Pseudorandom bit Generators for Secure Broadcasting Systems

Chung-Huang Yang 楊 中皇
Computer & Communication Research Laboratories
Industrial Technology Research Institute
Chutung, Hsinchu 31015, Taiwan, ROC
e-mail: v40ych@v0sun2.ccl.itri.org.tw

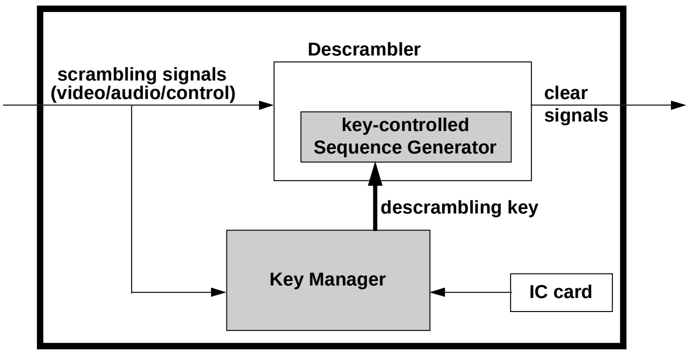
ABSTRACT

Pseudorandom bit generators play an essential role in high-security audio/video scrambling and addressing systems which allow pay-TV programs to be viewed only by authorized subscribers. This paper evaluated cryptographic strength of the bit generators proposed by the European Broadcast Unit and the Japan's Ministry of Posts and Telecommunications and some security weakness was found on the generators. Subsequently we proposed a new sequence generator which is free from any known cryptologic weakness.

1. INTRODUCTION

Since the advent of pay-TV in the 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 parameter. Descrambling occurs only in the homes of those who have been authorized. Fig. 1 shows the security architecture of a receiver/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 picture and sound 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, a set of secret keys are resident in the key manager unit or inside IC card.

Fig. 1 Security architecture of the decoder



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 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) [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 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 a *n*-stage LFSR output sequence will be 2^n -1 for any non-zero initial state (the *key*). Such a output sequence is called *maximum-length* sequence.

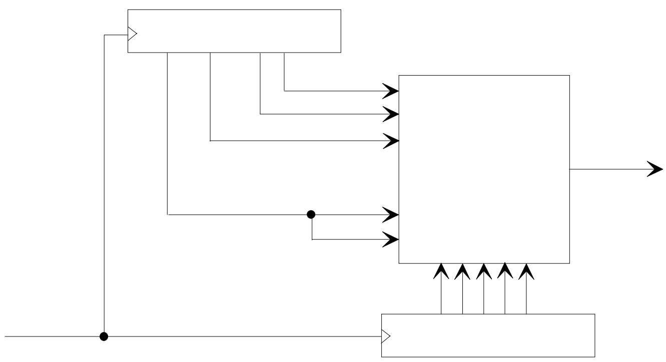
However, in spite of the large choice of the feedback connections in addition to large period and ideal randomness, maximum-length LFSR output sequences cannot be considered as secure without undergoing further cryptographic transformations. In fact, the initial state and feedback connection of a *n*-stage 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 PRBG PROPOSED BY EBU

The EBU scheme [7,8] 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 generators.

Fig. 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 [6,9] 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.

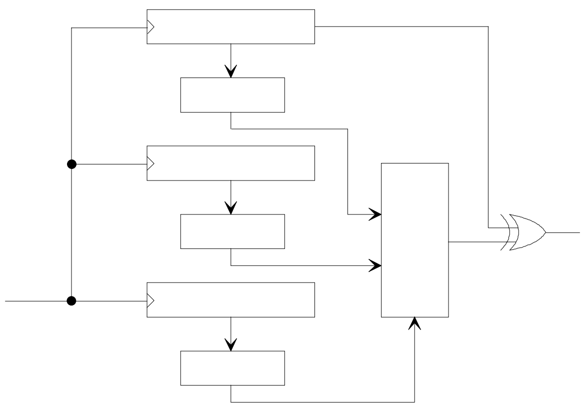
This means that the entire key of secrecy can be revealed by a working factor of the order 2^{29}, not the originally intended $2^{29+31}=2^{60}$. Since exhaustive searching has been applied, this does not mean that the generators are cryptographically insecure, but rather indicates that some precautions are required to compensate for the reduced security strength.

3. SECURITY OF THE PRBG PROPOSED BY JAPAN'S MINISTRY OF POSTS AND TELECOMMUNICATIONS

As illustrated in Fig.3, the PRBG proposed by the Japan's Ministry of Posts and Telecommunications [10] is to employ a two-to-one multiplexer and combine three LFSRs together. Here the secret key contains 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 [11] which was shown to be completely insecure by an analytic algorithm, without exhaustive searching, given at [12]. The computational complexity of the 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.

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 Fig. 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 [12] to attack the established Geffe's generator.

Fig. 3 The PRBG proposed by Japan's Ministry of Posts and Telecommunications

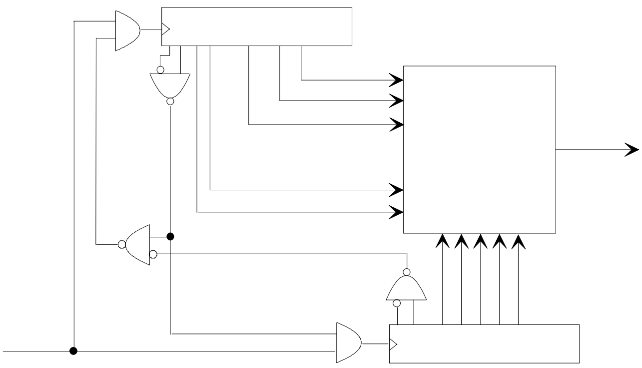


If the entire key of secrecy in Fig. 3 is equally distributed into three LFSRs, then our method will reveal the secret key by a working factor of the order $2^{(|K|/3)}$ instead of the originally intended $2^{|K|}$, where |K| denote the effective bit length of the secret key. Again since exhaustive searching 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. THE PROPOSED SEQUENCE GENERATOR

The idea of bilateral clock control [6,13] provides a good approach to safeguard the EBU multiplexing scheme. The proposed PRBG, shown in Fig. 4, is constructed on the basis of mutual clock control of two LFSRs used in the EBU generator. In the 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 which controls the clock signals to it.

Fig. 4 The proposed PRBG



In the proposed scheme we will use two 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 a prime number, then the output sequence will have a guarantee key-independent lower bound to the linear complexity [13]. An example of the proposal is to let $n = 34$, then period $P = 5\times 2^{32}-1 = 21{,}474{,}836{,}479$ and key-independent linear complexity $LC \geq (P-1)/2 = 10{,}737{,}418{,}239$. At present, there is no cryptologic weakness on the proposed scheme, to our knowledge.

5. 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 European Broadcast Unit and the Japan's Ministry of Posts and Telecommunications are both based on the idea of output control. 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 believe that a well-designed PRBG with clock control would provide better cryptographic strength than the one with output control alone.

6. ACKNOWLEDGEMENT

This paper is a partial result of the project no. 35P1600 conducted by the ITRI under sponsorship of the Minister of Economic Affairs, R.O.C.

7. 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. K.C. Zeng, C.H. Yang, D.T. Wei, and T.R.N. Rao, "Pseudorandom Bit Generators in Stream-Cipher Cryptography," IEEE *Computer* Magazine, Vol. 24, No. 2, Feb. 1991, pp. 8-17.
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. 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. Official Gazette, Japan Ministry of Posts and Telecommunications, January 25, 1990, No. 36, in Japanese (日本官報1990年1月25日郵政省告示第36號).
11. P.R. Geffe, "How to Protect Data with Ciphers That Are Really Hard to Break," *Electronics*, Jan. 4, 1973 , pp. 99 -101.
12. 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.
13. 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.

8. AUTHOR

Chung-Huang Yang is an Engineer at the Video Information Technology Division, CCL/ITRI. Before joining ITRI, he was with RSA Data Security, Inc., Redwood City, USA and NTT Network Information Systems Laboratories, Yokosuka, Japan. His current research interests include cryptography and computer arithmetic.