УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2017 Том 17 № 6 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2017 Vol. 17 No 6 ISSN 2226-1494 http://ntv.ifmo.ru/en

ALGEBRAIC MANIPULATION DETECTION CODES WITH PERFECT NONLINEAR FUNCTIONS UNDER NON-UNIFORM DISTRIBUTION

C. Carlet[a], A.B. Levina[b], , S.V. Taranov[b]

[a] University of Paris 8, Paris, France
[b] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: levina@cit.ifmo.ru

Article info
Received 06.10.17, accepted 26.10.17
doi: 10.17586/2226-1494-2017-17-6-1052-1062
Article in English

For citation: Carlet C., Levina A.B., Taranov S.V. Algebraic manipulation detection codes with perfect nonlinear functions under non-uniform distribution. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 6, pp. 1052–1062 (in English). doi: 10.17586/2226-1494-2017-17-6-1052-1062

Abstract
Classical methods of error detection are not efficient when an attacker controls the process of error injection. Nowadays the problem of providing high level of security for cryptographic systems, secret sharing schemes, flash memories and other communications, computation and storage systems is central to information security. To solve this problem the algebraic manipulation detection (AMD) codes have been proposed by Cramer at EUROCRYPT 2008. AMD codes represent a new class of nonlinear error detection codes which minimize the maximum of error masking probability. The paper presents the findings on behavior research of perfect nonlinear functions used in algebraic manipulation codes when the input distribution is not uniform. This research gives the detail review of behavior of perfect nonlinear functions and the maximum of error masking probability in case of different irreducible polynomials used for AMD codes. The received measurements can be used for selection of coding function that can be the most suitable for encoding information in specific situation such as given distribution of input codewords, irreducible polynomial and other parameters. The paper highlights the cases of parameter changing in coding system which do not change the error masking probability distribution or the changes are insignificant. These cases can be used to modify designs without reducing the stability of the entire integrity system to algebraic attacks that gives the possibility to customize the system for practical needs. Such parameters as the distribution of input codewords are also considered. They have an adverse effect on the stability of the system to algebraic manipulations. Changes in the input codeword distribution should be monitored in the integrity system, and additional transformations for input codewords should be used for security reasons or the encoding function within the integrity system should be changed.

Keywords
robustness, error masking probability, AMD codes, encoding function complexity, nonuniform distribution

УДК 004.056.2

КОДЫ, ОБНАРУЖИВАЮЩИЕ АЛГЕБРАИЧЕСКИЕ МАНИПУЛЯЦИИ, НА ОСНОВЕ СОВЕРШЕННО НЕЛИНЕЙНЫХ ФУНКЦИЙ НАД НЕРАВНОМЕРНЫМ РАСПРЕДЕЛЕНИЕМ

К. Карлет[a], А.Б. Левина[b], , С.В. Таранов[b]

[a]University of Paris 8, Париж, 93526, Франция
[b] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: levina@cit.ifmo.ru

Информация о статье
Поступила в редакцию 06.10.17, принята к печати 26.10.17
doi: 10.17586/2226-1494-2017-17-6-1052-1062
Язык статьи – английский

Ссылка для цитирования: Карлет К., Левина А.Б., Таранов С.В. Коды, обнаруживающие алгебраические манипуляции, на основе совершенно нелинейных функций над неравномерным распределением // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 6. С. 1052–1062. doi: 10.17586/2226-1494-2017-17-6-1052-1062

Аннотация
Стандартные методы обнаружения ошибок неэффективны в случаях, когда атакующий контролирует процесс внедрения ошибок. Проблема обеспечения высокого уровня защиты для криптографических систем, схем разделения секрета, флеш памяти и других систем передачи, обработки и хранения информации является одной из важнейших в области обеспечения информационной безопасности. Для решения данной проблемы Р. Крамером на EUROCRYPT

2008 были предложены коды, обнаруживающие алгебраические манипуляции (AMD-коды). AMD-коды являются новым классом нелинейных кодов, обнаруживающих ошибки, которые минимизируют максимальное значение вероятности маскировки ошибки. В данной статье представлены результаты изучения поведение кодов, обнаруживающих алгебраические манипуляции, на основе совершенно нелинейных функций при неравномерно распределении входных значений. Исследование дает подробный обзор поведения совершенно нелинейных функций и вероятности маскировки ошибки при различных неприводимых многочленах, используемых для AMD-кодов. Полученные результаты могут быть использованы для выбора функции кодирования, которая наиболее подходит для конкретной ситуации, задаваемой распределением входных кодовых слов, неприводимыми многочленами и другими параметрами. Выделены случаи изменения параметров системы кодирования, при которых распределение вероятности маскировки не изменяется или изменения незначительны. Эти варианты могут использоваться для модификации конструкций без снижения устойчивости всей системы целостности к алгебраическим атакам, что позволяет настроить систему под практические нужды. Рассмотрен такой параметр, как распределение входных кодовых слов, который отрицательно влияет на устойчивость системы. Изменения в распределении входных кодовых слов должны отслеживаться в системе обеспечения целостности, и в целях безопасности должны использоваться дополнительные преобразования для входных кодовых слов, либо изменяться функция кодирования внутри системы целостности.

Ключевые слова
надежность, вероятность маскировки ошибки, AMD-коды, сложность функции кодирования, неравномерное распределение

Introduction

As shown in [1–3], classical methods of error detection are not effective when the error distribution of a device is unknown or controlled by anattacker; they do not give the possibility to minimize the worst error masking probability. The majority of currently used linear and nonlinear codes have a set of undetectable errors, and their injection could compromise security in encoding devices. If an error configuration is controlled by an attacker, then he can produce an error changing of a correct codeword into a wrong codeword, exceeding the correction ability of the used code. In the case of linear codes, undetectable errors are codewords, so it is enough for the attacker to know only the code, used in the device, for the error injection. One of the models for error injection is algebraic manipulation. This model assumes that the attacker is able to modify the value of some abstract data storage devices without having read-access to the data. This model can be used for memory security [4–6], and for the other systems, such as secret sharing schemes [7]. In these cases, error configuration is absolutely unpredictable and depends on the attacker’s capabilities and method of fault injection.

The solution for the problem of algebraic manipulation was firstly introduced by Cramer et al [7]. Algebraic manipulation detection (AMD) codes may, in some sense, be viewed as keyless combinatorial authentication codes that provide security in the presence of an oblivious algebraic attacker. Its original applications included robust fuzzy extractors, secure message transmission and robust secret sharing. In recent years, however, a rather diverse array of additional applications in cryptography has emerged.

The nonuniformity of input values opens up wide opportunities for an attacker introducing errors, when he is able to find correlations between the error masking probability distributions for some encoding function and the probability distributions of the inputs. This correlation more likely enables the introduction of an error in the device, because in this case the probability of error masking is dependent on the input values. Today this question is being studied in details. There is a mechanism to reduce the maximum of error masking probability by Gray mapping [8]. However, in the paper [8] the authors do not analyse the effect of the encoding function parameters on minimization of the error masking probability.

This paper compares the error masking probability for several AMD codes basedon PN functions in cases of uneven distribution of the input codewords. As a PN function, we take the so-called Maiorana – McFarland functions defined as follows: denoting input s by (x, y) with $x, y \in F_{2^{k/2}}$, we have $F(x, y) = x \times \pi(y)$, where π is a permutation on $F_{2^{k/2}}$. We consider, in particular, $F_1(x, y) = xy$, $F_2(x, y) = xy^{-1}$ and $F_3(x, y) = xy^3$ (with the convention $0^{-1} = 0$ in the second case and with $k/2$ odd in the latter case so that $y \rightarrow y^3$ is a permutation). The purpose of the comparison is to identify the relationships between the probability of error masking and distribution of input values that enable an attacker to accelerate the error finding with the high probability of errors masking.

In the analysis of the encoding functions, the following issues are discussed in details:

- the error masking probability of encoding functions with the same nonlinearity and the code redundancy;
- what is the effect of changing the irreducible polynomial chosen to build the finite field, over which the PN function is defined.

For each probability distribution of error masking investigated, the following parameters are analyzed:

- maximums of error masking probability;
- number of the error masking probability maximums for given distributions;
- number of errors with error masking probability exceeding 0.5 (so-called "bad errors").

The studies carried out are also applicable to the class of wavelet robust codes presented in the works [9, 10].

Algebraic Manipulation Detection code

The model of algebraic manipulation over an abstract storage device has been firstly described by Cramer et al. in [11] and presented in Figure 1. Such device is denoted by $\sum(G)$ and can hold an element g from a finite Abelian group G. An attacker is not able to obtain any information about the element g stored in the device $\sum(G)$. However, he can change the stored element g by adding another element $e \in G$. This tampering is called *an algebraic manipulation*. After algebraic manipulation, the abstract storage device $\sum(G)$ will store the value $g+e$, we will call e an error. An adversary can choose the value e only on the basis of what he already knew about g before it was stored in the device (his *a priori* knowledge of g). AMD codes are supposed to encode an original information $s \in S$ as an element of $g \in G$ in such way that any algebraic manipulation is detected with high probability. It is known that the best option is to choose a perfect nonlinear function [12] for this encoding mapping. But this option is in fact optimal under the condition that the input distribution is uniform. In this paper, we analyse the case of non-uniform input distribution of AMD codes.

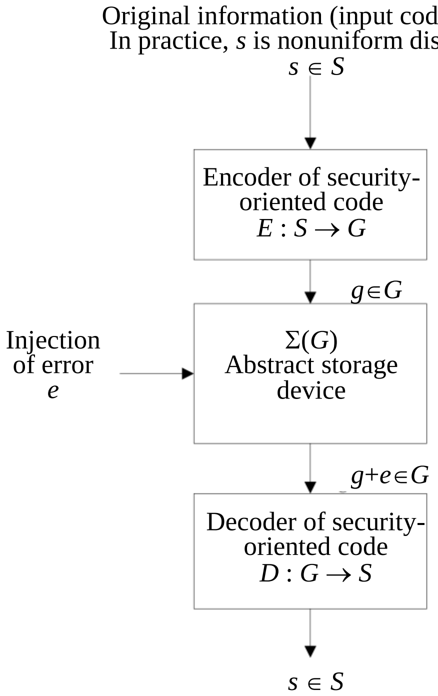
Original information (input codewords).
In practice, s is nonuniform distributed
$s \in S$
Encoder of security-oriented code
$E: S \to G$
$g \in G$
Injection of error
e
$\Sigma(G)$
Abstract storage device
$g+e \in G$
Decoder of security-oriented code
$D: G \to S$
$s \in S$

Figure 1. Model of algebraic manipulation and protection scheme based on AMD code

In the paper [11] Cramer et al. presents two types of injection attack: weak and strong. In weak attack, the adversary cannot choose the inputs. So, from the adversary's point of view the source s is uniformly distributed and the attacker only can inject any specific error pattern e in the storage device $\sum(G)$, but he cannot change value s at his own discretion.

In case of strong attack, the adversary can influence the outputs by choosing the inputs. In this case the adversary knows the value $s \in S$ and, moreover, he can choose it himself. In both types of fault injection attacks the value g stored in $\sum(G)$ is hidden from the attacker.

Definition 1 [11]. *Let m and n be two positive integers. An (m,n) AMD code is a pair of a probabilistic encoding functions $E: S \to G$ from a set S of size m into a finite Abelian group G of order n, and a deterministic decoding function $D: G \to S \cup \{\perp\}$ such that $D(E(s)) = s$ with probability 1 for every $s \in S$, where $\perp$ denotes combinations which are not included in the code.*

An AMD code is called "systematic" if set S is a group and the encoding function E has the form

$E: S \to S \times G_1 \times G_2$

$s \to (s, t, F(t,s))$,

for a function F, with t being randomly chosen with uniform probability in G_1.

Definition 2 [11]. *An AMD code is called weak ε-secure, $\varepsilon > 0$ if, for every s chosen at random from S and for every $e \in G$ sampled from G according to some distribution independent of s and $E(s)$, the probability that $D(E(s)+e) \notin \{s, \perp\}$ is at most ε.*

So in the system with an AMD code, when the decoding function gives the correct value s with probability $1-\varepsilon$ or the special symbol $\perp$, it means that algebraic manipulation has been detected.

Definition 3 [11]. *An AMD code is called strong ε-secure for $\varepsilon > 0$ if, for every $s \in S$ sampled at random from S and for every $e \in G$ sampled from G according to some distribution independent of $E(s)$, the probability that $D(E(s)+e) \notin \{s, \perp\}$ is at most ε.*

Before Cramer's work, in the works written by Mark Karpovsky et al [1, 13] the notion of *robust code* was presented, which is related to deterministic weak AMD code:

Definition 4 [6]. A code $C \in GF(2^n)$ is R-robust if the size of the intersection of the code C and any of its translates $\overline{C} = \{\overline{g} \mid \overline{g} = g + e, g \in C\}, e \in GF(2^n), e \neq 0$ is upper bounded by R:

$R = \max_{0 \neq GF(2^n)} |\{g | g \in C, g + e \in C\}|$

where $+$ is the componentwise addition modular two. A binary R-robust code C of length n with $M = card(C)$ is denoted by a triple (n, M, R) (Figure 2).

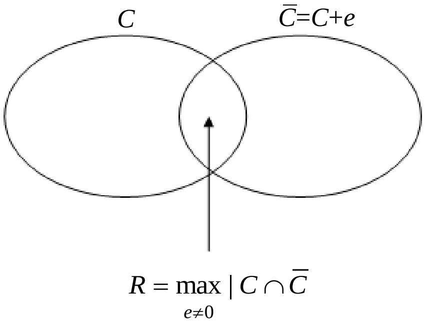

Figure 2. Definition of robust code

The code (which is not necessarily linear) is supposed systematic: there exists a subset I of positions in codewords, called an *information set* of C, such that every possible tuple of length $|I|$ occurs in exactly one codeword within the specified coordinates x_i: $i \in I$. The code equals then, up to a permutation of the codeword coordinates: $\{(s, F(s)); s \in S\}$ where S is a subgroup of G, for some (non necessarily linear) function F, and the encoding function $E: S \to G$ is then $E(s) = (s, F(s))$.

The probability of missing an algebraic manipulation ε with such a robust code equals the so-called probability of error masking, which is denoted $Q(e)$ and is defined as:

$Q(e) = \frac{card\ (C \cap (e+C))}{card\ (C)}$.

The maximum probability of error masking $\max_{e \neq 0} Q(e)$ is directly related to the robustness order of code $\max_{e \neq 0} Q(e) = \frac{R}{card\ (C)}$.

Weak AMD codes must provide the detection of algebraic manipulation with security parameter ε for the set of errors $(0 \neq e_s, e_x, e_f)$, on condition that the information part contains an error $e_s \neq 0$. Thus, the weak AMD codes are not tested for the set of errors with zero information part $(0 = e_s, e_x, e_f)$. Mark Karpovsky in [14] writes that $e_s \neq 0$ is a necessary condition for successful algebraic manipulation. However, for secure architectures, the integrity of redundant bits of codes is also important. For example, errors $(e_s, e_f = 0)$ have a high probability of error masking for some multilinear arithmetic codes [15]. Thus, it is necessary to perform analysis for the whole set of errors, not just for errors in the information part. Strong AMD codes must consider the case when the adversary injects errors, but does not alter the value s, as successful algebraic manipulation. That is, in strong AMD codes, injection of errors in redundancy part (and also in random part) of codeword g must be detected with probability that $D(E(s) + e) \notin \{\perp\}$ bounded above by ε. Examples of strong AMD codes are given in [16] Section 3 and [11] Section 6.

In this section, the main definitions of the AMD code theory are presented. The main characteristics of these structures are outlined.

Robustness and max *Q*(*e*) for perfect nonlinear functions

In the late 1980s the importance of highly nonlinear functions in cryptography was first discovered by Meier and Staffelbach from the point of view of correlation attacks on stream ciphers, and later by Nyberg in the early 1990s after the introduction of the differential cryptanalysis method. Perfect nonlinear (PN) and almost perfect nonlinear (APN) functions, which have the optimal properties for offering resistance against differential cryptanalysis, have since then been an object of intensive study by many mathematicians.

Perfect nonlinear functions play an important role in robust codes or deterministic weak algebraic manipulation detection codes also. The best possible codes which have maximum possible number of codewords for a given length and robustness are optimum robust codes which have perfect nonlinear encoding function.

Proposition. *Let* $C = \{(x, F(x)), x \in \mathbb{F}_2^k\}$, *where* F *is a vectorial function from* $\mathbb{F}_2^k$ *to* $\mathbb{F}_2^r$, *with* k *and* r *non-negative. Then C is optimum robust if and only if F is perfect nonlinear.*

In the case of weak model of algebraic manipulation, the robustness R and the error masking probability $Q(e)$ are defined by the encoding function F. In particular, under uniform distribution of input codeword, the error masking probability of a code based on a PN function $Q(e)$ is bounded above by $1/2^r$. Indeed, denoting

$e = (a, b)$, we have

$$card\ (C \cap (e + C)) = card\left(\left\{(x, y) \in (\mathbb{F}_2^k)^2;\ \begin{cases} x = y + a \\ F(x) = F(y) + b \end{cases}\right\}\right).$$

For every $a \neq 0$, this size equals 2^{k-r} by the definition of PN functions, and for $a = 0, b \neq 0$ it is null. Since C has size 2^k, this gives $\max_{e\neq 0} Q(e) = \frac{card\ (C\cap(e+C))}{card\ (C)} = \frac{2^{k-r}}{2^k} = 2^{-r}$.

Example 1. Let us consider the distribution of error masking probability of the systematic code with codewords $(x, y, xy), x, y \in \mathbb{F}_{2^r}$ based on the PN function $F(x, y) = xy$ with $r = 2$.

The error vector is $e = (e_x, e_y, e_F) \neq (0,0,0)$, and we have $C \cap (e + C) = \{(x, y, xy); (x + e_x)(y + e_y) = xy + e_F\} = \{(x, y, xy); e_y x + e_x y = e_x e_y + e_F\}$, and the error masking probability equals to 2^{-2} if $(e_x, e_y) \neq (0,0)$, whatever is e_F, and 0 if $(e_x, e_y) = (0,0)$ since then we have $e_F \neq 0$. Triples (e_x, e_y, e_F) are represented by the decimal numbers whose binary expansions are equal to these triples.

There are three errors $\{e_x = 0, e_y = 0, e_F \neq 0\}$ that are always detected by above described code ($Q(e) = 0$). Indeed, these errors are: $e_x = 00, e_y = 00, e_F = 01; e_x = 00, e_y = 00, e_F = 10; e_x = 00, e_y = 00, e_F = 11$.

This section shows the relationship between the nonlinearity of the coding function and the reliability of the code. Also the part explains why, for uniform distribution, the max $Q(e)$ is bounded above by $1/2^r$.

PN functions under different nonuniform distribution of input codewords

Robust codes do not provide protection against the strong model of algebraic manipulation. If there is a dependence between the data entered in the device and the manipulation, such that the distortion takes the value of the difference between a current codeword and any other one, then this distortion cannot be detected with a high probability.

Example 2. Let the distribution of the input codewords be nonuniform. Assume, there is a function $\phi(s)$ that determines the probability of occurrence of a given information message $s \in S$ at the input of abstract storage device $\sum (G)$ described above. Then, the error masking probability under nonuniform distribution of the outputs for given code C equals $Q(e) = \sum_{g+e\in C} \phi(s)$ [8], where g is the codeword corresponding to input information s (we have $g \in C$ by construction). For simplicity of reading, all binary vectors will be represented as integers. For instance, the distribution of error masking probability of optimum robust code $(x, y, xy), x, y \in \mathbb{F}_{2^2}$ under nonuniform distribution $\phi(s) = \begin{cases} 0.25, for\ s \in [8; 9] \\ 0.15, for\ s \in [7; 10] \\ 0.05, for\ s \in [6; 11] \\ 0.01,\ otherwise \end{cases}$ is shown in Figure 3, $s = (x|y)$ (since r is still equal to 2, s is a vector of length 4), where | denotes concatenation, and integers in brackets denote integer representation of binary word s. For instance, the entry $0.25, for\ s \in [8; 9]$ means that the probability that $s = (1,0,0,0)$ (resp. $s = (1,0,0,1)$) equals to 0.25.

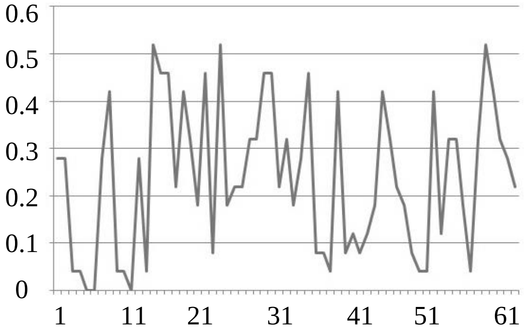

Figure 3. Distribution of error masking probability for code $(x, y, xy), x, y \in \mathbb{F}_{2^2}$ under nonuniform distribution. Ordinate is error masking probability for each possible error. Abscissa is decimal representation of error vectors

The set of errors $\{e_x = 0, e_y = 0, e_F \neq 0\}$ that are always detected (i.e. such that $Q(e) = 0$) by code is unchanged. The maximum of error masking probability drastically increases from 0.25 to 0.52, and we know that injection of errors with the high masking probability are dangerous for protected device. Moreover, optimum robust code under nonuniform distribution of input codeword already does not provide equal probabilities of detection for all possible errors.

To protect against strong algebraic manipulation, it is necessary to get rid of deterministic encoding procedures [15, 5]. For deterministic encoding functions, there is one correspondence between the input values s and codeword $g = (s, F(s))$. Therefore, the probability of occurrence of input values has a direct impact on the codewords. That is, if the probability of occurrence of the input value $p(s_1)$ equals to 0.8, then the probability of a corresponding codeword $p(g_1)$ is also equal to 0.8. So, deterministic encoding functions do not prevent the analysis of code for searching a high probability of error masking.

For providing randomness, the encoding process can be performed with the help of a random variable x that is independent of the input data s. For such *stochastic* encoding, each input value s corresponds to the set of codewords $g = \{(s, t_1, F(t_1, s)), \dots, (s, t_i, F(t_i, s))\}$, where i depends on the length of the random part t. Thus, even for the same input values, the output may be different. One input value corresponds to a few codewords; each one has its own set of errors with high probability masking. Indeed, to calculate the probability of error masking $Q(e)$ for all e, we need to count all sum $g + e$ for all errors e and for all codewords g. Thus, the maximum value of $Q(e)$ corresponds to several codewords g' such that $\{(C \cap (e + C)), e + C = \{e + g', g' \in C\}\}$ is performed. For a deterministic function, attacker can select one of these codewords g', and find the corresponding input value s'. Inputting the value s' and the simultaneous introduction of error e can compromise the encoding device. In the stochastic coding, input of values s' does not guarantee that we will get the required codeword g'.

Let us consider the codes $C_1 = \{(s, F(s)), s \in \mathbb{F}_2^k\}$ and $C_2 = \{(s, t, F(t, s)), s \in \mathbb{F}_2^k, t \in_R \mathbb{F}_2^m\}$ (with $F(s) \in \mathbb{F}_2^r, F(t, s) \in \mathbb{F}_2^r$), under some nonuniform distribution $\phi(s)$. For deterministic version C_1, the probability of codeword occurrence of g equals to $\phi(s)$. For stochastic version C_2, the probability of codeword occurrence of g equals to $\phi(s)2^m$. For analysing all possible combinations, the attacker can either control the random number generator (RNG) in the encoding device or have the ability to send the input s to the device until all combinations have been received. Thus, the attacker is able to compute a set of possible codewords (s, t), but not the encoded version of input s.

The computational complexity of the probabilistic encoding function for AMD codes depends on both the complexity of obtaining the random part t and the complexity of encoding function $F(t, s)$. In cryptographic applications and devices, the random part x can be generated by a RNG, that is already used in most of the modern cryptographic devices. In any case the probabilistic AMD codes have higher computational complexity than the robust codes (deterministic AMD codes). If there are problems with the generation of random values or if the computation power is not sufficient, it is preferable to use robust codes. But robust codes are poorly investigated in the case of nonuniformly distributed input s. This paper investigates the behavior of PN functions under non-uniform input different distribution.

The paper compares the following power PN functions:

1. $F(x, y) = xy$ and $F(x, y) = xy^{-1}$ where $x, y \in \mathbb{F}_{2^r}$ (for $r = 2,3,4,5$);
2. $F(x, y) = xy^3$ and $F(x, y) = xy^{-3}$ where $x, y \in \mathbb{F}_{2^r}$ (for $r = 3,5$).

For given values r, max $Q(e)$ is measured for all possible irreducible polynomials. Used polynomial is given in description of table with corresponding measurements.

Comparison of PN functions for r=2

We compared the functions already discussed earlier: xy and xy^{-1}, where $x, y \in \mathbb{F}_{2^r}$ are two parts of information of equal length r. These two functions have the same value of robustness and the maximum of error masking probability. Indeed, both encoding functions are perfect nonlinear functions, hence $\max_{e \neq 0} Q(e) = 1/2^r$. Comparison of the functions $F(x, y) = xy$ and $F(x, y) = xy^{-1}$ for various distributions and value $r = 2$ is shown in Table 1.

Distribution	xy	xy^{-1}
Uniform distribution	0.25	0.25
Bernouilli distribution	0.5598	0.5598
$\phi_1(g) = \begin{cases} 0.1, & for\ g \in [4; 9] \\ 0.04, & otherwise \end{cases}$	0.4	0.4
$\phi_2(g) = \begin{cases} 0.25, & for\ g \in [8; 9] \\ 0.15, & for\ g \in [7; 10] \\ 0.05, & for\ g \in [6; 11] \\ 0.01, & otherwise \end{cases}$	0.52	0.52

Table 1. Comparison of the error masking probability for the functions $F(x, y) = xy$ and $F(x, y) = xy^{-1}$ for value $r = 2$ over irreducible polynomial $x^2 + x + 1$. g denotes the codeword of code and $\phi(g)$ probability of codeword occurrence

In the case of a uniform distribution, the probability of codeword occurrence is the same for every input, or, in other words, $\phi(g_1) = \phi(g_2) = \ldots = \phi(g_{2^{2r}})$.

Bernouilli distribution of parameter $p \in [0; 1]$ that is:

$\phi(g) = \prod_{i=1}^{k} p^{g_i}(1 - p)^{1 - g_i}$.

There is no difference between codes based on these functions. For $r = 2$ most codewords in both codes coincide. These two codes are different in 6 codewords.

The difference between codes will be more explicit if we explore the functions for higher value of r, for example 4 and 5, but then a huge number of comparisons is needed for each codes (for example, for $r = 4$, the number of codewords is 2^8, the error space is 2^{12}).

Comparing the behavior of PN functions for r=3 under two irreducible polynomials

For comparison, the following PN functions have been chosen: $F(x,y) = xy$, $F(x,y) = xy^{-1}$, $F(x,y) = xy^3$, $F(x,y) = xy^{-3}$, where $x, y \in \mathbb{F}_{2^r}$ are information parts of length equal to r (supposed odd in the case of the two last functions so that $y \to y^3$ is bijective that is a necessary and sufficient condition for $F(x,y) = xy^3$ and $F(x,y) = xy^{-3}$ to be PN). We checked that for other choices of irreducible polynomials the maximum of error masking probability has not changed essentially. If we compare the max $Q(e)$ over irreducible polynomial $x^3 + x^2 + 1$ and $x^3 + x + 1$ it is seen that the differences are small. Table 2 presents the values for the same functions but for irreducible polynomial $x^3 + x^2 + 1$ (probability distributions of error masking $Q(e)$ are different, but the maximum value of $Q(e)$ remains unchanged in most cases).

Distribution $\boldsymbol{\phi(s), s = (x,y)}$	$\boldsymbol{xy}$	$\boldsymbol{xy^{-1} = xy^6}$	$\boldsymbol{xy^3}$	$\boldsymbol{xy^{-3}}$
Uniform distribution	0.0125	0.0125	0.0125	0.0125
Bernouilli distribution	0.5197	0.4631	0.4947	0.4189
$\phi_1(g) = \begin{cases} 0.84, & for\ g \in [31;34] \\ 0.260, & otherwise \end{cases}$	0.42	0.6166	0.6166	0.42
$\phi_2(g) = \begin{cases} 0.730, & for\ g \in [16;45] \\ 0.334, & otherwise \end{cases}$	0.1866	0.1721	0.1721	0.1866
$\phi_3(g) = \begin{cases} 0.144, & forg \in [1;44] \\ 0.920, & otherwise \end{cases}$	0.36	0.2745	0.2745	0.36
$\phi_4(g) = \begin{cases} 0.115, & for\ g \in [1;15] \\ 0.415, & for\ g \in [16;30] \\ 0.215, & forg \in [31;45] \\ 0.319, & otherwise \end{cases}$	0.2133	0.1824	0.1824	0.2133

Table 2. Comparison of maximum error masking probability for the functions $F(x,y) = xy$, $F(x,y) = xy^{-1}$, $F(x,y) = xy^3$ and $F(x,y) = xy^{-3}$ for value $r = 3$ over irreducible polynomial $x^3 + x + 1$

Measurements of the masking probability over irreducible polynomial $x^3 + x^2 + 1$ for distributions $\phi_1(g), \phi_2(g), \phi_3(g), \phi_4(g)$ yield results that coincide with a deviation of 0.05 with results in Table 2.

For $r = 3$, $xy^{-1} = xy^6$ is linearly equivalent to xy^3. It is interesting to see that with some distributions, two equivalent PN functions give the same error masking probability and with the others it can give different ones. However, polynomials $x^3 + x + 1$ and $x^3 + x^2 + 1$ are reciprocal of each other and they are the only primitive polynomials for $r = 3$.

For most distributions, the maximum values of the function $F(x,y) = xy^{-1}$ and $F(x,y) = xy^3$ are close to each other (disributions $\phi_2(g)$, $\phi_3(g)$, $\phi_4(g)$). If we look at the distribution of $Q(e)$ for function $F(x,y) = xy^{-1}$ and $F(x,y) = xy^3$ (Figure 4), we can see that distribution does not coincide fully. However, as shown in Figure 4, we can select error classes with the same values of error masking probability for both functions.

However, for distribution of input codewords $\phi_1(g) = \begin{cases} 0.84, & for\ g \in [31;34] \\ 0.260, & otherwise \end{cases}$, the maximum of error masking probability has a high value for function $F(x,y) = xy^{-1}$ (Figure 5). In comparison with the other encoding functions, $\max_{e \neq 0} Q(e)$ for function $F(x,y) = xy^{-1}$ under distribution ϕ_1 is very high, therefore using of this function under distribution ϕ_1 is undesirable.

The nonuniform distributions of input codeword can lead to jumps in the probability distribution of the error masking $Q(e)$. Figure 6 represents the case of correlation between the input distribution and injected error that give rise in error masking probability distribution. For example, we can see an error with a decimal representation 84 in Figure 6 or, in other words, the error with maximal $Q(e)$ for the distribution of $\phi_5(g)$ and an irreducible polynomial 100101.

Behavior of the error masking probability for encoding functions $F(x,y) = xy$ and $F(x,y) = xy^{-3}$ is also largely the same. As shown in Table 2 for these functions the maximums of error masking probability for all distributions except the Bernouilli coincide. Distribution of $Q(e)$ are different, but as in the case of functions $F(x,y) = xy^{-1}$ and $F(x,y) = xy^3$, there are set of errors with the same $Q(e)$.

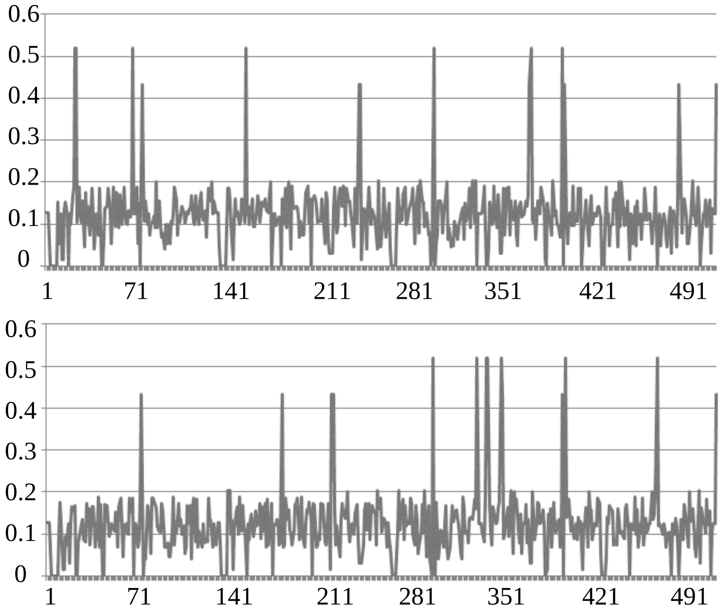

Figure 4. Distribution of error masking probability for encoding functions $F(x, y) = xy$ modulo $x^3 + x + 1$ (top graphic) and $F(x, y) = xy$ modulo $x^3 + x^2 + 1$ (lower graphic) under Bernoilli distribution. Ordinate is error masking probability for each possible error. Abscissa is decimal representation of error vectors

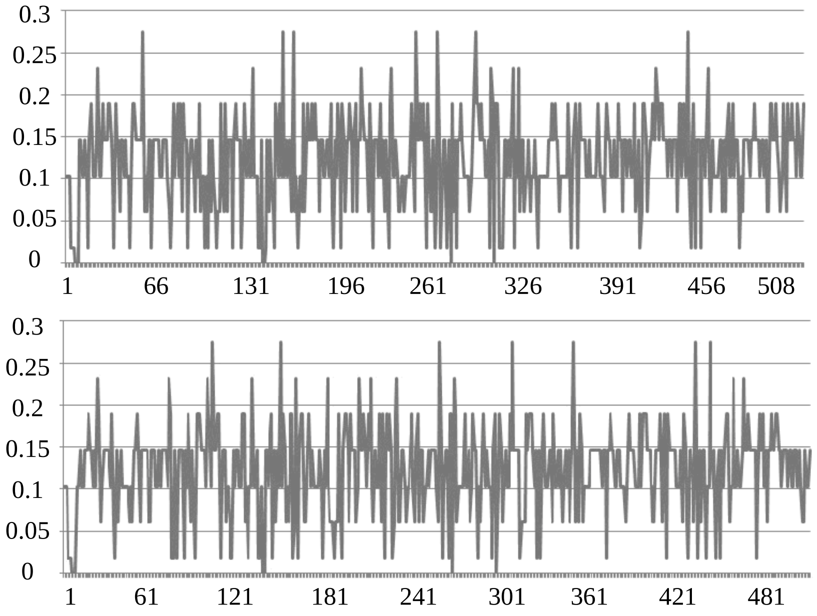

Figure 5. Distribution of error masking probability for encoding functions $F(x, y) = xy^{-1}$ (top graphic) and $F(x, y) = xy^3$ (lower graphic) under distribution $\phi_3(g)$. Ordinate is error masking probability for each possible error. Abscissa is decimal representation of error vectors

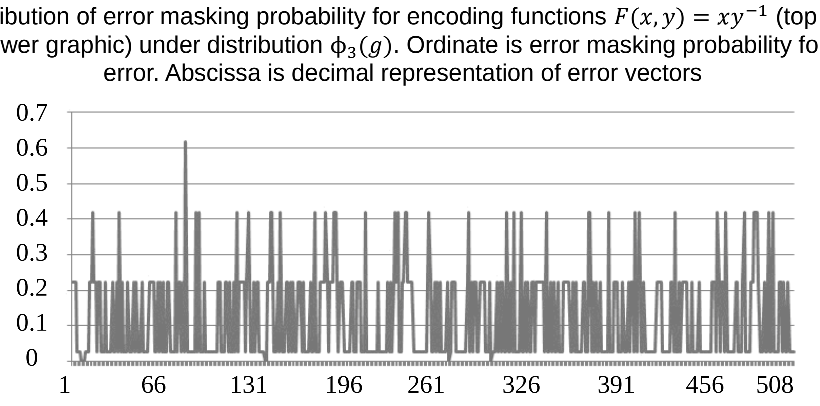

Figure 6. Distribution of error masking probability for encoding function $F(x, y) = xy^{-1}$ under nonuniform distribution $\phi_1(g)$. Ordinate is an error masking probability for each possible error. Abscissa is a decimal representation of error vectors

Comparison of PN functions for r=4 over two irreducible polynomials

Comparison of the functions $F(x,y)=xy$ and $F(x,y)=xy^{-1}$ for various distribution and value $r=4$ is shown in Table 3.

Distribution	$\boldsymbol{xy}$	$\boldsymbol{xy^{-1}}$
Uniform distribution	0.0625	0.0625
Bernoilli distribution	0.4987	0.2227
$\phi_1(g)=\begin{cases}0.856, & for\ g\in[51;106]\\ 0.2200, & otherwise\end{cases}$	0.2285	0.1222
$\phi_2(g)=\begin{cases}0.7100, & for\ g\in[101;200]\\ 0.3156, & otherwise\end{cases}$	0.112	0.0917
$\phi_3(g)=\begin{cases}0.1150, & for\ g\in[1;150]\\ 0.9106, & otherwise\end{cases}$	0.1358	0.1045
$\phi_4(g)=\begin{cases}0.930, & for\ g\in[101;130]\\ 0.1226, & otherwise\end{cases}$	0.48	0.1844

Table 3. Comparison of the error masking probability for the functions $F(x,y)=xy$ and $F(x,y)=xy^{-1}$ for value $r=4$ over irreducible polynomial x^4+x^3+1. g denotes the codeword of code and $\phi(g)$ probability of codeword occurrence

From Table 3 we can see that function $F(x,y)=xy$ has a lower error masking probability for all distributions.

Comparison of PN functions for r=5 over six irreducible polynomials

We have chosen one function with $r=5$ and tried all primitive polynomials in Table 4.

Distribution $\boldsymbol{\phi(s), s=(x,y)}$	**100101**	**101001**	**111101**	**101111**	**110111**
$\phi_1(g)=\begin{cases}\frac{1}{252}, w_H(s)=\ 5\\ 0, \quad otherwise\end{cases}$	0.05952	0.05952	0.051587	0.05556	0.05556
$\phi_2(g)=\begin{cases}1/120, w_H(s)=\ 3\\ 0, \quad otherwise\end{cases}$	0.08333	0.08333	0.08333	0.08333	0.08333
Bernouilli distribution	0.4880	0.4880	0.4880	0.4880	0.4880
$\phi_4(g)=\begin{cases}0.824, g\in[501;525]\\ 0.21000, \quad otherwise\end{cases}$	0.43713	0.43713	0.43713	0.43713	0.43713
$\phi_5(g)=\begin{cases}0.6424, g\in[301;725]\\ 0.4600, \quad otherwise\end{cases}$	0.04528	0.04528	0.04528	0.04528	0.04528

Table 4. Comparison of maximum error masking probability for the functions $F(x,y)=xy$ for value $r=5$ over all irreducible polynomial in $GF(2^5)$. Number of vector with hamming weight 5 in $GF(2^{10})$ equal to 252. $s=(x,y)$ is information part of codeword $g=(s,F(s))$. The denotion $w_H(s)$ means the Hamming weight of vector s

Distribution $\boldsymbol{\phi(s), s=(x,y)}$	**100101**	**101001**	**111101**	**101111**	**110111**	**111011**
$\phi_1(g)=\begin{cases}1/252, w_H(s)=5\\ 0, \quad otherwise\end{cases}$	0.06746	0.06746	0.05952	0.05556	0.05952	0.05952
$\phi_2(g)=\begin{cases}1/120, w_H(s)=\ 3\\ 0, \quad otherwise\end{cases}$	0.09167	0.09167	0.08333	0.08333	0.08333	0.08333
Bernouilli distribution	–	–	–	–	–	–
$\phi_4(g)=\begin{cases}0.824, g\in[501;525]\\ 0.21000, \quad otherwise\end{cases}$	0.17207	0.17207	0.17207	0.20520	0.17207	0.17207
$\phi_5(g)=\begin{cases}0.6424, g\in[301;725]\\ 0.4600, \quad otherwise\end{cases}$	0.03630	0.17207	0.03630	0.03630	0.03630	0.03630

Table 5. Comparison of maximum error masking probability for the functions $F(x,y)=xy^{-1}$ for value $r=5$ over all irreducible polynomial in $GF(2^5)$. Number of vector with hamming weight 5 in $GF(2^{10})$ equal to 252. $s=(x,y)$ is information part of codeword $g=(s,F(s))$. The denotion $w_H(s)$ means the Hamming weight of vector s

In the first line of Table 4, the irreducible polynomial of $GF(2^5)$ is presented. Polynomials are represented via binary coefficients, that is, for example, the 100101 denotes the polynomial x^5+x^2+1. The first column contains the distribution of input distributions $\phi(g)$. We made a simulation with a distribution uniform over some strict subset of $(F_{2^r}^2)$ and null outside, for instance the set of those (x,y) of Hamming weight $r=5$. A number of binary sequences with the length of 10 bits and hamming weight of 5 equals to 252. So, probability of occurrence for vector s with weight 5 equals to $1/252$. Each column presents the irreducible polynomial and corresponding maximum value of error masking probability for each distribution of input codeword.

For distribution $\phi_1(g)$ we get the different values of $\max Q(e)$, however, for another distribution maximum of error masking it does not depend on irreducible polynomial.

Based on the measurement results carried out in this section for codes constructed with the Maorana – McFarland functions, the following conclusions can be drawn:

- Tables 4 and 5 show how the changing of an irreducible polynomial that is used to construct codewords effects on the probability of error masking. From the tables we see that for the same distribution of input codewords, the using of reciprocal irreducible polynomials gives an equal maximum value of the error masking probability. Nonreciprocal irreducible polynomials give the masking probability maximum that is different from the other irreducible polynomials for same input codeword distribution (Values $\max Q(e)$ differ by at most 0.01).
- the set of input codeword distribution, codespace and irreducible polynomial can give jumps in the probability distribution of the error masking $Q(e)$.The examples of jumps can be seen in Figure 6 for error with a decimal representation 84.
- the probability distribution of the error masking given by equivalent codes coincide up to permutations (Figures 4 and 5).
- $\max Q(e)$ for equivalent codespaces are equal for identical irreducible polynomials, for example, the functions xy^{-1} and xy^3 or xy and xy^{-3} in Tables 2 and 3.

Conclusion

AMD codes based on PN functions are considered as the object of research. AMD codes present a new method of ensuring integrity for structural elements of device for processing, storing and transferring information, such as cache memory, RAM, logic and arithmetic elements in circuits. In this work AMD codes based on PN functions were tested for stability, made an overview of changes in the input codeword distribution, irreducible polynomials used to generate code spaces. As a result, cases were identified when it is possible to reduce the stability of code constructions. Such cases are possible if the coding function, the input codeword distribution or irreducible polynomial is changing. These cases should be taken into account when methods of integrity ensuring based on the considered code constructions are designed.

References

1. Karpovsky M.G., Taubin A. New class of nonlinear systematic error detecting codes // IEEE Transactions on Information Theory. 2004. V. 50(8). P. 1818–1820. doi: 10.1109/TIT.2004.831844
2. Karpovsky M.G., Kulikowski K.J, Wang Z., Robust error detection in communication and computational channels // Proc. Int. Workshop on Spectral Methods and Multirate Signal Processing. Citeseer, 2007.
3. Wang Z. , Karpovsky M. New error detecting codes for the design of hardware resistant to strong fault injection attacks // Proc. Int. Conference on Security and Management, *SAM. Las-Vegas, USA*, 2012.
4. Wang Z., Karpovsky M., Kulikowski K.J. Design of memories with concurrent error detection and correction by nonlinear sec-ded codes // Journal of Electronic Testing. 2010. V. 26. N 5. P. 559–580. doi: 10.1007/s10836-010-5168-5
5. Wang Z., Karpovsky M.G. Reliable and secure memories based on algebraic manipulation correction codes // Proc. 2012 IEEE 18th Int. On-Line Testing Symposium. Sitges, Spain, 2012. P. 146–149. doi: 10.1109/IOLTS.2012.6313861
6. Ge S., Wang Z., Luo P., Karpovsky M.G. Secure memories resistant to both random errors and fault injection attacks using nonlinear error correction codes // Proc. 2nd Int. Workshop on Hardware and Architectural Support for Security and Privacy. 2013. Art. 5.
7. Cramer R., Dodis Y., Fehr S., Padro C., Wichs D. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors // Lecture Notes in Computer Science. 2008. V. 4965. P. 471–488. doi: 10.1007/978-3-540-78967-3_27
8. Keren O., Shumsky I., Karpovsky M.G. Robustness of security-oriented binary codes under non-uniform distribution of codewords // Proc. 6th Int. Conf. on Dependability. Barcelona, Spain, 2013. P. 25–30.
9. Levina A., Taranov S. Creation of codes based on wavelet transformation and its application in ADV612 chips //

Литература

1. Karpovsky M.G., Taubin A. New class of nonlinear systematic error detecting codes. *IEEE Transactions on Information Theory*, 2004, vol. 50, no. 8, pp. 1818–1820. doi: 10.1109/TIT.2004.831844
2. Karpovsky M.G., Kulikowski K.J, Wang Z., Robust error detection in communication and computational channels. *Proc. Int. Workshop on Spectral Methods and Multirate Signal Processing*. Citeseer, 2007.
3. Wang Z. , Karpovsky M. New error detecting codes for the design of hardware resistant to strong fault injection attacks. *Proc. Int. Conference on Security and Management*, *SAM*. Las-Vegas, USA, 2012.
4. Wang Z., Karpovsky M., Kulikowski K.J. Design of memories with concurrent error detection and correction by nonlinear sec-ded codes. *Journal of Electronic Testing*, 2010, vol. 26, no. 5, pp. 559–580. doi: 10.1007/s10836-010-5168-5
5. Wang Z., Karpovsky M.G. Reliable and secure memories based on algebraic manipulation correction codes. *Proc. 2012 IEEE 18th Int. On-Line Testing Symposium*. Sitges, Spain, 2012, pp. 146–149. doi: 10.1109/IOLTS.2012.6313861
6. Ge S., Wang Z., Luo P., Karpovsky M.G. Secure memories resistant to both random errors and fault injection attacks using nonlinear error correction codes. *Proc. 2nd Int. Workshop on Hardware and Architectural Support for Security and Privacy*, 2013, art. 5.
7. Cramer R., Dodis Y., Fehr S., Padro C., Wichs D. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. *Lecture Notes in Computer Science*, 2008, vol. 4965, pp. 471–488. doi: 10.1007/978-3-540-78967-3_27
8. Keren O., Shumsky I., Karpovsky M.G. Robustness of security-oriented binary codes under non-uniform distribution of codewords. *Proc. 6th Int. Conf. on Dependability*. Barcelona, Spain, 2013, pp. 25–30.
9. Levina A., Taranov S. Creation of codes based on wavelet transformation and its application in ADV612 chips.

International Journal of Wavelets, Multiresolution and Information Processing. 2017. V. 15. N 2. P. 1750014. doi: 10.1142/S021969131750014X

10. Levina A., Taranov S. Spline-wavelet robust code under non-uniform codeword distribution // Proc. 3rd Int. Conf. on Computer, Communication, Control and Information Technology, C3IT 2015. Hooghly, India, 2015. Art. 7060125. doi: 10.1109/C3IT.2015.7060125
11. Cramer R., Fehr S., Padro C. Algebraic manipulation detection codes // Science China Mathematics. 2013. V. 56. N 7. P. 1349–1358. doi: 10.1007/s11425-013-4654-5
12. Nyberg K. Perfect non-linear s-boxes // Lecture Notes in Computer Science. 1992. V. 547. P. 378–386.
13. Kulikowski K.J., Karpovsky M.G., Taubin A. Robust codes and robust, fault-tolerant architectures of the advanced encryption standard // Journal of Systems Architecture. 2007. V. 53. N 2-3. P. 139–149. doi: 10.1016/j.sysarc.2006.09.007
14. Karpovsky M.G., Kulikowski K.J., Wang Z. On-line self error detection with equal protection against all errors // International Journal of Highly Reliable Electronic System Design. 2008.
15. Karpovsky M.G., Wang Z. Design of strongly secure communication and computation channels by nonlinear error detecting codes // IEEE Transactions on Computers. 2014. V. 63. N 11. P. 2716–2728. doi: 10.1109/TC.2013.146
16. Sunar B., Wang Z., Karpovsky M.G., Joshi A. Design of reliable and secure multipliers by multilinear arithmetic codes // Lecture Notes in Computer Science. 2009. V. 5927. P. 47–62. doi: 10.1007/978-3-642-11145-7_6

International Journal of Wavelets, Multiresolution and Information Processing, 2017, vol. 15, no. 2, pp. 1750014. doi: 10.1142/S021969131750014X

10. Levina A., Taranov S. Spline-wavelet robust code under non-uniform codeword distribution. *Proc. 3rd Int. Conf. on Computer, Communication, Control and Information Technology, C3IT 2015*. Hooghly, India, 2015, art. 7060125. doi: 10.1109/C3IT.2015.7060125
11. Cramer R., Fehr S., Padro C. Algebraic manipulation detection codes. *Science China Mathematics*, 2013, vol. 56, no. 7, pp. 1349–1358. doi: 10.1007/s11425-013-4654-5
12. Nyberg K. Perfect non-linear s-boxes. *Lecture Notes in Computer Science*, 1992, vol. 547, pp. 378–386.
13. Kulikowski K.J., Karpovsky M.G., Taubin A. Robust codes and robust, fault-tolerant architectures of the advanced encryption standard. *Journal of Systems Architecture*, 2007, vol. 53, no. 2-3, pp. 139–149. doi: 10.1016/j.sysarc.2006.09.007
14. Karpovsky M.G., Kulikowski K.J., Wang Z. On-line self error detection with equal protection against all errors. *International Journal of Highly Reliable Electronic System Design*, 2008.
15. Karpovsky M.G., Wang Z. Design of strongly secure communication and computation channels by nonlinear error detecting codes. *IEEE Transactions on Computers*, 2014, vol. 63, no. 11, pp. 2716–2728. doi: 10.1109/TC.2013.146
16. Sunar B., Wang Z., Karpovsky M.G., Joshi A. Design of reliable and secure multipliers by multilinear arithmetic codes. *Lecture Notes in Computer Science*, 2009, vol. 5927, pp. 47–62. doi: 10.1007/978-3-642-11145-7_6

Authors

Claude Carlet – Full professor, University of Paris 8, Paris, 93526, France, claude.carlet@gmail.com

Alla B. Levina – PhD, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, levina@cit.ifmo.ru

Sergey V. Taranov – Assistant, ITMO University, Saint Petersburg, 197101, Russian Federation, serg.tvc@mail.ru

Авторы

Карлет Клод – профессор, профессор, University of Paris 8, Париж, 93526, Франция, claude.carlet@gmail.com

Левина Алла Борисовна – кандидат физико-математических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, levina@cit.ifmo.ru

Таранов Сергей Владимирович – ассистент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, serg.tvc@mail.ru