This watermark does not appear in the registered version - http://www.clicktoconvert.com

SOME IMPLEMENTATIONS OF STOCHASTIC PRINCIPLES IN ELECTROMAGNETICS

A. G. Tyzhnenko

Department of Mathematics, Kharkiv National University, 9-A Lenin Ave., Ukraine

e-mail: tyzhnenko@ksue.edu.ua

Abstract

Stochastic comparison of signals in electromagnetic form or in numerical one is addressed. Due to such a comparison, one can identify a stochastic signal with some binary unit of information. That is, each bit of information can be transmitted as a stochastic signal with or without carrier. At a receiver, the identification of bits (1s or 0s) is proposed to do by measuring the correlation coefficient between received signal and two replicas, one of which corresponds to 1s and the other corresponds to 0s. This principle is used in the work for constructing a highly confidential scheme of communication, in which the security problem is solved on combined physical and mathematical level. Besides, stochastic comparison of electromagnetic signals is considered regarding to low-power radars and remote-managing locks.

1. INTRODUCTION

The safe communication problem is centuries old. Nowadays, it exhibits new features caused by impersonal electronic communications. For a gateway to the literature, one can see [1-3], for example. Because of these new features, the safe communication problem can be split into two parts:

- Type I problem – the safe data distribution;
- Type II problem – the computer's hard drive disk protection.

These problems are commonly considering on three levels:

- Mathematical level – encryption;
- Software level – that based on the Net and computer properties;

This watermark does not appear in the registered version - http://www.clicktoconvert.com

- Physical level – that based on physical principles.

To briefly outline the state of the art of safe communication problems, we consider some methods, the most interesting, as to our mind, from the wide variety of existed and potential ones.

The one-time-pad [1, 2, 3] is considering now as the most durable encrypting scheme. It solves the Type I problem. The most serious shortcoming is the key distribution problem, which causes the same security problem as that for data transmission. More than that, the key length must be exactly the same as that of the message that is not convenient. This method works on mathematical level.

The one-time-pad with quantum encrypting [3] is very interesting potential method, which is designing to solve the Type I problem on physical level. When this method will be completed, it seems to be a perfect encrypting method, which can completely solve the Type I problem.

The most widely used in practice encryption method is probably the public-key scheme [3]. It solves the Type I problem on sufficiently high level with the aid of mathematical principles. This method is not perfect, but gives very strong and convenient encryption that is sufficient, in main, for the common workers in the Internet.

One else very interesting encryption scheme based on physical principle, named as chaotic communication [4-7], is nowadays developing. This scheme is designing to perfectly solve the Type I problem. It seems to be the case after solving the synchronization signal safe transmission problem.

To solve both the Type I and Type II problems on software level the firewall schemes have been designed [1]. As any software scheme, a firewall does not provide perfect security. However, it can solve the safe communication problem on a high level sufficient for common using in the Net.

Summing, we can note that the safe communication problem is solved to date on some practically sufficient level for common utilization in the Net. What is remained unsolvable is totally safe communication problem needed for special cases. We propose in this work a new scheme that solves this problem on a combined physical and mathematical level. Totally secure communication may be obtained at the

This watermark does not appear in the registered version - http://www.clicktoconvert.com

expense of bit rate decreasing in the data exchange process. In the core of the method proposed lies a physical principle according to which a would-be eavesdropper or intruder has limited opportunity for bit identification compared to that at a receiver. Such identification level for an eavesdropper can be diminished intentionally to that one for which decrypting is impossible regardless of a computer system used for these purposes.

2. BITS CAMOUFLAGING AND IDENTIFICATION PROBLEMS

In the case of binary encoded information, each bit (1 or 0) is associated in our method with some definite information-bearing signal, which consists of the set of equidistant in time samples:

$$x = \{x_i\}_{i=1,N} \tag{1}$$

If amplitude-modulated sinusoidal signal is used for communication,

$$u(t) = x(t)\sin\omega t \tag{2}$$

then the samples,

$$x_i = x(t_i) \tag{3}$$

are local extremum values spaced uniformly in time.

Alternatively, if wideband nonsinusoidals are used as information-bearing signals, x_i is associated with impulse extremal value at the moment t_i. Also, the set $\{t_i\}_{i=1,N}$ is spaced equidistant in time.

Thus, each bit of a message is supposed to be transmitted as the N-length signal of the type (1). Let all 1s are transmitted with the aid of any one but fixed N-length realization of pseudorandom distributed signal,

$$x^{(1)} = \{x_i^{(1)}\}_{i=1,N}; \tag{4}$$

and all 0s - with the aid of any other fixed N-length realization from the same population,

$$x^{(0)} = \{x_i^{(0)}\}_{i=1,N}; \tag{5}$$

As the bit-bearing signals, we use in this work the Gauss normal distributed samples with population mean zero and standard deviation one of the type (4), (5).

This watermark does not appear in the registered version - http://www.clicktoconvert.com

These signals are distributed from transmitter to receiver instead of 1s and 0s. While transmitting, original signals (4), (5) are altered due to presence of noise and boosting, and become as the following:

$$\tilde{x}^{(1)} = a\left(x^{(1)} + z\right) \tag{6}$$

$$\tilde{x}^{(0)} = b\left(x^{(0)} + z\right) \tag{7}$$

Here, $z = \{z_i\}_{i=1,N}$ is any realization of white Gaussian noise. Note that there are different realizations of noise z in (6) and (7) due to randomly affected noise environment. At the same time, the signals (4) and (5) are the same for all 1s and 0s correspondently. The amplitudes a and b may be not equal to one as in (4), (5) due to boosting, for instance. At a receiver, the coming signals (6), (7) are compared with known replicas, which are exactly the same as the original signals (4), (5). As the comparison method, we use the correlation coefficient between two signals, x and y, of the same length:

$$r(x, y) = \int x(t)\, y(t)\, dt \Big/ \sqrt{\int x^2(t)\, dt \int y^2(t)\, dt}$$

Such a comparison method is known as a robust and independent from multiplication of signals by constant value. The last issue is very important in communications because the received and original signals may have different amplitudes, a and b in (6), (7) compared to the ones in (4,5).

That is, the identification of bits at a receiver is done by measuring of correlation coefficients between coming signals and replicas:

$$r_{1\,1} = r\left(x^{(1)}, \tilde{x}^{(1)}\right) \tag{8}$$

$$r_{0\,0} = r\left(x^{(0)}, \tilde{x}^{(0)}\right) \tag{9}$$

$$r_{1\,0} = r\left(x^{(1)}, \tilde{x}^{(0)}\right) \tag{10}$$

$$r_{0\,1} = r\left(x^{(0)}, \tilde{x}^{(1)}\right) \tag{11}$$

The measurements are fulfilled at N equidistant snapshots $\{t_i\}_{i=1,N}$, (3), if we know exactly the beginning moment of the message. Otherwise, we have to measure the correlation coefficients at N equidistant snapshots as well, but in this case, we have to

This watermark does not appear in the registered version - http://www.clicktoconvert.com

do this 10 times, for example, on the interval between samples. Such a discretization is approximately optimal.

It is clear that the coefficients r_1 and r_0 are close to one but the remains are close to zero. To identify the bit 1, we define the threshold $k^{(1)}$ as follows:

$$k^{(1)} = (\bar{r}_1 + \bar{r}_0)/2 \qquad (12)$$

Analogously, to identify the bit 0, we define the threshold $k^{(0)}$ as follows:

$$k^{(0)} = (\bar{r}_0 + \bar{r}_1)/2$$

Here, the quantities $\bar{r}_1, \bar{r}_0, \bar{r}_0, \bar{r}_1$ are the corresponding mean values of coefficients (8)-(11) and can be estimated with the aid of the Monte Carlo experiment for known noise level. Technically, the coefficients (8)-(11) are measured on N-points set $\{t_i\}_{i=1,N}$ for each simulation by snapshot period or by one tenth of this period. If the correlation coefficient, $r(x, x^{(1)})$, measured in real time exceeds the critical value $k^{(1)}$, (12), then the N-length signal $\{x_i\}$ represents the bit 1 on some confidence level that can be estimated theoretically. Analogously, if measured $r(x, x^{(0)})$ exceeds the critical value $k^{(0)}$, then the N-length signal $\{x_i\}$ represents the bit 0 on the same, practically, confidence level.

Worth noting that if we are not warring about security, we can use the above-depicted scheme for noise-protected communication. Table 1 demonstrate the Type I errors, namely the errors of rejecting the true zero hypothesis, H_0: the received signal, which has been verified with the aid of replica (4), really represents bit 1, for some signal to noise ratio (SNR) and bit-bearing signal lengths. The results are the same for both 1s and 0s.

Table 1. Identification errors of 1s or 0s represented by N-length signals in noise environment.

N	SNR	10	5	1	1/5	1/10
10	Type I error	0	$1.5\cdot10^{-4}$	$1.1\cdot10^{-4}$	0.31	0.33
50	Type I error	0	0	$7.2\cdot10^{-4}$	0.08	0.12
100	Type I error	0	0	$1.1\cdot10^{-4}$	$6.5\cdot10^{-3}$	0.07
200	Type I error	0	0	$2.4\cdot10^{-5}$	$4.5\cdot10^{-4}$	$3.5\cdot10^{-3}$
300	Type I error	0	0	$1.2\cdot10^{-8}$	$5.1\cdot10^{-8}$	$1.0\cdot10^{-3}$

This watermark does not appear in the registered version - http://www.clicktoconvert.com

As we can see from this table, to realize the communication in noise environment we have to use more samples in bit-bearing signal. Theoretically, this issue can be realized by increasing both the modulation frequency and the bit-bearing signal length. Worth noting that noise may be caused not only due to fluctuations of medium features, but also due to other signals propagated along the same transmission line. Because of that, increasing in noise protection gives potentially an opportunity to transmit several signals at the same time on the same carrier.

The new scheme of secure communication is based on above considerations. However, with the goal of increasing security level, we enlarge intentionally the SNR to definite level. Then, a cryptanalyst have to compare two signals with noise, namely, $x+z$ and $x+z'$, where z and z' are two different noise realizations. Because of that, the maximum correlation coefficient, which a cryptanalyst can find during scanning the message, is the following:

$$r_{cr} = r(x+z, x+z)$$

On the other hand, a receiver registers significantly larger correlation coefficient

$$r_{rec}^{(0,1)} = r(x^{(0,1)}, x^{(0,1)})$$

because replicas at a receiver do not contain noise. Here, x represents the part of a message used by a cryptanalyst for scanning the message with the goal of finding bits. If $x = x^{(1)}$, for example, then cryptanalysts sees $r_{cr} = r(x^{(1)}+z, x^{(1)}+z)$, but receiver registers $r_{rec}^{(1)} = r(x^{(1)}, x^{(1)})$, and $|r_{cr}| < |r_{rec}^{(1)}|$

This issue is due to presence of artificial noise added to bit-bearing signal transmitted. This one permits to identify bits at a receiver on darn small Type I error level, which depends on both the SNR and bit-bearing signal length. On the other hand, a cryptanalysts can identify bits only on sufficiently high error level. As it will be further shown, namely this physical issue prevents a would-be cryptanalysts from finding bits with fidelity.

However, only this issue cannot prevent completely the bits identification by a cryptanalyst. This is because we cannot add so strong noise to bit-bearing signals that the Type I error of bits identification for an eavesdropper will be large enough to prevent totally such identification. If we will do that, the bit error rate at a receiver will not be sufficiently small. To improve the situation, we use 2*N*-length packet to

This watermark does not appear in the registered version - http://www.clicktoconvert.com

transmit each N-length bit-bearing signal. The N, from each $2N$ randomly distributed samples of each packet, consist of bit-bearing samples, $\{x_i + z_i\}_{i=1N}$, placed randomly among all other samples. Other N samples are white Gaussian noise ones, $\{g_m\}_{m=1N}$. Full packet, which represents a bit, can be then represented mathematically as $\{x_i + z_i\} \cup \{g_m\}$.

The distribution of bit-bearing signal samples, $\{x_i + z_i\}_{i=1N}$, among $2N$ places in the packet is unique and known at transmitter and receiver only. A noise $\{g_m\}$ is much more stronger than that of $\{z_i\}$ in bit-bearing signals. Such camouflaging scheme can be so optimized that it can become totally unbreakable regardless of cryptanalysis method employed and computer possibilities. To prove this, consider the bit identification process at a receiver and compare it to that which can be used by a cryptanalyst. At a receiver, the presence of additional noise $\{g_m\}$ does not change the identification process because receiver knows the bit-bearing samples distribution inside the packet. An eavesdropper, on the other hand, does not know this one. To find bits, he has to investigate the message's structure. However, as is clear from above, this structure is statistically uniform. Indeed, both bit-bearing signals (4), (5) are some fixed realizations from the same normal population. To prevent repeating of these signals in the message, we add to them random realizations of white Gaussian noise with signal to noise ratio about one. Hence, the bit-bearing signals (5), (6) have the same statistical features and non-repeating structures. This one prevents to find bits with the aid of finding the structure repeated. Because of that, the only one method for a cryptanalyst to find bits is the same that uses a receiver while registering bits, viz., the correlation coefficient measuring. To this end, a bit-finder has to take a part of the message as a base M-length signal and scan step by step the rest of the message finding the sharp increasing in the correlation coefficient. Phenomenologically, this is only one way to find bits. However, this way can produce no result if the base signal does not contain some bit-bearing samples. Hence, the length of a base signal, M, must be large enough. If a bit-finder wants to have S bit-bearing samples in the base signal, he should take M at least more than $2S$. Further, we take $M = 2S$ while estimating the complexity of bit-finder's efforts, regarding it will be an underestimation. That is, let us consider that from $2S$ chosen samples, S samples belong to the bit-bearing signal, but an analyst does not know which of them

This watermark does not appear in the registered version - http://www.clicktoconvert.com

specifically. In this case, he has to try various combinations from $2S$ samples by S ones. Such combinations will be C_{2S}^{S}. With each such a combination in hand, an analyst should evaluate the correlation coefficients between the base signal and each 2S-length part of the message while scanning this one step by step using the chosen part as the base. Such steps should be at least 1 0 N. If such a search will be successful, a bit-finder should continue the finding of all other bit-bearing samples. Hence, an approximate number of trials will be of about

$$\nu_{2N}^{S} = 2_{2S}^{S} N\ 0_{2N}^{N} C\ +(C_{2S}^{S} -)$$

Inverse number to the ν_{2N}^{S} estimates approximately a theoretical probability of finding the needed distribution of all N bit-bearing samples in the packet. Realistically, it may happen only if the correlation coefficient between the base signal with the found S bit-bearing samples and corresponding part of the message, let r_S^b, can be significantly distinguished from the background, let r_S^0. Here, there arises the second crucial point, which prevents bits identification with fidelity. Indeed, because of huge amount of trails, ν_{2N}^{S}, in the finding process, the significance level of bits identification must be darn near to zero, in order to identify bits with fidelity by an analyst. However, due to the added noise, $\{g_m\}$, in each packet, the Type I error of bit identification for a cryptanalyst can be maintained on very high level, namely, about of (1-10)%. This issue completely prevents a cryptanalyst from bit identification on some acceptable level. There exists, however, another one potential opportunity for a cryptanalyst to find bits. He can use the whole $2N$-length signal as the base one. Such signal contains both all bit-bearing samples with noise, $\{x_i^{(0,1)}\}$, and strong noise ones, $\{g_m\}$. However, due to existence of strong noise samples $\{g_m\}$, the correlation coefficient between the base and message signals is not distinguished on sufficiently significant level from background correlation in this case. This point is demonstrated further.

It is very important to note that this scenario does not depend on computer possibilities. This issue is, really, a result of following causes:

- The presence of noise in bit-bearing signals;

This watermark does not appear in the registered version - http://www.clicktoconvert.com

- The random distribution of bit-bearing samples among strong noise samples in bit-bearing packets.

This issue depends only on the length N of bit-bearing signals and signal to noise ratio in both the bit-bearing signal and other samples in the packet. Due to the first cause, a receiver's correlation coefficients for bits are significantly larger than those for a cryptanalyst. Due to the second cause, to find bits a cryptanalyst has to try huge number of combination. This one prevents to identify bits with fidelity because the identification error (α) is sufficiently large, and erroneous identification could be realized many times in the finding process.

Regarding to the above, we have to note that the proposed method has supposed unconventional data acquisition scheme in which magnitude of signal samples are measured and represented further as numbers in floating point format. After that, computer analyzes these numbers. Such a scheme prevents from transmitting some illegal bit-represented information inside the computer area. The latter one prevents completely a computer from any intruding. Note that this issue is due to a new data acquisition scheme, which alters the physical principle of communication between two computers.

3. NUMERICAL SIMULATIONS OF THE SAS

Now, we demonstrate some possibilities and merits of the above considered stochastic communication scheme (SAS). At first, we should note that, as known, the correlation coefficients are normally distributed. This one permits to estimate with fidelity the identification error (the Type I error, α) at a receiver and for a would-be cryptanalyst. Because of principle importance of this issue, this point has been justified in our research with the aid of the Kolmogorov-Smirnov criterion.

From the bit-rate point of view, the length of bit-bearing packets should be as shorter as possible. On the other hand, the sorter is the packet the harder is to camouflage bits completely in noise. The compromise can be achieved in each specific case separately. Consider the more or less optimal case when the bit-bearing signal consists of 50 samples ($N = 50$). In this case, it is rational to chose the signal to noise ratio in bit-bearing signal, $SNR = 0.8$, and the signal to noise ratio in the rest part of the bit-bearing packet, $SNRN = 0.2$. To calculate statistical features of

This watermark does not appear in the registered version - http://www.clicktoconvert.com

correlation coefficients measured at a receiver and by an eavesdropper, we use the Monte Carlo experiment on 1000 trials.

Suppose a bit-finder takes a part of the message as a base for scanning the message. Let it contains $S = 25$ samples of the bit-bearing signal. Further, let this part be of $2S$ length that will be really so in average. A bit-finder does not know the distribution of S bit-bearing samples in the taken $2S$-length part of the message. Because of that, he must do C_{2S}^{S} trials in finding theirs distribution choosing each time a new combination of samples (S from $2S$). A bit-finder has to do such procedures step by step at least $20N$ times while comparing the taken base part with all other $2S$-length parts of the message – approximately $2N \cdot C_{2S}^{S}$ measurements. Each measurement has to be compared with the mean background correlation coefficient with the goal of finding outlier, which might represent bit. At a receiver, on the other hand, the distribution of bit-bearing samples is known and it takes only a few measurements to identify bits. The Monte Carlo simulation of bit identification process at a receiver and for a would-be eavesdropper, which has taken an S-length part of the message as a replica, is shown in Figure 1 for $S = 25$ from 50 samples of a bit-bearing packet. Figure 1 a) shows the correlation coefficient of the replica and a bit-bearing signal measured at a receiver (upper set) and the background (lower set), which consists of the measurements of correlation coefficients of this replica with other signals. We can see here a very good separation of bit-identifying correlation coefficients (upper values) and the background coefficients (lower values). Figure 1 b) shows the correlation coefficients measured by a bit-finder, which takes a large part of the message that contains supposedly all samples of bit-bearing signal. We can see here that in this case the measured correlation coefficient (solid black curve) is buried in the background noise.

This watermark does not appear in the registered version - http://www.clicktoconvert.com

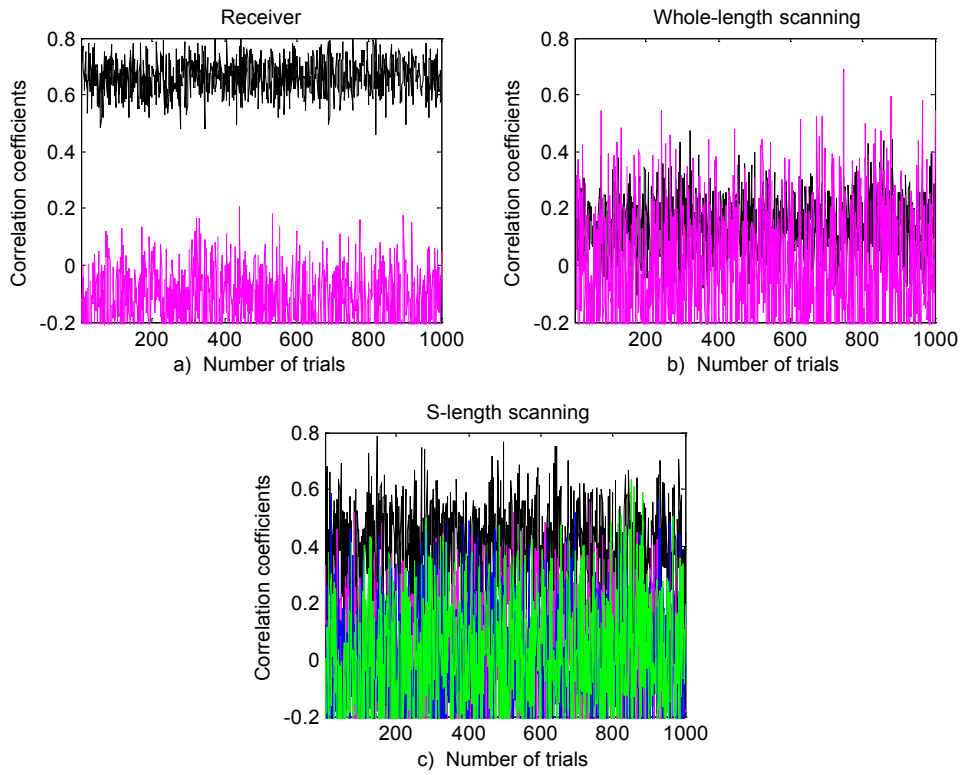

Figure 1. Monte Carlo experiment on 1000 trials for $N = 50$, $SNR = 0.8$, $SNRN = 0.2$, and $S = 25$. a) The correlation coefficient of the replica and a bit-bearing signal measured at a receiver (upper set) and the background (lower set), which consists of the measurements of correlation coefficients of this replica with other signals. b) The correlation coefficient of a large part of the message taken by a bit-finder as a replica and other parts of the message. c) The correlation coefficient of an S-length part of the message taken by a bit-finder as a replica and other S-length parts of the message.

Figure 1 c) shows the most important case when a bit-finder takes smaller part of the message, let it be of S-length. With this part in hand, he scans the rest of the message with the goal of finding bits. Obviously, he wants to use the least possible length of such a part to find bits because the number of trials is proportional to C_{2S}^{S}. However, as we can see in Fig. 1 c), one cannot take sufficiently small S-length and, at the same time, identify bits with fidelity. Figure shows that in any case for $S = 2$ such identification is impossible. Really, the correlation coefficient measured by a bit-finder (solid black curve) is buried partially in noisy background. These heuristic results can be justified on formal mathematical level. To this end, we note that correlation coefficients are distributed normally. This one can be easily verified using the Kolmogorov-Smirnov criterion. This issue permits to calculate the Type I error of identification (α) for both a receiver and a bit-finder. To this end, the mean correlation coefficients and theirs standard deviations are calculated by averaging all magnitudes exhibited in Fig. 1. With known statistical features in hand, we calculate

This watermark does not appear in the registered version - http://www.clicktoconvert.com

the threshold magnitudes for receiver and bit-finder as the mean of corresponding bit-bearing and background correlation coefficients ($k^{(0,1)}$ for a receiver, and $\tilde{k}^{(0,1)}$ for a bit-finder). Then, an identification error at a receiver:

$$\alpha^{(0)} = 1 - P(k^{(0)} > k^{(1)}),$$

and for a bit-finder:

$$\tilde{\alpha}^{(0)} = 1 - P(k^{(0)} > \tilde{k}^{(1)}).$$

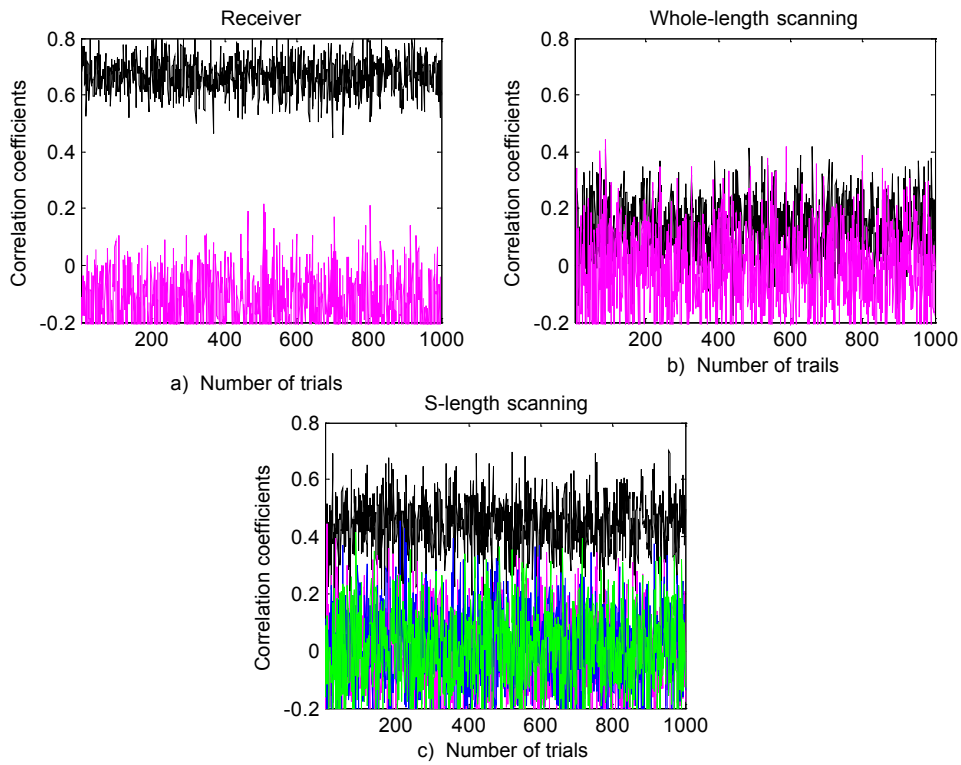

Figure 2. Monte Carlo experiment on 1000 trials for N = 50, SNR = 0.8, $SNRN$ = 0.2, and S = 50. a) The correlation coefficient of the replica and a bit-bearing signal measured at a receiver (upper set) and the background (lower set), which consists of the measurements of correlation of this replica with other signals. b) The correlation coefficient of a large part of the message taken by a bit-finder as a replica and other parts of the message. c) The correlation coefficient of an S-length part of the message taken by a bit-finder as a replica and other S-length parts of the message.

For considered case of N = 50, SNR = 0.8, and $SNRN$ = 0.2, the identification error of bits identification at a receiver, $\alpha^{(0)} \sim 2.5 \cdot 10^{-8}$. As to a bit-finder, if he takes accidentally the whole 2N-length packet as a base signal for scanning, the identification will be not possible at all (see Figure 1 b). If a bit-finder takes sufficiently small 2S-length signal with S = 25 as a base one, he has to try

This watermark does not appear in the registered version - http://www.clicktoconvert.com

$\nu_{2S}^{S} \approx 2.5 \cdot 10^{1}$ times for finding bits. However, all these trials are of little use because the identification error in each trial, $\tilde{\alpha}^{(0,1)} \sim 0.$. Hence, while finding the needed distribution of bit-bearing samples, a bit-finder might be in error approximately $0.\cdot \nu_{2S}^{S} \approx 2.5 \cdot 10^{10}$ times. It is obvious that in this case he cannot find bits with fidelity. A bit-finder can identify bits with minimum error if he takes exactly 2*N*-length part of the message as a base signal and such a part will contain $S = N$ samples of bit-bearing signal. To find theirs distribution among 2N samples of the bit-bearing packet, a bit-finder has to try $\nu_{2N}^{N} \approx 1.0 \cdot 10^{3}$ times while finding bits. Bit identification error in each trial for $S = N = 50$, $\tilde{\alpha}^{(0,1)} \sim 0.0$. Then, finding the needed distribution of bit-bearing samples, a bit-finder might be in error approximately $0.0 \cdot \nu_{2S}^{S} \approx 2.0 \cdot 10^{20}$ times. This situation is demonstrated in Fig. 2. The identification error at a receiver in this case is naturally the same as in Fig. 1. A situation changes in Fig. 2 c) only. As a bit-finder takes larger base signal, the obtained correlation coefficient, r_c, in the case of coincidence of bit-bearing samples in base and test parts, becomes larger. This issue we can see here in increasing value of its mean level. However, the magnitudes of correlation coefficient, r_c, and background coefficients are notably overlapped. It is sufficient to completely prevent bits from finding due to a huge amount of trials needed in finding process.

As to identification at a receiver, we have completely another situation. First, the bits identification error is very small, $\alpha^{(0,1)} \sim 10^{-2}$, and if the beginning moment of the message is known, we try only ones, else we try ten time as a maximum. Hence, a receiver's identification error is quite acceptable. Worth noting that one can drastically diminish this error at the expanse of the bit-bearing signal length increasing.

As to efficiency of the SCS considered, it is clear that its communication rate is lower than that of existed schemes. On the other hand, the SCS can ensure totally safe communication inside some special Nets. Such a Net can be easily developed by reorganizing existed input/output protocols. Such I/O protocols must ensure on physical level the receiving and transmitting the above-considered bit-bearing packets instead of traditional bits. Because of an eavesdropper cannot decamouflage bits and use them for intrusion into the computer system, the SCS can completely solve both

This watermark does not appear in the registered version - http://www.clicktoconvert.com

the safe data transmission and data storing problems. More than that, the key-combinations of bit-bearing packets can be loaded into the cipher/decipher code electronically from a floppy disk immediately before the communication, and then it may be deleted. This issue prevents keys from stealing by other persons. In addition, the key-combinations can be changed from a transmitter only if a receiver is not accessible to human contacts.

The effectiveness of the SCS can be drastically improved if we encode letters with the aid of above-mentioned set of samples. In this case, we need not use the binary encoding of information at all. To this end, we need to have as many latter-bearing packets as those of different letters and separate signs used. Noting that evaluation of correlation coefficients is not computationally expensive, one can use 30-40 keys in the SCS without problems. Worthwhile to emphasize that the problem of letters repeating with definite frequencies, which commonly arises in letters encoding process, is not the case for the SCS. On the other hand, the letters repeating frequencies can be easily done identical at the expense of the letter-bearing packets number increasing.

Besides above-mentioned opportunities, the SCS gives rise to completely secure private communication by e-mail. To this end, the recipients should have simple software developed in the MATLAB, for example. An encrypted in the MATLAB message can be represented as a MAT file, which can be sent simply by e-mail. Such a file consists of a string of numbers in floating point format, which represent latter-bearing packets. To prevent the hard drive disk from hacking, one can encrypt and decrypt messages using a standalone computer. More than that, such a computer might have only the main frame of the encrypting/decrypting code without keys. The keys may be loaded from a floppy disk. Using the considered version of the SCS, to transmit one encrypted standard page of a text, which contains 4500 signs, one has to send by e-mail a MAT file of about 3.5 MB volume.

Summing, we can note that safe data distribution and store problems can potentially be solved with the aid of proposed method due to the following points:

- An eavesdropper can measure a far lower correlation coefficient than that at a receiver due to noise mixed into transmitted bit-bearing signal. Therefore, a bit identification error probability at a receiver is darn near to zero, but that at a

This watermark does not appear in the registered version - http://www.clicktoconvert.com

cryptanalyst device is usually more than 0.01, and can easily be done more than 0.1 if it is needed, but at the expense of more samples in bit-bearing signals.

- To identify bits at a receiver, one has to measure correlation coefficient only ones, if the beginning of a message is known, or ten times maximum, otherwise. At the same time, a cryptanalyst has to try huge amount times in the bit-finding process due to unknown distribution of signal samples between all other samples of the bit-bearing packet, and this one leads to realization of erroneous identifications many times even for arbitrary small probabilities.

In addition, as it follows from general considerations, to prevent illegal intrusions inside a computer system, we have to break any direct bit-based connection between computers. Nowadays, all safeguard software systems, such as firewalls, for example, and intruder's codes are operated in the same computer area. If this situation will continue in future, the war between defenders and intruders will continue forever. The method proposed in this work permits to break direct bit-based connection between computers. Therefore, neither one can send any illegal information, which can be comprehended by computer. To do that, one has to decamouflage and identify bits buried in noise.

These issues ensure theoretically both the safe communications and safe data storing on hard drives.

4. LOW-POWER RADARS

Identification and localization of weak radar signals returned from a target and buried in noise are steel of great importance [9-11]. To this end, the wavelet analysis has been used in [9], the higher-order statistics has been implemented in [10], and the hybridization of these two has been developed in [11]. Many other methods are also used for this purpose. In this work, we propose a simple statistical method identification of weak radar pulses buried in noise. We consider here sufficiently long impulses with carrier frequency f_0 (Fig. 3). Here, the samples considered above exhibit step-wise behavior. Conditionally, theirs magnitudes can be put to ± 1. At a receiver, we measure permanently the samples in N equidistant snapshot points 10 times a half-period. A distance between snapshot points equals to the half of a period

This watermark does not appear in the registered version - http://www.clicktoconvert.com

of the carrier. Theoretically, we need to measure samples of coming signal in extremal points only. However, due to signals are buried in noise, it is possible that we do not know exactly where are these extremal points. Because of that, we need to measure samples permanently by time interval $\Delta = \theta \cdot 1/f_0/2$. At that, maximum time shifting from extremal points for at least one from 10 measurements is less or equal to Δ. The measured N samples provide the evaluation of correlation coefficient between incoming signal and a replica. As a replica, we can use a set of ones with interchanging signs, which correspond to transmitted signal. Received signal has other amplitude, and more, it acquires a random commodity. Signal attenuation that diminishes its amplitude is equivalent to multiplication by a number and hence do not affect the correlation coefficient. This is not the case for random component. Its presence reduces drastically the correlation coefficient, and, in principle, can prevent coming signals from identification and localization.

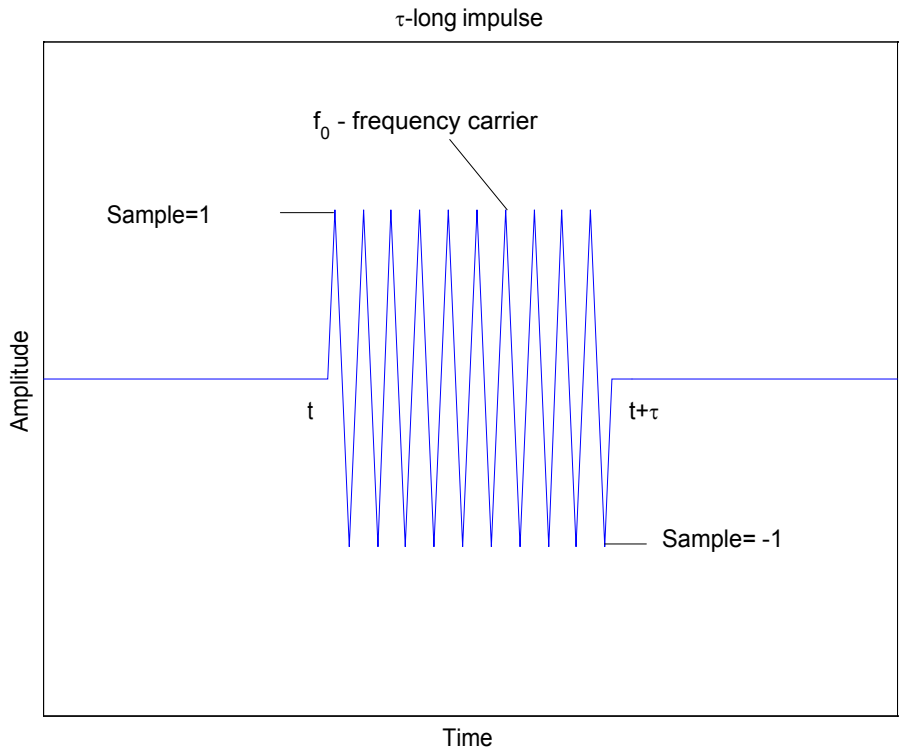

Figure 3. Conventional τ - long impulse with f_0 - frequency carrier. Here, samples are step-wise behaved.

Despite the same principle of stochastic comparing of electromagnetic signals as we have used for safe communication, its utilization for radars has some peculiarities. Consider now these new features. Let $\{x_i\}$ be a N-length set of signal samples in

This watermark does not appear in the registered version - http://www.clicktoconvert.com

extremal points, $\{x_i^{(\Delta)}\}$ - samples in the same points but shifted by one Δ-period, and $\{z_i\}$ - the same length set of white Gaussian noise samples. During permanent measuring of correlation coefficients by period Δ, we can obtain the following correlation coefficients with replica $\{x_i\}$:

$$r_s = r(x + z, x) \tag{13}$$

for "signal+noise" samples measured in extremal points,

$$r_\Delta = r(x + z, x^{(\Delta)}) \tag{14}$$

for "signal+noise" samples measured in shifted by one Δ-period points,

$$r_n = r(z, x)$$

for noise samples only. Note that the other shifted sets of points we do not consider because the identification and localization of returned signal should be done by the maximal correlation coefficient. The latter will be in between of the two, (13) and (14). We demonstrate later these two coefficients do not differ significantly. Accounting for normally distributed correlation coefficients, we can estimate signal identification error probability (α) for given signal to noise ratio (SNR). Some of such probabilities are given in Table 1 for $N = (1, 3, 6) \cdot 10^4$.

Table 1. Identification error probabilities.

SNR (dB)		-18	-21	-24
$N = 1 \cdot 10^4$	E	3.39	2.17	~1
	E_Δ	3.17	2.02	~1
	α	$4.3 \cdot 10^{-20}$	$5.2 \cdot 10^{-10}$	$8.4 \cdot 10^{-5}$
	α_Δ	$2.6 \cdot 10^{-20}$	$1.0 \cdot 10^{-9}$	$3.0 \cdot 10^{-4}$
SNR (dB)		-21	-24	-27
$N = 3 \cdot 10^4$	E	4.81	1.78	1.44
	E_Δ	4.53	1.65	1.53
	α	$1.3 \cdot 10^{-40}$	$3.4 \cdot 10^{-8}$	$7.5 \cdot 10^{-6}$
	α_Δ	$2.6 \cdot 10^{-40}$	$3.1 \cdot 10^{-7}$	$3.6 \cdot 10^{-5}$
SNR (dB)		-24	-27	-30
$N = 6 \cdot 10^4$	E	4.62	2.97	1.71
	E_Δ	4.34	2.77	1.58
	α	$9.3 \cdot 10^{-40}$	$1.3 \cdot 10^{-10}$	$1.2 \cdot 10^{-7}$
	α_Δ	$6.5 \cdot 10^{-30}$	$1.8 \cdot 10^{-10}$	$8.9 \cdot 10^{-7}$

This watermark does not appear in the registered version - http://www.clicktoconvert.com

Besides the identification error probabilities, we give in this table the statistical excess magnitudes, namely, for non-shifted measurements:

$$E = \frac{m\ e\ (a_s n) + r\ 3_s\ t\ (d\ r}{m\ e\ (a_n n) + r\ 3_n\ t\ (d\ r}$$

and for shifted by one Δ-period ones:

$$E_\Delta = \frac{m\ e\ (a_\Delta n) + r\ 3_\Delta\ t\ (d\ r}{m\ e\ (a_n n) + r\ 3_n\ t\ (d\ r}$$

The excesses E and E_Δ demonstrate the identification error probability less than $7\ .\ 2\ 1^{-6}$(if these quantities are more than one, which is due to the 3σ-rule. Note that the identification error probabilities, as well as mean and standard deviation values, were calculated with the aid of the Monte Carlo experiment on 1000 trials.

As we can see in Table 1, the sifting of measuring by period less than Δ increases the identification error probability but not significantly. Due to this issue, one can use this method in the case when exact location of returned impulse is a priory unknown. Also, we can see that if a large number of samples are used, one can identify and locate very weak radar pulses. Note that the larger is a number of samples, the larger is a pulse length for the same carrier frequency, and the larger is the detection range of radar system. Then, if we used $f_0 = 3$ G H, the pulse length would be at least 1.7 μs for $N = 1\ \cdot 1^{4}$(, 5.0 μs for $N = 3\ \cdot 1^{4}$(, and so on. . If we used $f_0 = 1\ 0$ G H, the pulse length would be at least 0.5 μs for $N = 1\ \cdot 1^{4}$(. That is, if we want to identify weaker signals, we have to use more samples. At that, to prevent the detection range from increasing, we have to increase the carrier frequency.

A brief comparison with the paper [11], in which the state of the art in this field is exhibited, shows the proposed method can identify weaker signals with less computational efforts. For example, to identify signal of $SNR =$ -18 dB with fidelity, in [11] were used 131072 samples, which were treated with the aid of sufficiently complex techniques. More to the point, it seems that technique in [11] does not permit to diminish SNR beyond –24 dB. Our method permits to do that without additional computational burden.

This watermark does not appear in the registered version - http://www.clicktoconvert.com

5. REMOTE-MANAGING LOCKS

Unbreakable remote-managing locks are of great importance, but not developed to date. A wide variety of secret schemes have been developed, but all have some shortcomings and are not perfect. The main problem here is the same as that for safe computer: all safeguard software systems and intruder's codes are operated in the same computer area. The method proposed in this work permits to break direct bit-based connection between locks and remote keys. This one becomes possible due to altering the data acquisition scheme, in which the transmitted samples are measured and transformed into numbers in floating point format, and, after this procedure only, represented in binary form. Therefore, neither one can distribute any illegal bit-based code into a lock's microprocessor area. To do that, one has to decamouflage and identify bits buried in noise. The latter one is impossible, as we have demonstrated above.

Note that implementation of the new data acquisition scheme needs to alter the physical principle of communication between locks and keys.

In spite of the same principle as for safe computer, which can be used for developing safe lock, the latter one has its own specific features. As lock opening code, an amplitude-modulated signal, which contains $2N$ samples, is to be used. The first N samples represent an electronic key (old e-key), which opens a lock. The second one is used for creating a new e-key.

The old e-key consists of a definite N-length realization of pseudorandom value, which is distributed by definite law, and noise with signal to noise ratio, $SNR = 1$, which has the same distribution law.

The second N-length signal is a definite N-length realization of pseudorandom value as well, quite analogously to the first one.

The old e-key is altered each time, but after opening the lock only. A new e-key is constructed at the lock and key from samples of the second transmitted N-length part by definite permutation of its samples and adding noise with $SNR = 1$. The permutation law is unique for each lock and represents the main secret.

This watermark does not appear in the registered version - http://www.clicktoconvert.com

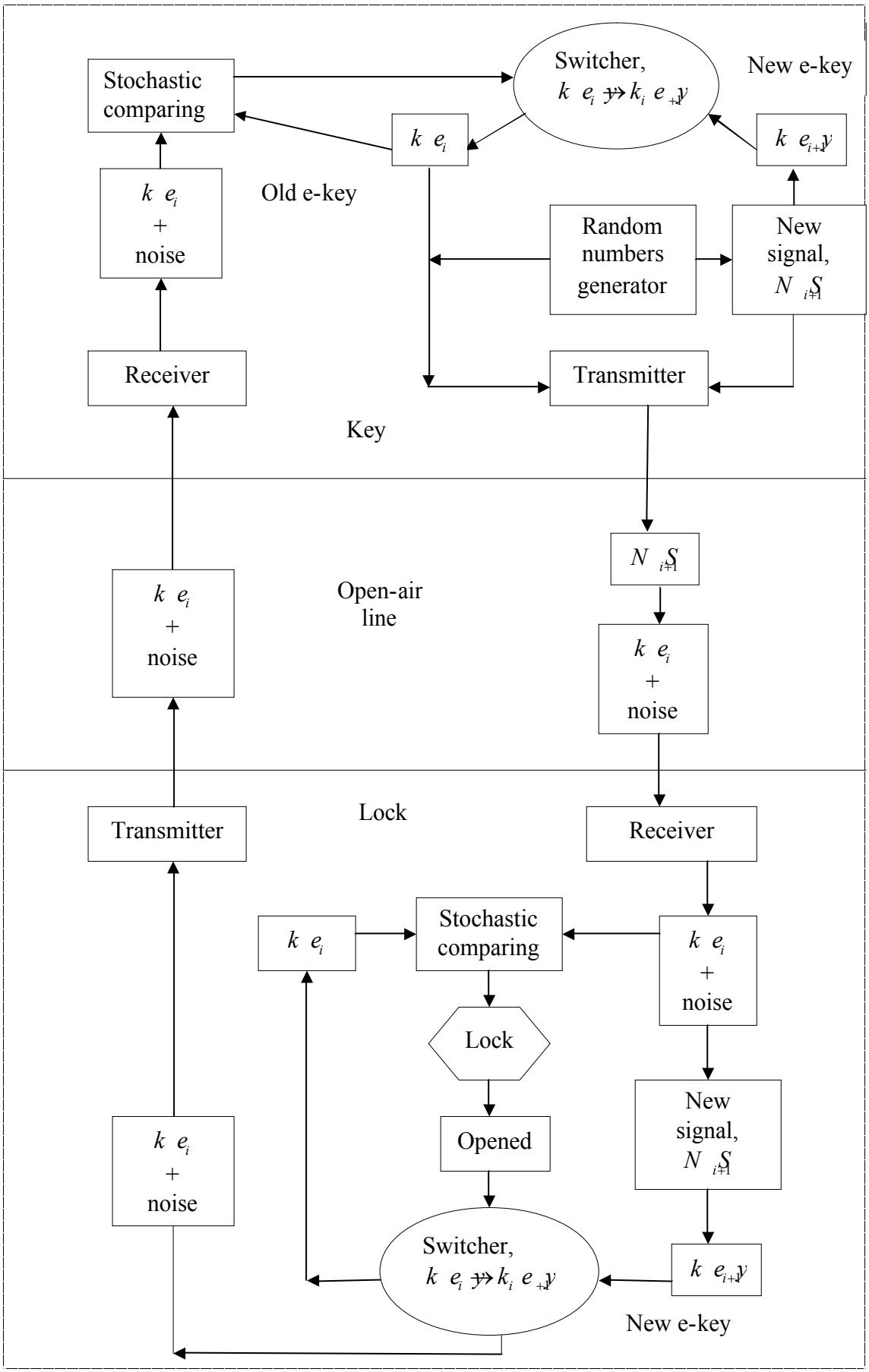

Figure 4. Remote managing lock's block-diagram.

This watermark does not appear in the registered version - http://www.clicktoconvert.com

Summing, the whole cycle of remote managing lock functioning can be depicted as follows. Originally, the old e-key is contained both at the lock and key. To open the lock, the key transmits the old e-key with noise as the first *N*-length signal and a new *N*-length signal (NS) as the second one. Using the old e-key replica, the lock identifies the received e-key and opens doors. Note that added noise does not prevent e-key from identification as it has been shown in previous sections. After opening doors, the lock creates a new e-key using the NS, and transmits the received old e-key with noise back to the key as opening conformation. The latter one gives rise to create a new e-key at the key and replace the old e-key with it. At that, the cycle is over. All these are demonstrated in Fig. 4.

As to the breakability of such a lock, consider some possible methods:

- A breaker records two transmitted signals and compares their samples. Without noise added to the old e-key, he can recover the permutation scheme used for constructing a new e-key from the NS with the aid of simple comparing of samples, viz., those of the first *N*-length signal of the second transmission and the second one of the first transmission. Severe noise, with $SNR = 1$, added to e-key prevents completely such opportunity.
- A breaker tries to find e-key by the Monte Carlo experiment or by consequent permutations of the NS *N*-length samples. This is not the case due to two causes. Firstly, the probability to guess the right combination is darn near to zero. For 50 samples, for instance, such a probability is of about $3 \cdot 3 \cdot 10^{-60}$. Secondly, in contradistinction to the stochastic communications, a breaker does not have an opportunity for finding the needed combination without addressing to the lock. However, the false attempts may be stopped on 2-3 minutes after each 3 - 4 false trials, for example.

Finally, the method proposed prevents a breaker from intruding into the microprocessor area. As we have demonstrated in Section 3, a breaker has no opportunity to distribute some bit-based information into operational area because it will be denied on physical level. At that, we consider this method permits to develop absolutely unbreakable remote-managing locks.

Besides security problem, there are some problems regarding usage conveniences. One of these is a reserve key. The method permits to solve this

This watermark does not appear in the registered version - http://www.clicktoconvert.com

problem without significant complication of the scheme. To design such a lock, one has to use separately two initial e-keys at the lock. If one key is lost, for instance, one can use the second key exactly in the same manner as the first one. More than that, the lost key can be easily disabled and one can use of this lock further. It is clear that the same principle can be used to design a common lock with many users, which can be utilized in private dwellings and offices.

6. CONCLUSIONS

Some applications of stochastic principles in comparing of electromagnetic signals or series of numbers in floating point format have been considered in the paper. One of such applications is safe communication, which is tied with the safe computer problem. Both these problems can be solved with the aid of the new method of information distribution. For this, a text may be transformed into binary code and then each bit transformed into series of random samples. Such series may be electrical signals or numbers in floating point format. It is also possible the other scenario: letters of a text are transformed directly into the series of random samples. Both the two are acceptable in different practical cases.

As has been shown in the work, there is no opportunity to decamouflage bits or letters with the aid of cryptanalysis of intercepted message. More to the point, the communication line may be so designed that no one intruder can send any bit-based information into the computer area. These merits are possible only at the expense of significant diminishing of information exchange rate. However, high noise protected features of such communication lines can in part compensate this shortcoming.

Two other applications of stochastic comparing of electromagnetic signals have been considered in the paper. The first is connected with the weak radar signal detection and localization problem. Considering the carrier wave amplitudes of radar pulse as samples and measuring its correlation coefficient with replica, we can improve significantly the probability of identification and localization of a radar impulse buried in noise. This one is possible at the expense of radar detection range increasing. To prevent this increasing, one has to increase the carrier wave frequency as well. Theoretically, following this step, one can decrease the SNR far lower than –30 dB. The second application is connected with unbreakable remote-managing locks for cars, dwellings, and offices. Such problems as lost keys and locks of common use

This watermark does not appear in the registered version - http://www.clicktoconvert.com

can be solved without significant increasing in designing and manufacturing cost. Physical principle used in the method prevents any intrusion into the microprocessor's area, and that prevents locks from breaking.

REFERENCES

[1] Bruce Schneier, *Applied Cryptography*, 2nd edition, John Wiley & Sons, New York, 1995.

[2] Bruce Schneier, *Secrets and Lies: Digital Security in a Network World*, John Wiley & Sons, New York, 2000.

[3] Simon Singh, *The Code Book*, Doubleday, New York, 1999.

[4] D. Ham, X. Li, S. A. Denenberg, T. H. Lee, and D. S. Ricketts, "Ordered and Chaotic Electrical Solitons: Communication Perspectives," *IEEE Commun. Mag.* vol. 44, no. 12, Dec. 2006, pp.126-34.

[5] L. M. Pecora and T. L. Carroll, "Synchronization in Chaotic Systems," *Physical Rev. Lett.*, vol. 64, no. 8, Feb. 1990, pp. 821-25.

[6] K. M. Cuomo and A. V. Oppenheim, "Synchronization of Lorenz-based Chaotic Circuits with Application to Communication," *IEEE Trans. Circuits and Sys. //*, vol. 40, no. 10, Oct. 1993, pp. 626-33.

[7] R. Roy and K. S. Thornburg Jr., "Experimental Synchronization of Chaotic Lasers," *Physical* Rev. *Lett.*, vol. 72, no. 13, Mar. 1994, pp. 2009-15.

[8] M. Toyoshima, S. Yamakawa, T. Yamawaki, K. Arai, M. Garcia-Talavera, A. Alonso, Z. Sodnik, and B. Demelenne, "Long-Term Statistics of Laser Beam Propogation in an Optical Ground-to- Geostationary Satellite Communication Link," *IEEE Trans. Antennas Propag.*, vol. 53, no. 2, Feb. 2005, pp. 842-50.

[9] L. Nikias and A. P. Petropulu, *High-Order Spectra Analysis: A Nonlinear Signal Processing* Framework, New Jersey: PTR Prentice Hall, 1993.

[10] D. L. Donoho, "Denoising by soft-thresholding," IEEE Transactions on Information Theory, vol. 41, no. 3, May 1995, pp. 613-27.

[11] O. A. M. Aly, A. S. Omar, and A. Z. Elsherbeni, "Detection and Localization of RF Radar Pulses in Noise Environments Using Wavelet Packet Transform and Higher Order Statistics," *Progress in Electromagnetic Research, PIER 58*, 2006, pp. 301-17.