On the Design of High-Speed Pseudorandom bit Generators for Secure Broadcasting Systems

Chung-Huang Yang
Department of Information Management
National Kaohsiung First University of Science and Technology
1 University Road, Yenchao, Kaohsiung, Taiwan 824, R.O.C.
http://www.nkfu.edu.tw/~chyang/
email: chyang@ccms.nkfu.edu.tw

Abstract. Pseudorandom bit generators play an essential role in audio or video conditional-access control systems which allow broadcasting programs to be viewed only by authorized subscribers. This paper evaluated cryptographic strength of bit generators proposed by the European Broadcast Unit (EBU) and the Japan's Ministry of Posts and Telecommunications and some security weakness was found on the generators. Subsequently we gave a method to safeguard the EBU's sequence generators that is free from any known cryptologic weakness and we also proposed a self clock-control scheme which generates sequences with non-Mersenne prime periods suitable for cryptographic purposes.

Keywords: conditional access, stream cipher, pseudorandom bit generator, linear feedback shift-register, linear complexity, number theory

1. Introduction

Since the advent of pay-TV in the early 1950s, scrambled transmission of television signals has generated a great deal of interest. In a typical conditional-access control system [1-4], a group of channels is transmitted in the scrambled form and all the decoders in each subscriber's home receive the same signal consisting of scrambled components and access control parameters. Successful descrambling occurs only in the homes of those who have been authorized. Figure 1 shows the security architecture of a typical receiver or decoder in a conditional-access broadcasting system.

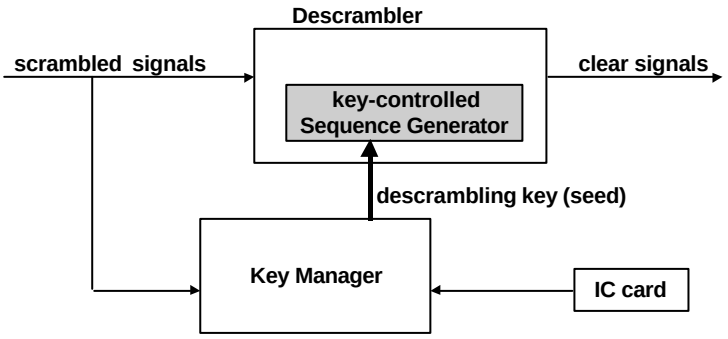

Figure 1 Security architecture of a typical addressable TV decoder

Scrambling operation is generally based upon a pseudorandom bit generators (PRBG) controlled by a secret *key*, changed at very frequent intervals, while a decoder would reproduce the original video and audio signals of

certain programs (or services) if a correctly encrypted descrambling key was received. Furthermore, in such addressable system, the decoder could be completely activated or deactivated according to subscriber's status or the program (service) in use. In practice, for reason of security, sets of secret keys are resident in a hardware key manager unit or inside an IC card.

The function of a PRBG 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 (hackers) should not be able to generate other elements 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) [5] circuits which have been in use for a long time for generating cycle redundancy check, or as pattern generators on VLSI built-in self-testing, or as error encoders/decoders. A LFSR contains 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 a *n*-stage LFSR can be completely determined by using just *2n* successive bits of the output sequence (see, for example, [6]).

Without knowing the secret keys, the hacker has the complete knowledge both about the nature of the signals under transmission and also about everything of the decoder which are invariant and key independent. With regarding the security, no general criterion at the present time has been developed to certify the security of key-controlled sequence generators, and many schemes have been proposed and then broken. The only way of cryptanalysis (attacking) is by trial and error, subjecting the generator to all known cryptanalytic techniques.

2. Security of the Sequence Generators Proposed by the EBU

The EBU scheme [7-9] uses a 32-to-1 multiplexer as a nonlinear transforming function of two maximum-length LFSRs. Figure 2 shows the general structure of this sequence generator.

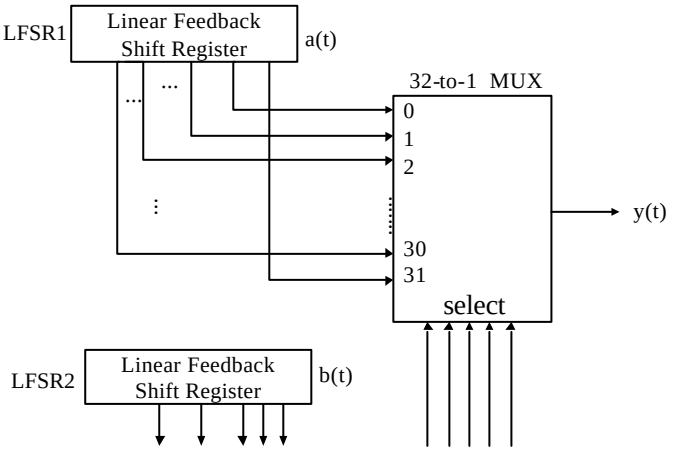

Figure 2 The PRBG proposed by the European Broadcasting Union (EBU)

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 non-zero 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 (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) $LC = (2^{29}-1)\times 31 \approx 1.7\times 10^{10}$. This undoubtedly makes output sequence of such PRBG more secure than a pure LFSR circuit. Nevertheless, it has been shown [10,11] 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 [12], which exploited the re-synchronous mechanism in the video signals.

3. Security of the Sequence Generators Proposed by the MPT

As illustrated in Figure 3, the PRBG proposed by the Japan's Ministry of Posts and Telecommunications (MPT) [13] is to employ a two-to-one multiplexer and combine three LFSRs together. Here the secret key might contain the initial values of the LFSR1, LFSR2, LFSR3, and possibly with the setting of nonlinear feedforward functions NF1, NF2, and NF3. This scheme is an improvement version of the Geffe generator [14] that was shown to be completely insecure by an analytic algorithm [15], without exhaustive searching. The computational complexity of the analytic algorithm, in terms of bit operations, is of order *O(n)*, where *n* denotes the largest length of the LFSRs taking part in the system.

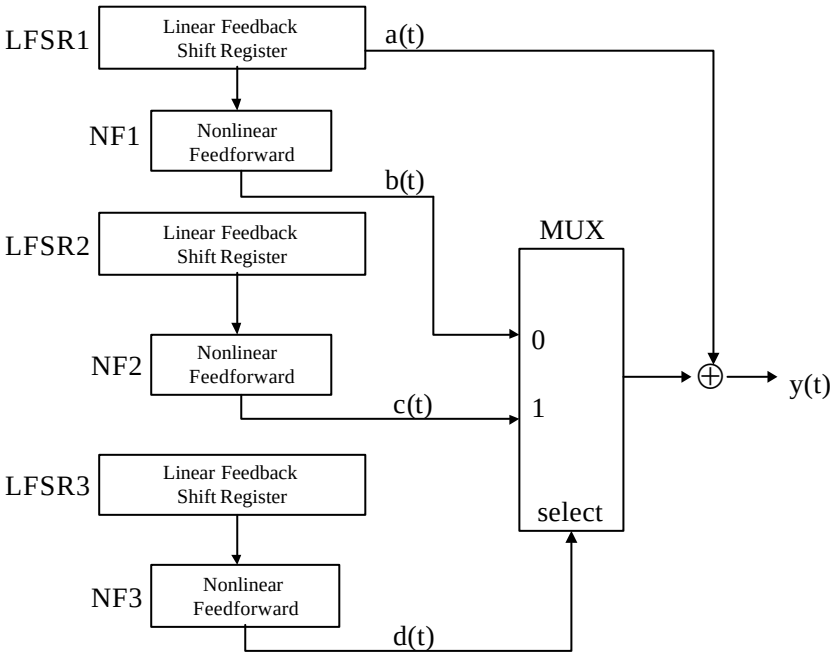

Figure 3 The PRBG proposed by Japan's Ministry of Posts and Telecommunications (MPT)

Our attack starts with the observation that if we exhaustively try every possible initial value of the LFSR1, a subkey of the entire key of secrecy, then we would encounter with sequence of {y'(t)=y(t) exclusive-OR a(t)} instead of {y(t)}. Although detailed information about the nonlinear feedforward function shown in Figure 3 is not

publicly available at present, we might make use the fact that every periodic sequence can be produced by a LFSR of suitable length and consider sequence {y'(t)} as a sequence produced by a Geffe generator with three input sequences {b(t)}, {c(t)} and {d(t)}. We then applied the analytic method [14] to attack the established Geffe's generator.

If the entire key of secrecy in Figure 3 is equally distributed into three LFSRs, then our method will reveal the secret key by a working factor of the order $2^{|K|/3)}$ instead of the originally intended $2^{|K|}$, where |K| denote the effective bit length of the secret key. Again since exhaustive searching has been applied, this only indicates that the LFSR2 and LFSR3 do not contribute substantially to the cryptographic strength of the PRBG as a whole and some precautions are required.

4. Security Enhancement of the EBU Sequence Generators

The idea of bilateral clock control [11, 16] provides a good approach to safeguard the EBU multiplexing scheme. The resulting PRBG, shown in Figure 4, is constructed on the basis of mutual clock control of two LFSRs used in the EBU generator. In the enhanced EBU scheme, we 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.

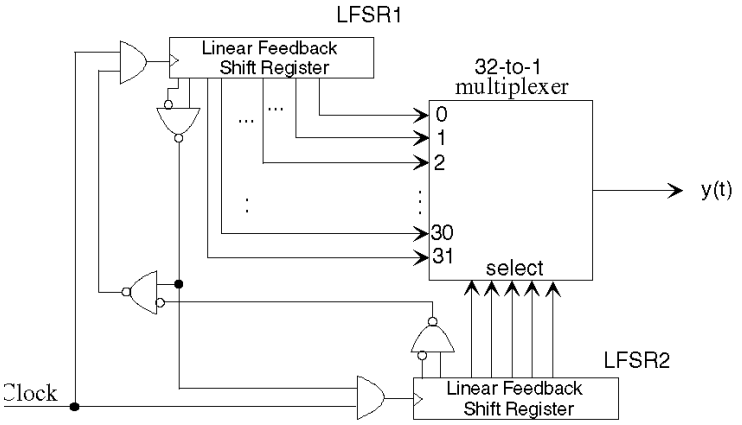

Figure 4 The enhanced MUX-LFSR sequence generator

Large prime numbers have been intensively considered in connection with the design and analysis of public-key cryptosystems. 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, 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 [16].

In the enhanced scheme we use a pair of maximum-length LFSRs with same length. The output sequence $\{y(t)\}$ has period $P = 5\times 2^{n-2}-1$, where n is the number of stages at both LFSRs. If P is an odd prime number, then the output sequence will have a guarantee key-independent lower bound to the linear complexity. 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 $n = 50, 56, 74, 150, 186, 250, 272, 276$ will also produce sequences with lower bound to the linear complexity comparable with their prime period. At present, there is no known cryptologic weakness on the proposed scheme.

We shall make an analysis of the state diagram of the generator thus constructed. The state diagram, shown in the Figure 5, is consisted of a total of $3\times 2^{n-2}-1$ cycles with $2\times 2^{2n-4}$ branches (*source state* in Figure 5) connected to these cycles and each cycle has identical length of $5\times 2^{n-2}-1$.

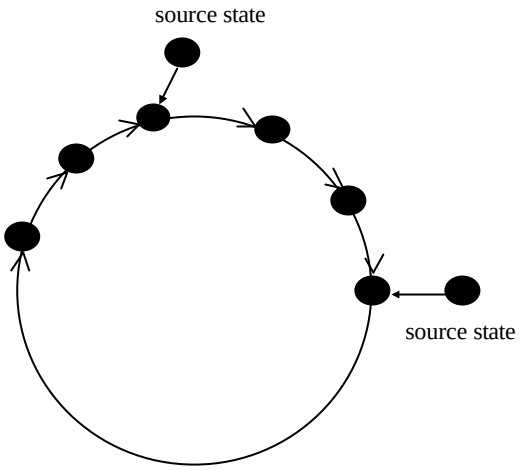

Figure 5 The state diagram for the generator given in Figure 4

.

5. Self Clock-Controlled Sequences with Prime Periods

As mentioned above, pseudo-random binary sequences with non-Mersenne periods have a series of cryptographic merits. Such sequences would have key-independent lower bound to the linear complexity and we could apply further cryptographic transformations, such as to improve the statistics of the output, without influencing the established bound, 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 [16], the authors proposed a new class of sequence generator, which generates a sequence with period of the form $h\times 2^m-1$, using two mutual clock-control LFSRs. Here we shall construct sequences with prime period using a self-clocking LFSR, where a single LFSR control its own clock.

In the new scheme, shown in Figure 6, 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 a stop-and-go type clock-control scheme.

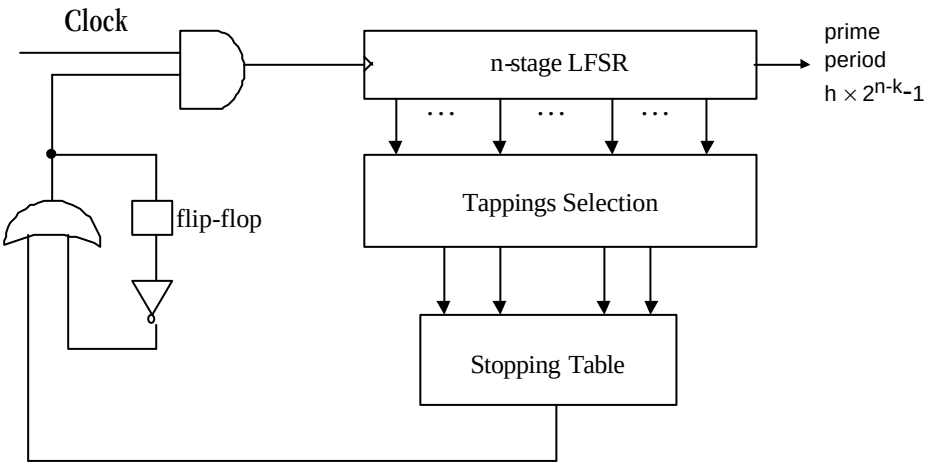

Figure 6 The self-clocking generator with prime state period

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 $2^n-1+(2^n/4) = 5\times 2^{n-2}-1$. Similarly, if the number of zeros in the table is exactly 50%, then we have period = $3\times 2^{n-1}-1$, and so on.

6. Conclusions

It is the requirement in conditional-access control systems that the video signal should be scrambled under the control of an encryption system and key-controlled pseudorandom bit generators (PRBGs) are commonly used as a basis for such purpose. The PRBGs proposed by the EBU and MPT are both based on the idea of output control while we proposed a new class of self clock-control sequence generator which produces large non-Mersenne prime period and a linear complexity comparable with the period. Although at present there is no generally applicable and practically checkable criterion for the design of cryptographically secure PRBGs, however, based on the cryptanalytic experience conducted in this paper, we feel that a well-designed PRBG with clock control would provide better cryptographic strength than the one with output control alone.

References

1. CCIR Report 1079-1, *General Characteristics of a Conditional-Access Broadcasting System*, 1986.
2. K. Lucas, "HDB-MAC, A Conditional-Access HDTV Transmission Format", *Proc. AIAA*, pp. 209-216, 1990.
3. F.J.W. van Let, "Key Words about Encryption, MAC and HDTV," *International Broadcasting Convention*, 1992, pp. 251-256.
4. D. Angebaud and J. Giachette, "Conditional Access Mechanisms for All-Digital Broadcast Signal," *IEEE Trans. Consumer Electronics*, Vol. 38, No. 3, August 1992, pp. 188-194.
5. S.W. Golomb, *Shift Register Sequences*, revised edition, Aegean Park Press, Laguna Hills, Cali., 1982.
6. James L. Massey, "Shift-Register Synthesis and BCH Decoding," *IEEE Trans. Inf. Theory*, 1969, pp. 122-127.
7. EBU, *Specification of the Systems of the MAC/Packet Family*, EBU Tech. 3258, 1986.
8. 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.
9. S.M. Jennings, *A Special Class of Binary Sequences*, University of London, 1980, Ph.D. Thesis.
10. K.C. Zeng, C.H. Yang, D.T. Wei, and T.R.N. Rao, "Pseudorandom Bit Generators in Stream-Cipher Cryptography," IEEE *Computer*, Vol. 24, No. 2, Feb. 1991, pp. 8-17.
11. 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.
12. J. Daemen, R. Govaerts, J. Vandewalle, ``Cryptanalysis of MUX-LFSR based scramblers," *Proc. 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
13. Official Gazette, Japan Ministry of Posts and Telecommunications, January 25, 1990, No. 36 (**日本官報**1990**年**1**月**25**日郵政省告示第**36**號**), in Japanese.
14. P.R. Geffe, "How to Protect Data with Ciphers That Are Really Hard to Break," *Electronics*, Jan. 4, 1973, pp. 99-101.

15. K.C. Zeng, C.H. Yang, and T.R.N. Rao, "An Improved Linear Syndrome Algorithm in Cryptanalysis with Applications," *Advances in Cryptology - Crypto'90*, Springer-Verlag Lecture Notes in Computer Science, Vol. 537, 1990, pp. 34-47.
16. 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.