New Construction of Algebraic Manipulation Detection Codes Based on Wavelet Transform

Alla Levina, Sergey Taranov
ITMO University
St.Petersburg, Russia
{alla_levina, serg.tvc}@mail.ru

***Abstract*—This article presents the new construction of security-oriented codes that provides protection of device against algebraic manipulations. New construction of algebraic manipulation detection codes based on wavelet decomposition. The proposed error-detecting schemes can significantly improves the reliability of storage systems and channels of information transmission. The presented code constructions provides a significant gain in the systems that are already has wavelet transformation. In these systems the coefficients of scaling functions are already calculated and it can be used in the proposed constructions, it gives the gain in rate of information processing and have lower maximum of error masking probability.**

I. Introduction

In case of nonuniform input codeword distribution, classical error detecting codes do not ensure protection against error injection attacks, so in our case we try protect information systems in case of nonuniform input codeword distribution. The attacker can inject any configuration of errors and can inject errors that can not be detected by classical linear and nonlinear codes. For example, for linear codes such dangerous errors are errors that equal to codeword of the linear code. Injection of such error became possible with very high development of side channel attacks, examples of such attacks can be found in the articles [1, 2, 3]. In the [4], M.G. Karpovsky proves that the linear codes are not suited for the protection of information systems against this type of attacks, because they have a high percentage of masking errors, so for protection against of side channel attacks, it is used the codes detecting algebraic manipulations or AMD codes.

Algebraic manipulation detection code is a new class of security-oriented codes that detects any configuration of errors in case of nonuniform input codeword distribution. Codes detecting algebraic manipulations was developed by both R. Cramer [5] and M.G. Karpovsky [6]. AMD codes allow to detect any errors configuration with given probability, moreover this type of code is capable to detect an error in case of nonuniform input codewords distribution.

Mostly all encoding functions of existing security-oriented codes have a high computational complexity. A large number of multiplication operations and the use of random number generators leads to a low rate of encoding that is critical at present time. This article presents the two construction of *weak* AMD codes that are based on wavelet decomposition. The proposed constructions have a relatively higher rate of coding in the systems with uses wavelet coefficients. At the same time security parameters, such as the error masking probability and the number of undetectable errors are not reduce. In this article will be shown characteristic comparison of the proposed construction and existing AMD codes.

II. Wavelet transform

The wavelet transform is widely used for signal compressing, processing and image analysis. This type of transformation has all advantages of the Fourier transform, and moreover wavelet basis are localized in time that allows to analysis a signal in interested levels of decomposition. The idea of the discrete wavelet transform is to divide the signal $s(t)$ into two components: approximating $A_m(t)$ and detailing $D_m(t)$

$$S(t) = A_m(t) + \sum_{i=1}^{m} D_i(t), \tag{1}$$

where m denotes a certain scale or decomposition (reconstruction) level of signal $s(t)$. This separation allows to delete the noise from signal or to compress the information. Wavelet transform has the relative complexity compared with the Fourier transform, but the using of the so-called fast wavelet transformation simplifies the process of decomposition. Proofs for the above properties can be found in the manual of wavelet transform, M.N. Yudin [7].

The idea of wavelet transform bases on the notion of multiresolution analysis. The multiresolution analysis are description of $L^2(R)$ via hierarchically nested spaces:

$$\cdots \subset V_2 \subset V_1 \subset V_0 \subset V_{-1} \subset V_{-2} \subset \cdots,$$

Given spaces satisfy the following conditions:

1) $\cap_{m\in\mathbf{Z}} V_m = 0$,

2) $\cup_{m\in\mathbf{Z}} V_m = L^2(R)$,

3) the function and its compressed version must belong to the space V_{m-1}:

$$s(t) \in V_m \Leftrightarrow s(2t) \in V_{m-1},$$

In this article, the first level of wavelet decomposition is used. So the scale m in the formula (1) takes the value 1. Hence, the formula (1) can be represent as

$$s(t) = A_1(t) + D_1(t).$$

It is possible to calculate the approximations of function $s(t)$ in spaces V_1 and W_1, where W_1 is orthogonal complements of the subspace V_1 in V_0. The presentation of wavelet transformation via the wavelet ψ and scaling ϕ functions has the form

$$s(t) = \sum_k a_{1k}\phi_{1k}(t) + \sum_k d_{1k}(t)\psi_{1k},$$

where a_{1k} and d_{1k} are approximating and detailing coefficients, k is a shift relative to original basis function.

Scaling functions ϕ_{1k} is basis of corresponding space V_1. So approximating and detailing coefficients can be represented as scalar multiplication $a_{1k} = \langle s(t), \phi_{1,k}\rangle$, $d_{1k} = \langle s(t), \psi_{1,k}\rangle$.

As $V_1 \subset V_0$ are nested and $\phi_{1k}(t)$ is orthonormal basis of V_1, so

$$a_{1k} = \sqrt{2}\sum_n a_{0k,n}h_{n+2k},$$

$$d_{1k} = \sqrt{2}\sum_n d_{0k,n}g_{n+2k},$$

where n is a shift equals to the degree of using wavelet. Sequences h_n and g_n called the coefficients of scaling and wavelet function correspondingly.

Denote discrete values of signal $s(t)$ as vector $v^i = \{v_1, v_2, v_3, \cdots, v_N\}$. This vector can be transform to vector v^{i+1} that consist of coefficient a_{1k} and d_{1k}. So, one step of wavelet transform of the sequence v_i can be presented as follow:

$$\begin{bmatrix} a_{1,0} \\ a_{1,1} \\ \vdots \\ a_{1,N/2-1} \\ d_{1,0} \\ d_{1,1} \\ \vdots \\ d_{1,N/2-1} \end{bmatrix} = \begin{bmatrix} h_1 & h_2 & \cdots & h_N \\ h_{N-1} & h_N & \cdots & h_{N-2} \\ \cdots & \cdots & \cdots & \cdots \\ h_3 & h_4 & \cdots & h_2 \\ g_1 & g_2 & \cdots & g_N \\ g_{N-1} & g_N & \cdots & g_{N-2} \\ \cdots & \cdots & \cdots & \cdots \\ g_3 & g_4 & \cdots & g_2 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ \vdots \\ \vdots \\ v_N \end{bmatrix},$$

where $\{h_1, h_2, \cdots, h_N\}$ and $\{g_1, g_2, \cdots, g_N\}$ are coefficients of scaling and wavelet functions.

The main application of codes based on wavelet transform can be the storage, processing and transmission of images and video. The relationship between wavelet transform and error-correcting coding can be represent on the mathematical level. As was described above, the wavelet transform is a partition of signal into two components. Partition can be viewed as a division of the original flow on approximating and detailing components. Thus, the wavelet transform has two main maps $V_{m-1} \to V_m$ and $V_{m-1} \to W_m$ that can be expressed in terms of coefficients of scaling function ϕ and wavelet function ψ. Denote $h_1, ..., h_N$ as the coefficients of scaling functions ϕ and $g_1, ..., g_N$ as coefficients of wavelet function ψ, so wavelet transform can be represented as a set of two cyclic matrices:

$$H = cir_d(h_1, h_2, \cdots, h_N);$$

$$G = cir_d(g_1, g_2, \cdots, g_N),$$

where d is a shift of matrix equals to the order of the used wavelet. This division into two main components can be used in the theory of error-correcting coding. A major class of error-correcting codes are systematic codes in which each codeword is divided into information and redundant parts. One of the basic approach to the construction of wavelet code is using information part of the code as wavelet approximating component $A_m(t)$ and accordingly the redundant parts as detailing component $D_m(t)$. This approach is described in detail in [8, 9].

The wavelet transform can be used for creation of new error detecting codes, including security-oriented codes. In particular, representation of information and random part of AMD code as approximating and detailing components of wavelet transformation allows to get new construction of AMD codes. Detailed algorithms for wavelet AMD codes and investigation of their characteristics will be discussed in the next sections of this article.

III. Model of algebraic manipulation and their application in the security-oriented codes

Let consider notion of algebraic manipulation and AMD codes which are necessary for description of the wavelet AMD code constructions. AMD (Algebraic Manipulation Detection) codes are a generalization of robust codes for the case of algebraic manipulations. Consider the concept of *abstract storage device* $\sum G$ proposed in [5]. Let the device stores an element g from a finite abelian group G. An attacker can not get the value of an element g stored in the device $\sum G$, but he can change the current value by introducing an additive error $\delta \in G$. Such mechanism of error injection is called algebraic manipulation. After the algebraic manipulation, abstract storage device will contain a value $g + \delta$. An attacker can choose the value of $delta$ using only a priori knowledge about the g. AMD code encodes the input data $s \in S$ to the value of $g \in G$ such that the probability of algebraic manipulation was as high as possible. Short description of algebraic manipulation model are presented on Fig. 1.

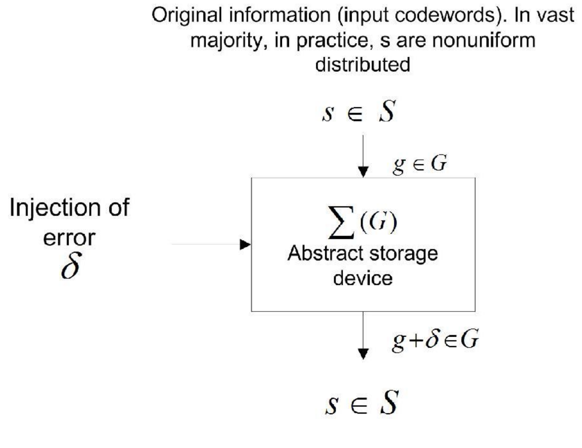

Fig. 1. Model of algebraic manipulation on the example of storage device

In the article [5], R. Cramer et al. allocate *weak* and *strong* models of algebraic manipulation for the abstract storage device $\sum G$. In the case of *weak* model the attacker has no way to choose the input values s. Thus, in this model input values s are uniformly distributed, and the attacker can only introduce some error δ in the device and can not change the value of s on its own discretion.

In the case of *strong model* the attacker can select input values s from the set S or change the occurrence probability of

s. In this case, the attacker knows the current value of $s \in S$, moreover he can select the following input value at its own discretion. In both models, the introduction of the error value g stored in $\sum G$, should be known to the attacker.

Definition 1. Let G is a group of order n, and S is a set of the size m. Then (m, n, ε) AMD code is a combination of the probability encoding function $E : S \to G$ and deterministic decoding function $D : G \to S \cup \perp$, such that $D(E(s)) = s$ with probability 1 for each δ.

1) AMD code is called *strong* if for any $s \in S$ and $\delta \in G$ the probability that $D(E(s) + \delta) \notin \{s, \perp\}$ is ε.

2) AMD code is called *weak* if for every $\delta \in G\{0\}$ and $s \in S$, the probability that $D(E(s) + \delta) \neq \perp$ less than ε.

3) AMD code is called *systematic* if the set S is a group and encoding function E has the following form

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

$$S \to (s, x, f(x, s)),$$

where $f : G_1 S \times G_1 \to G_2$ is a certain function, x is randomly selected from G_1.

Reliability of AMD code is based on the fact that for any $x \in S$ and $\delta \in G$ the probability that the $x + \delta$ does not belong to the allowed codeword combination less than a given threshold ε:

$$Pr[D(E(x) + s) \notin x] \leq \varepsilon.$$

The *strong* AMD codes performs the probabilistic encryption. In probabilistic encoding process, some random sequence are added for achieving a low probability of error masking. *Weak* AMD codes do not use the probabilistic encryption. In weak AMD codes, reduction of the error masking is achieved by using of non-linear functions and additional transform of input codewords, for example Gray transform. This article presents the developed construction of *weak* AMD codes.

The two main parameters for AMD codes are

1) the robustness R and maximum number of undetected errors $R = max(x : x + e \in C)$;

2) the maximum of error masking probability which is a relationship

$$max\ Q(s) = \frac{max(x : x \in C, x + e \in C)}{M}, \tag{2}$$

where M is the number of codewords in code C, x is codeword, e is error vector. The smaller the value of the above parameters, the more robustness of the AMD code.

Also it is worth mentioning about the importance of systematic AMD codes. This type of codes is more flexible in the choice of parameters than perfect codes for the same code rate. Described in this article AMD code constructions are systematic.

IV. Algebraic manipulation detection code construction based on wavelet transform

In this section for building code construction will be used approximating A_1 and detailing D_1 components of wavelet transform. These components are obtained after the wavelet transform of the first order of the original information sequence s was made. It can be calculate with known coefficients of scaling function using the cyclic matrix H and G as described in the previous section. Discussed below designs are considered for the wavelets order equals to 2, so the matrix H, G have size $N/2 \times N$, where N is the length of the original sequence s. The calculation process for components A_1 and D_1 is a matrix-vector multiplication s: $A_1 = H\ s\ s$; $D_1 = G * s$. Information part of systematic AMD code consist of approximating component $A_1 = y = \{y_1, ..., y_{N/2}\}$, in order, the redundancy part is the detailing component of wavelet transform $D_1 = x = \{x_1, ..., x_{N/2}\}$.

The construction of the weak AMD code based on the scalar multiplication.

Consider the following code structure. Code C consist of the following codewords

$$(y \in GF(2^{sr}) | x \in GF(2^{sr}) | f(y, x) \in GF(2^r)),$$

where y approximating component of wavelet transform, x detailing component, s is the length of the vector in the AMD code, $f(x, y) = \sum_{i=1}^{s} x_i\, s\, y_i$ - scalar multiplication of vectors x and y, $|$ is concatenation symbol.

The approximating component y and the detailing component x are considered as vectors of a finite field $GF(2^r)$. The scalar product of vector x and y is redundant part of AMD code.

Theorem 1. Described above code construction is AMD code and has a maximum of error masking probability $max\ Q(s) = 2^{-r}$.

Proof. According to AMD code definition

$$Pr[D(E(x) + e) \notin x] \leq \varepsilon, \tag{3}$$

where x is a codeword, D and E denote respectively the decoding and encoding functions, e is injected error.

For AMD code, threshold ε is the robustness parameter R, hence the solution of inequality (3) will coincide with the solution of the next error masking equation

$$F(y, x) + s_f = f(y + s_y, x + e_x);$$

$$\sum_{i=1}^{s} x_i\ s\ y_i + e_f = \sum_{i=1}^{s} (x_i + e_{x_i}) * (y_i + e_{y_i}); \tag{4}$$

Transfer all parameters that depend on the information part on the left side of equation (4):

$$E_f = \sum_{i=1}^{s} (x_i * s_{y_i} + y_i * e_{x_i} + s_{x_i} * s_{y_i}) \tag{5}$$

This code is AMD code if it can detect errors with $e_y \neq 0$. Indeed, according to the definition of AMD code given in Section 2, it can be argued that described construction is AMD code with threshold $\varepsilon = 1/2^s$.

It can be seen that there is no combination of y and e ($e_y \neq 0$), such that inequality (5) holds for $\forall x$, therefore, for fixed values of y and an e ($e_y \neq 0$), the right side of the expression (5) is constant. Moreover left side of equation (5) will not be equal to this constant, if at least one $e_y \neq 0$, hence the error $e_y \neq 0$ will be detected, and the considered construction is AMD code.

Let's find the maximum of error masking probability for the proposed construction. Let k be the number of variables in the equation (5). Thus, the error masking equation (5) is the equation of the first degree of the k variables $x_i \in GF(2^r)$. Therefore, this equation has a $2^{r(k-1)}$ roots, hence the robustness for this code is $R = 2^{r(k-1)}$. By definition, the maximum of error masking probability equals $max\ Q(e) = 2^{-r}$.■

The construction of the weak AMD code based on Maiorana-McFarland function

In this construction approximating component y and detailing component x are divided into equal parts, which are represented as vectors in a Galois field. In order, the multiplication of derived vectors are the encoding function for given construction.

Consider the following encoding function

$$F(y,x) = x_1 \cdot y_1 + x_2 \cdot y_2 + ... + x_r \cdot y_r,$$

where $x_r \cdot y_r$ multiplication in Galois field $GF(2^r)$, r is the length of each part. The encoding function is perfect nonlinear function. This function also is called as *Majorana-McFarland function.*

Theorem 2. The construction of the wavelet AMD code based on Maiorana-McFarland function is a weak AMD code and has a maximum of error masking probability $max\ Q(e) = 2^{-r}$.

Proof. For proof, it is necessary to consider the relationship between the nonlinearity of encoding functions P_f and robustness parameter R of AMD code. In articles [10, 11], it is proved that between the above parameters there is a clear dependence $R = P_f 2^k$ where R is a robustness, P_f is nonlinearity parameter of encoding function, the k is the number of information symbols in the codewords of code construction. As shown in [12], the nonlinearity of function can be find by using the derivative

$$P_f = \max_{e_x \in GF(2^r)} \max_{e_y \in GF(2^r)} Pr(D_{e_x} F(x,y) = e_y) = 1/2^r,$$

where r is a length of redundancy part of the codeword. $F(x,y)$ is some function depending from two parameters x and y, e_x and e_y are error corresponding to parts x and y. Thus, according to definition of AMD code, proposed above AMD code is a code with a threshold $\varepsilon = R = 2^{k-r}$, where k is the sum of the lengths of the main stream of x and wavelet flow y.

For finding of the maximum of error masking probability, it is necessary to analyze the number of solutions for the error masking equation

$$F(k) + e_f - f(k + e_k) = 0 \Rightarrow$$

$$F(k) + e_f = f(k + e_k),$$

where k is the sum of the lengths for main stream x and wavelet flow y, e_k and e_f are errors for information and redundant parts correspondingly. The last equation have no more than 2^{k-r} solutions. That is for every $e = (e_k, e_f)$, there are no more than R values of k for which the error masking equation are correctly. Since the k denotes the length of the concatenation vector of x and y, hence, there is no more R solutions respect to the variable x for which the error will be masked. Thus, by definition of the error masking probability, we get $max\ Q(e) = R/2^k = 2^{kr}/2^k = 2^{-r}$.■

V. Algebraic Manipulation Detection Codes under Nonuniform Input Codeword Distribution

Nonuniform distribution of the input codewords has a huge impact on the parameters of the security-oriented code. By controlling the input codewords, attacker has the possibility to reduce the maximum of error masking probability. Thus, the attacker increases the chances of successful error implementation in the device even if it uses AMD codes for protection.

Let's consider a simple example of how the changing of the input codeword distribution effects on the error masking probability $Q(e)$. May the code C receives the information sequence s on the input. Let's the encoding function of code C have the form $F(x,y) = xy$, where x and y are two equal part of input information, so $s = (x|y)$. Redundancy part of code are multiplication of vector x and y in field $GF(2^r)$, where r is length of these parts. Codewords of given code C have the form $(x|y|xy)$, where xy are field multiplication. The length of codewords equal to $3r$ and a number of codewords equal to 2^{3r}. We will consider behaviour of these constructions under uniform and nonuniform distributions.

For a uniform distribution of the codewords, the probability of each input codeword is $p(s) = \frac{1}{M}$, where M is the number of codeword of code C. Let's calculate the error masking probability $Q(e)$ for each error e using the formula (2). The obtained distribution of $Q(e)$ presented in Fig. 2.

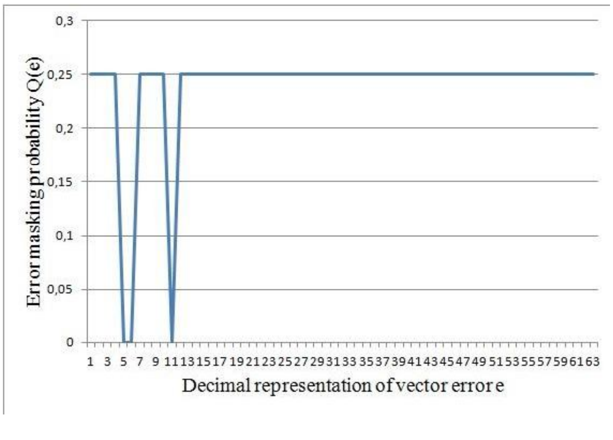

Fig. 2. Distribution of error masking probability for code C under uniform input codeword distribution

As can be seen from Fig. 2, the resulting distribution of error masking $Q(e)$ is almost uniform, except for a few errors, for which the probability $Q(e)$ is equal to zero. However, the zero probability of error masking is not dangerous from the security point, since their implementation will be detected by any input codeword s. In turn, errors with a high probability of error masking are the most dangerous. Note that for considered function the maximum value is equal to 0.25. Usually, the errors are suitable for implementation, if the probability of error masking exceeds 0.5.

But mostly, the distribution of probability of input codeword are nonuniform. Moreover, this distribution can be defined by an attacker. For example, the probability of input value s will be taken according to the following piecewise function

$$p(s) = \begin{cases} 0.25, for\ s \in [8;9] \\ 0.15, for\ s \in [7;10] \\ 0.05, for\ s \in [6;11] \\ 0.01,\ otherwise \end{cases}$$

where integers in square brackets are decimal representation of binary input s. Fig. 3 shows the distribution of error masking Q(e) calculated according to the formula (2).

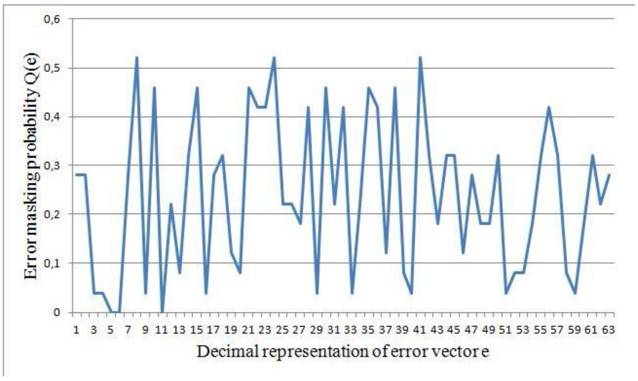

Fig. 3. Distribution of error masking probability for code C in case of nonuniform distribution of input codeword

It is clear from Fig. 3 that distribution of $Q(e)$ far from a uniform distribution. The figure shows that there are at least 3 errors with the error masking probability greater than 0.5. In case of the injection of these errors, more than half of the codewords of C will lead to algebraic manipulation. Thus, the opportunity to influence on the input values s is a powerful tool for the attacker. Therefore, all the security-oriented codes must be checked for cases of nonuniform distribution of the input codewords.

For further measurements of error masking probability, the following distribution functions of input codewords were used:

1) uniform distribution $p(s) = 1/16$ for all s

2) distribution 1

$$p(s) = \begin{cases} 0.25, for\ s \in [8;9] \\ 0.15, for\ s \in [7;10] \\ 0.05, for\ s \in [6;11] \\ 0.01,\ otherwise \end{cases}$$

3) distribution 2

$$p(s) = \begin{cases} 0.1, for\ s \in [4;9] \\ 0.04,\ otherwise \end{cases}$$

4) distribution 3

$$p(s) = \begin{cases} 0.5, for\ s \in [6] \\ 0.1, for\ s \in [7;8;9;10;11] \\ 0,\ otherwise \end{cases}$$

5) distribution 4

$$p(s) = \begin{cases} 0.2, for\ s \in [4;6;8] \\ 0.1, for\ s \in [2;3;5] \\ 0.01,\ otherwise \end{cases}$$

From Tables I, II and III it can be seen that the proposed AMD wavelet codes provides gain in encoding rate in systems that uses wavelet transform. Moreover, proposed wavelet AMD codes have higher error masking probability under nonuniform distribution of input codewords. Thus proposed construction can be successfully used for protection of storage devices if there is a possibility of algebraic manipulation.

TABLE I. COMPARING OF MAXIMUM OF ERROR MASKING PROBABILITY FOR CASE OF NONUNIFORM DISTRIBUTION OF INPUT CODEWORDS FOR R=2

Compared construction	max Q(e) uniform distribution	max Q(e), nonuniform distribution 1
Wavelet AMD code based on Maorana-McFarland function	0,0625	0,0742
Wavelet AMD code based on scalar production	0,0625	0,0793
AMD code based on Reed Solomon codes	0,1250	0,1334
AMD code based on multiplication in field	0,0078	0,0119

TABLE II. COMPARING OF MAXIMUM OF ERROR MASKING PROBABILITY FOR CASE OF NONUNIFORM DISTRIBUTION OF INPUT CODEWORDS FOR R=2

Compared construction	max Q(e), nonuniform distribution 2	max Q(e), nonuniform distribution 3
Wavelet AMD code based on Maorana-McFarland function	0,0838	0,0835
Wavelet AMD code based on scalar production	0,0723	0,0722
AMD code based on Reed Solomon codes	0,1586	0,1270
AMD code based on multiplication in field	0,0093	0,0099

TABLE III. COMPARING OF RATE ENCODING FOR INFORMATION PROCESS OF 1MB AND LENGTH OF CODE CONSTRUCTION N=12 AND INFORMATION PART EQUAL 4

Compared construction	Rate of encoding in system with wavelet	Rate of encoding in system without wavelet
Wavelet AMD code based on Maorana-McFarland function	0, 54 s	0, 42 s
Wavelet AMD code based on scalar production	0, 56 s	0, 51 s
AMD code based on Reed Solomon codes	0, 43 s	0, 43 s
AMD code based on multiplication in field	0, 68 s	0, 68 s

In this article was presented comparison of developed AMD code constructions and nonlinear security-oriented codes. For comparison, software models of encoding process was designed for all considered constructions. For system with wavelet transform, a comparison of encoding rate was performed for ADV621 system that makes video compression by using Daubechies wavelets. Also a comparison for nonuniform codeword distribution of input codeword was made. The measurement results are shown in Tables I, II and III. Detailed description of AMD code construction based on Reed-Solomon codes and based on the multiplication in the field are presented in [13, 14].

VI. Conclusion

The article presents the new construction of weak AMD codes based on wavelet transform. Using of the developed code in systems with wavelet transform reduces the computational complexity of encoding and decoding process. The proposed coding methods are more resistant to algebraic manipulation than existing AMD codes, in particular developed codes are more stable to algebraic manipulation than AMD codes based on Reed-Solomon codes.

References

[1] P. Kocher,J. Jaffe, B. Jun, "Differential power analysis", in Advances in Cryptology CRYPTO 99, ser. Lecture Notes in Computer Science, 1999, V. 1666, pp. 789–789.

[2] S. P. Skorobogatov, R. J. Anderson, "Optical fault induction attacks", in Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems, Springer-Verlag, 2003, pp. 2–12.

[3] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, C. Whelan, "The sorcerer's apprentice guide to fault attacks", Proceedings of the IEEE, 2006, V. 94, N. 2, pp. 370–382.

[4] M.G Karpovsky, K. Kulikowski, Z. Wang, "Robust Error Detection in Communication and Computation Channels", Keynote paper, Int. Workshop on Spectral Techniques, 2007, pp. 1–15.

[5] R. Cramer, S. Fehr, C. Padro, "Algebraic manipulation detection codes", Science China Mathematics, 2013, V. 56, N. 7, pp. 1349–1358

[6] W. Zhen, M. Karpovsky, "Algebraic manipulation detection codes and their applications for design of secure cryptographic devices", On-Line Testing Symposium (IOLTS), 2011 IEEE 17th International, 2011, pp. 234–239

[7] M. N. Yudin, Y. A. Farkov, D. M. Filatov, "Inrodution in wavelet analysis" Moscow Geological Prospecting Academy Publishing, 2001, p. 72.

[8] A. B. Levina, S. V. Taranov, "Algorithms of Constructing Linear and Robust Codes Based on Wavelet Decomposition and its Application", Springer Book Codes, Cryptology, and Information Security, 2015, pp. 247–258.

[9] A. B. Levina, S. V. Taranov, "Spline-wavelet robust code under non-uniform codeword distribution", IEEE Conference Publications Computer, Communication, Control and Information Technology (C3IT), 2015, pp. 1-5

[10] M. G. Karpovsky, K. Kulikowski, Z. Wang, "On-Line Self Error Detection with Equal Protection Against All Errors", Int. Journal of Highly Reliable Electronic System Design, 2008, pp. 124–130

[11] M. G. Karpovsky, Z. Wang, Design of Strongly Secure Communication and Computation Channels by Nonlinear Error Detecting Codes // IEEE Trans Computers, 2013, V. 63, N. 11, pp. 2716–2728.

[12] C. Carlet, C. Ding, "Highly Nonlinear Mappings", J. Complexity Issues in Coding and Cryptography, 2004, V. 20, pp. 205–244.

[13] Z. Wang, M. G. Karpovsky, "Reliable and secure Memories based on algebraic manipulation correction codes", On-Line Testing Symposium (IOLTS), 2012 IEEE 18th International, pp. 146–149.

[14] Z. Wang, M. G. Karpovsky, K. J. Kulikowski, "Design of memories with concurrent error detection and Correction by non-linear SEC-DED codes", J. Electronic Testing, 2010, V. 5, N 5, pp. 559-580.