Proceedings of the Federated Conference on Computer Science and Information Systems pp. 227–230 DOI: 10.15439/2019F134 ISSN 2300-5963 ACSIS, Vol. 18

Spline-Wavelet Bent Robust Codes

Alla Levina,
University ITMO, ul. Lomonosova 9
and
St. Petersburg Electrotechnical University "LETI", Professora Popova str., 5
Russia, Saint-Petersburg,
Email: alla_levina@mail.ru

Gleb Ryaskin,
University ITMO, Saint-Petersburg, Russia.
Email: ryaskingleb20@gmail.com

Igor Zikratov
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Saint-Petersburg , Russia.
Email: igzikratov@yandex.ru

Abstract. **This paper presents an application of spline-wavelet transformation and bent-functions for the construction of robust codes. To improve the [1]non-linear properties of presented robust codes, bent-functions were used. Bent-functions ensure maximum non-linearity of functions, increasing the probability of detecting an error in the data channel. In the work different designs of codes based on wavelet transform and bent-functions are developed. The difference of constructions consists of using different grids for wavelet transformation and using different bent-functions. The developed robust codes have higher characteristics compared to existing. These codes can be used for ensuring the security of transmitted information.**

I. INTRODUCTION

Wavelet transformation has become well known and widely used in many fields of science [1-3]. The basic concepts of wavelet theory can be found in the work of Daubechies [3]. Also, wavelet theory has found implementation in the technical fields such as data compression, signal analysis, and communication applications [4-7].

One new direction of implementing wavelet theory is error protection codes [6-7, 9-15]. Error detecting codes are used for the protection in telecommunication channels, they ensure the reliability and security of devices from soft, hard errors and side channel attacks [17]. The purpose of error correcting codes is to provide digital communication over the channel in such a way that errors in the transmission of bits can be detected and corrected by the receiver. This goal is achieved by using coding algorithms that convert information before sending it [16-19].

By exercising various effects on the hardware component of a cryptographic device in order to cause distortion of information at some stages of coding, managing and analyzing errors, an attacker can change the information transmitted over the channel. This type of attack is called a calculation error attack [17]. To provide protection against this type of attack, robust codes built on non-linear functions are used because linear functions do not show all errors due to linear properties [16-17]. And often the most interesting are non-linear functions for which the property of non-linearity is bent function [8].

In this article, was investigated the properties of robust codes constructed on bent functions and wavelet decompositions. Will be presented various methods for constructing this class of codes, their advantages and disadvantages are analyzed, and their comparison with existing codes is carried out.

II. WAVELET TRANSFORM

In this section, will be explained the idea of wavelet transformation [1-7], more detailed information can be found in the works of Daubechies [3].

Let function s(t) belong to the Hilbert space $L^2(R)$ with the scalar product $\langle f(t), g(t)\rangle = \int f(t)g(t)dt$ and the norm $\int |s(t)|^2 < \infty$. The idea of the wavelet transform is based on the partition of the signal s(t) into two components, approximating $A_m(t)$ and detailing $D_m(t)$.

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

where m denotes the decomposition (reconstruction) level.

In this article, will be used wavelet transformation or rather a spline-wavelet transformation for creating an error detection code. In this paper will be explained the idea of splain-wavelet transformation, only for the splines of the first order, which will be used for the construction of codes.

Let X be a non-uniform grid of elements, $X = \{x_j\}_{j\in Z}$, where Z is the set of integers. Splines of the first order on the grid X are defined as follows:

$$\omega_j(t) = (t - x_j)(x_{j+1} - x_j)^{-1}, t \in [x_j, x_{j+1}),$$
$$\omega_j(t) = (t - x_j)(x_{j+1} - x_j)^{-1}, t \in [x_{j+1}, x_{j+2}),$$
$$\omega_j(t) = 0, t \notin [x_j, x_{j+2}),$$

$where\ \omega_j(t) - splines, x_j - elements\ of\ X.$

In the process of wavelet decompositions, some element x_k is thrown out of the grid X, after this transformation a new grid $\tilde{X}$, on the basis of which new splines $\widetilde{\omega_j}(t)$ are constructed. New and old splines are interconnected. This relationship between the elements $\widetilde{\omega_j}(t)$ and $\omega_j(t)$ can be shown by the formulas:

$$\tilde{x}_j = x_j, if\ j \le k-1,\ \tilde{x}_j = x_{j+1},\ if\ j \ge k,$$
$$\varepsilon = x_k, \widetilde{\omega_j}(t) = \omega_j(t), if\ j \le k-3$$
$$\widetilde{\omega_j}(t) = \omega_{j+1}(t), if\ j \ge k$$
$$\widetilde{\omega}_{k-2}(t) = \omega_{k-2}(t) + \widetilde{\omega}_{k-2}(x_k)\omega_{k-1}(t)$$
$$\widetilde{\omega}_{k-1}(t) = \omega_{k-1}(t) + \widetilde{\omega}_{k-1}(x_k)\omega_{k-1}(t)$$

With the help of spline-wavelet decompositions, it is possible to create a large number of different codes constructions among themselves.

III. BENT FUNCTION

The measure of nonlinearity is an important characteristic of a Boolean function in cryptography. Linearity and properties close to it often indicate a simple (in a certain sense) structure of this function and, as a rule, represent a rich source of information about many of its other properties. The problem of constructing Boolean

This work was supported by the grant of Russian Science Foundation pr. № 17-71-20077

functions possessing nonlinear properties naturally arises in many areas of discrete mathematics. And often the most interesting are those functions for which these properties are extreme. Such Boolean functions are called bent functions. A bent function can be defined as a function that is extremely poorly approximated by affine functions [1].

The nonlinearity of a function *f* is the distance from f to a class of affine functions. Lets denote the nonlinearity of the function f in terms of $N_f : N_f = d(f, A(n)) = \min_{g \in A(n)} d(f, g)$, where *A(n)* is the class of linear functions.

The function $f \in P_2(n)$ is called maximally nonlinear if $N_f = 2^{n-1} - 2^{(n/2)-1}$.

Definition: A bent function is a Boolean function with an even number of variables for which the Hamming distance from the set of affine Boolean functions with the same number of variables is maximal.

Example: $f(x_0, x_1, x_2, x_3) = x_0x_1 + x_2x_3$

From the point of view of cryptography, the important criteria that a Boolean function *f* of n variables must satisfy are the following:

1) equilibrium — the function f takes values 0 and 1 equally often;

2) the propagation criterion $PC(k)$ of order k- for any nonzero vector $y \in Z_2^n$ weight at most k, the function $f(x + y) + f(x)$ is balanced;

3) the maximum nonlinearity - the function f is such that the value of its nonlinearity NF is maximal;

The bent function matches the criteria for propagation and maximum non-linearity, which allows it to detect all errors in the channel and to have a uniform probability of detecting errors, but the function is not balanced.

IV. SPLINE-WAVELET ROBUST CODE

In this section, will be described the rules for the formation of code words for a particular code construction, a comparison of these codes with examples of linear and nonlinear codes are also will be given.

Robust codes are nonlinear systematic error-detecting codes that provide uniform protection against all errors without any (or that minimize) assumptions about the error and fault distributions, capabilities and methods of an attacker [12, 16-18].

Let *M* = | *C* |, this is the number of codewords in code *C*. By the definition of an R-robust code, there are no more than R code words that cannot be detected for any fixed error *e*.

$$R = max\ |\{x \mid x \in C, x + e \in C\}|$$

The probability of masking the error *e* can be defined as:

$$Q(e) = \frac{|\{x \mid x \in C, x+e \in C\}|}{M}$$

One of the main criteria for evaluating the effectiveness of a robust code is the maximum error masking probability. The maximum error masking probability can be defined as

$$max\ Q(e) = max\ \frac{|\{x \mid x \in C, x+e \in C\}|}{M} = \frac{R}{M}$$

The following is the construction of robust codes based on bent functions and spline-wavelets with the static grid, and grid based on the codeword. The additional elements are calculated on the basis of bent functions from information elements and spline-wavelet elements, the result is also a bent function. The function for the additional elements is the bent function (code Kerdock), the elements are the informational elements and wavelet elements. So, the new function is created, because wavelet elements are the function of several informational elements. This function is also bent function, it was checked for all grid values. The new bent function is created, with another properties.

Let $c = \{c_1, c_2, \dots, c_{n-1}, c_n\}$ denotes the code word of some shared (n, k) code. Then $\{c_1, c_2, \dots, c_{k-1}, c_k\}$ is the information part, and $\{c_{k+1}, \dots, c_n\}$ - additional.

Construction 1. Spline-wavelet bent robust code with a static grid.

In this construction, for all code, a grid is selected $x = \{x_1, x_2, \dots, x_{n-1}, x_k\}$, any elements are discarded at the discretion of the specialist, the number of discarded items is equal to $(n - k)/2$. Number of characters is strictly even and multiple 4, attitudes $\frac{k}{n} = \frac{2}{3}$. The ejected elements will be denoted by the set $z = \{z_1, \dots, z_{(n-k)/2}\}$. The wavelet elements will be denoted by the set $b = \{b_1, \dots, b_{(n-k)/2}\}$. Let $c = (c_1, c_2, \dots, c_n)$ - vector field $GF(2^n)$, $1 \le i \le n$. The vector c belongs to the code if

$$c_{k+j} = b_j = c_{z_i} + c_{z_i+1} + (x_{z_i+2} + x_{z_i-1})(x_{z_i+2} + x_{z_i})^{-1}(c_{z_i-1} + c_{z_i+1})$$

For even z_i:

$$c_{k+j+(n-k)/2} = c_1 * c_2 + \dots + b_j * c_{z_i-1} + \dots + c_{k-1} * c_k$$

For odd z_i:

$$c_{k+j+(n-k)/2} = c_1 * c_2 + \dots + b_j * c_{z_i+1} + \dots + c_{k-1} * c_k$$

Where $1 \le j \le (n - k)/2, k$ – the number of parity symbols in the code, $z_i \in z$,+ - addition mod 2, $c_{k+j+(n-k)/2}$ is the bent function's element.

This construction is built on a static grid, which is not always good, because it will be necessary to transfer the grid between the receiver and the transmitter.

Construction 2. Spline-wavelet bent robust code with a grid based on the codeword.

In this construction, for all code, a grid is selected $x = \{x_1, x_2, \dots, x_{n-1}, x_k\}$, based on the information part of the codeword, and depending on the number of the ejected element. The grid is equal to the shift relative to the number of the element that is thrown, that is x[i]=c[(i-z_i)(mod n-k)]. The wavelet elements will be denoted by the set $b = \{b_1, \dots, b_{(n-k)/2}\}$. Let $c = (c_1, c_2, \dots, c_n)$ - vector field $GF(2^n)$, $1 \le i \le n$. The vector c belongs to the code if

$$c_{k+j} = b_j = c_{z_i} + c_{z_i+1} + (x_{z_i+2} + x_{z_i-1})(x_{z_i+2} + x_{z_i})^{-1}(c_{z_i-1} + c_{z_i+1})$$

For even z_i:

$$c_{k+j+(n-k)/2} = c_1 * c_2 + \dots + b_j * c_{z_i-1} + \dots + c_{k-1} * c_k$$

For odd z_i:

$$c_{k+j+(n-k)/2} = c_1 * c_2 + \cdots + b_j * c_{z_i+1} + \cdots + c_{k-1} * c_k$$

Where $1 \le j \le (n-k)/2, k$ - the number of parity symbols in the code, $z_i \in z$,+ - addition mod 2.

This construction is built on a grid, based on the codeword, and it is solves the problem of the transfer grid, but the algorithm is more time consuming. Created constructions have better parameter than existing, presented example will show the difference between created constructions and existing solutions.

Example: Consider the composition of construction 1 and construction 2 for *n=8* and *k =4*.

In order to obtain the code of this kind, we will consider redundant symbols, as a result of the bent-function of the additional stream b and other information symbols. It is necessary to make sure that the result of the interaction of the main stream and the additional one is also a bent function. The number of the ejected element is taken equal to three (the number of the ejected element does not affect anything, you can throw out other elements, getting other formulas, but this does not affect the final result).

Formulas for decomposition and reconstruction when the element is kicked out under the number k have the form, provided that $x_{k+2} \neq x_k$:

$$b_k = c_k - c_{k+1} - (x_{k+2} - x_{k-1})(x_{k+2} - x_k)^{-1}(c_{k-1} - c_{k+1})$$

$$c_k = b + c_{k+1} - (x_{k+2} - x_{k-1})(x_{k+2} - x_k)^{-1}(c_{k-1} - c_{k+1})$$

As a bent function for the code, will be take the formula $f = c_1c_2 + c_3c_4 + c_5c_6 + c_7c_8$. When the third element will be thrown out. The element c_3 will be replaced on the additional flow element b_3, and c_5 on the additional flow element b_5. Functions takes the form $f_1 = c_1c_2 + b_3c_4 + c_5c_6 + c_7c_8$ and $f_2 = c_1c_2 + c_3c_4 + b_5c_6 + c_7c_8$, the addition goes modul 2, corresponds to the operation XOR.

Because these functions are bent functions, so, independently of the values of the grid, the function f is a bent-function. The result of the function f will be used as a redundant symbol $r_0 = f_1$, and the redundant symbol $r_1 = b_1$ (element of additional stream), $r_2 = f_2, r_3 = b_2$.

Let's compare this code with different values of a grid with a linear code and a robust code of the same length. In the example, as the linear code was taken Hamming code (8,4). Redundant symbols for a nonlinear code will be equal to $r_0 = c_1c_2 + c_3c_4 + c_5c_6 + c_7c_8$, $r_1 = c_1c_3 + c_2c_4 + c_6c_8 + c_5c_7$, $r_2 = c_1c_5 + c_2c_6 + c_3c_7 + c_4c_8$, $r_3 = c_1c_3 + c_2c_4 + c_6c_8 + c_5c_7$ (code Kerdock).

Let's draw up a graph of error detection probabilities for a spline-wavelet code with a static grid — construction 1, for a spline-wavelet code with a codeword-based grid — construction 2, for a "robust" Kerdock code and a linear code, the result is displayed in Figure 1.

The Hamming code does not match the equiprobability of the error, which makes this code vulnerable to attack by the attacker, in contrast to the Kerdock code and construct 1.

The average probability of detecting an error is insignificantly different for the construction 1, the construction 2, and the robust Kerdock code. In the case of linear code, the probability is uneven, which makes this code vulnerable to attacks on third-party channels.

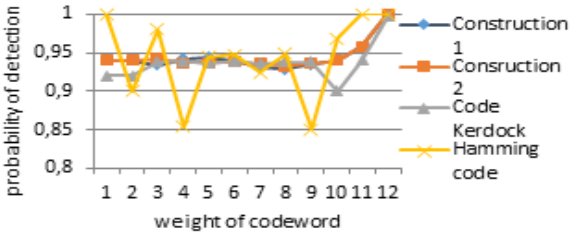

Fig. 1. Error detection probability for different code constructions

Compare the number of the maximum probability of masking errors of these codes and display the results in Table 1, as well as the time, is taken to encode 4000 bytes.

Table 1. Probability of maximum error concealment for different code constructs

Code	maximum probability of error concealment, Q(e)	Number of time measurement, sec
Construction 1	0,5	0,045
Robust code Kerdock	0,5	0,067
Hamming code	1	0,037
Construction 2	0,46875	0,067

Codes constructed on the basis of spline-wavelet decompositions using bent functions have a number of advantages in different characteristics compared to other codes. Construction 1 has good coding time, does not have undetectable errors. Construction 2 has the bad coding time, but has no undetected errors, and has the smallest value of the maximum probability of masking the error.

For codes based on bent functions and wavelet transformations, there will always be an even number of information symbols, since bent functions exist only for an even number of variables, and codes have poor coding time scores compared to linear codes.

V. SPLINE-WAVELET CODE ON BENT FUNCTION WITH DIFFERENT DEGREES

In the case of construction 1, the degree of the bent functions is equal to 2, in the case of the construction 2, the degree of the bent functions is 3 or 2, depending on the symbols to be erased. As a result, an assumption immediately arises that an increase in the degree of the curved function can give the best values for the parameter R.

The degree of the bent function cannot exceed *n / 2* [8], and therefore one can not single out a single construction for an arbitrary number of variables.

In this section will be shown functions with different degrees based on spline wavelets and information symbols for n = 8, they will be compared by the parameter R. For each number of variables, bent functions were constructed on the basis of spline wavelets. For all functions, the wavelet element is calculated from the same function:

$$Wave_k = c_k - c_{k+1} - (x_{k+2} - x_{k-1})(x_{k+2} - x_k)^{-1}(c_{k-1} - c_{k+1})$$

Functions for n=8 presented in table 2, also given the conditions of the grid and the degree of function.

Table 2. Spline wavelet Bent functions for n=8

Number of function	Grid	Function	Deg(f)
1	$x_i = c_i$	$f_i = c_{i+1} * c_{i+3} * c_{i+4} + c_{i+2} * c_{i+3} * c_{i+5} + Wave_{i+2} * c_{i+6} + c_i * c_{i+3} + c_i * c_{i+5} + c_{i+2} * c_{i+3} + c_{i+2} * c_{i+4} + c_{i+2} * c_{i+5} + c_{i+3} * c_{i+4} + c_{i+3} * c_{i+5} + c_{i+6} * c_{i+7}$	4
2	Static	$f_i = c_i * c_{i+1} * Wave_{i+2} + c_{i+1} * c_{i+3} * Wave_{i+4} + c_i * c_{i+1} + c_i * c_{i+3} + c_{i+1} * c_{i+5} + c_{i+2} * c_{i+4} + c_{i+3} * c_{i+4} + c_{i+6} * c_{i+7}$	3
3	$x_i = c_{7-i}$	$f_i = c_i * c_{i+1} + Wave_{i+2} * c_{i+3} + c_{i+4} * c_{i+5} + c_{i+6} * c_{i+7}$	4
4	Static	$f_i = c_i * Wave_i + c_{i+1} * Wave_{i+2} + c_{i+2} * Wave_{i+4} + c_i * c_{i+3} + c_{i+1} * c_{i+5} + c_{i+2} * c_{i+3} + c_{i+2} * c_{i+4} + c_{i+2} * c_{i+5} + c_{i+3} * c_{i+4} + c_{i+3} * c_{i+5} + c_{i+6} * c_{i+7}$	2

Let's compile the code constructions for all the above functions with 2 redundant symbols $r_0 = f_0$, $r_1 = f_1$. Calculate the parameter R and maximum probability of error concealment, the results are listed in Table 3.

Table 3. Parameter R for n=8

Function	The degree of bent function	R	maximum probability of error concealment, Q(e)
Function №1	4	96	0,375
Function №2	3	120	0,46875
Function №3	4	96	0,375
Function №4	2	128	0,5

The degree of the bent function different from 2 gives a better result for the parameter R. The number of calculations and the time spent on coding information is more compared to the codes built on bent functions with a power of 2. When these codes are used in the case protection against attack by an attacker, then the parameter R is more important. Using spline wavelets, it is possible to build a large number of robust codes, build bent functions and increase their degree, thereby improving the quality of robust codes. So new construction is created with parameter R lower than construction 1 or construction 2.

Spline-wavelet robust code with lower value R

Let $c = \{c_1, c_2, \dots, c_{n-1}, c_n\}$ denotes the code word of some shared (n, k) code. Then $\{c_1, c_2, \dots, c_{k-1}, c_k\}$ is the information part, and $\{c_{k+1}, \dots, c_n\}$ - additional, $n = k + 2$. Grid is selected depending on the spline wavelet function, $f_i(c_1, c_2, \dots, c_{k-1}, c_m)$ is a function from table 2, $m = 8$. The vector c belongs to the code if

$$c_{k+1} = f_0(c_1, \dots, c_m) + c_{m+1} * c_{m+2} + \dots + c_{k-1} * c_k;$$

$$c_{k+2} = f_1(c_1, \dots, c_m) + c_{m+1} * c_{m+2} + \dots + c_{k-1} * c_k.$$

This construction allows better protection against side-channel attacks, because parameter R and maximum probability of error concealment Q(e) lower than existed solutions, but it takes more time for the coding information.

Conclusion

In this paper, was described as the error-correcting coding scheme based on wavelet transformation and bent functions. For the proposed scheme, was created wavelet robust codes on bent functions. The robust wavelet code has no undetectable errors, so it ensures reliable protection against the error injection, also has the high values of the parameter R.

REFERENCES

[1] I. G. Burova and U. K. Demyanovich, Theory of Minimal Spline (SPSU, 2000).

[2] G. Caire, R. L. Grossman and H. V. Poor, Wavelet transforms associated with finite cyclic groups, IEEE Trans. Inf. Theory 39(4) (1993) 1157–1166.

[3] I. Daubechies, Ten Lectures on Wavelets, CBMS-NSF Conference Series in Applied Mathematics (SIAM, 1992).

[4] U. K. Demyanovich, Calibration ratio for B-splines on nonuniform net, Mat. Model T 13(3) (2001)

[5] U. K. Demyanovich, Minimal Splines and Wavelets (Vestnik SPSU, 2008)

[6] F. Fekri, R. M. Mersereau and R. W. Schafer, Theory of wavelet transform over finite fields, IEEE International Conference on Acoustics, Speech, and Signal Processing 3 (1999) 1213–1216.

[7] F. Fekri, S. W. McLaughlin, R. M. Mersereau and R. W. Schafer, Double circulant selfdual codes using finite-field wavelet transforms, Applied Algebra, Algebraic Algorithms and Error Correcting Codes Conference (Springer, 1999), pp. 355–364

[8] Tokareva N., Bent Functions: Results and Applications to Cryptography, 2015.

[9] A. Levina and S. Taranov, Spline-wavelet robust code under nonuniform codeword distribution, in 3rd Int. IEEE Computer, Communication, Control and Information Technology (IEEE, 2015).

[10] A. B. Levina and S. V. Taranov, Algorithms of constructing linear and robust codes based on wavelet decomposition and its application, Cryptology, and Information Security (Springer, 2015), pp. 247–258.

[11] A. B. Levina and S. V. Taranov, Second-order spline-wavelet robust code under nonuniform codeword distribution, Procedia Comput. Sci. 62 (2015) 297–302.

[12] A. B. Levina and S. V. Taranov, Construction of linear and robust codes that is based on the scaling function coefficients of wavelet transforms, J. Appl. Ind. Math. 9(4) (2015) 540–546.

[13] A. B. Levina and S. V. Taranov, New construction of algebraic manipulation detection codes based on wavelet transform, Proceedings of the 18th Conference of Open Innovations Association FRUCT - 2016, pp. 187-192

[14] A. B. Levina and S. V. Taranov, Creation of codes based on wavelet transformation and its application in ADV612 chips, International Journal of Wavelets, Multiresolution and Information Processing - 2017, Vol. 15, No. 2, pp. 1750014

[15] A. B. Levina and S. V. Taranov, AMD codes based on wavelet transform, 2017 Progress In Electromagnetics Research Symposium - Fall (PIERS-FALL) - 2017, pp. 2534-2539

[16] Akdemir K.D., Wang Z., Karpovsky M. G., Sunar B., Design of Cryptographic Devices Resilient to Fault Injection Attacks Using Nonlinear Robust Codes // Fault Analysis in Cryptography, 2011.

[17] Karpovsky M.G., Kulikowski K., Wang Z., Robust Error Detection in Communication and Computation Channels // Keynote paper, Int. Workshop on Spectral Techniques, 2007.

[18] Carlet C. Boolean functions for cryptography and error correcting codes // Chapter of the monograph «Boolean Methods and Models», Cambridge Univ. Press (P. Hammer, Y. Crama eds.), 2007.

[19] MacWilliams, F.J. and Sloane, N.J.A., The Theory of Error-Correcting Codes. Elsevier-North-Holland, Amsterdam, 1977.