# On the Design of Clock-Controlled Pseudorandom Bit Generators with Prime Periods

Chung-Huang Yang 楊中皇
Graduate Institute of Information and Computer Education 資訊教育研究所
National Kaohsiung Normal University 國立高雄師範大學
chyang@computer.org http://crypto.nknu.edu.tw/

## Abstract

The central problem in stream-cipher cryptography is the difficulty of generating a long unpredictable sequence of binary signals from a short and random key. In this paper, we apply the idea of bilateral stop-and-go control to safeguard the EBU's MUX-LFSR sequence generators and we propose a new self clock-control scheme which generates sequences with key-independent non- Mersenne prime periods suitable for cryptographic purposes.

**Key words:** stream cipher, keystream, pseudorandom, prime, factorization, clock-controlled

## 1. Introduction

The central problem in stream-cipher cryptography is the difficulty of generating a long unpredictable sequence of binary signals from a short and random key. The function of a pseudorandom bit generators (PRBG) in cryptography is to produce a stream of unpredictable binary digits (bits) under the control of a secret key and it should be computationally infeasible to predict any element in the sequence with better than 50-50 chance without knowing the key. That is, given a portion of the output sequence, the attackers should not be able to generate other element forwards or backwards. The elements appear to be *random* in the local sense, but they are in some way repeatable, hence only *pseudorandom*.

Most common PRBGs are consisting of linear feedback shift-register (LFSR) [3] circuits which have been in use for a long time for generating cycle redundancy check, or as error encoders/decoders. A LFSR is consisted of a shift register of $n$ flip-flops (*stages*) and a feedback connection such that each element of the output sequence is a fixed linear function of the previous $n$ elements. The feedback connections will decide the period and statistical behavior of the output sequence. By properly selecting the feedback connection, period of an $n$-stage LFSR output sequence would be $2^n - 1$ for any non-zero initial state (the *seed* or *key*). Such an output sequence is called *maximum-length* sequence. However, in spite of the large choice of the feedback connections in addition to large period and ideal randomness, maximum-length LFSR output sequences cannot be considered as secure without undergoing further cryptographic transformations. In fact, the initial state and feedback connection of an $n$-stage LFSR can be completely determined by using just $2n$ successive bits of the output sequence (see, for example, [7]).

Large prime numbers have been intensively considered in connection with the design public-key cryptosystems. Nevertheless, sequence generators with large non-Mersenne state periods have a large key-independent lower bound $Ord_p(2)$ to the linear complexity of the output sequences (the *linear complexity* of a binary sequence is the smallest length of the LFSR that could produce the sequence; it is often referred to as an important measure of the unpredictability of sequences), where $p$ is the prime period of the sequences and $Ord_p(2)$ is the order of 2 in the multiplicative group of integer modulo $p$. Namely, it has been shown [10] that if a binary sequence $\mathbf{b}$ has an odd prime period $p$, then its linear complexity will be bounded from below by the order of 2 modulo $p$, i.e.,

$$\mathrm{LC}(\mathbf{b}) \geq Ord_p(2) \quad (1)$$

In [10], the authors proposed a class of sequence generator, which generates a sequence with period of the form $h \times 2^m - 1$, using two mutual clock-control LFSRs with same length. As illustrated in Fig. 1, we have a pair of LFSRs, preloaded with secret key and each of the two LFSRs controls the clock pulses to the other, which will produce sequences with large non-Mersenne prime state periods. Output sequences of the PRBG in Fig. 1 actually will have period of the form $p = 5 \times 2^{n-2} - 1$, where $n$ is the number of stages at both LFSRs.

In this paper, we examine the PRBG previously proposed by the European Broadcasting Union (EBU) [2, 4, 5] and give a possible attack. Subsequently, we propose a scheme which enhances the security of EBU's PRBG scheme with the use of mutual clock control. We then propose a new PRBG scheme with self clock control, which will produce sequences with large non-Mersenne prime state periods.

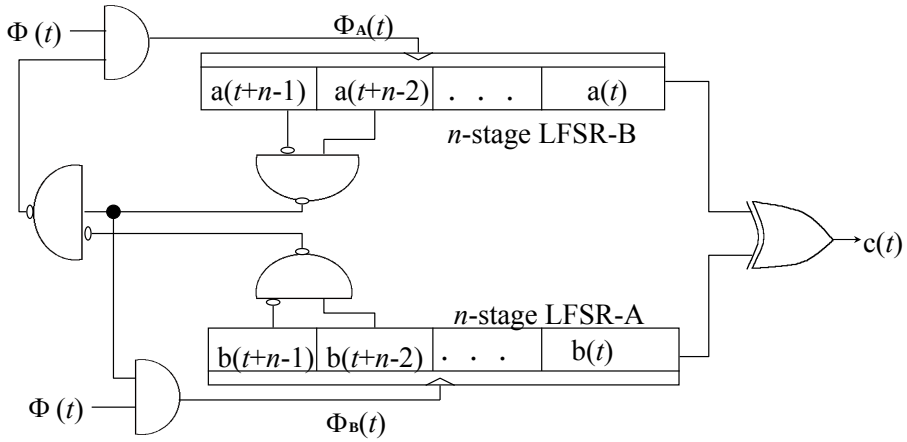


Figure 1: A pseudorandom bit generator based on bilateral step control [10, 11]

## 2. Security Enhancement of the MUX Sequence Generator

The European Broadcasting Union (EBU) scheme [2, 4, 5] uses a 32-to-1 multiplexer as a nonlinear combining function of two maximum-length LFSRs. Figure 2 shows the general structure of this sequence generator.

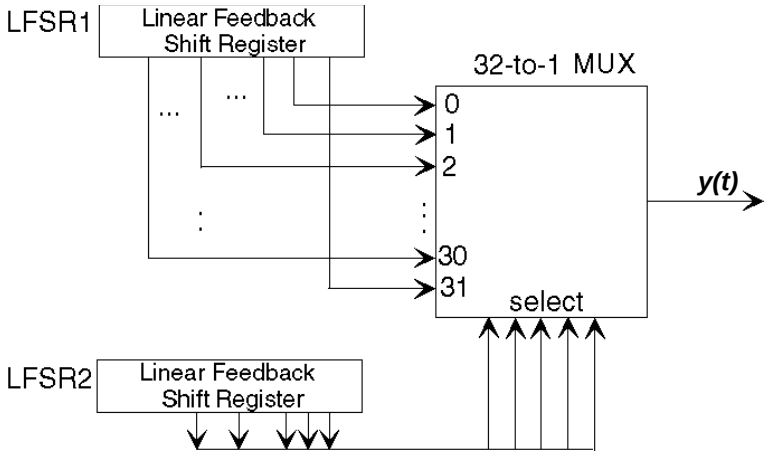


Figure 2: The PRBG proposed by the European Broadcasting Union (EBU)

The content of LFSR2 (a 29-stage LFSR) is used to select one bit from the content of LFSR1 (a 31-stage LFSR) as output element and the secret key is the initial nonzero contents

at both LFSRs. The output sequence has period $P = (2^{29} - 1)(2^{31} - 1) \approx 2^{60} \approx 10^{18}$ and linear complexity $LC = (2^{29} - 1) \times 31 \approx 1.7 \times 10^{10}$. This undoubtedly makes output sequence of such PRBG more secure than a pure LFSR circuit. Nevertheless, it has been shown [9] that an algebraic test based on the estimation of the consistency probability of a system of linear algebraic equations could be used to attack such PRBG by exhaustive searching concentrated on the LFSR2 subkey, with $2^{29} - 1$ possible nonzero values.

This means that the entire key of secrecy can be revealed by a working factor of the order $2^{29}$, not the originally intended $2^{29+31} = 2^{60}$. Since exhaustive searching has been applied, this does not mean that the generators are cryptographically insecure, but rather indicates that some precautions are required to compensate for the reduced security strength. Recently, the EBU generator was shown to be subjected to a new type of recursive attack [1], which exploited the re-synchronous mechanism in the video signals.

The idea of bilateral clock control [10, 11] provides a good approach to enhance and safeguard the EBU multiplexing scheme. The resulting PRBG, shown in Fig. 3, is constructed on the basis of mutual clock control of two LFSRs used in the EBU generator. In the scheme, we again have a pair of LFSRs, preloaded with secret key and each of the two LFSRs controls the clock pulses to the other. Both LFSRs are now made inseparable from each other, so that in attacking one of them the attacker must also take into consideration the other that controls the clock signals to it. This is a stop-and-go type scheme and at most one of the two stopping signals, *A(t)* and *B(t)*, will be zero to stop one of the LFSRs at any given time.

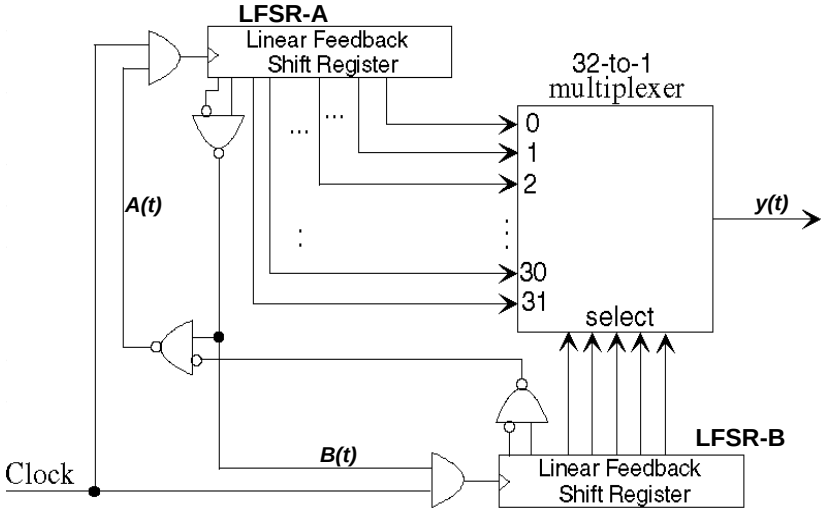


Figure 3: The enhanced MUX-LFSR sequence generator

In the enhanced scheme, we use two maximum-length LFSRs with same length *n* and use a 32-to-1 multiplexer as a nonlinear combining function of two LFSRs. Let

$$(a(t + n - 1), a(t + n - 2), ..., a(t + 1), a(t))$$

denote content of the *n* -stage LFSR-A at a given time *t* and

$$(b(t + n - 1), b(t + n - 2), ..., b(t + 1), b(t))$$

denote content of the other *n*-stage LFSR-B at a given time *t*. Each of these LFSRs controls the clock pulses to the other in the following way:

- If the leftmost two bits of LFSR-A satisfy, $(a(t + n - 1), a(t + n - 2)) = (0, 1)$, then $B(t) = 0$ and the clock pulse to LFSR-B is to be blocked;
- If the leftmost two bits of LFSR-B satisfy, $(b(t + n - 1), b(t + n - 2)) = (0, 1)$, but $(a(t+n-1), a(t+n-2)) \neq (0, 1)$, then $A(t) = 0$ and the clock pulse to LFSR-A is to be blocked.

Thus, if we denote the *t*-th pulse from the clock by $\Phi(t)$, then the $(t+1)$-th pulses to

LFSR-A and LFSR-B will be

$$\Phi_A(t+1) = A(t) \cdot \Phi(t+1), \tag{2}$$

and

$$\Phi_B(t+1) = B(t) \cdot \Phi(t+1), \tag{3}$$

where

$$B(t) = \overline{\overline{a(t+n-1)} \cdot a(t+n-2)} \tag{4}$$

and

$$A(t) = \overline{\overline{a(t+n-1)}a(t+n-2)} \cdot \overline{b(t+n-1)b(t+n-2)}$$

The phase space of the generator consists of vector-pairs of the form $\mathbf{s} = (\mathbf{s}_A, \mathbf{s}_B)$, where

$$\mathbf{s}_A \triangleq (a(t+n-1), a(t+n-2), \ldots, a(t)) \tag{5}$$

$$\mathbf{s}_B \triangleq (b(t+n-1), b(t+n-2), \ldots, b(t)) \tag{6}$$

are $n$-bit non-zero vectors, so that the total number of *admissible states* of the generator is

$$(2^n - 1)^2.$$

We shall make an analysis of the state diagram of the generator thus constructed. The state diagram will compose of branched cycles, and we will use the following terminology [6] to describe its structure.

**Definition.** We say that an admissible state **s** is the *predecessor* of a state **s*** or **s*** is the *successor* of the s, if our generator can go over from **s** to **s*** in one step (clock) of work. A state is called a *source state* to the generator if it has no predecessor.

State diagram of the enhanced EBU scheme, shown in Fig. 4, is consisted of a total of $3\times2^{n-2}-1$ cycles with $2\times2^{2n-4}$ branches (source states in Fig. 4) connected to these cycles and each cycle has identical length of $5 \times 2^{n-2} - 1$.

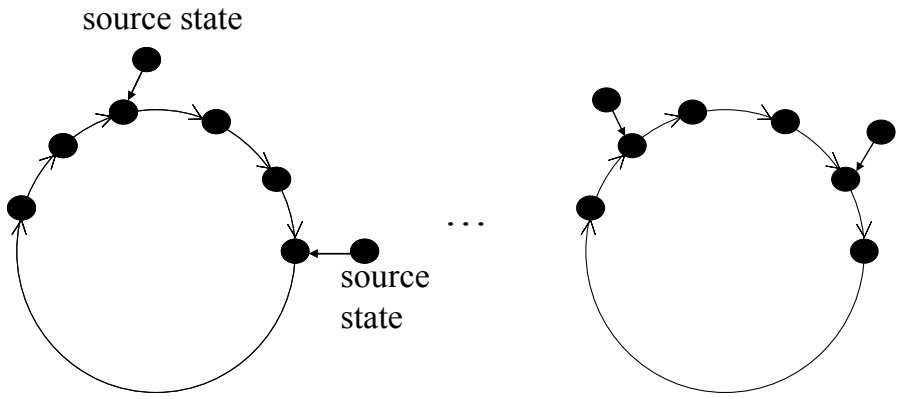


Figure 4: The state diagram for the generator given in Fig. 3

Theorem [10]

(iii). There are $2^{2m-4}$ source states in the state diagram of the generator, and an admissible state $\mathbf{s} = (\mathbf{s}_A, \mathbf{s}_B)$ is a source state if and only if

$$(a(t+n-1), a(t+n-2)) = (0, 1), \tag{7}$$

$$(b(t+n-2), b(t+n-3)) = (0, 1); \tag{8}$$

(iii). Every branch to a cycle starts with a source state has length 1, and at any non-source state there is at most one entering branch;

(iii). The non-source states in the state diagram fall in

$$3 \times 2^{n-2} - 1 \tag{9}$$

cycles, each of length

$$5 \times 2^{n-2} - 1. \tag{10}$$

The output sequence $y(t)$ in the enhanced MUX scheme has period $p = 5\times2^{n-2}-1$, where

$n$ is the number of stages at both LFSRs. If period $p$ is a prime number, then the output sequence will have a guarantee key-independent lower bound to the linear complexity (LC) [10], LC $\geq Ord_p(2)$. An example is to let $n$ = 34, then period $p = 5\times 2^{32}-1 \approx 2\times 10^{10}$ is a prime and we have a key-independent linear complexity LC $\geq (p-1)/2 \approx 10^{10}$. Let $n$ = 50, 56, 74, or 150 will also produce sequences with lower bound to the linear complexity comparable with their prime period, LC $\geq Ord_p(2)$. To compute the order of 2 module period $p$, $Ord_p(2)$, we need to perform the complete factorization of $(p-1)/2$. Table 1 shows the period and the lower bound to the linear complexity for the output sequences produced by the enhanced EBU scheme.

Table 1: The lower bound to the linear complexity for the enhanced MUX-LFSR sequence generator

| number of stages $n$ | period $p$ | lower bound to linear complexity |
|---|---|---|
| 4 | 19 | 18 |
| 6 | 79 | 39 |
| 10 | 1279 | 639 |
| 12 | 5119 | 2559 |
| 14 | 20479 | 10239 |
| 16 | 81919 | 40959 |
| 20 | 1310719 | 218453 |
| 34 | $2.147 \times 10^{10}$ | $1.074 \times 10^{10}$ |
| 50 | $1.407 \times 10^{15}$ | $7.037 \times 10^{14}$ |
| 56 | $9.007 \times 10^{16}$ | $4.504 \times 10^{16}$ |
| 74 | $2.361 \times 10^{22}$ | $1.181 \times 10^{22}$ |
| 150 | $1.784 \times 10^{45}$ | $2.287 \times 10^{43}$ |

## 3. Self Clock-Controlled Sequences with Prime Periods

In designing a secure keystream generator, one of the first concerns of the cryptographer is to guarantee a large enough key-independent lower bound to the linear complexity of the output sequences. More desirably, if such a lower bound can be made to be of an order of magnitude approximately equal to that of the period.

As mentioned above, generators with large non-Mersenne state periods have at least the following cryptographic merits:

- There is a key-independent lower bound $Ord_p(2)$ to the linear complexity of the output sequence. However, if $p = 2^m - 1$ is a Mersenne prime, then $Ord_p(2) = m$. This is the reason why non-Mersenne primes are to be considered.
- The output sequence can be subjected to arbitrary further cryptographic transformations, such as to improve the statistics of the output, without influencing the established lower bound to its linear complexity, provided the transformation do not put it into a constant sequence. This fact puts a once-for-ever end to the linear complexity issue in all the related cryptographic considerations.

In [10], the authors proposed a class of sequence generator, which generates a sequence

with period of the form $h \times 2^m - 1$, using two mutual clock-control LFSRs, where $3 \leq h$ is an odd integer. Here we shall construct sequences with prime period using only one self-clocking LFSR, where a single LFSR control its own clock. In the new scheme, shown in Fig. 5, pseudo-random binary sequences with arbitrary prime periods of the form $h \times 2^m - 1$ could be produced by carefully setting up the stopping table (for example, a ROM or RAM). This is also a stop-and-go scheme where the stopping signal, *A(t)*, won't have two consecutive zeros.

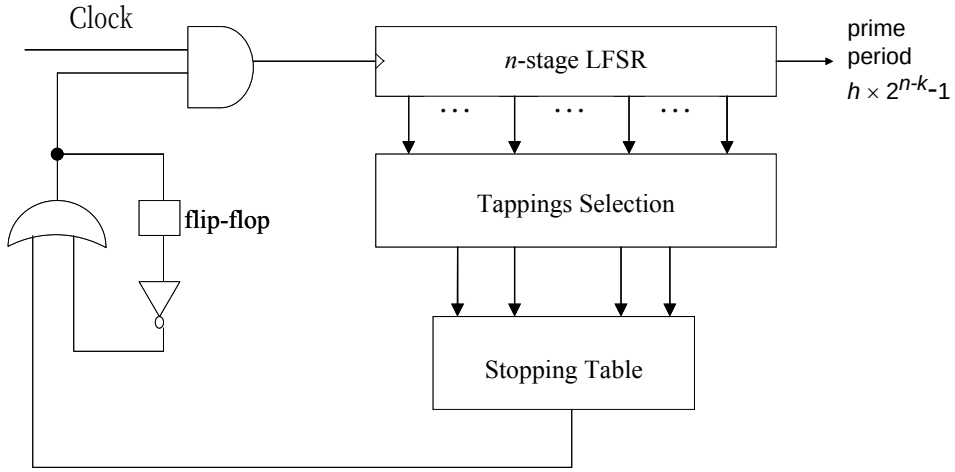


Figure 5: The proposed self-clocking generator with prime state period

To generate a large key-independent lower bound $Ord_p(2)$ to the linear complexity of the output sequence, one might select m out of n possible positions from the *n*-stage LFSR, $m \leq n$, and control contents of the 2*m*-to-1 stopping table. If the number of zeros in the table output is exactly 25% while the number of ones is exactly 75%, then the period of output sequence, assuming the LFSR is preloaded with a non-all-zero value, will be $(2^n - 1) + (2^n/4) = 5 \times 2^{n-2} - 1$. Fig. 6 shows the self-clocking sequence generator to produce an output sequence with such period. It will produce sequences with prime period, by letting $n$ = 4, 6, 10, 12, 14, 16, 20, 34, 50, 56, 74, 150, …etc. Table 1 also gives the period and the lower bound to the linear complexity for the output sequences produced by the scheme given in Fig. 6.

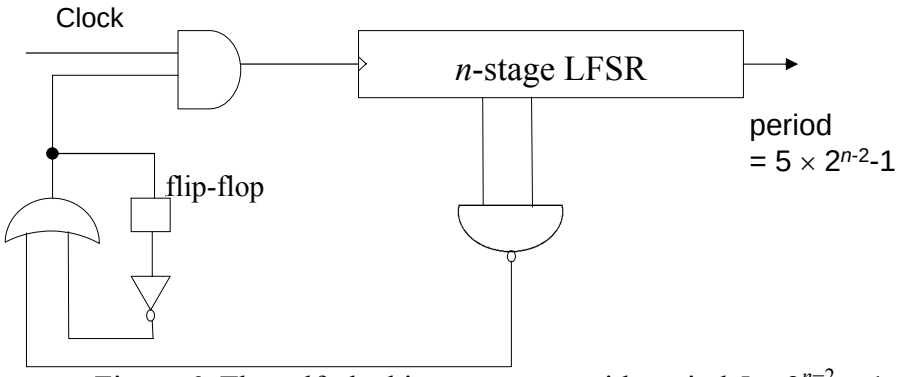


Figure 6: The self-clocking generator with period $5 \times 2^{n-2} - 1$

Similarly, if the number of zeros in the table is exactly 50%, then we have period $p = (2^n - 1) + (2^n/2) = 3 \times 2^{n-1} - 1$. Fig. 7 shows a self-clocking sequence generator to produce an output sequence with such period.

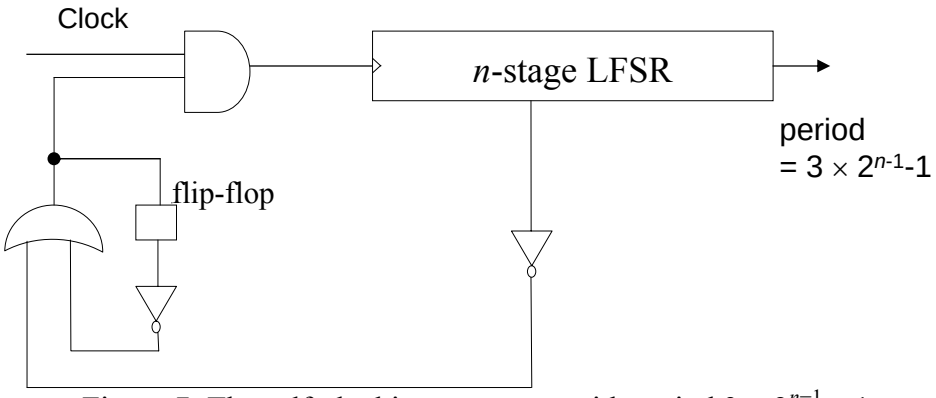

Figure 7: The self-clocking generator with period $3 \times 2^{n-1} - 1$

Necessary and sufficient conditions for prime numbers of the form $h \times 2^m - 1$ have been discussed in literature [8].

## 4. Conclusion

We proposed a scheme which enhances the security of EBU's PRBG (pseudorandom bit generator) scheme with the use of mutual clock control. We also proposed a new PRBG scheme with self clock control. Both of the proposed mutual and self clock-controlled schemes could produce sequences with large non-Mersenne prime periods and automatically have a key-independent low bound to the linear complexity (LC), LC$\geq$ $Ord_p(2)$, where $p$ is the period of output sequence. The computation of $Ord_p(2)$ would require performing factorization of $(p-1)/2$.

## Acknowledgement 致謝

作者於美國路易斯安那大學(University of Louisiana at Lafayette)就讀博士班1988~1990期間,恰逢大陸資訊安全國家重點實驗室(http://home.is.ac.cn/)創辦主任曾肯成(Kencheng Zeng)教授應邀至該校訪問，約有兩年蒙曾教授指導stream cipher的研究。作者非常感謝曾教授的啟蒙及教導，在此領域研究有任何成就的話，皆該歸功於曾教授。曾肯成教授不幸於去年5月13日病逝於北京，享年77歲。

## References

[1] J. Daemen, R. Govaerts, and J. Vandewalle, "Cryptanalysis of MUX-LFSR based scramblers," *Proceedings of the 3rd symposium on State and Progress of Research in Cryptography*, 1993, pp. 55-61. http://www.esat.kuleuven.ac.be/~cosicart/ps/JD-9300.ps.gz

[2] EBU, *Specification of the Systems of the MAC/Packet Family*, EBU Tech. 3258,1986.

[3] S.W. Golomb, *Shift Register Sequences*, revised edition, Aegean Park Press, Laguna Hills, Cali., 1982.

[4] S.M. Jennings, *A Special Class of Binary Sequences*, University of London, 1980, Ph.D. Thesis.

[5] S.M. Jennings, "Multiplexed Sequences: Some Properties of the Minimum Polynomial," *Proceeding of the Workshop on Cryptography*, Springer-Verlag Lecture Notes in Computer Science, Vol. 149, 1982, pp. 189-206.

[6] Z. Koahve, *Switching and Finite Automata Theory*, McGraw-Hill, 1978.

[7] J. L. Massey, ”Shift-Register Synthesis and BCH Decoding,” *IEEE Trans. Inf. Theory*, 1969, pp. 122-127.

[8] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhauser Boston, Inc., 1985.

[9] K.C. Zeng, C.H. Yang and T.R.N. Rao, ”On the Linear Consistency Test in Cryptanalysis with Applications,” *Advances in Cryptology - Crypto’89*, Springer-Verlag Lecture Notes in Computer Science, Vol. 435, 1989, pp. 164- 174.

[10] K.C. Zeng, C.H. Yang, and T.R.N. Rao, ”Large Primes in Stream Cipher Cryptography,” *Advances in Cryptology - Auscrypt’90*, Springer-Verlag Lecture Notes in Computer Science Vol. 453, 1990, pp. 194-205.

[11] K.C. Zeng, C.H. Yang, D.Y. Wei, and T.R.N. Rao, ”Pseudorandom Bit Generators in Stream-Cipher Cryptography,” *IEEE Computer*, Vol. 24, No. 2, Feb. 1991, pp. 8-17.