ISSN: 0974-5823 Vol. 6 No. 3 October-December, 2021

International Journal of Mechanical Engineering

Evaluation of the Effect of Desynchronization of Equilibrium Information Processing on the Effectiveness of Masking Information in Side-Channels

Daniil Olegovich Korotaev
Department of Telecommunication Systems, NRU MIET, Zelenograd, Moscow, Russia.

Valentin Viktorovich Slyusar
Institute SPINTech, NRU MIET, Zelenograd, Moscow, Russia.

Alexander Vladimirovich Sharamok and Alexander Alexandrovich Bakhtin
Department of Telecommunication Systems, NRU MIET, Zelenograd, Moscow, Russia

Date of Submission: 18th April 2021 Revised: 19th September 2021 Accepted: 27th October 2021

How to Cite: **Korotaev, et. al. (2021). Evaluation of the Effect of Desynchronization of Equilibrium Information Processing on the Effectiveness of Masking Information in Side-Channels. International Journal of Mechanical Engineering 6(3), pp.1736-1748**

Abstract **- The article presents the results of simulation and experimental measurements when protecting information leaks through side-channels in the context of radio masking problem formulation. In the course of simulation and measurements, the effect of desynchronization (offset) between the signals of direct and inverse data representation in the equilibrium code on the suppression of informative signals in side-channels was investigated. The simulation results are represented by the numerical characteristics of the spectral components in the side-channel. Desynchronization generally negatively affects the quality of masking informative signals in side-channels, as well as that at low degrees of desynchronization, the informative component contains information about changes in the values of processed or transmitted data symbols, the level of desynchronization does not equally affect signal suppression in different spectral ranges; essential is the phase shift of harmonics of signals of direct and inverse data representation. The simulation results are in qualitative agreement with the experimental measurements. As further studies, it is planned to conduct experimental studies using processed data of other types, for example, random data, as well as improving the accuracy of measurement results by improving the experimental setup**.

Index Terms - Electronic masking, equilibrium codes, side-channels, synchronization.

INTRODUCTION

The development of hardware/software trusted platforms in a secure execution involves solving a range of specific tasks. In such devices, in addition to implementing various functional and trust requirements, it is necessary to implement the tasks of protection against possible removal of open information and dangerous information through channels of side electromagnetic radiation and interferences (hereinafter referred as side-channels) [1].

In the previously published work [2], a method of protection against information leakage through side-channels by employing side-channel masking with active interference is considered. The type of optimal interference for the side-channel is justified. This method of masking consists in simultaneous (synchronous) processing or transmission of useful information along with the information presented in an inverse form. Instead of processing one bit of binary data, two bits should be processed in parallel. This data presenting method is called in [2] the equilibrium code. An important condition of the method considered in [2] is the requirement of synchronous parallel processing of both values of the equilibrium data representation, and the results given in [2], are justified for the ideal processing synchronization of the equilibrium code.

The problem of synchronizing information processing in computing facilities is non-trivial and cannot be solved perfectly [3]. In practical implementation, processes of information processing are always accompanied by certain desynchronization process; both processes are carried out in parallel. Considering this circumstance, it is necessary to assess, how suitable the method considered in [1] is for practical implementation.

The purpose of the present study is to model the method of protection against information leakage in the side-channel, justified in [1], and to determine the effect of

desynchronization between the signals of direct and inverse data representation in the equilibrium code on the suppression of informative signals in the side-channels.

The novelty of the study lies in the current absence of simulation results and experimental data, confirming the effectiveness of the method justified in [1], as well as the lack of theoretical and experimental data on the effect on the effectiveness of this method of the characteristics of real information security tools (IST), in particular, characteristic, such as the impossibility of ensuring perfect synchronization between signals in direct and inverse representation.

COORDINATION OF SIMULATION PARAMETERS AND EXPERIMENTAL CONDITIONS

To determine the degree of influence of the desynchronization of calculations in the direct and reverse representation of the equilibrium code data, it is proposed to simulate such calculations in the MATLAB Simulink environment, followed by conducting a full-scale experiment with measuring the signal of side-channels, and comparing then the results of simulation and measurement to discuss and assess the obtained results for compliance with each other.

It is important to initially coordinate the simulation conditions and conduct a full-scale experiment. Considering the sufficiently wide capabilities for setting up simulations in Simulink, the restrictions are stipulated by the means used in the full-scale experiment, namely, equilibrium code-based signal generating means.

Keysight Technologies/Agilent N8241A signal generator [4], able to generate signals by issuing 1.25 GSa/s, was used in the experiment. The employment of the signal generator in the experiment, the experimental setup, and the order of measurements are described below. From the standpoint of matching the simulation parameters and the subsequent conditions of the experiment, the generation of the output signal sample frequency by the generator is an important parameter. For a frequency of 1.25 GHz, the period between counts is 0.8 ns.

The next important point is the type of signal used in simulation and the experiment. As indicated in [2], the measurement should be carried out for a signal simulating the processing or transmission of a signal in a computer system, for example, on internal data transmission buses in a computer. With relatively small volumes the transmitted data for an external observer look like random data. For this reason, it is acceptable to use random data or data that look like random, to transmit them in an equilibrium code with subsequent simulation and measurement. In this case, difficulties arise with conducting experimental measurements, since for correct measurement it is necessary to synchronize the measuring instruments with the transmitted data. When using truly random data, this is associated with some practical difficulties. For this reason, the authors decided to use a relatively short sequence that looks random and has good autocorrelation characteristics. For these purposes, a Barker code of length 13 was used with the value, represented in binary code as 1111100110101_2 [5].

SIMULINK MODEL FOR COMPUTATIONAL EXPERIMENT

Figure 1 presents a model developed in the Simulink environment, simulating the effect of desynchronization of direct and inverse data representation when presented in an equilibrium code.

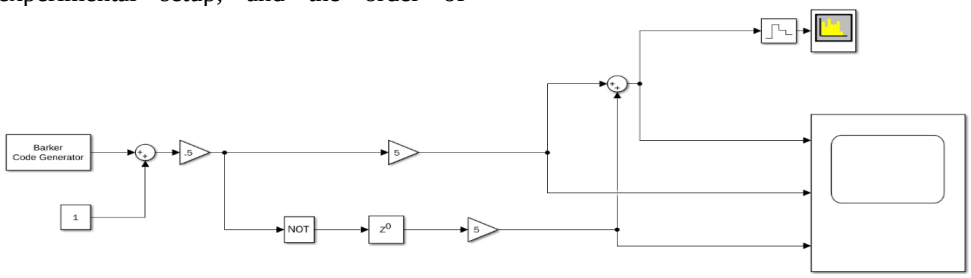

FIGURE 1
SIMULINK MODEL FOR SIMULATION

As mentioned above, the signal source was simulated in the form of a Barker code of length 13 from the corresponding source (Barker Code Generator). Since the generator forms a signal, represented at levels -1 and 1, it was transformed to levels 0 and 1 due to the summation with a constant signal of level 1 and subsequent division by 2.

To form an inverse representation of the signal, the latter, having levels 0 and 1, was inverted with subsequent conversion to levels 0 and 5 in the direct and inverse representation of the signals. The resulting signal is shown in Figure 2.

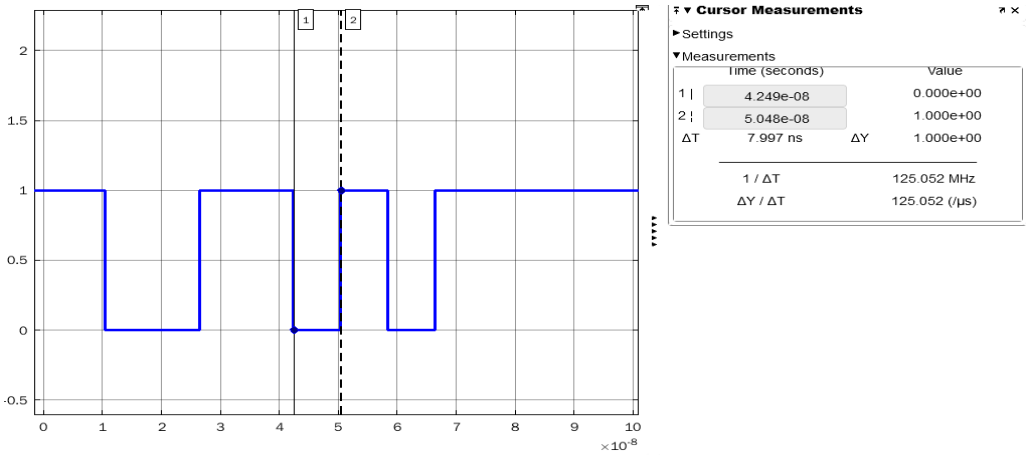

FIGURE 2
BARKER CODE 13 SIGNAL IN SIMULINK OSCILLOSCOPE

The signal, shown in Figure 1 corresponds to the chosen Barker code of length 13 with a value of 1111100110101_2. The duration of one symbol is 8 ns and the frequency is 125 MHz. That is, one symbol of the simulated signal corresponds to 10 counts, generated by the selected signal generator. The frequency of 125 MHz for one symbol of a digital signal fully corresponds to the upper limits of the clock frequencies of modern computing devices such as microcontrollers [6].

The desynchronization of the direct and inverse representation of signals was simulated by introducing a delay in the signal line in the inverse representation. The delay line allows delaying by the specified number of signal samples. Considering the peculiarities of the subsequent experiment, the model used clocking with a frequency of 1.25 GHz, which allowed for a minimum delay of 0.8 ns and subsequent delays of 1.6, 2.4, 3.2 ns, etc. Exactly these delays were used in the simulation.

It is known [5] that the summation of signals is carried out in the radio channel. For this reason, to simulate the signal in the side-channel, the signal was summed up in direct and inverse representation, followed by its output to the oscilloscope and spectral analyzer of the corresponding blocks of the Simulink system.

Figure 3 shows the fragments of the signals in the direct and inverse representation, as well as their sum at the inverse signal delays equal to 0.8, 1.6, 2.4, and 3.2 ns.

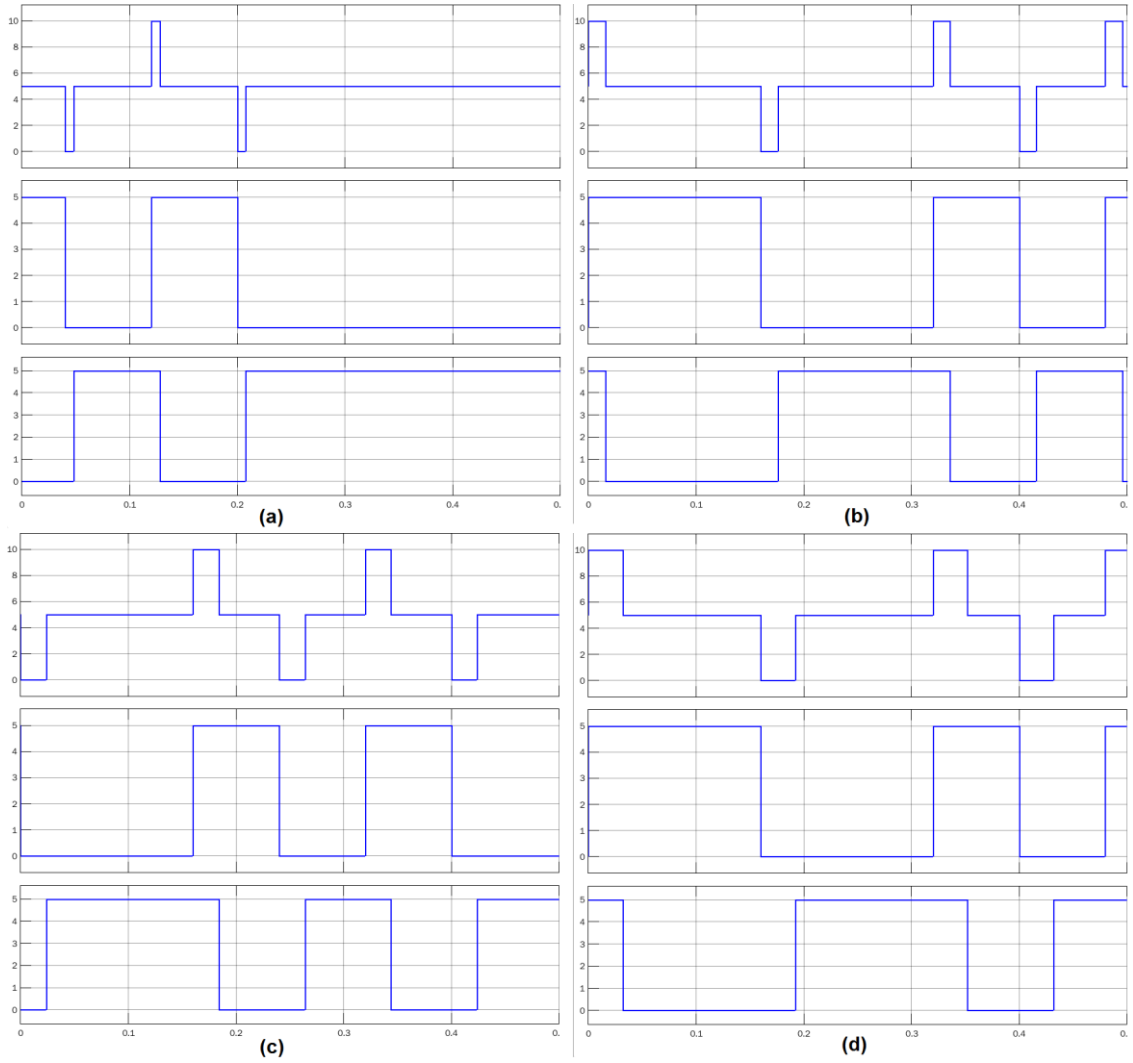

FIGURE 3
SIGNALS, DESYNCHRONIZED BY 10% (A), 20% (B), 30% (C) AND 40% (D), AND THEIR SUMS

Figure 3 shows that when a desynchronization between the direct and inverse representation of the equilibrium code appears, an informative component appears in the side-channel in the form of a pulse with a length equal to the value of desynchronization. The informative component carries information about the change of the processed or transmitted information to the opposite, from 0 to 1 or from 1 to 0.

The figures do not show the sum of the signals in the absence of a delay, since in this case, the sum of the signals degenerates into a constant signal with level 5, which corresponds to the principles set out in [1].

Figure 4 shows the spectrum of a signal representing a Barker code of length 13 in the range from 0 to 625 MHz with the above-noted time-frequency characteristics.

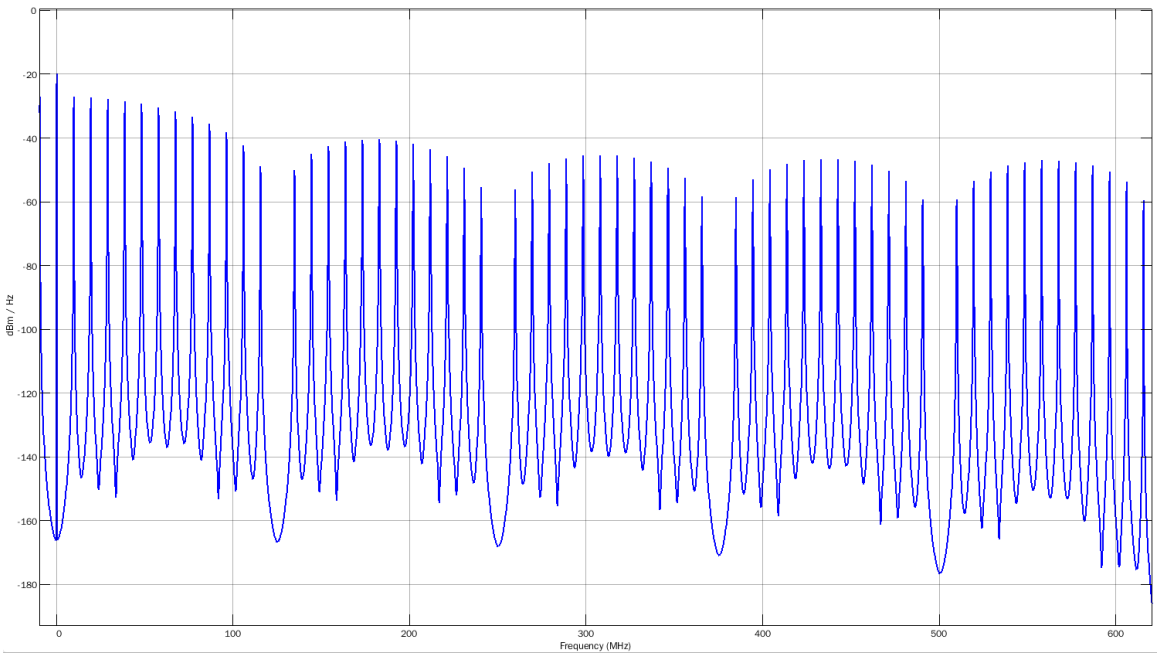

FIGURE 4
THE SPECTRUM OF THE BARKER CODE SIGNAL OF LENGTH 13 WITHIN THE RANGE FROM 0 TO 625 MHZ

Figure 4 shows characteristic spectral components with frequencies that are multiples of 9.615 MHz, which corresponds to the frequency of the Barker code of length 13, and the suppression of components at frequencies that are multiples of 125 MHz, which corresponds to the frequency of one character of the digital signal. Based on Figure 4, the range from 0 to 600 MHz can be divided into characteristic 125 MHz ranges: 0-125, 125-250, 250-375, 375-500, and 500-625 MHz. To understand the signal level of the spectral components, Table 1 shows the minimum and maximum values of the signals in each of the ranges for the signal shown in Figure 4.

TABLE 1
MAXIMUM AND MINIMUM SIGNAL LEVELS FOR CHARACTERISTIC RANGES OF THE SPECTRUM

Frequency range (MHz)	0-125	125-250	250-375	375-500	500-625
Maximum level frequency (MHz)	9.613	182.724	307.693	432.663	567.322
Maximum level value (dBm/Hz)	-24.2032	-38.0869	-41.0624	-43.9576	-44.2773
Minimum level frequency (MHz)	115.356	240.402	365.372	490.417	509.644
Minimum level value (dBm/Hz)	-46.4308	-51.9219	-54.6981	-57.0799	-56.9347

Only for the first range, the maximum signal level corresponded to the first harmonic in the concerned range. For the other ranges, the maximum harmonic was located in the middle of the range. The minimum signal levels corresponded to the last harmonics in the ranges, except for the last range from 500 to 625 MHz. Here, the minimum value of the signal corresponded to the first harmonic in the range. The spectrum, shown in Figure 4 corresponds to typical spectra for such signals [5].

SPECTRAL CHARACTERISTICS OBTAINED IN THE SIMULINK MODEL

The spectral patterns, obtained during simulation are not very informative in their visual representation, but even from them, it is possible to see some features of the spectra of the received signals. Figure 5 shows the spectra in the range from 0 to 125 MHz for signals that are desynchronized by 10% (1 count, 0.8 ns), 20% (2 counts, 1.6 ns), 30% (3 counts, 2.4 ns), and 40% (4 counts, 3.2 ns).

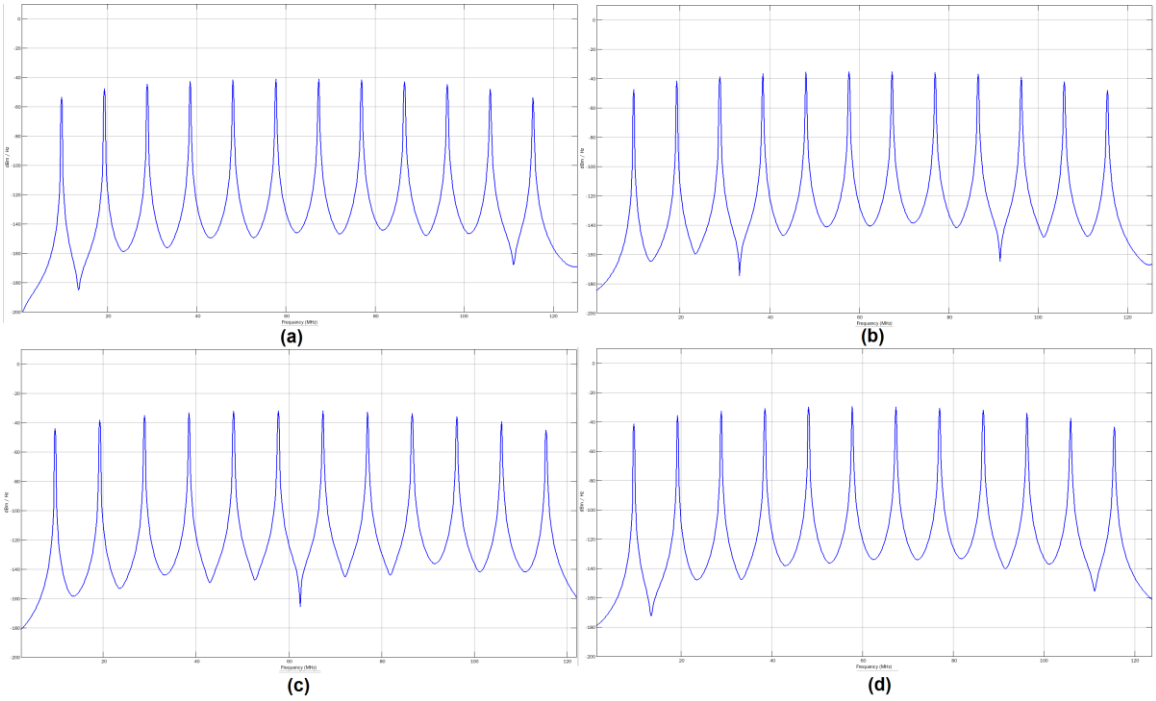

FIGURE 5
SPECTRA IN THE RANGE FROM 0 TO 125 MHZ FOR SIGNALS, DESYNCHRONIZED BY 10% (A), 20% (B), 30% (C), AND 40% (D)

Table 2 shows the numerical characteristics, corresponding to the spectra presented in Figure 5.

TABLE 2
SIGNAL LEVELS FOR THE FREQUENCY RANGE FROM 0 TO 125 MHZ

	Level of signal (dBm/Hz)	Signal level at desynchronization (dBm/Hz)			
Harmonic frequency (MHz)	Barker code	10 %	20%	30%	40%
9.613	-24.2032	-50.5193	-44.5013	-43.99	-41.4972
19.226	-24.4727	-44.7708	-38.7603	-38.249	-35.7748
28.839	-24.9289	-41.7093	-35.7116	-35.2024	-32.7571
38.452	-25.583	-39.8706	-33.8906	-33.3833	-30.9799
48.065	-26.4529	-38.8099	-32.8528	-32.348	-29.999
57.678	-27.5657	-38.3484	-32.4194	-31.9179	-29.636
67.291	-28.9629	-38.4177	-32.522	-32.0245	-29.8229
76.904	-30.7102	-39.0178	-33.1606	-32.6683	-30.5606
86.517	-32.9183	-40.2173	-34.4038	-33.9178	-31.9184
96.13	-35.7952	-42.1952	-36.4307	-35.9522	-34.0763
105.743	-39.8061	-45.3961	-39.686	-39.2167	-37.48
115.356	-46.4308	-51.2845	-45.6344	-45.1759	-43.596

As can be seen from Figure 5 and Table 2, the greatest signal suppression in the range from 0 to 125 MHz is carried out with a lower desynchronization equal to 10%, which is consistent with intuitive expectation. Below are a graphical representation and a Table with data for the range from 250 to 375 MHz, the conclusions for which are not so obvious and require additional clarification.

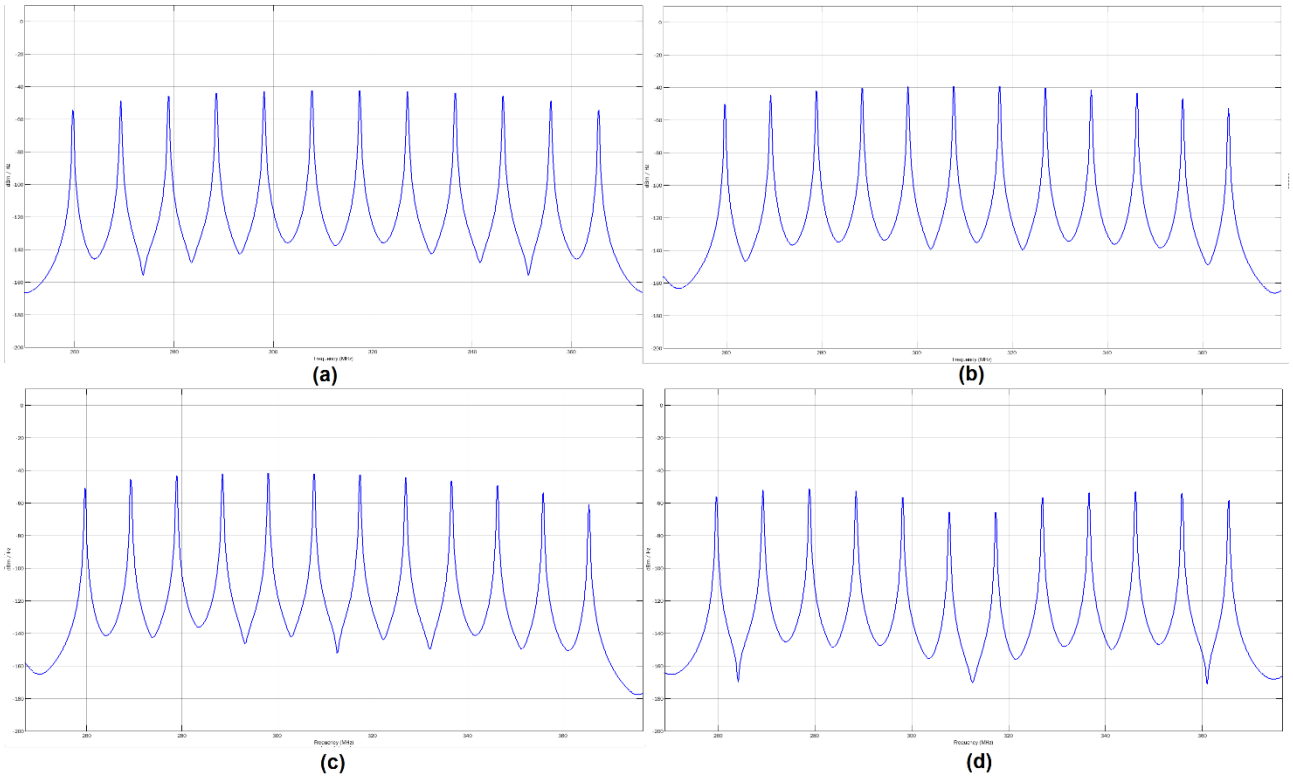

FIGURE 6
SPECTRA OF THE RANGE FROM 250 TO 375 MHZ FOR SIGNALS, DESYNCHRONIZED BY 10% (A), 20% (B), 30% (C), AND 40% (D)

Table 3 shows the numerical characteristics, corresponding to the spectra shown in Figure 6.

TABLE 3
SIGNAL LEVELS FOR THE RANGE FROM 250 TO 375 MHZ

	Level of signal (dBm/Hz)	Signal level at desynchronization (dBm/Hz)			
Harmonic frequency (MHz)	Barker code	10 %	20%	30%	40%
259.628	-52.3615	-50.6748	-50.4785	-50.8341	-56.0684
269.241	-46.8118	-44.8571	-44.9531	-45.6958	-52.2521
278.854	-43.9363	-41.7266	-42.1155	-43.2807	-51.5702
288.467	-42.2713	-39.8188	-40.5014	-42.13	-52.8584
298.08	-41.3728	-38.689	-39.6667	-41.8056	-56.4471
307.693	-41.0624	-38.1584	-39.4328	-42.1368	-65.7489
317.307	-41.2723	-38.1584	-39.6427	-42.977	-65.9588
326.92	-42.003	-38.689	-40.2969	-44.34	-57.0774
336.533	-43.3234	-39.8188	-41.5535	-46.402	-53.9105
346.146	-45.4127	-41.7266	-43.5919	-49.3675	-53.0466
355.7692	-48.716	-44.8571	-46.8573	-53.7184	-54.1564
365.3846	-54.6981	-50.6748	-52.8151	-60.9755	-58.4051

It can be seen from Figure 6 and Table 3 that the greatest signal suppression in the range from 250 to 375 MHz is noted at a 40% desynchronization. This result is not obvious and requires further clarification.

RESULTS OF THE SPECTRUM SIMULATION AND PHASES CHANGE OF THE SPECTRUM COMPONENTS

To interpret the data, obtained during the simulation, we will construct spectral masks of the simulated signals. Figure 7 shows spectral masks for Barker code signals, as well as signals, desynchronized by 10, 20, 30, and 40% in the range from 0 to 625 MHz.

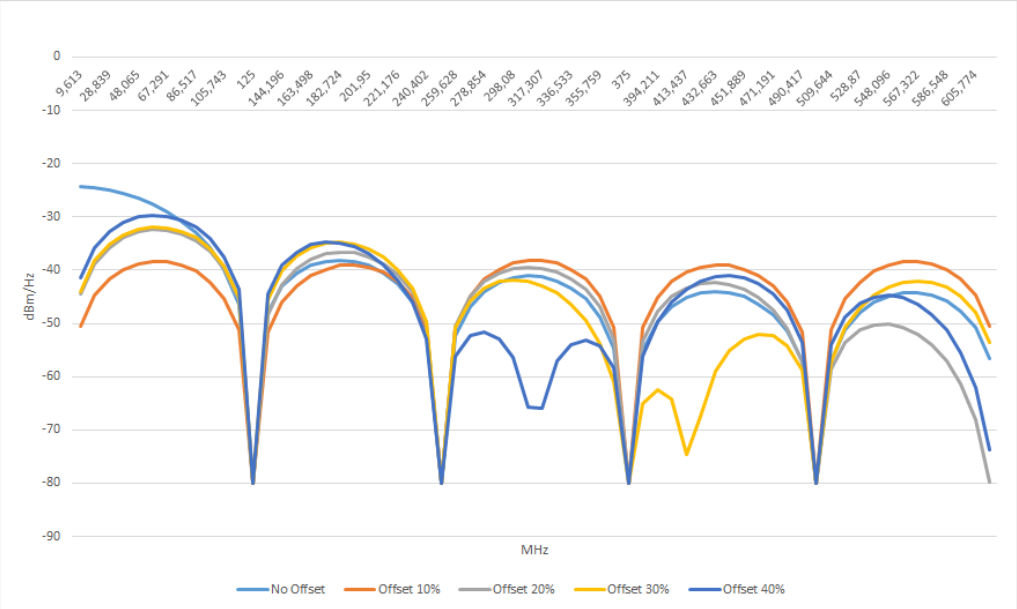

FIGURE 7
SPECTRAL MASKS FOR THE BARKER CODE SIGNAL AND DESYNCHRONIZED SIGNALS WITH NO OFFSET AND WITH OFFSETS EQUAL TO 10, 20, 30, AND 40%

Figure 7 shows that in the range from 250 to 375 MHz, the best suppression is carried out at 40% desynchronization, in the range from 375 to 500 MHz, the best suppression is carried out at 30% desynchronization. In the range from 0 to 125 MHz, radiant suppression is carried out by a signal, desynchronized by 10%. In all three cases, suppression is carried out at 15-25 dB. However, for example, in the range from 250 to 375 MHz, the signal, desynchronized by 10%, exceeds the reference signal of the Barker code by 5 dB.

To explain these results, let us consider the phase shift, resulting from desynchronization for harmonics at different frequencies. At the same shift of signals in time at different frequencies, a different phase shift occurs. Figure 8 shows phase shifts at different frequencies at various degrees of desynchronization.

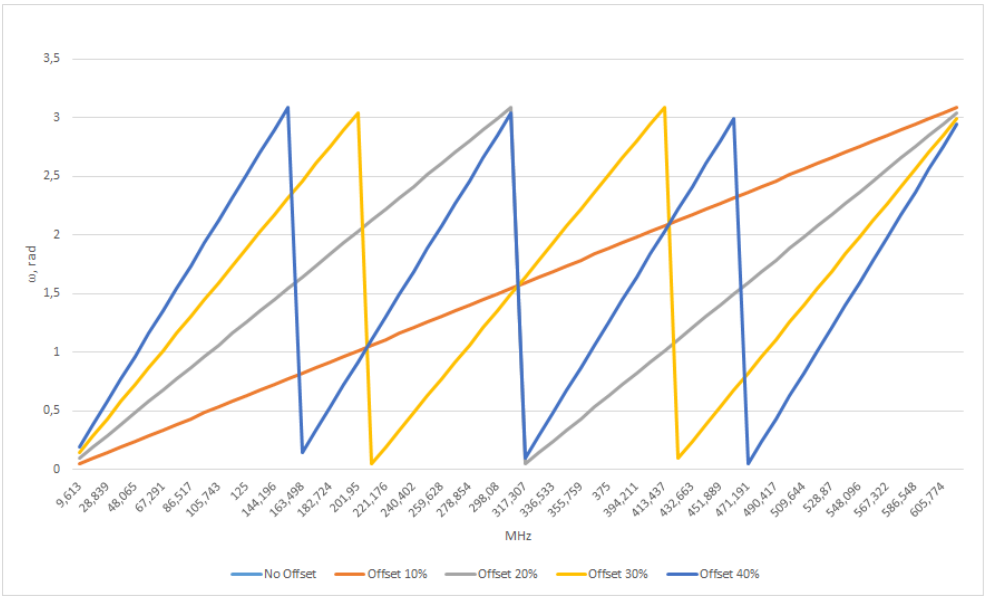

FIGURE 8
PHASE SHIFT AT DIFFERENT FREQUENCIES AT VARIOUS DEGREES OF DESYNCHRONIZATION

A comparison of Figures 7 and 8 shows that the greatest suppression occurs at a phase shift of harmonics equal to a radian, which corresponds to the known results and explains the "pits" of suppression and "peaks" of signal amplification, visible in Figure 7.

EXPERIMENTAL MEASUREMENT OF THE SPECTRAL CHARACTERISTICS

To conduct the experimental measurements, the setup shown in Figure 9, was assembled.

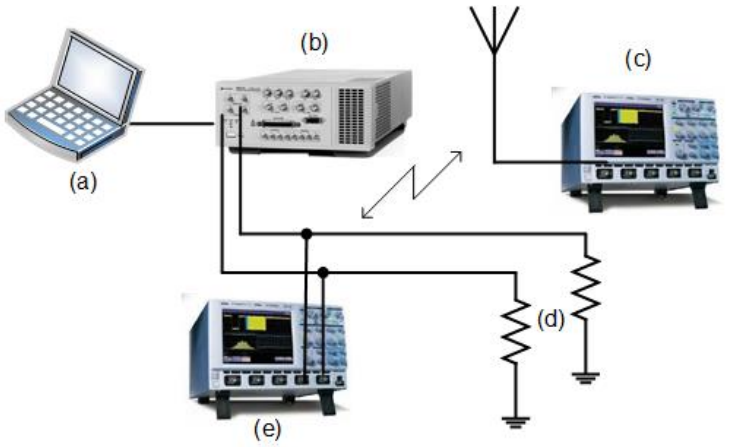

FIGURE 9
EXPERIMENTAL SETUP

The following designations apply in Figure 9: (a) laptop-based control computer; (b) Keysight Technologies/Agilent N8241A signal generator; (c) Rohde & Schwarz spectrum analyzer; (d) signal terminating resistors; (e) LeCroy Wave Runner 6000a digital oscilloscope.

The shape of the signals and their shift relative to each other were set from the control computer, while the signals were generated by a signal generator and issued in two lines terminated to the ground. The shape of the signals and their shift relative to each other were measured using a LeCroy oscilloscope, and the spectrum analysis of the emitted signal was carried out using a Rohde & Schwarz spectrum analyzer.

Figure 10 shows the shape and time characteristics of the generated Barker code signal of length 13. In Figure 10, the logical values 0 and 1 are indicated under the corresponding signal levels.

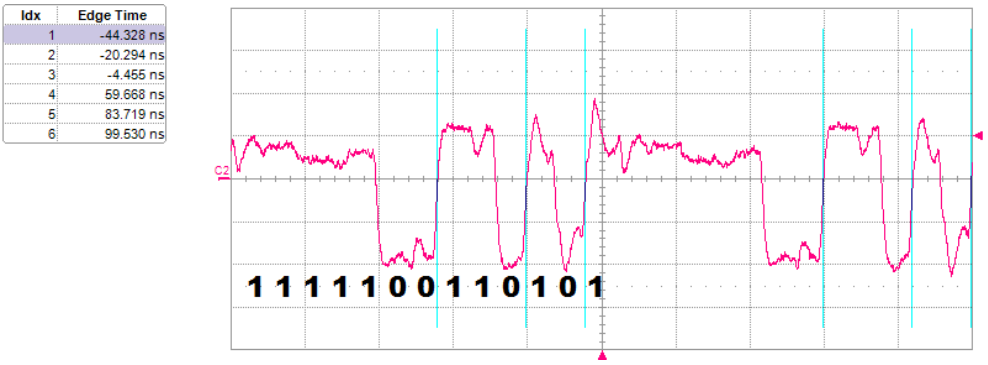

FIGURE 10
TYPE OF EXPERIMENTAL SIGNAL OF THE BARKER CODE 13

Figure 10 shows that the time characteristics of the experimental signal correspond to the characteristics of the signal, used in the Simulink simulation. Thus, the set cut-off edges corresponding to -44.328 ns and -4.455 ns cover five signal symbols; the length of one symbol is (-4.455 – (-44.328))/5 = 7.9746 ns, which, Considering measurement errors, corresponds to a given symbol length of 8 ns and a clock frequency of 125 MHz.

Figure 11 shows the Barker code signal and the inverted signals shifted by 10, 20, and 30%.

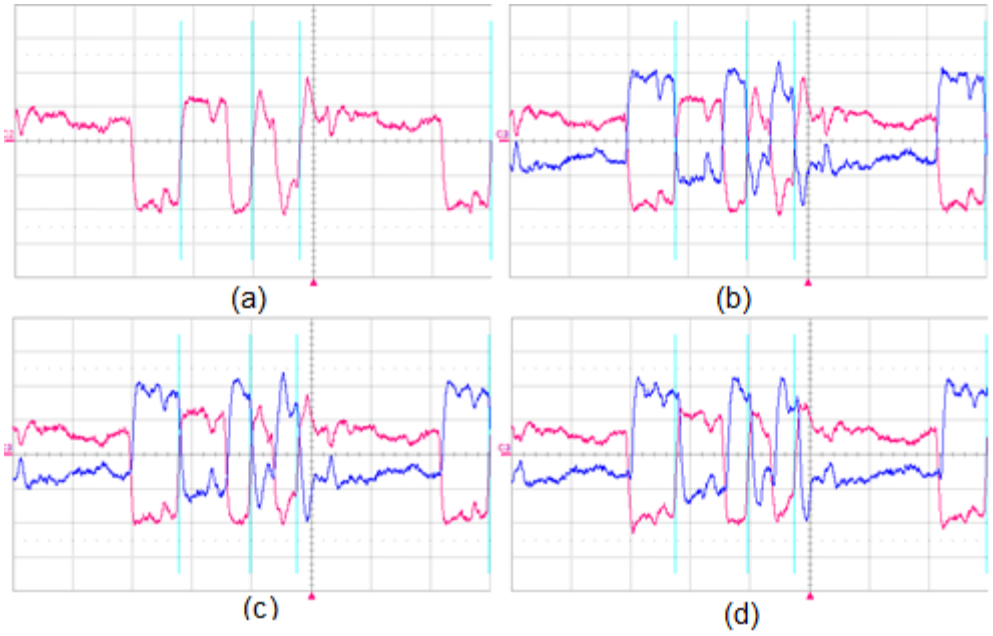

FIGURE 11
SIGNAL (A) AND INVERTED SIGNALS, SHIFTED BY 10 (B), 20 (C), AND 30% (D)

To verify the theoretical results, spectrum measurements were carried out in the most characteristic region in the vicinity of 317 MHz, where, according to the simulation, the greatest signal suppression for 40% desynchronization should be observed. The corresponding signal levels for the frequency 317.307 MHz are shown in Table 3.

During measurements at a frequency of 317.3 MHz, a spectral component was detected, whose measurement results at various degrees of signal desynchronization are shown in Figure 13. Figure 12 shows the harmonic at 317.3 MHz for the Barker code signal not masked by interference, and the Barker code signal in the equilibrium code, i.e. masked by interference.

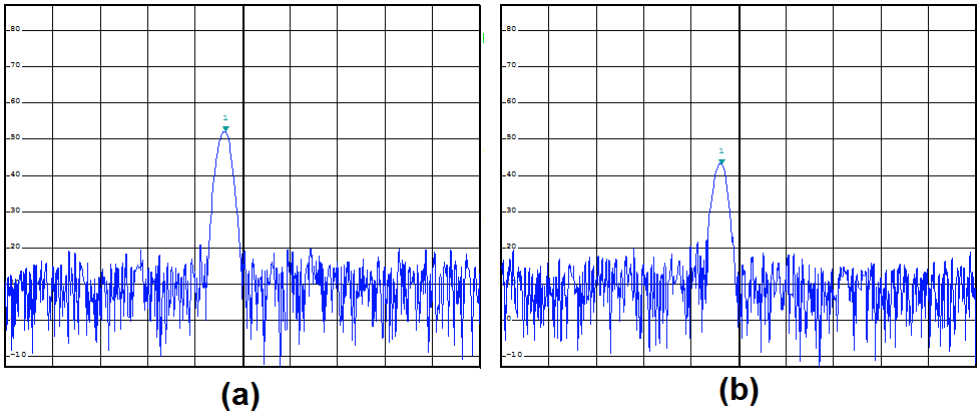

FIGURE 12
HARMONIC AT 317.3 MHZ FOR THE BARKER CODE SIGNAL (A) AND THE BARKER CODE SIGNAL IN THE EQUILIBRIUM CODE (B)

Figure 12 shows that the application of the equilibrium code leads to harmonic suppression at 317.3 MHz at the level of 10 dB.

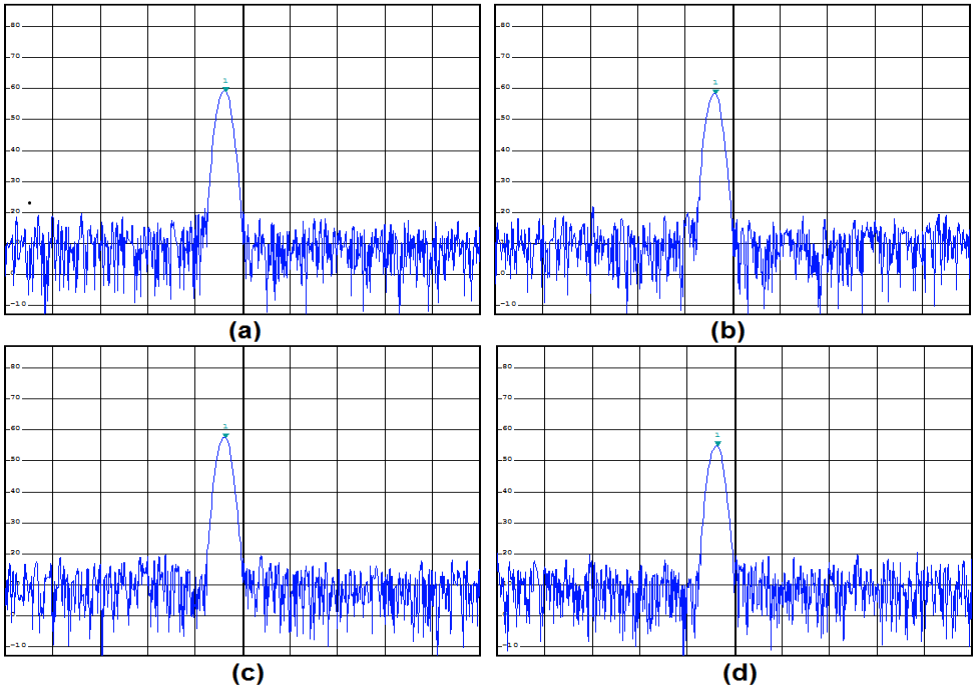

FIGURE 13
317.3 MHz HARMONIC FOR SIGNALS IN THE EQUILIBRIUM CODE, SHIFTED BY 10 (A), 20 (B), 30 (C), AND 40% (D)

The measurement results in Figure 13 show that for harmonics at a frequency of 317.3 MHz, the signal suppression during 40% desynchronization is more by several dB compared to desynchronizations by 10, 20, and 30%, which is consistent with the above-described simulation results. At the same time, this suppression is significantly less than that resulted from simulation. This discrepancy can be explained by the shortcomings of the used experimental setup, which did not allow obtaining accurate quantitative estimates. However, qualitatively the measurement results coincide with the quantitative values obtained during simulation.

RESULTS

The results of the present study are as follows.

1. When simulating the influence of desynchronization between signals of direct and inverse data representation in the equilibrium code on the suppression of informative signals in side-channels, it was shown that desynchronization in general negatively affects the quality of masking informative signals in side-channels.

2. When simulating the appearance of informative components in side-channels in case of desynchronization between the signals of direct and inverse data representation in the equilibrium code, it was shown that at low degrees of desynchronization (up to 40%), the informative component contains information about changes in the values of processed or transmitted data symbols.

3. The value of desynchronization does not equally affect signal suppression in different spectral ranges, since essential is the phase shift of harmonics of signals of direct and inverse data representation. The best suppression is achieved at a phase shift of a radian. Figure 14 shows graphs reflecting the levels of the Barker code signal, the signal, suppressed by an inverse signal with 40% desynchronization, and the phase change of harmonics by a signal with 40% desynchronization in the range from 0 to 625 MHz. The graphs shown in Figure 17 demonstrate the noted research outcome.

FIGURE 14
SIGNAL LEVELS OF THE BARKER CODE, SIGNAL WITH A 40% DESYNCHRONIZATION, AND PHASE CHANGE OF THE HARMONICS OF THE SIGNAL IN THE RANGE FROM 0 TO 625 MHZ

4. The simulation results are confirmed by qualitative consistency of the results obtained during the simulation with the results of experimental measurement.

DISCUSSION

Recently, there has been an increased interest in open research in the field of protection against leaks through side-channels and the organization of side-channel attacks. In [7], [8], several attacks, quite effective in some cases, are considered, and in [9], [10] – methods of countering these attacks. The proposed methods of countering side-channel attacks consist in introducing randomness into the data in the course of their processing [11], [12]. A special case of introducing randomness is masking the processed data with random data [13], [14] or using random shuffling (mixing) of the processed data [15], [16].

From the perspective of the present study, the most interesting are the known methods of countering side-channel attacks, developed based on the characteristics, inherent in the equipment used [17], [18] or the architecture of the system in general [11].

The implementation of devices with dual-rail logic [18] is the closest method to the one considered in the present work on leakage protection via a side-channel. Well-known studies [19] have shown the lack of significant advantages in using devices with dual-rail logic compared to traditional CMOS microelectronic devices in terms of protection cost-effectiveness.

Based on the analysis of the known protection methods against leakage through side-channels, it can be argued that the method considered in [2] is not investigated previously. The present study allowed considering some aspects of its implementation in real hardware, namely, from the standpoint of the effect of desynchronization on the effectiveness of this method.

The results of this study have some limitations and require further improvements and additional research. In particular, it is necessary to carry out simulation using other types of processed data, for example, random data, or when transmitting data in the form of alternating binary 0 and 1. Besides, for the measured values given in this paper, it is necessary to perform better measurements over a wider range of the spectrum. Similar measurements should be carried out for other types of processed data.

Another important step in the study of the concerned method is its implementation in real equipment, for example, built on FPGA chips, and conducting a study to determine the effectiveness of the considered method in this device.

At the same time, the results of the present work are encouraging and indicate the effectiveness of the considered method of protection against side-channel attacks.

CONCLUSION

Well-known studies [2] substantiate the theoretical optimality of the equilibrium information processing method when protecting against leakage in the side-channel. Engineering practice shows that not all theoretically effective methods can be implemented in practice, or their effectiveness is significantly reduced when implemented in practice. In this regard, it is necessary to evaluate the possibility and effectiveness of the implementation of theoretical solutions, and the method, discussed in [2] is no exception.

In this article, an attempt is made to investigate one of the aspects of the practical implementation of the equilibrium information processing method from the perspective of the desynchronization of signals of direct and inverse data representation. According to the authors, desynchronization is the most critical aspect of the equilibrium processing method when protecting against side-channel leaks.

The application of the results, presented in this study, based on the considered method of information processing in the equilibrium code is assumed in trusted hardware and software IST, developed within the framework of the activities of the Leading Research Center "Trusted Sensor Systems" of the National Research University of Electronic Technology – MIET. Prerequisites for the possibility of implementing the considered method consist in the development of microelectronic technologies for creating custom-made specialized computing devices, as well as an additional increase in the reliability of information processing devices when using the considered method. In this regard, the

application of the method becomes less costly and more cost-effective when implementing trusted microelectronic devices.

ACKNOWLEDGMENT

This article was performed in the framework of the program titled "Trusted sensor systems" (Agreement No. 009/20 dated April 10, 2020) with financial support by the Ministry of Communications and Mass Media of the Russian Federation and AO RVC. Project ID: 0000000007119P190002.

The simulation was performed in the Simulink Onramp environment under evaluation license #9722511, for which the authors express their gratitude to MathWorks, Inc.

The authors express their gratitude to Vasily Kochetkov and Alexander Orlov, employees of the National Research University MIET (Institute of MPSU of NIU MIET), for the given opportunity to use signal generation equipment and kind assistance in its use during experimental measurements.

REFERENCES

[1] Sobolev, A.N., Kirillov, V.M., "Fizicheskie osnovy tekhnicheskikh sredstv obespecheniya informatsionnoi bezopasnosti" ["Physical foundations of technical tools protecting information safety"], Guidebook, *Moscow, Russia: Gelios ARV*, 2004.

[2] Lyubushkina, I.E., Zverev, E.M., Sharamok, A.V., "Implementation of information security devices in equilibrium codes", *Journal of Theoretical and Applied Information Technology*, Vol. 98, No. 23, 2020, pp. 3909-3920. Available from: http://www.jatit.org/volumes/Vol98No23/24Vol98No23.pdf

[3] Wakerly, J.F., "Digital design: principles and practices", Vol. 1, *Englewood Cliffs, N.J.: Prentice-Hall*, 2000.

[4] Keysight Technologies, N8241A Arbitrary waveform generator synthetic instrument module 1.25 GSa/s or 625 MSa/s, Technical Overview, 2017.

[5] Sklar, B., Harris, F., "Digital communications: fundamentals and applications" (Communications Engineering & Emerging Technology Series from Ted Rappaport)", 3rd ed., *Pearson*, 2020.

[6] ESP8285 Datasheet, Related product: ESP8285N08, ESP8285H16, Version 2.3, Espressif Systems, 2021.

[7] Genkin, D., Pipman, I., Tromer, E., "Get your hands off my laptop: physical side-channel key-extraction attacks on PCs", *Journal of Cryptographic Engineering*, Vol. 5, 2015, pp. 95-112. https://doi.org/10.1007/s13389-015-0100-7

[8] Suzuki, D., Saeki, M., "Security evaluation of DPA countermeasures using dual-rail pre-charge logic style" In: Goubin, L., Matsui, M. (Eds.), Cryptographic hardware and embedded systems - CHES 2006. CHES 2006. Lecture notes in computer science, Vol. 4249, *Berlin, Heidelberg, Germany: Springer*, 2006, pp. 255-269. https://doi.org/10.1007/11894063_21

[9] Barenghi, A., Brevi, M., Fornaciari, W., Pelosi, G., Zoni, D., "Integrating side-channel security in the FPGA hardware design flow" In: Bertoni, G.M., Regazzoni, F. (Eds.), Constructive side-channel analysis and secure design. COSADE 2020. Lecture notes in computer science, Vol. 12244, *Cham, Switzerland: Springer*, 2020, pp. 275-290, https://doi.org/10.1007/978-3-030-68773-1_13

[10] Tebelmann, L., Danger, J.-L. Pehl, M., "Self-secured PUF: protecting the loop PUF by masking" In: Bertoni, G.M., Regazzoni, F. (Eds.), Constructive side-channel analysis and secure design. COSADE 2020. Lecture notes in computer science, Vol. 12244, *Cham, Switzerland: Springer*, 2021, pp. 293-314, https://doi.org/10.1007/978-3-030-68773-1_14

[11] He, W., de la Torre, E., Riesgo, T., "An interleaved EPE-Immune PA-DPL structure for resisting concentrated EM side-channel attacks on FPGA implementation" In: Schindler, W., Huss, S.A. (Eds.), Constructive side-channel analysis and secure design. COSADE 2012. Lecture notes in computer science, Vol. 7275, *Berlin, Heidelberg, Germany: Springer*, 2012, pp. 39-53. https://doi.org/10.1007/978-3-642-29912-4_4

[12] Sasdrich, P., Mischke, O., Moradi, A., Güneysu, T., "Side-channel protection by randomizing look-up tables on reconfigurable hardware" In: Mangard, S., Poschmann, A. (Eds.), Constructive side-channel analysis and secure design. COSADE 2015. Lecture notes in computer science, Vol. 9064, *Cham, Switzerland: Springer*, 2015, pp. 95-107. https://doi.org/10.1007/978-3-319-21476-4_7

[13] Müller, N., Moos, Th., Moradi, A., "Low-latency hardware masking of PRINCE" In: Bhasin, S., De Santis, F. (Eds.), Constructive side-channel analysis and secure design. COSADE 2021. Lecture notes in computer science, Vol. 12910, *Cham, Switzerland: Springer*, 2021, pp. 148-167, https://doi.org/10.1007/978-3-030-89915-8_7

[14] Amerbaev, V.M., Tel'pukhov, D.V., Sharamok, A.V., "Sposob skrytogo slozheniya i osobennosti ego realizatsii" ["Concealed summation and peculiarities of its implementation"], *Izvestiya vuzov: Elektronika*, Vol. 3, No. 77, 2009, pp. 26-32.

[15] Kutzner, S., Nguyen, P.H., Poschmann, A., Wang, H., "On 3-share threshold implementations for 4-bit S-boxes" In: Prouff, E. (Ed.), Constructive side-channel analysis and secure design. COSADE 2013. Lecture notes in computer science, Vol. 7864, *Berlin, Heidelberg, Germany: Springer*, 2013, pp. 99-113. https://doi.org/10.1007/978-3-642-40026-1_7

[16] Udvarhelyi, B., Bronchain, O., Standaert, F.-X., "Security analysis of deterministic re-keying with masking and shuffling: application to ISAP" In: Bhasin, S., De Santis, F. (Eds.), Constructive side-channel analysis and secure design. COSADE 2021. Lecture notes in computer science, Vol. 12910, *Cham, Switzerland: Springer*, 2021, pp. 168-183. https://doi.org/10.1007/978-3-030-89915-8_8

[17] Robisson, B., Bouder, H.L., "Physical functions: the common factor of side-channel and fault attacks?", *Journal of Cryptographic Engineering*, Vol. 6, 2016, pp. 217-227. https://doi.org/10.1007/s13389-015-0111-4

[18] Nawaz, K., Kamel, D., Standaert, F.X., Flandre, D. "Scaling trends for dual-rail logic styles against side-channel attacks: a case-study" In: Guilley, S. (Ed.), Constructive side-channel analysis and secure design. COSADE 2017. Lecture notes in computer science, Vol. 10348, *Cham, Switzerland: Springer*, 2017, pp. 19-33. https://doi.org/10.1007/978-3-319-64647-3_2

[19] Vadnala, P.K., Großschädl, J., "Faster mask conversion with lookup tables" In: Mangard, S., Poschmann, A. (Eds.), Constructive side-channel analysis and secure design. COSADE 2015. Lecture notes in computer science, Vol. 9064, *Cham, Switzerland: Springer*, 2015, pp. 207-221. https://doi.org/10.1007/978-3-319-21476-4_14