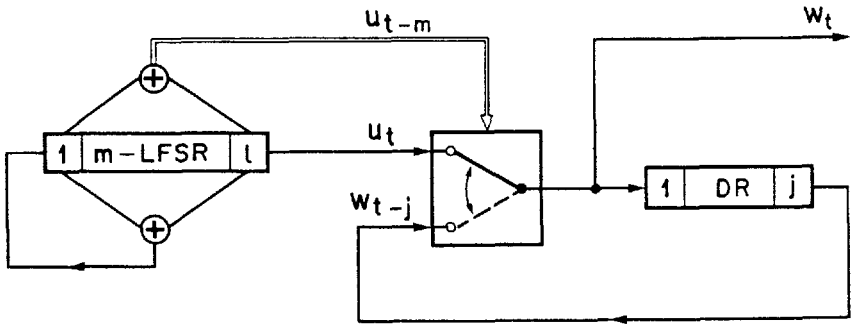

FIGURE 1
The nonlinear binary sequence generator.

- a delay logic which generates a cyclic shift u_{t-m} of u_t. (Such a logic may be based on the shift-and-add property of m-sequences [3]);

- a delay register DR of length j, with j relatively prime to $2^{\ell}-1$;

- a switch, controlled by u_{t-m}, which connects either u_t (if $u_{t-m}=0$) or w_{t-j} (if $u_{t-m}=1$) to its output.

With the connections as shown in Figure 1, the output sequence $\{w_t\}$ of the generator satisfies the recursion

$$w_t = (1 \oplus u_{t-m})u_t \oplus u_{t-m}\, w_{t-j} \quad , \quad t \geq 0 \quad , \qquad (1)$$

with initial conditions,

$$w_t = r_{-t-1} \quad , \quad -j \leq t \leq -1 \quad , \qquad (2)$$

where $\{r_t\}_{t=0}^{j-1}$ denotes the initial content of the delay register DR.

A detailed analysis of the properties of the sequence $\{w_t\}$ will be presented in a more extended paper [4]. Here we restrict ourselves to a brief summary of our main results.

We first note that the generator is selfsynchronizing in the sense that for t larger than some transient time $t_E < \ell j$, the solution $\{w_t\}$ of Eq. (1) becomes periodic and independent of the initial conditions $\{r_t\}$. If the period $T = 2^\ell - 1$ of the m-sequence $\{u_t\}$ is prime and larger than 3, then $\{w_t\}$ also has period T.

For our further analysis we now assume that the two delays m and j are related by

$$m = kj \quad , \quad k \leq \ell - 1 \quad . \tag{3}$$

Then the (unique) periodic solution to Eq.(1) is explicitly given by

$$w_t = u_t \oplus u_{t-kj}(u_t \oplus u_{t-j}) \oplus u_{t-kj}\, u_{t-(k+1)j}(u_{t-j} \oplus u_{t-2j}) \tag{4}$$

$$\oplus \ldots \oplus u_{t-kj}\, u_{t-(k+1)j} \cdots u_{t-(2k-1)j}(u_{t-(k-1)j} \oplus 1) \quad .$$

Through Eq. (4), the output sequence $\{w_t\}$ of our generator is expressed in terms of the m-sequence $\{u_t\}$ via a nonlinear function of order k+1. We observe that the highest order term of this function is a single product of k+1 equally spaced shifts of u_t,

$$u_{t-(k-1)j}\, u_{t-kj} \cdots u_{t-(2k-1)j} \quad . \tag{5}$$

It is this specific property that enables us to derive a lower bound on the linear complexity of the sequence $\{w_t\}$:

Theorem 1: Let f denote a nonlinear function combining the cyclic shifts of an m-sequence $\{u_t\}$ of period $2^\ell - 1$, and let the highest order term of f be a product of the form $u_t\, u_{t+j} \cdots u_{t+(n-1)j}$, with $n \leq \ell$ and $(j, 2^\ell - 1) = 1$. Then the linear complexity L of the sequence defined through f is bounded from below by $L \geq \binom{\ell}{n}$.

It follows that the linear complexity L_w of the sequence $\{w_t\}$ represented by Eq. (4) is bounded from below by

$$L_w \geq \binom{\ell}{k+1} \quad , \quad k \leq \ell - 1 \quad . \tag{6}$$

For a given ℓ, this bound is optimal if k+1 = $[\ell/2]$. It then becomes

$$L_w \geq \binom{\ell}{[\ell/2]} \sim \sqrt{\frac{2}{\pi\ell}}\, 2^\ell \quad , \qquad \ell >> 1 \quad , \tag{7}$$

which is of the same order of magnitude as Key's corresponding upper bound [2],

$$L_w \leq \sum_{i=1}^{[\ell/2]} \binom{\ell}{i} \sim \frac{1}{2}\, 2^\ell \quad , \qquad \ell >> 1 \quad . \tag{8}$$

The proof of Theorem 1 is given in Ref. [4], and we note that essentially the same result has been derived independently by R. Rueppel [5]. Recently, we also became aware of a paper by Kumar and Scholtz [6] where a closely related theorem is used to establish a lower bound on the maximum-achievable linear complexity in a family of bent-function sequences.

The proof is based on a result due to Key [2] which can be stated as follows. Let α be a primitive element of GF(2^ℓ), and let $\{s_t\}$ be a binary sequence of period $T = 2^\ell - 1$ whose elements are represented in the form

$$s_t = \bigoplus_{h=1}^{\ell} \bigoplus_{x \in H_h^T} \gamma_x\, \alpha^{tx} \quad , \qquad \gamma_x \in GF(2^\ell) \quad , \tag{9}$$

where H_h^T denotes the set of integers in $\{0,1,\ldots,T-1\}$ with Hamming weight h. Then the linear complexity L of $\{s_t\}$ is equal to the number of nonvanishing coefficients γ_x.

Now Theorem 1 is concerned with sequences

$$s_t = \prod_{\kappa=0}^{n-1} u_{t+\kappa j} \quad + \text{lower order terms} \quad , \tag{10}$$

where $\{u_t\}$ is an m-sequence of period $2^\ell - 1$ and therefore has the representation [7]

$$u_t = \bigoplus_{i=0}^{\ell-1} \gamma^{2^i}\, \alpha^{t2^i} \quad , \qquad \gamma \in GF(2^\ell) \quad , \tag{11}$$

with α a primitive root of the characteristic polynomial of $\{u_t\}$. In general, the determination of the expansion coefficients γ_x for s_t, obtained by inserting Eq. (11) into Eq. (10), is prohibitively complex. Those coefficients γ_x, however, for which the Hamming weight of x is maximal (i.e. equal to n), all originate exclusively from the highest order term in Eq. (10) and can be expressed explicitly as Vandermonde determinants. If $n \leq \ell$ and $(j, 2^\ell - 1) = 1$, none of these $\binom{n}{\ell}$ coefficients vanishes, so that the linear complexity L of $\{s_t\}$ is at least $\binom{n}{\ell}$.

Let us finally summarize some results on the statistical properties of the sequence $\{w_t\}$ generated by our nonlinear generator (Eq. (4)). The fraction of ones, $P\{w_t=1\}$, is given by

$$P\{w_t=1\} = \frac{1}{2}\left(1 + \frac{2^{\ell-k+1}}{2^\ell-1}\right) \quad , \quad k \leq \ell-1 \quad , \qquad (12)$$

so that for large values of ℓ and k the balance between zeros and ones in $\{w_t\}$ is almost ideal. The autocorrelation function $C_w(\tau)$, however, exhibits peaks (of exponentially decreasing magnitude) at $\tau = j, 2j, \ldots$. These peaks are due to the special structure of our generator (j is the length of the delay register DR, see Figure 1). In addition, the probability that w_t coincides with u_t is close to 3/4, and thus deviates considerably from the ideal value of 1/2.

To overcome these leakage problems ,and to eliminate the peaks in the autocorrelation function, the simple generator of Figure 1 obviously has to be modified. It turns out that the structure allows for a variety of corresponding modifications which leave the lower bound on the linear complexity unchanged, and which moreover introduce a convenient additional key multiplicity [4].

REFERENCES

[1] H. Beker and F. Piper, Cipher Systems. London: Northwood Books, 1982.
S.W. Golomb, Shift register sequences. Revised edition, Laguna Hills, California: Aegean Park Press, 1982.

[2] E.L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators", IEEE Trans.Inform.Theory, vol. IT-22, pp. 732-736, Nov. 1976.

[3] S.H. Tsao, "Generation of delayed replicas of maximal-length linear binary sequences", Proc. IEEE, vol. 111, pp. 1803-1806, Nov. 1964.

[4] J. Bernasconi and C.G. Günther, "Analysis of a nonlinear feed-forward logic for binary sequence generators", submitted to IEEE Trans.Inform.Theory.

[5] R.A. Rueppel, New approaches to stream ciphers. Ph. D. Thesis, ETH-Zürich, 1984.

[6] P.V. Kumar and R.A. Scholtz, "Bounds on the linear span of bent sequences", IEEE Trans.Inform.Theory, vol. IT-29, pp. 854-862, Nov. 1983.

[7] N. Zierler, "Linear recurring sequences", J.Soc.Indust.Appl.Math., vol. 7, pp. 31-48, March 1959.