ELECTRONICS AND ELECTRICAL ENGINEERING

ISSN 1392 – 1215 *2007. No. 7(79)*

ELEKTRONIKA IR ELEKTROTECHNIKA

ELECTRONICS

T170

ELEKTRONIKA

Unpredictable Cryptographic Pseudo-Random Number Generator based on Non-linear Dynamic Chaotic System

A. Čitavičius, A. Jonavičius

Department of Electronics and Measurements Systems, Kaunas University of Technology,
Studentų str. 50, LT-51368 Kaunas, Lithuania, phone: +370 37 300539; e-mail: Algis.Citavicius@ktu.lt

S. Japertas

Department of Telecommunications, Kaunas University of Technology,
Studentų str. 50, LT-51368 Kaunas, Lithuania, phone: +370 5 2735752; e-mail: Saulius.Japertas@ktu.lt

Introduction

Hardware noise generators, for example [1,2], are very useful and perspective for the cryptographic applications. But nevertheless the application of hardware noise generators has a very high implementation cost.

Classical pseudo-random number generators (PRNG) are unsuitable for cryptographic applications despite the goodness of their statistical characteristics. Among them are linear feedback shift registers (LFSR) and linear congruential random number generators [3]. However quite small number of output samples causes a backward and forward prediction property. This is valid even for some well known generators based on non-linear dynamic chaos systems. One of them well known example named as logistic generator is a non-linear system described by the equation [4]:

$$x_t = ax_{t-1}(1 - x_{t-1}),\ 0 \le x_{t-1} \le 1. \qquad (1)$$

The structure defined by the latter equation is quite simple. The crypto analysis of this generator expressed by the recurrence polynomial equation is presented in [3]. But nevertheless the idea to use the non-linear chaotic dynamic system for the cryptographic secure PRNG construction seems to be perspective.

We can formulate two groups of requirements for unpredictable cryptographic PRNG. The first one is absence of backward and forward prediction and the second one - resistance under the serious cryptographic attacks.

The absence of backward prediction means that having the arbitrary finite set of samples x_t, $x_{t+1} \ldots, x_n$ it is impossible to restore the previous samples x_0, $x_1 \ldots$, x_{t-1}. Analogously absence of forward prediction means that having x_0, $x_1 \ldots$, x_{t-1} it is impossible to predict the following samples x_t, $x_{t+1} \ldots, x_n$. The backward and forward unpredictable generator we denominated as unpredictable generator and hence as cryptographic secure generator.

There are a lot of empty data intervals in the data sequences transmitted over the telecommunication channels. These intervals are coded with the same symbol. So, if ciphering is performed by the PRNG, there are additional opportunity for adversary to reveal a current state of such generator and hence to perform its prediction.

As it can be seen and in more details explained later the generator (1) is backward unpredictable even when coefficient a is known and is forward predictable independent of a is known or a is unknown. This property follows from the simplicity of the mathematical structure of this generator (1). Thus for construction of secure generator the additional complexity should be added.

We present here some original construction of cryptographic secure PRNG based on certain construction of non-linear dynamic chaotic system.

The problem we have solved is the following: the constructed generator has a complex structure and thus has a backward and forward unpredictability property. We denominated this generator as unpredictable.

The problem was solved by the certain connection of several PRNG and non-linear dynamic chaotic system. The cryptographic security of proposed generator is considered in the sense of its unpredictability and is investigated theoretically. By using some fundamental concepts and under some assumptions it is proved that proposed PRNG has a provable cryptographic security.

The theoretical background for the PRNG construction

In [5] the following theorem is proved.

Theorem 1. The pseudo-random bit generator exists if and only if a one-way function (OWF) [6] exists.

We will construct below the secure generator by proving the following implications. We define some abstract generator and prove that if certain conditions hold then the backward and forward prediction corresponds to the inversion of some one-way functions (OWF). This implication coincides with the statement of Theorem 1 and hence guarantees the existence of secure generator.

Firstly we remind some OWF definitions.

A function $F: X \to Y$ is said to be an OWF if for all $x \in X$ it is "easy" to compute the value $F(x) = y \in Y$ but it is "hard" to invert it. The term easy means that $F(x)$ can be computed by polynomial-time algorithm (*P*-algorithm), while $F^{-1}(y)$ algorithm belongs to the class of *NP*-problems (algorithms). Recall that *NP*-problems are those which require an exponential-time algorithms since the polynomial time algorithms for theirs solution are unknown.

The more rigorous OWF definition requires a specialization of polynomial-time algorithms to the deterministic polynomial-time and probabilistic polynomial-time.

Definition 1. A function $F: X \to Y$ is called an OWF if the following conditions hold.

1. There exists a deterministic polynomial-time algorithm A, so that on input $x \in X$ the value $A(x) = F(x)$ can be computed.

2. For every probabilistic polynomial-time algorithm A', every polynomial p and all sufficiently large N are the probability satisfies the following inequality.

$$\mathrm{Prob}[A'(F(x), N) \in F^{-1}F(x)] < 1/p(N), \qquad (2)$$

where N is some parameter defining the input data length.

This definition is very strong in the sense of probability measure and is not adequate for our considerations. For the cryptographic applications it is not sufficient to find any element of $F^{-1}F(x)$ but rather the certain single element of this set. Therefore we present a weakened form of (2).

We can simplify the (2) by considering the problem of exact backward and forward prediction property. Assume $Y = X$ and we would like to predict the exact values x_0 and x_n by having the sample values x_t, x_{t+1}, …, x_{t+m}, where $0 < t < t + m < n$.

Then instead of (2) we propose to use the following definitions

$$\mathrm{Prob}_1[A_1'(F^t(x_0)) = x_0] < 1/p(t), \qquad (3)$$

$$\mathrm{Prob}_2[A_2'(F^n(x_t)) = x_t] < 1/p(n), \qquad (4)$$

where Prob_1, A_1' and Prob_2, A_2' are the probability and algorithm of backward prediction and probability and algorithm of forward prediction correspondingly.

Let us consider the non-linear dynamic chaos system described by non-linear subjective function f in the form

$$x_t = f(x_{t-1}). \qquad (5)$$

Let function f provide a 2 to 1 mapping $f: X \to X$, i.e. for all images $x_i \in X$, $f^{-1}(x_i)$ has two different preimages $x_{1,i-1}$ and $x_{2,i-1}$ in X, where X, as above, is some finite set of numbers.

Assume function $f(x)$ on value $x = x_t$ can be calculated in polynomial time. Let the same is true to calculate two preimages $x_{1,i-1}$ and $x_{2,i-1}$ by inverting $f(x_i)$. By definition, having the initial value $x = x_{t-n}$ the calculation of x_t formally can be expressed by the formula

$$x_t = f^t(x_0). \qquad (6)$$

Proposition 1. The function f^n is an OWF.

Proof. Due to f being a surjection form 2 to 1, the probability to guess the actual value x_{t-1} by having x_t is $1/2$. Hence the some probability to find the value x_t is $(1/2)^t$, i.e.

$$P\{x = x_0 \mid f^t(x_0) = x_t\} = \left(1/2\right)^t. \qquad (7)$$

For every polynomial $p(t)$ there exists some sufficiently large t that the following inequality holds

$$\left(1/2\right)^t < \frac{1}{p(t)}. \qquad (8)$$

Then we obtained a (3) inequality. The proof is completed.

The proof of Proposition 1 allows us to use the chaotic generator. Therefore we must solve the problem of how to construct the forward unpredictable generator.

We propose to use several different generators with the same domain and range set X and a procedure of it random switching to produce the forward unpredictable sequence. Then we must to decide of how to produce a random switch function $s(x)$ and to choose concrete generators to be switched.

By refereeing to the result [5] we can construct a PRNG based on the function f with the properties defined above.

Let the output of random switch function $s(x)$ is connected with the some non-linear dynamic random number generator, which depends on the some parameter β. Then the parameter β can be changed randomly. The suitable candidate can be chosen of the form [7]:

$$x_{t+1} = (1+\beta)(1+1/\beta)^{\beta} \cdot x_t(1-x_t)^{\beta}, \qquad (9)$$

where β is integer in the range $1 \le \beta \le 4$, $x_t \in X = [0,1]$. The set X can be interpreted as a set of float numbers in computer presentation. This equation is a generalization of (1), since when $\beta = 1$ then we obtain (1).

Let the switching function is realized by some simple PRNG, i.e. linear congruential generator [3]. Then for

example after the adequately chosen parameters a, b and q the generator produces a sequence z_t, $t = 0,1...$ satisfying relation

$$z_t = (az_{t-1} + b) \bmod q. \quad (10)$$

In this case we need only to extract two bits from each sample z_t to produce the parameter β assignment in (9).

Linear congruential generator is repetitive, i. e. has a period. This generator will have a maximum period if:

1. b and q are relatively prime;
2. $a-1$ is divisible by all prime factors of q;
3. $a-1$ is a multiple of 4 if q is a multiple of 4.

Linear congruential generator didn't have good correlation characteristics, but the samples, generated be this generator, are uniform distributed.

The other solution could be a Blum-Blum-Schub (BBS) generator [7] application to produce two independent. But BBS generator operates more slowly.

Assumption 1. Let we have simple auxiliary generator (AG) producing a series of two bits in each sample of being statistical independent and uniformly distributed.

Let the AG, satisfying the Assumption 1, assigns the value β to the generator defined by (9) and thus performs a switching procedure of four alternative generators.

Proposition 2. If the Assumption 1 holds, then the forward recurrence function (9) is an OWF.

Proof. If Assumption 1 holds then the probability to predict the sample x_{t+1} by having x_t from (9) is $1/4$. Correspondingly, the probability to predict x_{t+n} by having x_t is $(1/4)^n$, taking into account (6). Then there exists a polynomial time algorithm A_2', such that

$$\mathrm{Prob}_2[A_2' f^n(x_t) = x_{t+n}] = \left(1/4\right)^n, \quad (11)$$

where f and f^n are defined by (9).

For the sufficiently large n for every polynomial $p(x)$, we have the inequality

$$\left(1/4\right)^n < p(n). \quad (12)$$

This proves the proposition.

So, by referencing to the Theorem 1 the Propositions 1 and 2 allows us to construct a pseudo random function generators.

Unpredictable PRNG construction

The proposed PRNG construction consists of two main parts:

1. The auxiliary generator (AG).
2. The non-linear dynamic chaos system (NLDCS).

The structure of the generator is presented in Fig.1.

The initiation of PRNG is performed by loading the initial conditions to all generators by the switch S. Δ^{-1} is the backward shift operator.

The AG yields the output β with two of digits. These two bits defines a one concrete generator of four described by (9).

As mentioned above linear congruential generators have limited maximum period and this means that linear congruential generator begins reiterate, when reaches the maximum period with defined parameters. To have bigger maximum period and to have better statistical characteristics AG could be implemented by some way, shown in Fig. 2.

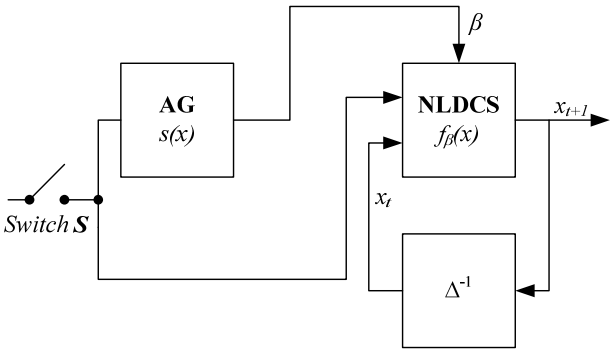

Fig. 1. The PRNG with provable cryptographic security

Two linear congruential generators in Fig. 2 generate pseudo-random bit sequences. Each n bit sequence of the generator is summarized by modulo 2 operations. The concrete value of β consist of two bits. Then two bits are transformed to decimal code. Since β must be integer in the range $1 \le \beta \le 4$, the constant equal to 1 is added to the decimal code of β.

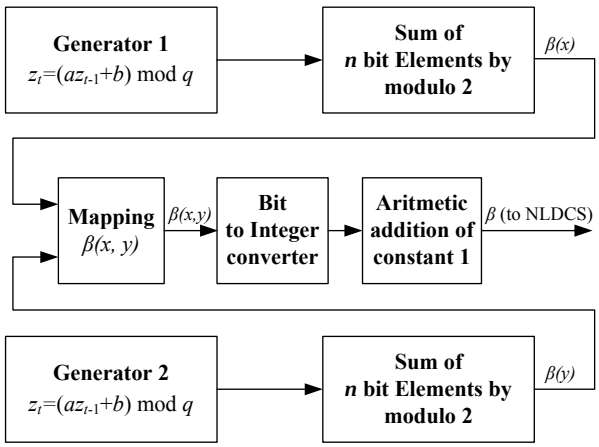

Fig. 2. AG implementation

For the additional security of presented PRNG it is required that the output sample x_{t+1} of NLDCS should be the uniformly distributed. The requirement of statistical independence is not necessary since it is satisfied by the AG.

Such decomposition of very important properties essentially simplifies the entire PRNG construction and provides great design flexibility.

The method of this problem solution and related results will be presented in the further paper.

Conclusions

1. Cryptographically secure PRNG based on certain construction of non-linear dynamic chaotic system seems to be perspective for its own statistical characteristics. However it is few described in open cryptographic publications.

2. To create a good cryptographic secure PRNG based on certain construction of non-linear dynamic chaotic system we recommend to use a non-linear dynamic chaotic system, witch parameter β is generated from auxiliary generator to get backward and forward unpredictable sequences.

3. Inserting an additional blocks we have constructed unpredictable generator in the sense that by noticing (recovering) the output of the generator it is impossible to perform the backward and forward prediction.

References

1. **Tamaševičius A.**, **Mykolaitis G., Bumblienė S., Baziliauskas A., Krivickas R. V., Lindberg E.** Chaotic Colpitts oscillator for the ultrahigh frequency range. Nonlinear Dynamics. 2006. – Vol. 44, No. 1-4. – P. 159–165.
2. **Čenys A.**, **Tamaševičius A., Baziliauskas A., Krivickas R. V., Lindberg E.** Hyperchaos in coupled Colpitts oscillators // Chaos, Solitions & Fractals. – Oxford, 2003. – Vol. 17, No. 2–3. – P. 349–353.
3. **Schneier B.** Applied cryptography. Protocols, algorithms and source code in C. – John Wiley&Sons. – 1996.
4. **Schuster H. G., Just W.** Deterministic chaos. Fourth, Revised and Enlarged Edition. – WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim. – 2005.
5. **Hastad J., Impagliazzo R., Levin L., Luby M.** A pseudorandom generator from any one-way function // SIAM Journal on Computing, 1999. – No. 28(4). P. 1364–1396.
6. **Sakalauskas E., Tvarijonas P., Raulynaitis A.** Key Agreement Protocol (KAP) using conjugacy and discrete logarithm in group representation level // Informatika. – 2007. – Vol. 18, No. 1. – P. 115–124.
7. **Menezes A., Oorschot van P., Vanstone S.** Handbook of Applied Cryptography. – CRC Press, 1996. – 816 p.

Submitted for publication 2007 03 22

A. Čitavičius, A. Jonavičius, S. Japertas. Unpredictable Cryptographic Pseudo-Random Number Generator based on Non-linear Dynamic Chaotic System // Electronics and Electrical Engineering. – Kaunas: Technologija, 2007. – No. 7(79). – P. 29–32.

Most of pseudo-random number generators are unsuitable for cryptographic applications despite their statistical and correlation characteristics due to its backward and forward predictability. The prediction can be performed by noticing (or recovering) some output sequences of generators. To solve this problem, we recommend using a non-linear dynamic chaotic system and an auxiliary generator with complex structure, based on pseudo-random number generators, which produce secret parameter β necessary for non-linear dynamic chaotic system. Thus we get an unpredictable cryptographic pseudo-random number generator based on non-linear dynamic chaotic system with forward and backward unpredictable properties. The theoretical background and possible structure of cryptographic secure pseudo-random number generator are presented. Ill. 2, bibl. 7 (in English; summaries in English, Russian and Lithuanian).

А. Читавичюс, А. Йонавичюс, С. Япертас. Непредсказуемый криптографический генератор псевдослучайных чисел, основанный на нелинейной динамической хаотической системе // Электроника и электротехника. – Каунас: Технология, 2007. – № 7(79). – С. 29–32.

Большинство псевдослучайных генераторов чисел являются неподходящими для криптографии, несмотря на их статистические и корреляционные особенности из-за их прямой и возвратной предсказуемости. Предсказание может быть выполнено, наблюдая (или восстанавливая) некоторые последовательности на выходе генераторов. Для решения этой проблемы рекомендуется использовать нелинейную динамическую хаотическую систему и вспомогательный генератор со сложной структурой, на основе псевдослучайных генераторов чисел, генерирующий необходимый для нелинейной динамической хаотической системы секретный параметр β. В этом случае получается непредсказуемый криптографический генератор псевдослучайных чисел, основанный на нелинейной динамической хаотической системе с прямой и возвратной непредсказуемостью. В статье описаны теоретические основы и возможная конструкция для разработки криптографически безопасного генератора псевдослучайных чисел. Ил. 2, библ. 7 (на английском языке; рефераты на английском, русском и литовском яз.).

A. Čitavičius, A. Jonavičius, S. Japertas. Nenuspėjamas kriptografinis pseudoatsitiktinių skaičių generatorius netiesinės, dinaminės, chaotinės sistemos pagrindu // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2007. – Nr. 7(79). – P. 29–32.

Bėl galimo tiesioginio ir atgalinio sekos narių numatymo dauguma pseudoatsitiktinių skaičių generatorių nėra tinkami naudoti kriptografijoje, nepaisant jų statistinių ir koreliacinių savybių. Numatyti galima stebint (arba atkuriant) kai kurias generatoriaus išėjime gautas sekas. Problemai spręsti šiame straipsnyje siūloma naudoti netiesinę dinaminę chaotinę sistemą ir sudėtingos struktūros papildomą generatorių pseudoatsitiktinių skaičių generatorių pagrindu, kuriuo naudojantis generuojamas netiesinei dinaminei chaotinei sistemai reikalingas slaptas parametras β. Taip gautas generatorius generuoja seką, kurios būsimų ar prieš tai buvusių sekos narių neįmanoma numatyti iš jau žinomų sekos narių. Straipsnyje aprašomi šio generatoriaus konstravimo teoriniai pagrindai, pasiūlyta galima jo schema. Il. 2, bibl. 7 (anglų kalba; santraukos anglų, rusų ir lietuvių k.).