Spread Spectrum Based on Semiconductor Superlattices True Random Sequence

Minmin Guo[1, a], Yongming Nie[1, b *] and Xin Ding[1, c]

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

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

*The corresponding author

Keywords: Spread spectrum communication; Physical random sequence; Encryption; Stream cipher

Abstract. A setup for information transmission based on physical random sequence spreading method, which is generated by physical random number generator based on room-temperature chaotic oscillations in weakly coupled semiconductor superlattices, is demonstrated. The spreading processing and auto-correlationg theories are investigated in detail. Then, the temporal waveforms and auto-correlation intensity distributions of plaintext information, physical random sequence and spreaded seauence were experimentally tested respectively. Both theoretical and experimental results indicate that the physical random sequence can effectively use to accomplish spread spectrum, which has significant value in the future secure information transmission.

Introduction

With the rapid development of information technology, spread spectrum communication technology becomes more and more mature. Generally, spread spectrum communication technology uses a random code sequence to modulate information data implementing spread spectrum, which can greatly reduce power spectral density and obtain a higher signal to noise ratio. To our knowledge the successful and mature application of random sequence is just pseudo-random sequence not only in spread spectrum communication systems, but also in ranging systems, software testing systems, radar systems and stream ciphers. However, pseudo-random sequence is generated by deterministic algorithm, which is predictable no matter how complex the algorithm is for example m-sequence and gold sequence [1, 2]. Physical random sequence can effectively solve the problem, which is essential for our modern information based society especially in cryptography that is generated by physical random number generators not depending on complex algorithms but rather on a physicsal process that includes radioactive decay, photon arrival, beamsplitter based methods and so on to provide true randomness [3-7].

In this manuscript, physical random sequence generated by physical random number generator based on semiconductor superlattices is introduced into the spread spectrum communication systems [8]. Firstly, theoretical analysis was investigated in detail. Then, the setup based on physical random sequence for spectral spreading was demonstrated. Subsequently, the preoperties of spreaded spectrum signals were tested and the results such as time and spectral properties and physical random number based spread spectrum advantages were obtained. At last, conclusions were given.

Theory Analyses

The spread spectrum main process can be expressed as follows, which is similar to the pseudo random spread pectrum technology [9, 10]. At the transmitter terminal, the signal for transmitting can be expressed as following under the physcal random sequence modulating.

$$f(t)=\sqrt{2P_0}S(t)PRN(t)\cos(\omega_0 t+\varphi_0) \tag{1}$$

P_0 Is the transmitting signal power, $S(t)$ is information code, PRN is physical random number and φ_0 is initial phase.

$$r(t) = \sqrt{2P_r} S(t-\tau) PRN(t-\tau)\cos(\omega_0 t + \varphi) + n(t) \tag{2}$$

P_r Is the received signal power, $n(t)$ is additive noise in transmission and τ is phase delay. The last object that the spread spectrum receiver should achieve is to remove the physical random number sequence and carrier delay, and then the signal $S(t)$ can be obtained. The whole process can be demonstrated in Fig. 1.

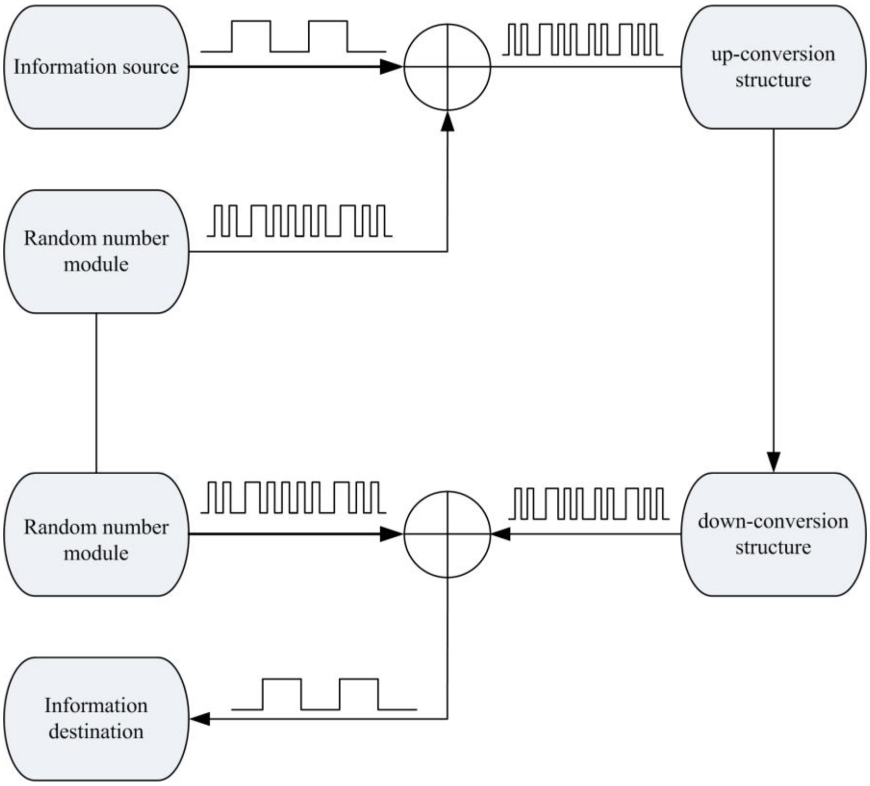

Figure 1. Schematic of spread spectrum process based on physical random code sequence

In Fig. 1, the sychronization of the two random number generators can adopt the zero-lag synchronization (ZLS) based on mutual coupling, in which the chaotic oscillations are simultaneously synchronized in spite of an arbitrary large physical distance between the chaotic oscillators. The phenomenon of ZLS between two or more chaotic semiconductor lasers attracted theoreticaland experimental interests because of promising applications to public-channel cryptography without relying on number theory, as in other existing methods [8, 11, 12].

The balance property should stay the same even after spread spectrum. The difference between the total number "one" and "zero" of $f(t)$ should be the same as $r(t)$.

$$\left|\sum_{k=0}^{N-1}(-1)^{f_k}\right| / \left|\sum_{k=0}^{N-1}(-1)^{r_k}\right| = 1 \tag{3}$$

f_k Is the kth binary element of $f(t)$ and r_k is the kth binary element of $r(t)$. For ideal sequence, no matter how long the sequence is the difference between zero number and one number should be no more than 1. The experimental results will be given in the third section.

For binary physical random sequence $PRN(t)$, the definition of auto-correlation can be obtained by the following formula.

$$R_{PRN}(\tau) = \frac{1}{N}\sum_{k=0}^{N-1}(-1)^{PRN_k}(-1)^{PRN_{k+\tau}} \tag{4}$$

where N is the tototal number of the binary physical random sequence code. It is easily to under stand that spreading spectrum operation should not change the auto-correlation characters of the sequence, which will be proved in the third section.

Experimental 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. Dirrerent physical random sequences were randomly selected with varing lengthes, which were demonstrated in Table 1. The testing results of the tations between ones to zeros were also given.

Table 1 The testing results of physical random sequence balance property

Serial number	Sequence length/bit	Number of ones	Ones ration
1	13400	6720	0.5015
2	26800	13423	0.5009
3	40200	20059	0.4990
4	53600	26787	0.4998
5	67000	33493	0.4999
6	80400	40176	0.4997
7	93800	46831	0.4993
8	107200	53548	0.4995
9	120600	60240	0.4995
10	134000	66965	0.4997

According to Table 1, it is easily to find that the number of ones in the sequence is about 50% not related to the lengthes of the sequences.

The time domain properties and auto-correlation characteristics of the physical random sequence and sequence after spreading are described in Fig. 2.

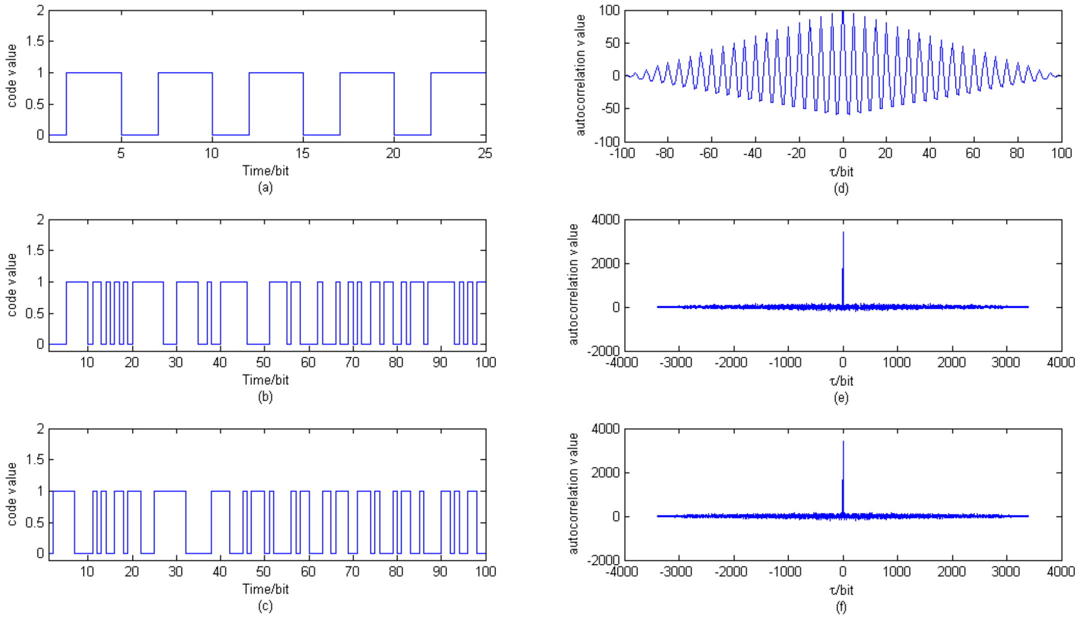

Figure 2. The time domain properties and auto-correlation characteristics of the physical random sequence before and after spreading

Fig. 2 (a) was the sequence of plaintext, which was the information before spreading, (b) was the physical random sequence, (c) was the spreaded sequence, (d), (e) and (f) were the autocorrelations of (a), (b) and (f). It is easy to find that physical random sequence spreading sequence has the same autocorrelation proerties as the physical random sequence itself not related to the periodicity of the plaintext though the time waveform has significant difference, which proves that physical random sequence can effectively realize the information spreading.

Conclusions

In this manuscript, a setup for information transmission based on physical random sequence spreading method, which is generated by physical random number generator based on room-temperature chaotic oscillations in weakly coupled semiconductor superlattices, is demonstrated. The spreading processing and auto-correlationg theories are similar to the pseudo random sequence. Testing results proved the physical random sequence spreading sequence has the same autocorrelation proerties as the physical random sequence itself not related to the periodicity of the plaintext though the time waveform has significant difference, which proves that physical random sequence can effectively realize the information spreading.

References

[1] M. K. Simon, J. K. Omura, R. A. Scholtz, et al., Spread Spectrum Communications Handbook, Beijing: Post & Telecom Press, 2002.

[2] G. Xao, C. Liang, Y. Wang, Pseudorandom Sequences and Applications, Beijing: National Defence Industry Press, 1985: 167-183.

[3] M. Stipcevic and R. Ursin, An On-Demand Optical Quantum Random Number Generator with In-Future Action and Ultra-Fast Response, Scientific reports, 5:1-8, 2014.

[4] A. Figotin, A random number generator based on spontaneous alpha-decay, PCT patent application WO0038037A1.

[5] M. Stipcevic and B. Medved Rogina, Quantum random number generator based on photonic emission in semiconductors, Rev. Sci. Instrum. 78, 045104:1–7 (2007).

[6] J. G.Rarity, P. C. M. Owens and P. R. Tapster, Quantum random-number generator and key sharing, J. Mod. Opt. 41, 2435–2444 (1994).

[7] A. Stefanov, N. Gisin, O. Guinnard, et al., Optical quantum random number generator, J. Mod. Opt. 47, 595–598 (2000).

[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] J. J. Spiler and D. T. Magill, The Delay-Lock Discriminator-An optimum Tracking Device, Proc. IRE, 49(9):1403~1416 (1961).

[10] H. Du, Q. Ding and Z. Yang, The Research of Code Synchronization of Spread Spectrum Communication System based on FPGA, Second International Conference on Innovations in Bio-inspired Computing and Applications, 171-174 (2011).

[11] E. Klein, Stable isochronal synchronization of mutually coupled chaotic lasers, Physical Review E 73, 066214 (2006).

[12] A. Englert, Zero lag synchronization of chaotic systems with time delayed couplings, Physical Review Letters 104, 114102 (2010).