Journal of ELECTRICAL ENGINEERING, VOL. 64, NO. 4, 2013, 230–237

RANDOM BINARY SEQUENCES IN TELECOMMUNICATIONS

Slavko Šajić * — **Nebojša Maletić** *
Branislav M. Todorović ** — **Milan Šunjevarić** **

Realization of modern telecommunication systems is inconceivable without use of different binary sequences. In this paper, an overview of random binary sequences used in different telecommunication systems is given. Basic principles of pseudo-random, chaotic, and true random sequence generation are presented, as well as their application in telecommunications in respect to advantages and drawbacks of the same. Moreover, particular scheme for true random binary sequence generation is given, as well as results of randomness assessment obtained by NIST statistical test suite. Finally, short insight into importance of random binary sequence in secure communications is given.

K e y w o r d s: binary sequences, pseudo-random sequences, chaotic sequences, true random sequence, secure communication, cryptography, quantum cryptography

1 INTRODUCTION

Random binary sequences are widely used in the field of secure communications [1, 2]. There are three different types of random generators used: pseudo-random, chaotic, and true random binary sequence generators.

A pseudo-random binary sequence generator (PRBSG) generates sequences of binary symbols with properties that are approximately close to random [3, 4]. Some of them are realized by using shift registers [3], while the others are algorithmic based [5, 6]. Pseudo-random binary sequence is completely determined by a relatively small set of initial states and feedback network or recursive relation. Since pseudo-random binary sequences exhibit a behavior that relies on a finite number of states and transitions between those states, they cannot produce true random outputs as they are finite state mechanisms. Pseudo-random sequence is deterministic and after N elements it starts to repeat itself, where N denotes the period of the pseudo-random sequence. Pseudo-random binary sequences are important in practice for simulations. Also, they are widely used in spread spectrum communications [2] as well as in cryptographic applications [7].

An important class of random sequences is, so called, class of chaotic sequences [8–12]. Although there is no universally accepted mathematical definition of chaos, a commonly used one for chaotic sequence says that it is random-like deterministic sequence which is generated sequentially by using a mapping function $X_{n+1} = f(X_n)$ and an initial value X_0, but whose distribution looks like white noise [13]. This sequence has merit that knowing only two information, namely: a mapping function and an initial value, the same sequence can be regenerated. These sequences are also widely used in spread spectrum communications and cryptography [13–16].

Although some PRBSGs produce sequences which pass all statistical pattern tests for randomness, they cannot be claimed as true random binary sequence generators (TRBSGs) [17].

In the field of cryptographic applications, the need for true random binary numbers arises as modern communication systems increasingly employ electronic transactions and digital signature application for authenticity. It is of high importance to secure privacy during these operations. That was the reason for developing true random binary sequence generator, which should indicate high unpredictability for usage in encryption for digital communications. A true random binary sequence generator is a hot topic in the last years [18–24].

It is a postulate that true random numbers cannot be generated mathematically. Hence, computer algorithms cannot be used for that. The generation of true random binary sequences based on non-deterministic physical mechanisms is of paramount importance for cryptography and secure communications. We refer to true random binary sequence generator as random engine built on microscopic phenomena such as thermal noise or other quantum phenomena. These physical processes are theoretically unpredictable in practice. The unpredictability is justified by the chaos theory [8]. This theory suggests that even though microscopic phenomena are deterministic, real-world macroscopic systems evolve in ways that cannot be predicted in practice because one would need to know the initial conditions at microscopic level to an accuracy that grows exponentially over time.

2 PSEUDO–RANDOM BINARY SEQUENCES

Pseudo-random binary sequences (PRBSs) are deterministic sequences and are widely used in signal processing and data transmission. Pseudo-random binary sequence is a periodic sequence of symbols which within its period has features similar to random. They are often used in secure communications systems, such as spread

* Faculty of Electrical Engineering, University of Banja Luka, Patre 5, 78000 Banja Luka, Bosnia-Herzegovina, sajic@etfbl.net, nebojsa.maletic@etfbl.net ** RT-RK d.o.o, Institute for Computer Based Systems, Narodnog Fronta 23A, 21000 Novi Sad, Serbia, branislav.todorovic@rt-rk.com, micosun@eunet.rs

DOI: 10.2478/jee-2013-0033, Print ISSN 1335-3632, On-line ISSN 1339-309X,

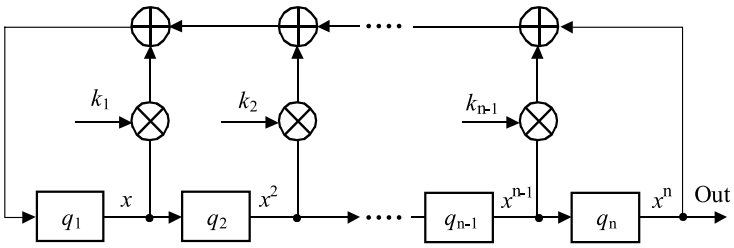

Fig. 1. Linear pseudo-random sequence generator

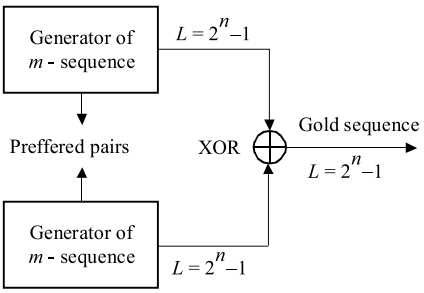

Fig. 2. Gold sequence generator

spectrum systems which were developed for military communications [2]. Nowadays they are widely used for many commercial applications such as cellular mobile radio, indoor communications, and satellite communications.

In general, there are two types of pseudo-random sequences: linear and nonlinear. Both of them can be implemented either in digital hardware or by computer software. Digital hardware consists of two parts: a shift register consisting of n stages and a feedback function. If a feedback function is realized by using only XOR operations (modulo-2 adders), as is shown in Fig. 1, generated pseudo-random sequence is said to be linear.

Linear pseudo-random sequence generator is represented by n-degree polynomial with coefficients and variable defined on GF(2) as follows [5]

$$f(x) = 1 \oplus k_1 x \oplus \cdots \oplus k_{n-1} x^{n-1} \oplus x^n \,. \qquad (1)$$

One can see that degree of the polynomial is equal to the length of the shift register n. Maximal length of the linear PRBS is equal to $N = 2^n - 1$ and its period is $T = N\,Tb$, where the binary symbol duration is denoted with Tb. These sequences are known as m-sequences. In order for a particular linear PRBS to be a maximal length PRBS, the polynomial must be a primitive polynomial mod 2. Any linear PRBS of maximal length N can be reconstructed after examining only $2n$ successive binary symbols of the stream by using Berlekamp-Massey algorithm [25]. Hence, linear PRBS of maximal length (m-sequence) should not be used for cryptographic applications. Nevertheless, due to their good autocorrelation properties, m-sequences are suitable for use in spread spectrum systems synchronization, for radio-location, in synchronous CDMA (Code Division Multiple Access) systems (these systems can use only one m-sequence and its cyclic shifts), in systems with large delay spreads in multipath channels, and for communication channel testing. However, m-sequences of the equal length have poor cross-correlation properties. Asynchronous CDMA systems require different sequences with low value of cross-correlation in order to minimize multiple-access interference (MAI). Surely, small-limited set of m-sequences with low value of cross-correlation function can be found. However, the size of set is usually insufficient for use in CDMA applications. This led to other sequences with better cross-correlation properties, such as Gold, Kasami, Walsh-Hadamard, JPL (Jet Propulsion Laboratory) sequences, *etc.*

Gold sequences represent an important class of sequences that allow construction of long sequences with three valued autocorrelation function [26]. They have better cross-correlation properties than the m-sequences. For their generation a preferred pair of m-sequences is used. Preferred pairs are obtained by minimizing the side lobes of the cross-correlation function of m-sequences. A method for acquiring Gold sequences is shown in Fig. 2.

Total number of these sequences in a set is 2^n+1. This set is made of two m-sequences, while others, 2^n-1, are made on different initial states of LFSR (Linear Feedback Shift Register). The greatest side lobe in autocorrelation function of a Gold sequence or in cross-correlation of any two Gold sequences is $2^{(n+2)/2}+1$ for even n and $2^{(n+1)/2}+1$ for odd n.

Good correlation properties make them suitable for broader application in communications, such as asynchronous CDMA, satellite communication (GPS), *etc.* In these systems, synchronization is possible based on the autocorrelation property of the Gold sequence [27].

Kasami code sequences [28] are derived from m-sequences in similar manner as the Gold sequences. They are divided in two classes: the small and the large Kasami set. The small Kasami set has the family size of $2^{n/2}$ sequences, each with a period of $2^n - 1$, for n even. The autocorrelation and cross-correlation functions of these sequences take on values from the set $\{-1\,,\, -(2^{n/2}+1)\,,\, 2^{n/2}-1\}$. The maximum value of absolute cross-correlation for any pair of sequences from the small set is $2^{n/2}+1$. The large Kasami set contains both the set of Gold sequences and the small set of Kasami sequences as its subsets. The maximum value of absolute cross-correlation for any pair of sequences from the large set is $2^{(n+2)/2}$ [29]. The autocorrelation and cross-correlation properties of the large set are inferior to those of the small set, but the large Kasami set has larger

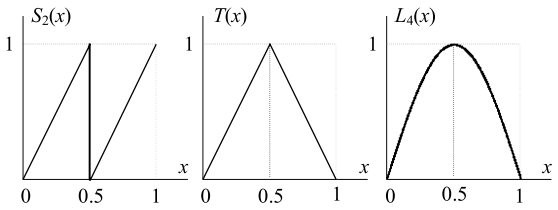

Fig. 3. Primer of one-dimensional mapping functions

number of sequences. Kasami code sequences are used in asynchronous CDMA, 3G wireless schemes [30]. Although the small Kasami set has low peak cross-correlation function which is important for MAI reduction, the relatively small family size limits its wide applications as signature codes in CDMA systems [31].

The JPL (Jet Propulsion Laboratory) ranging codes are constructed by moduo-2 addition of two or more m-sequences whose lengths are relatively prime to one another. Length of the resulting JPL code sequence is equal to the product of the lengths of the composite code sequences. There are several advantages to such a technique: (a) very long codes used for unambiguous ranging over long ranges are available; (b) these long codes are generated by a relatively small number of shift register stages; and (c) synchronization of receiver can be accomplished by separate operations on the component codes [32]. The JPL ranging code sequences have $2P$ autocorrelation values, where P is the number of component code sequences. Synchronization is accomplished by sequentially synchronizing the component code sequences. Sequential synchronization requires searching through a maximum of $\sum_{i=1}^{P}\left(2^{n_i}-1\right)$ code chips of the JPL code sequence of length $\prod_{i=1}^{P}\left(2^{n_i}-1\right)$, where $2^{n_i}-1$ is the length of i-th composite code sequence. This greatly reduces the time for the synchronization.

In addition to the above sequences, other special sequences, called Walsh-Hadamard code sequences, are often used. Walsh-Hadamard code sequences are obtained from the Hadamard matrix which is a square matrix where each row in the matrix is orthogonal to all other rows, and each column in the matrix is orthogonal to all other columns. The Hadamard matrix H_N is generated by starting with zero matrix and applying the Hadamard transform successively. Each column or row in the Hadamard matrix corresponds to a Walsh-Hadamard code sequence of length N. Orthogonality between rows codes in the Hadamard matrix is defined such that the cross-correlation values associated with zero offset between the pair of sequences is zero [33]. This implies orthogonality between code sequences which makes them suitable for use in CDMA systems. However, these sequences are not m-sequences so they can be used only in synchronous CDMA systems (multi-carrier CDMA and the cellular CDMA system IS-95).

Further, wideband CDMA (W-CDMA) supports variety of services with different data rates. Here, variable length orthogonal sequences that provide different spreading factor are especially interesting [34]. Method proposed in [34] is based on modified Hadamard matrix.

Nonlinear pseudo-random sequence generator performs AND and/or OR operations in feedback function. Another method uses the output from three linear feedback systems as an address to a look-up table. This method combines the three output bits to produce one bit based on the look-up table. Nonlinear PRBS cannot be recovered by knowing a part of it. It makes them more suitable for use in secure communication and spread spectrum systems.

3 CHAOTIC BINARY SEQUENCES

In recent years, sequences derived from chaotic phenomena are being considered for use in secure communication and for spread spectrum systems. Chaotic sequences are generated from nonlinear dynamic systems. These are unpredictable, deterministic systems, often described by the system of parameterized differential equations (Lorentz system, Chua's oscillator, *etc*). Their essential feature is that they exhibit noisy-like behaviour because of its strong sensitivity to initial conditions. Also, a simple method to obtain chaotic sequences is to use mapping functions. One-dimensional mapping functions, shown in Fig. 3, are often used [9, 11].

Bernoulli's step $S_2(x)$ maps real numbers defined on interval $(0,1)$ into same interval and is defined by

$$x[n+1] = S_2(x[n]) = 2x[n] \mod 1\,,\ n = 0,1,2,3,\ldots \tag{2}$$

and $x[n]$ is defined on $(0, 0.5) \cup (0.5, 1)$.

Tent mapping $T(x)$ is defined on interval $(0,1)$ as

$$T(x) = \begin{cases} 2x\,, & 0 < x < 1/2\,, \\ 2(1-x)\,, & 1/2 < x < 1\,. \end{cases} \tag{3}$$

Logistic map $L_4(x)$ is also defined on interval $(0,1)$ as

$$x[n+1] = r\,x[n](1-x[n])\,, \quad n = 0,1,2,\ldots \tag{4}$$

where r is a constant.

This mapping exhibits chaotic behavior for $r > 3.57$. However, for $r = 4$ logistic mapping becomes self mapping. It maps real numbers, $x[n]$, defined on interval $(0,1)$ to itself. Further, other mapping functions such as Chebyshev map, piecewise-linear (PWL) map, skew-tent map, Henon map, Bernoulli map, and Lozi map can be used.

Depending on initial condition $x[0]$, given mapping functions can generate different real valued arrays on interval $(0,1)$. For generating non-repetitive binary sequences from (2), (3) and (4) a transformation θ_t, which is defined as

$$\theta_t = \begin{cases} 0\,, & x < t\,, \\ 1\,, & x \geq t \end{cases} \tag{5}$$

where t is a threshold value, can be used. Using threshold function, chaotic binary sequence is obtained. These sequences are non-periodic, deterministic generated and

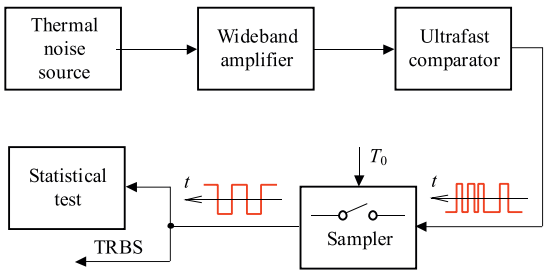

Fig. 4. A block-scheme of true random binary sequence generator

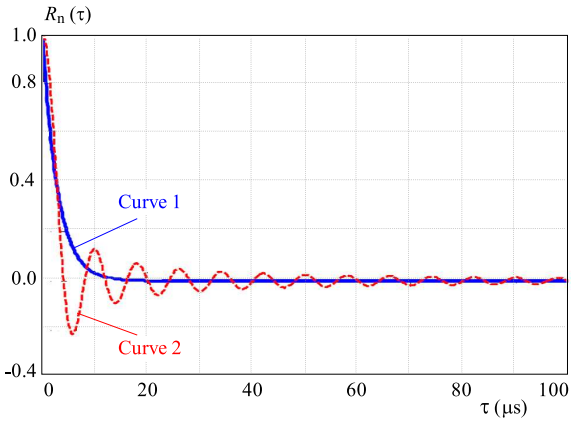

Fig. 5. Autocorrelation functions at the output of comparator (blue – solid) and at the output of the wideband amplifier (red – dashed)

sensitive to initial condition. Since they are managed by one or more parameters, slightly parameter change generates completely new chaotic sequence. Chaotic sequences can offer many advantages such as low probability of interception, security of transmission, resistance to jamming, and robustness in multipath environments [35]. The significant drawback is their sensitivity dependence to initial conditions which gives worse performance of chaotic synchronization schemes at low signal-to-noise ratio (SNR) compared to conventional communication systems.

4 TRUE RANDOM BINARY SEQUENCES

Unlike the pseudo-random and chaotic sequence generators, true random binary sequence generators (TRBSGs) use a non-deterministic source to produce randomness [18–24], [36–39]. Most of them operate by measuring unpredictable natural processes such as thermal noise, atmospheric noise, unstable lasers, nuclear decay, antenna noise, acoustic noise, *etc.* TRBSG generates an infinite sequence of mutually independent binary symbols. When generator is restarted, it never reproduces earlier generated sequence.

Due to its "natural" origin two random sequences cannot be synchronized, so they cannot be used for system synchronization. It is not possible to generate two identical and synchronous random sequences, one on the transmitting side and another on receiving side. Good correlation properties and their unpredictability make them suitable for secure communication. TRBG can be used for security (encryption/decryption) keys generation, to seed pseudo-random or chaotic sequence generator, for purpose of digital signature.

Now, we will first refer to an old literature problem. Assuming that the stationary white Gaussian process with the constant power spectral density $N_0/2$ in frequency range $-\infty < f < \infty$ is low-pass filtered within frequency band $-B < f < B$, at the output continuous-time wide sense stationary Gaussian process with the power spectral density

$$S_N(f) = \begin{cases} \frac{N_0}{2}, & -B < f < B, \\ 0, & \text{elsewhere} \end{cases} \tag{6}$$

is present. Its autocorrelation function is

$$R_N(t) = \frac{N_0 B \sin(2\pi B t)}{2\pi B t}. \tag{7}$$

Based on (7), if the signal at the output of low-pass filter (LPF) is sampled at time instants $t = k/2B$, $k = 1, 2, \ldots$, then the samples are mutually uncorrelated. Using the samples binary sequence can be produced. Further, in [38] it was shown that the per-sample joint entropy of binary sequence equals 1 when sampling is done in the zeros of autocorrelation function. Since the above method is hard to implement in practice due to non-ideal transfer function of LPF another method can be used.

A method for true random binary sequence generation using a thermal noise source is given in Fig. 4.

By its nature, thermal noise is random process with zero mean and Gaussian distribution of amplitudes. Generated noise is amplified by wideband amplifier. Since the thermal noise has a relatively uniform spectral power density over wide frequency range (up to 10^{11} Hz), it is desirable that amplifier's bandwidth be as large as possible. Amplified noise excites an ultrafast comparator with decision threshold equals to zero. At the output of comparator binary sequence of random binary symbol duration is obtained.

Autocorrelation function of binary signal at the output of ultrafast comparator is

$$R(\tau) = A^2 e^{-2c|\tau|}, \tag{8}$$

where A denotes signal amplitude and c is the average number of passes through zero [36] (intersections with time axis) per sec. Figure 5 shows autocorrelation functions according to the scheme depicted in Fig. 4 and expressions (7) and (8).

In the proposed model, c depends on the bandwidth of wideband amplifier and the speed of comparator. Furthermore, autocorrelation function which is decreasing by exponential law tends to zero with τ increasing. This means that the random process with autocorrelation function

Table 1. Results of sequences testing by NIST tests

Test No.	Test name	$T_0 = 5\,\mu$s		$T_0 = 10\,\mu$s		$T_0 = 20\,\mu$s		$T_0 = 200\,\mu$s	
		P value	Random	P value	Random	P value	Random	P value	Random
1	Frequency	0.888	Yes	0.262	Yes	0.829	Yes	0.928	Yes
2	Frequency Block	1.000	Yes	0.945	Yes	0.684	Yes	0.822	Yes
3	Runs	0.000	No	0.000	No	0.634	Yes	0.593	Yes
4	Longest Runs of Ones	0.000	No	0.029	Yes	0.445	Yes	0.900	Yes
5	Rank	0.470	Yes	0.164	Yes	0.274	Yes	0.867	Yes
6	DFT	0.000	No	0.486	Yes	0.927	Yes	0.340	Yes
7	NonOverlappingTemplateMatching	–	No	–	No	–	Yes	–	Yes
8	Overlapping Template Matching	0.000	No	0.000	No	0.616	Yes	0.924	Yes
9	Universal	0.000	No	0.639	Yes	0.249	Yes	0.730	Yes
10	Linear Complexity	0.986	Yes	0.831	Yes	0.963	Yes	0.690	Yes
11	Serial	0.000 0.000	No	0.000 0.061	No	0.341 0.353	Yes	0.963 0.974	Yes
12	Approximate Entropy	0.000	No	0.000	No	0.391	Yes	0.724	Yes
13	Cumulative Sums	0.993	Yes	0.505	Yes	0.866	Yes	0.929	Yes
14	Random Excursions	–	No	–	No	–	Yes	–	Yes
15	Random Excursions Variant	–	Yes	–	No	–	Yes	–	Yes

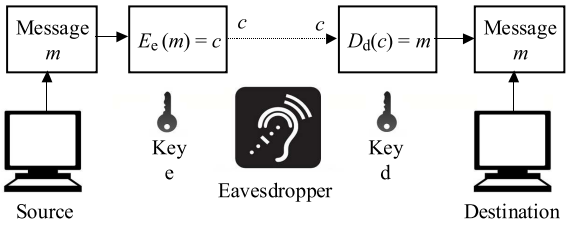

Fig. 6. Cryptosystem generic block-scheme

given by (8) has no periodic spectral components. If binary signal at the output of comparator is sampled every T_0 sec, where $R(\tau = \tau_0) \cong 0$, true random binary sequence with binary symbol duration of T_0 is generated. For example, if the number of intersections with time axis is $c = 10^7$, signal amplitude is $A = 1$ and sampling period is $T_0 = 1\,\mu$s, the value of autocorrelation function at $\tau = T_0$ is $R(\tau = T_0) = 2\times10^{-9}$. Thus, assumption of mutually uncorrelated samples is justified. Hence, generated binary signal can serve as entropic source.

The proposed scheme can be used to generate true random binary sequences of high bit rates, depending on the speed of electronic circuits that process thermal noise. In applications where the rate of sequence generation is not crucial, proposed generator scheme can use frequency limited noise sources instead of thermal noise source. In this case, wideband amplifier and ultrafast comparator are not required. Band-limited noise sources occur in many electronic devices; hence, such configuration of TRBSG is very suitable for practical implementation. Especially convenient are narrowband radio channels where signal at receiver's output, in the absence of RF signal at receiver's input, provides band-limited noise source which can be used for true random binary sequence generation. Convenience of this generator is the result of the fact that it does not require additional mapping (digital post-processing) to improve certain statistical properties [40]. In order to asses that binary sequence generated from pseudo-random, chaotic or true random generator is cryptographically secure, it should be subjected to a variety of statistical tests to conclude weather the sequence is showing some specific characteristics that the truly random binary sequence would show. There are several statistical test suits available for assessing the randomness. The most popular ones are: NIST statistical test suite [41], the DIEHARD statistical test suite [42], the Crypt-XS suite of statistical tests [43], and the Donald Knuth statistical tests set [44]. The result of NIST tests randomness assessment of the binary sequence derived from the scheme depicted in Fig. 4 is shown in Table 1.

Four different sampling rates are used, and for each, results of testing the randomness are shown. For each test corresponding probability value (P value) is calculated. It is the probability that the perfect random generator would produce the sequence less random than the sequence that was tested for the kind of non-randomness assessed by the test. Significance level of 0.01 was used. This means that 1 out of 100 tested sequences would be rejected. For some tests P values are not given (–) because these tests calculate more than one P value.

5 BINARY SEQUENCE IN INFORMATION SECURITY

With the frequent electronic data exchange information security is becoming an important and indispensable element in data transmission and storage. Security is especially important and crucial in modern communication systems that use public networks (*eg* Internet) for transmission of confidential data (e-commerce, e-banking) and encryption is one way to ensure the necessary security. The old and the basic problem of cryptography is secure data transmission over insecure channel. This entails several problems such as encryption, authentication and

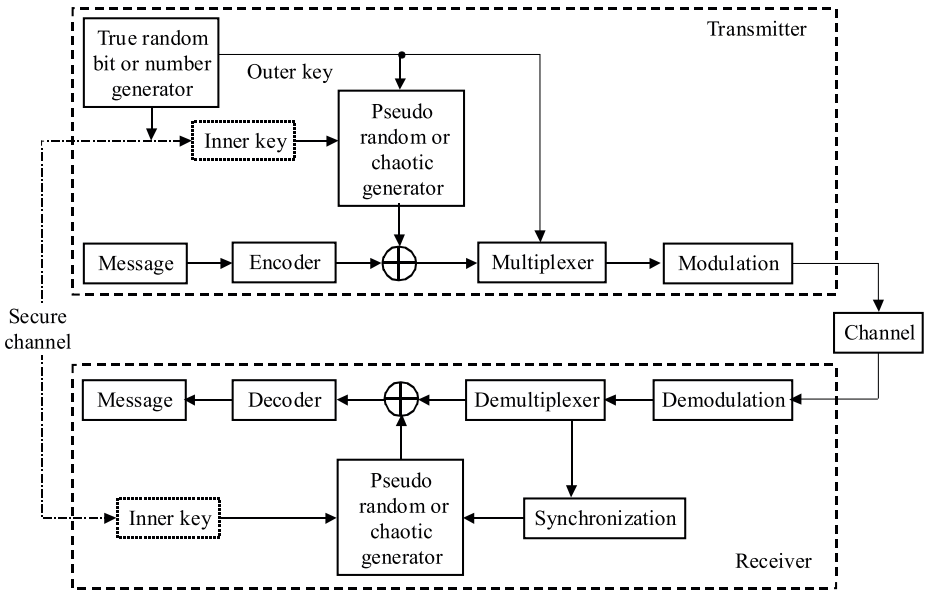

Fig. 7. Block scheme of typical communication system that uses binary sequence for information encoding

key exchange. The basic block-scheme of cryptosystem is given in Fig. 6.

Source emits message m, and applying encryption key e generates cryptogram (encrypted message) c which transmits through the insecure channel. At the receipt place original message is generated after applying decryption key d on received cryptogram c. Then message is delivered to the user. When it comes to security in public networks essential notions are secrecy and authenticity. The secrecy protects decryption method and assumes that the message cannot be determined from the cryptogram. The authenticity protects encryption method and assumes that false cryptogram cannot be inserted instead of the real one without two sides in communication not being aware of it. Cryptosystems can be divided into symmetrical and asymmetrical. In symmetrical cryptosystems (systems with one key) keys for encryption and decryption methods are identical, $e = d$, or one key can be easily determined from the other one *ie* encryption and decryption methods can be easily determined one from another. Both methods must be kept secret to ensure the secrecy and the authenticity. An example of such system is DES (Data Encryption Standard) [26]. In asymmetric cryptosystem there are two keys e and d, $e \neq d$, and encryption and decryption process differ. This means that one key can be revealed, and the other remains unknown. The known key is called the public key and is used for the encryption. The key used for decryption is the secret key and is known only by the user. These systems are also known as public key system [45]. There are several algorithms that use public key system, but only a few of them are safe and practical, from which three are used for encryption and digital signature: RSA, ElGamal, and Rabin [46]. By careful choice of encryption method and key, cryptosystem can be made practically safe. This means that although an attacker could theoretically decrypt the message, it is unlikely to succeed because of processing power and time needed for this are beyond the capabilities of the attacker.

The lack of classical crypto-system is that secure communication is only possible after key exchange. Even though the key is transmitted over secure channel there is no way to know whether the key is sent securely *ie* weather a potential eavesdropper managed to get the key. Quantum cryptography is one way to overcome this issue [1].

Quantum cryptography uses the uncertainty of the quantum world. Using it one can set up the channel that cannot be eavesdropped (interfered) without two sides in communication not being aware of it. The eavesdropper cannot copy unknown quantum state due to no-cloning theorem [47], [48]. Quantum cryptography is used to obtain and distribute keys, but no for data transmission. Quantum communication implies encoding the information in quantum states (qubits) and then using a quantum superposition and quantum interpenetration and sending qubits, secure communication system can be set up. As a medium for transmission optical fiber or radio is used. Several systems that use quantum communication are currently implemented. The main problem of those systems is short length of the quantum channel [48, 49].

At the end, typical block scheme of communication system that uses binary sequences for information encoding and decoding is shown in Fig. 7.

There are two identical binary sequence (pseudo-random or chaotic) generators at transmitter and receiver side. Initial state of the generator defines outer (public) and inner (secret) key, which is random generated. Outer (public) key transfer is done through information channel which is subject to interception. Message signal is masked with the sequence of bits generated at transmitting pseudo-random or chaotic generator. First

transmitting packet contains synchronization bits and outer (public) key. Next packets contain encrypted information. Then packets are modulated and transmitted through communication channel (wired, wireless). At receiver side the demodulation is done and the first packet with synchronization bits and outer (public) key is obtained. Based on outer (public) and inner (secret) keys estimate of the initial state of the pseudo-random or chaotic generator used at transmitter side is done. Starting generator with properly estimated initial state allows reproduction of binary sequence copy from transmitter. Reverse process is done at receiver in order to obtain original message. Inner (secret) key is only known to transmitter and receiver and distribution is done through the special channel.

6 CONCLUSION

In this paper pseudo-random, chaotic and true-random binary sequences used in telecommunications are analyzed. Pseudo-random sequences are simple to generate, relatively easy to synchronize and can be mathematically described. Even though they are easily to intercept in comparison to chaotic sequences, they are still predominately used in today's communication systems.

Chaotic sequences relative to pseudo-random sequences have certain benefits such as greater resistance to interception, small probability of interception, and greater transmission security. Thus, use of chaotic sequences in communication systems became interesting research topic [1–4]. However, the lack of chaotic sequence application is its sensitivity to initial condition which in channel with low SNR gives poorly results in synchronization in classic communication systems. Furthermore, in hardware implementation map generators need high precision mixers. That is much more complicated than conventional pseudo-random generators with shift registers. Even though, chaotic sequences are still very interesting topic to research.

Information security is need in modern communication systems. Confidential data exchange (e-commerce, e- banking) place high demand on secure communication. Thus, true random binary sequences are prerequisite for achieving secure communication. Using random sequences as security keys raises security on much higher level. Reliable distribution of encryption and decryption keys is not an easy task, even in situation when the key is sent through secure channel. This issue can be resolved by using quantum cryptography. It can be used for key distribution and generation. Quantum channel cannot be eavesdropped without two sides in communication not being aware of it.

Acknowledgements

The third and the fourth author were supported by the Ministry of Education and Science of the Republic of Serbia under Grant TR-32030.

References

[1] van TILBORG, H. C. A.—JAJODIA, S. (Eds.): Encyclopedia of Cryptography and Security, Springer, 2011.

[2] TORRIERI, D.: Principles of Spread-Spectrum Communication Systems, Springer, 2005.

[3] GOLOMB, S. W.: Shift Register Sequences, Holden-Day Inc., San Francisco, 1967.

[4] SARVATE, D. V.—PURSLEY, M. B.: Crosscorrelation Properties of Pseudorandom and Related Sequences, Proc. of the IEEE **68** No. 5 (May 1980), 593–619.

[5] TAUSWORTHE, R. C.: Random Numbers Generated by Linear Recurrence Modulo Two, Mathematics of Computation **19** (1965), 201–209.

[6] LEWIS, T. G.—PAYNE, W. H.: Generalized Feedback Shift Register Pseudorandom Number Algorithm, Journal of the ACM **20** (1973), 456–468.

[7] LUBY, M.: Pseudorandomness and Cryptographic Applications, Princeton University Press, 1996.

[8] BLACKLEDGE, J.: Cryptology, Fractals and Chaos, Woodhead Publishing, 2011.

[9] KOHDA, T.—TSUNEDA, A.: Pseudonoise Sequences by Chaotic Nonlinear Maps and their Correlation Properties, IEICE Trans. Commun. **E76-B** No. 8 (1993), 855–862.

[10] KOHDA, T.—TSUNEDA, A.: Statistics of Chaotic Binary Sequences, IEEE Trans. Inform. Theory **43** No. 1 (1997), 104–112.

[11] SANG, T.—WANG, R.—YAN, Y.: Constructing Chaotic Discrete Sequences for Digital Communications based on Correlation Analysis, IEEE Trans. Signal Processing **48** No. 9 (2000), 2557–2565.

[12] SETTI, G.—MAZZINI, G.—ROVATTI, R.—CALLEGARI, S.: Statistical Modeling of Discrete-Time Chaotic Processes-Basic Finite-Dimensional Tools and Applications, Proc. IEEE **90** No. 5 (2002), 662–690.

[13] HEIDARI-BATENI, G.—McGILLEM, C. D.: Chaotic Sequences for Spread Spectrum: An Alternative to PN-Sequences, Proc. IEEE Int. Conf. on Selected Topics in Wireless Communications (ICWC 92), Vancouver (Canada), 1992, pp. 437–440.

[14] HEIDARI-BATENI, G.—McGILLEM, D.: A Chaotic Direct-Sequence Spread-Spectrum Communication System, IEEE Trans. Commun. **42** No. 2/3/4 (1994), 1524–1527.

[15] MAZZINI, G.—ROVATTI, R.—SETTI, G.: Interference Minimization by Autocorrelation Shaping in Asynchronous DS-CDMA Systems: Chaos-based Spreading is Nearly Optimal, Electronics Letters **35** (1999), 1054–1055.

[16] PARLITZ, U.—ERGEZINGER, S.: Robust Communication based on Chaotic Spreading Sequences, Phys. Lett. A **188** (1994), 146–150.

[17] HORAN, D.—GUINEE, R. A.: A Novel Stream Cipher for Cryptographic Applications, Proc. of IEEE. Military Communications Conference (IEEE MILCOM 06), Washington DC, 2006, pp. 1–5.

[18] BLASZCZYK, M.—GUINEE, R. A.: A novel Modelled True Random Binary Number Generator for Key Stream Generation in Cryptographic Applications, Proc. of IEEE. Military Communications Conference (IEEE MILCOM 08),, San Diego, California, 2008, pp. 1–7.

[19] BARDIS, N. G.—MARKOVSKYI, A. P.—DOUKAS, N.—KARADIMAS, N. V.: True Random Number Generation based on Environmental Noise Measurements for Military Applications, Proc. of the 8th WSEAS International Conference on Signal Processing, Robotics and Automation (ISPRA 09), Cambridge, UK, 2009, pp. 68–73.

[20] KANTER, I.—AVIAD, Y.—REIDLER, I.—COHEN, E.—ROSENBLUH, M.: An Optical Ultrafast Random Bit Generator, Nature Photonics **4** No. 1 (2010), 58–61.

[21] YALCIN, M. E.—SUYKENS, J. A. K.—VandeWALLE, J.: True Random Bit Generation from a Double-Scroll Attractor, IEEE Transactions on Circuits and Systems I: Regular Papers **51** No. 7 (2004), 1395–1404.

[22] WILLIAMS, C. R. S.—SALEVAN, J. C.—LI, X.—ROY, R.—MURPHY, T. E.: Fast Physical Random Number Generator using Amplified Spontaneous Emission, Optics Express **18** No. 23 (2010), 23584.

[23] LI, P.—WANG, Y. C.—ZHANG, J. Z.: All-Optical Fast Random Number Generator, Optics Express **18** No. 19 (2010), 20360.

[24] LIU, Z.—PENG, D.: True Random Number Generator in RFID Systems Against Traceability, Proc. of IEEE Consumer Communications and Networking Conference (CCNC 06), Las Vegas, Nevada, 2006, pp. 620–624.

[25] MASSEY, J. L.: Shift-Register Synthesis and BCH Decoding, IEEE Trans. Inform. Theory **15** No. 1 (Jan 1969), 122–127.

[26] GOLD, R.: Optimal Binary Sequences for Spread Spectrum Multiplexing, IEEE Trans. Inform. Theory **IT-13** (1967), 619–621.

[27] GOLD, R.: Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions, IEEE Trans. Inform. Theory **IT-14** (1968), 154–156.

[28] KASAMI, T.: Weight Distribution Formula for some Class of Cyclic Codes, Tech. Report No. R-285, Univ. of Illinois, 1966.

[29] DINAN, E. H.—JABBARI, B.: Spreading Codes for Direct Sequence CDMA and Wideband CDMA Cellular Networks, IEEE Commun. Mag. **36** No. 9 (1998), 48–54.

[30] GLISIC, S.—VUCETIC, B.: Spread Spectrum CDMA Systems for Wireless Communications, Artech House, Inc., Boston, 1997.

[31] GUIZANI, M.: Wireless Communication Systems and Networks, Kluwer Academic Publishers, Boston, 2004.

[32] DIXON, R. C.: Spread Spectrum Systems with Commercial Applications, John Wiley & Sons, Boston, 1994.

[33] ABU-RGHEFF, M. A.: Introduction to CDMA Wireless Communications, 1st ed, Elsevier, 2007.

[34] ADACHI, F.—SAWAHASHI, M.—OKAWA, O.: Three-Structured Generation of Orthogonal Spreading Codes with Different Length for Forward Link of DS-CDMA Mobile Radio, Electronic Letters **33** No. 1 (1997), 27–28.

[35] KADDOUM, G.—CHARGÉ, P.—ROVIRAS, D.: A Generalized Methodology for Bit-Error-Rate Prediction in Correlation-Based Communication Schemes using Chaos, IEEE Communications Letters **13** No. 8 (Aug 2009).

[36] MURRY, H. F.: A General Approach for Generating Natural Random Variables, IEEE Transactions on Computers (Dec 1970), 1210–1213.

[37] BUCCI, M.—GERMANI, L.—LUZZI, R.—TRIFILETTI, A.—VARANOUOVO, M.: A High-Speed Oscillator-based Truly Random Number Source for Cryptographic Applications on a Smart Card IC, IEEE Transactions on Computers **52** (Apr 2003), 403–409.

[38] GOV, N. C.—MIHCAK, F. K—ERGUN, S.: True Random Number Generation via Sampling From Flat Band-limited Gaussian Processes, IEEE Transactions on Circuits and Systems-I: Regular Papers **58** No. 6 (June 2011).

[39] YALCIN, M. E.—SUYKENS, J. K.—VANDEWALLE, J.: True Random Bit Generation from a Double Scroll Attractor, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications **51** (July 2004), 1395–1404.

[40] ŠAJIĆ, S.—TODOROVIĆ, B. M.—MALETIĆ, N.: True Random Binary Sequence Generator for Secure Communications, in Proc of 10th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS'11), vol. 2, Niš, Oct 2011, pp. 723–726.

[41] RUKHIN, A.*et al*: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, National Institute of Standards and Technology (NIST), Special Publication 800-22, Revision 1a, April 2010.

[42] MARSAGLIA, G.: Diehard: a Battery of Tests of Randomness http://stat.fsu.edu/geo/diehard.html, 1996.

[43] GUSTAFSON, H. *et al*: A Computer Package for Measuring Strength of Encryption Algorithms, Journal of Computers & Security **13** No. 8 (1994), 687–697.

[44] KNUTH, D.: The Art of Computer Programming, Seminumerical Algorithms, Vol. 2, 3rd edition, Addison Wesley, Reading, Massachusetts, 1998.

[45] STINSON, D. R.: Cryptography — Theory and Practice, CRC Press, Boca Raton, 1995.

[46] DIFFIE, W.—HELLMAN, M. E.: New Directions in Cryptography, IEEE Trans. Inform. Theory **IT-22** (1976), 644–654.

[47] MENEZES, A.—van OORSCHOT, P.—VANSTONE, S.: Handbook of Applied Cryptography, CRC Press, 1997.

[48] BENNETT, C. H.—BRASSARD, G.: Quantum Cryptography: Public Key Distribution and Coin Tossing, proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179.

[49] HRG, D.—BUDIN, L.—GOLUB, M.: Quantum Cryptography and Security of Information Systems, Proceedings of the 15th International Conference on Information and Intelligent Systems, IIS2004, Varaždin, Croatia, 2004.

Received 12 March 2012

Slavko Šajić, born in 1961, received DiplEng and MSc degree in Electronics and Telecommunications from the Faculty of Electrical Engineering, University of Banja Luka, in 1983 and 2007, respectively. Prior to joining the Faculty of Electrical Engineering, he was with ČAJAVEC-Telekomunikacije i Elektronika, Banja Luka. He is currently working as Senior Teaching Assistant at the Faculty of Electrical Engineering, University of Banja Luka, where he is pursuing towards his PhD degree. His areas of interest are in spread spectrum systems, synchronization.

Nebojša Maletić, born in 1986, received BSc and MSc degree from the Faculty of Electrical Engineering, University of Belgrade in 2008 and 2010, respectively. He is a PhD student at the Faculty of Electrical Engineering, University of Belgrade. His areas of interest are in wireless communications, microwave engineering.

Branislav M. Todorović was born in Belgrade, Serbia, in 1959. He received Dipl Eng and MSc degrees from the Faculty of Electrical Engineering, University of Belgrade, and PhD degree from the Faculty of Technical Sciences, University of Novi Sad, in 1983, 1988 and 1997, respectively. He is a Senior Research Fellow at the RT-RK, Institute for Computer Based Systems, and a Full Professor at the Military Academy, University of Defence, Belgrade. Prior to joining RT-RK, he was with the Institute of Microwave Techniques and Electronics IMTEL-Komunikacije, Centre for Multidisciplinary Research, and the Military Technical Institute (VTI, Institute of Electrical Engineering) in Belgrade. His research interests are in the wide area of radio telecommunications and digital signal processing. He has authored or co-authored about 100 peer-reviewed journal and conference papers and three books.

Milan Šunjevarić, born in 1948, received his Dipl Eng, MSc, and PhD degree from the Faculty of Electrical Engineering, University of Zagreb in 1972, 1976 and 1984, respectively. He is currently working as a Senior Research Fellow at the RT-RK, Institute for Computer Based Systems, Novi Sad, and a Visiting Professor at the Faculty of Electrical Engineering, University of Banja Luka. His main areas of interest are in mobile communications systems.