Analysis of Physical Random Number Properties Generated by Semiconductor Super Lattices

Fangzhen Duan[1, a], Yongming Nie[1, b *], Xibao Xu[1, c] and Xuehua Yang[1, d]

[1]China Satellite Maritime Tracking and Controlling Department, Jiangsu, Jiangyin, China, 214431

[a]nwy1986@163.com, [b]nwy1986@163.com, [c]290505026@163.com, [d]yimonie@163.com

*The corresponding author

Keywords: Physical random number; Encryption; Cross correlation; Linear complexity

Abstract. The proerties of fast physical random-number that is generated based on room-temperature chaotic oscillations in weakly coupled superlattices are investigated in detail, including the balansability, the linear complexity, the cross-correlation, and auto-correlation characteristics. Experimental and simulating reasults indicate that the ratio between the number of ones and zeros is 10001:10000 and the correlations are excellent and the linear complexity is good, which proves the physical random-number generated ased on room-temperature chaotic oscillations in weakly coupled superlattices can be used in the information secure communications effectively.

Introduction

Binary pseudo-random number that has good balance, correlation and linear complexity can generated with mature methods [1-8], which has been widely used in many areas such as numerical simulations, statistical mechanics, gaming industry, cryptography and communication. However, the fatal short coming of binary psedo-random number is its pseudo-random properties, which limits its application. For example the periodicity will make pseudo-random sequence encryped information being deciphered easily. Fortunately, the true random sequence that is generated based on physical sources, including radiative decay, frequency jitter, photon emission and detection, electronic noise and atmosphere noise [9-11], can overcome the short coming. In theory, it can really realize the absolute for its excellent random properties with no periodicity. In this manuscript, the proerties of fast physical random-number that is generated based on room-temperature chaotic oscillations in weakly coupled superlattices are investigated in detail [8], including the balansability, the linear complexity, the cross-correlation, and auto-correlation characteristics. Experimental testing and numerical simulating are given in detail.

Theory Analyses

Balnaced Property. The balanced code has a smaller cross-correlation sidelobe value and a narrower amplitude range, which is very important for the use of the sequence. For binary random sequence $\{a_i\}$, it can be presented as follows.

$$a = (a_0, a_1, a_2 \cdots a_{N-1}) \tag{1}$$

If the difference between the total number “one” and “zero” of sequence $\{a_i\}$ is no more than one, the sequence can be known as balanced sequence, which satisfies the following expression.

$$\left| \sum_{k=0}^{N-1} (-1)^{a_k} \right| \le 1 \tag{2}$$

Autocorrelation and Cross Correlation. Autocorrelation and cross correlation properties of both pseudo-random sequence and true random sequence are important for their application in code-division multiple access systems, spread spectrum communication systems, radar systems and so on [12, 13]. The theory process can be expressed as follows. The cross correlation of function $f(t)$ and $g(t)$ can be given by the following formula.

$$R_c(\tau) = \int_{-\infty}^{+\infty} f(t)g(t-\tau)dt \tag{3}$$

If $f(t)$ and $g(t)$ are essentially equal, the auto-correlation function can be obtained.

$$R_a(\tau) = \int_{-\infty}^{+\infty} f(t)f(t-\tau)dt \tag{4}$$

The above twoformulas are general experssions. For binary random sequence $\{a_i\}$, the defination of auto-correlation can be obtained by the following formula.

$$R_a(\tau) = \frac{1}{N}\sum_{k=0}^{N-1}(-1)^{a_k}(-1)^{a_{k+\tau}} \tag{5}$$

Where τ is valued according to $0 \le \tau \le N-1$.

For excellent random sequence, the best auto-correlation property is binary correlation, which can be presented as the following form.

$$E\left[R_a(\tau)\right] = \begin{cases} 0, & \tau \neq 0 \\ 1, & \tau = 0 \end{cases} \tag{6}$$

In the above expression E presents the mathematic expectation.

Linear Complexity. Generally, the linear span of m-sequence is short relative to their period, which has easy predictability making it unsuitable for some applications. The linear span of a sequence is one measure of its predictability. Any "good" random sequence must have large linear span comparable to its period [14, 15]. The sequence linear span L can be obtained based on the following formula [16].

$$L = \sum_{i \in I} n^{w(i)} \tag{7}$$

Where $w(i)$ is the Hamming weight and the sum is 0 if $I = \varnothing$.

Experimental and Simulating Results

A high speed all-electronic physical random bit generator based on chaotic current oscillations of semiconductor superlattice at room temperature generating the random sequence provided by Suzhou Institute of Nano-tech and Nano-bionics of Chinese Academy of Sciences. The cross-correlation and auto-correlation characteristics are described in Fig. 1.

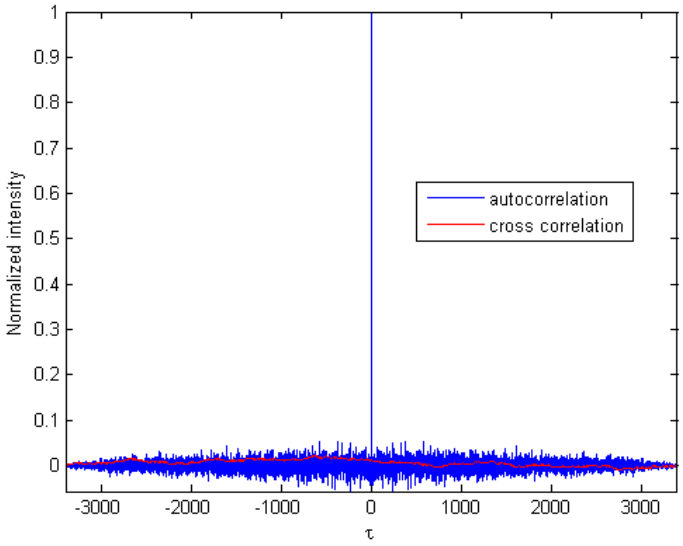

Figure 1. Schematic of the cross-correlation and auto-correlation characteristics

Based on Fig. 1, it is easily to find that auto-correlation and cross-correlation properties of the physical random sequence are excellent. Further caculating results indicate that the signal rejection ratio can reach as high as 76 dB, which can effectively satify the requirement of normal information tansmission.

At present, the pseudo random sequence's linear span length is short because all pseudo random sequences have periodicity property no matter how long they are. Such easy predictability makes them unsuitable for some applications requiring pseudorandom bits. Fortnately, there is no periodicity property of the physical random sequence. The linear complexity property is shown in Fig. 2.

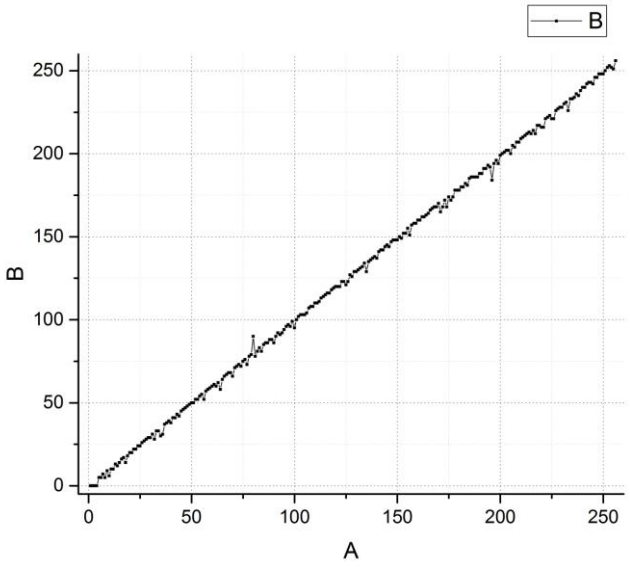

Figure 2. Schematic of the linear complexity

We randomly extract 256 consecutive binary numbers of the sequence to give the result shown in Fig. 2. It is easy to find that the linear complexity increases with the length of the sequence, which is better than the pseudo random sequence and means it can resist the linear attack method more effectively.

After processing, the ratio between the number of ones and zeros is 10001:10000. The randomness of the generated sequences is verified using the NIST and TestU01 statistical test suites.

Conclusions

We have presented general results on the balansability, the linear complexity, the cross-correlation, and auto-correlation of a new class of binary sequences that are obtained based on room-temperature chaotic oscillations in weakly coupled superlattices are investigated in detail, including characteristics. The results imply that the binary sequences under consideration have good balanced proerty, excellent correlations and perfect linear complexity, which proves the physical random-number generated ased on room-temperature chaotic oscillations in weakly coupled superlattices, can be used in the information secure communications effectively.

References

[1] J. Eichenauer and J. Lehn, A non-linear congruential pseudo random number generator. Statistische Hefte 27, 315–326 (1986).

[2] A. Peinado and A. Fuster-Sabater, Generation of pseudorandom binary sequences by means of linear feedback shift registers (LFSRs) with dynamic feedback, Math. Comput. Model, 57: 2596–2604 (2013).

[3] J. D. Golic, New methods for digital generation and postprocessing of random data, IEEE, Tansactions on computers, 55(10): 1217-1229, (2006).

[4] O. Y. Lui, C. H. Yuen and K. W. Wong, A pseudo-random number generator employing multiple Renyi maps. Int. J. Mod. Phys. C 24, 1350079 (2013).

[5] M. François, T. Grosges, D. Barchiesi and etc, R. A new pseudo-random number generator based on two chaotic maps. Informatica, 24, 181–197 (2013).

[6] H. Hu, L. Liu and N. Ding, Pseudorandom sequence generator based on Chen chaotic system. Comput. Phys. Commun. 184, 765–768, (2013).

[7] M. François, T. Grosges, D. Barchiesi and etc, Pseudo-random number generator based on mixing of three chaotic maps. Commun. Nonlinear Sci. Numer. Simulat. 19, 887–895 (2014).

[8] W. Li, I. Reidler and Y. Aviad, Fast Physical Random-Number Generation Based on Room-Temperature Chaotic Oscillations inWeakly Coupled Superlattices, Physical Review Letter, 111, 044102, (2013).

[9] M. Stipcevic and R. Ursin, An On-Demand Optical Quantum Random Number Generator with In-Future Action and Ultra-Fast Response, Scientific reports, 6:1-8, 2014.

[10] F. Brandao, R. Ramanathan, A. Grudka and etc,Realistic noise-tolerant randomness amplification using finite number of devices, Nature communication, 11345-6, 2016.

[11] M. Stipcevic, Active quenching circuit for single-photon detection with Geiger mode avalanche photodiodes, Appl. Opt. 48:1705–1714 (2009).

[12] V.Edemskiy and A.Palvinskiy, The linear complexity of binary sequences of length 2pwith optimal three-level autocorrelation, Information ProcessingLetters, 2016, 116: 153–156.

[13] S.W. Golomb and G. Gong, Signal Design for Good Correlation: For Wire-less Communications, Cryptography and Radar Applications, Cam-bridge University Press, 2005.

[14] E. L. Key, “An analysis of the structure and complexity of nonlinear binary sequence generators”, IEEE Trans. Inform. Theory, 22(6):732-736, 1976.

[15] R. A. Rueppel, “New Approuclies to Stream Ciphers”, Ph.D. thesis, Swiss Fed. Inst. Technol., 1984.

[16] A. H. Chan and R. A. Games, “On the Linear Span of Binary Sequences Obtained from Q-Ary M-Sequences, Q Odd”, IEEE Trans. Inform. Theory, 36(3): 548-552, 1990.