



SCALab

SCA Research Lab

Wavelet transformation and its application in information security

Alla Levina
BFA 2017

Wavelet transformation

$$c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7, \dots, c_{2L-1}$$
$$c_1, c_3, c_5, c_7, \dots, c_{2L-1}$$

Wavelet transformation:

$$a_j = (c_{2j} + c_{2j+1})/2, \quad b_j = (c_{2j} - c_{2j+1})/2, \quad j = 0, 1, \dots, L-1.$$
$$c_{2j} = a_j + b_j, \quad c_{2j+1} = a_j - b_j, \quad j=0, 1, \dots, L-1$$

Main stream: $a_0, a_1, a_2, a_3, a_4, a_5, a_6, \dots, a_{L-1}$

Wavelet stream: $b_0, b_1, b_2, b_3, b_4, b_5, b_6, \dots, b_{L-1}$

Timeline

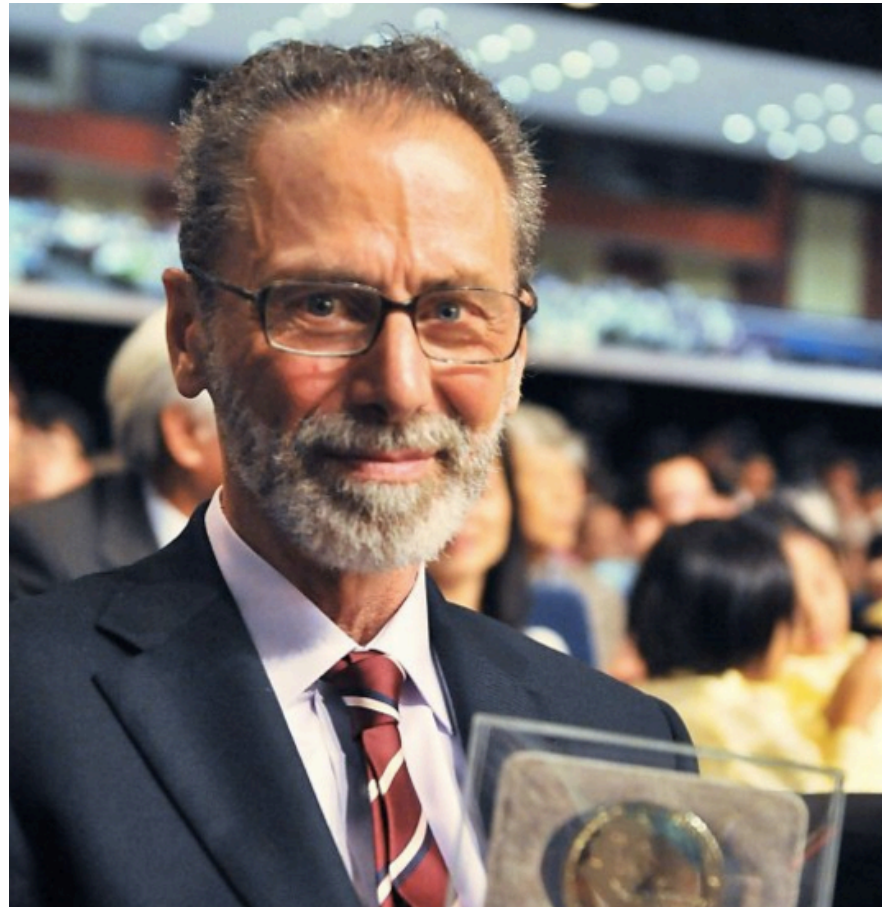
- ✓ First wavelet (Haar wavelet) by Alfréd Haar (1909)



- ✓ Since the 1980s: Yves Meyer, Stéphane Mallat, Ingrid Daubechies, Ronald Coifman, Ali Akansu, Victor Wickerhauser

Timeline

Yves Meyer [Abel Prize](#) in 2017



Spline-wavelet transformation

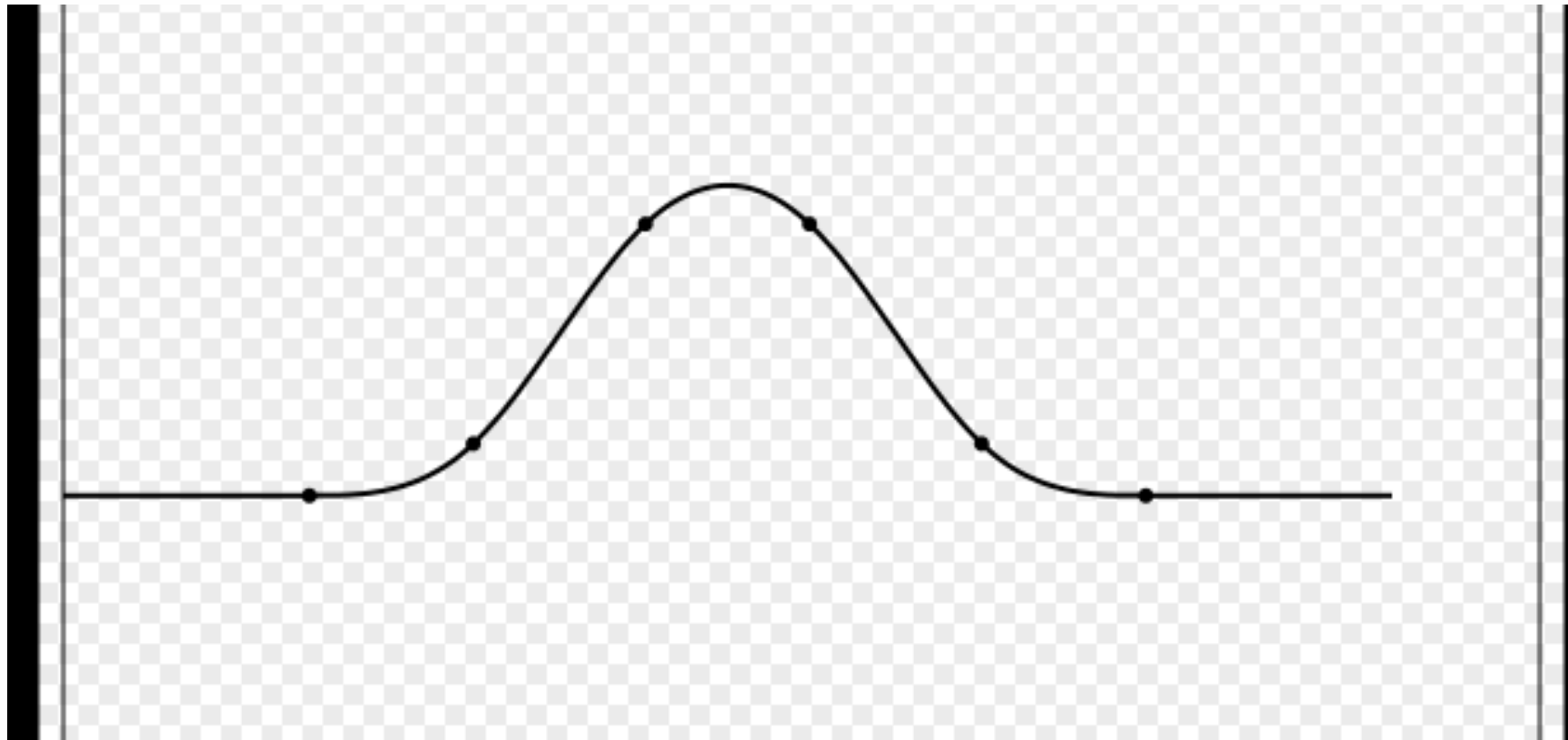
In mathematics, a spline is a special function defined piecewise by polynomials.

Let \mathbb{Z} be the set of all integers. On finite or infinite interval (α, β) of the real axis \mathbb{R}^1 consider the net: $X \triangleq \{x_j\}_{j \in \mathbb{Z}}$,

$$X : \quad \dots < x_{-1} < x_0 < x_1 < \dots,$$

for which $\alpha = \lim_{j \rightarrow -\infty} x_j$, $\beta = \lim_{j \rightarrow +\infty} x_j$, $\forall j \in \mathbb{Z}$.

Cubic Spline



Timeline

- The interpolatory spline wavelets introduced by C.K. Chui and J.Z. Wang
1991 «A cardinal spline approach to wavelet»
- 1990 Demjanovich Y.K. «Локальная аппроксимация на многообразии»



Spline-wavelet transformation

$$a_i = c_i \quad \text{for } i \leq k - 3,$$

$$a_{k-2} = -(\bar{x}_k - \xi)(\xi - \bar{x}_{k-2})^{-1}c_{k-3} + \\ + (\bar{x}_k - \bar{x}_{k-2})(\xi - \bar{x}_{k-2})^{-1}c_{k-2},$$

$$a_i = c_{i+1} \quad \text{for } i \geq k - 1,$$

$$b_j = 0 \quad \text{for } j \neq k - 1,$$

$$b_{k-1} = \left[(\bar{x}_{k+1} - \xi)(\bar{x}_k - \xi)c_{k-3} - (\bar{x}_{k+1} - \xi)(\bar{x}_k - \bar{x}_{k-2})c_{k-2} + \right. \\ \left. + (\bar{x}_{k+1} - \bar{x}_{k-1})(\xi - \bar{x}_{k-2})c_{k-1} - (\xi - \bar{x}_{k-1})(\xi - \bar{x}_{k-2})c_k \right] \times \\ \times (\bar{x}_{k+1} - \bar{x}_{k-1})^{-1}(\xi - \bar{x}_{k-2})^{-1}.$$

Spline-wavelet transformation

$$c_j = a_j + b_j \quad \text{for } j \leq k - 3,$$

$$c_{k-2} = a_{k-3}(\bar{x}_k - \xi)(\bar{x}_k - \bar{x}_{k-2})^{-1} +$$

$$+ a_{k-2}(\xi - \bar{x}_{k-2})(\bar{x}_k - \bar{x}_{k-2})^{-1} + b_{k-2},$$

$$c_{k-1} = a_{k-2}(\bar{x}_{k+1} - \xi)(\bar{x}_{k+1} - \bar{x}_{k-1})^{-1} +$$

$$+ a_{k-1}(\xi - \bar{x}_{k-1})(\bar{x}_{k+1} - \bar{x}_{k-1})^{-1} + b_{k-1},$$

$$c_j = a_{j-1} + b_j \quad \text{for } j \geq k.$$

Spline-wavelets (wavelets) transformation in information security

- ✓ Wavelet linear codes
- ✓ Spline-wavelets linear codes
- ✓ Spline-wavelets robust codes
- ✓ Wavelet robust codes/AMD codes
- ✓ *Bent Functions build on spline-wavelet transformation*

Wavelet codes

Wavelet transformation

Wavelet transform can be represent in matrix form:

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_{N/2} \\ w_1 \\ w_2 \\ \vdots \\ w_{N/2} \end{bmatrix} = \begin{bmatrix} h_1 & h_2 & \cdots & h_N \\ h_{N-1} & h_N & \cdots & h_{N-2} \\ \cdots & \cdots & \cdots & \cdots \\ h_3 & h_4 & \cdots & h_2 \\ g_1 & g_2 & \cdots & g_N \\ g_{N-1} & g_N & \cdots & g_{N-2} \\ \cdots & \cdots & \cdots & \cdots \\ g_3 & g_4 & \cdots & g_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ \vdots \\ x_N \end{bmatrix} \quad (1),$$

where $\{x_1, x_2, \dots, x_N\}$ is the original sequence, $\{v_1, v_2, \dots, v_{N/2}\}$ is the main sequence, $\{w_1, w_2, \dots, w_{N/2}\}$ is wavelet sequence, $\{h_1, h_2, \dots, h_N\}$ and $\{g_1, g_2, \dots, g_N\}$ are coefficients of scaling function.

Linear wavelets codes

where

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_{N/2} \end{bmatrix} = H_{N/2,N} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ \vdots \\ x_N \end{bmatrix}$$

$$H_{N/2,N} = \mathbf{H} = \begin{bmatrix} h_1 & h_2 & \cdots & h_N \\ h_{N-1} & h_N & \cdots & h_{N-2} \\ \cdots & \cdots & \cdots & \cdots \\ h_3 & h_4 & \cdots & h_2 \end{bmatrix} =$$

$$= \text{cir}_2\{h_1, h_2, \dots, h_N\}$$

(cir_2 denotes circulant matrix with shift 2).

Similarly, for wavelet part:

where \mathbf{G} is the generator matrix of linear code

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_{N/2} \end{bmatrix} = \mathbf{G} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ \vdots \\ x_N \end{bmatrix}$$

Robust codes (nonlinear codes)

Mark Karpovsky, Boston University



Robust codes

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.

One of the main criteria for evaluating the effectiveness of a robust code is the *error masking probability*. The error masking probability $Q(e)$ can be defined as:

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

where C is the robust code, x is a codeword that belongs to the code C , e is an error, and M is the number of codewords in the code C .

Robust codes

Optimum robust code $(n, M, R)_q$ is robust code that has the maximum possible number of codewords M for a given n and robustness R with respect to:

$$M^2 - M \leq R(q^n - 1)$$

Method of constructing Systematic Robust code from Linear Codes

Let C_L be a binary linear code with length n and amount of redundant elements r . Code L can be made into a nonlinear systematic robust code:

1. by taking multiplicative inverse in $GF(2^r)$ of r redundant bits:

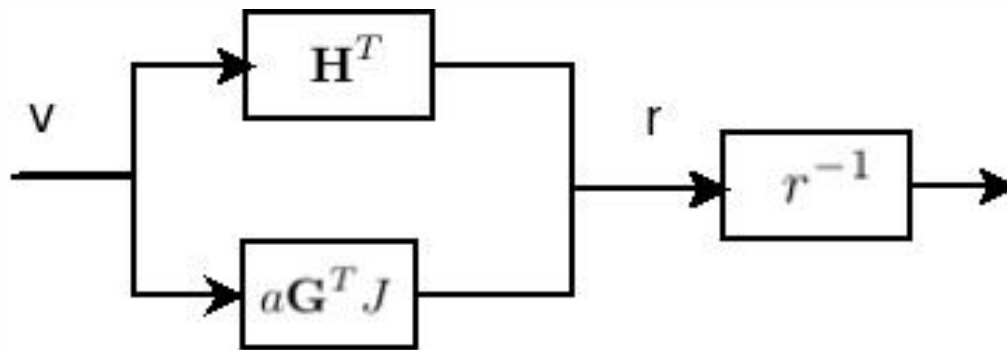
$$C_L = (x, v) \mid x \in GF(2^k), v = (Px)^{-1} \in GF(2^r)$$

2. by calculation the cube in $GF(2^r)$ of r redundant bits:

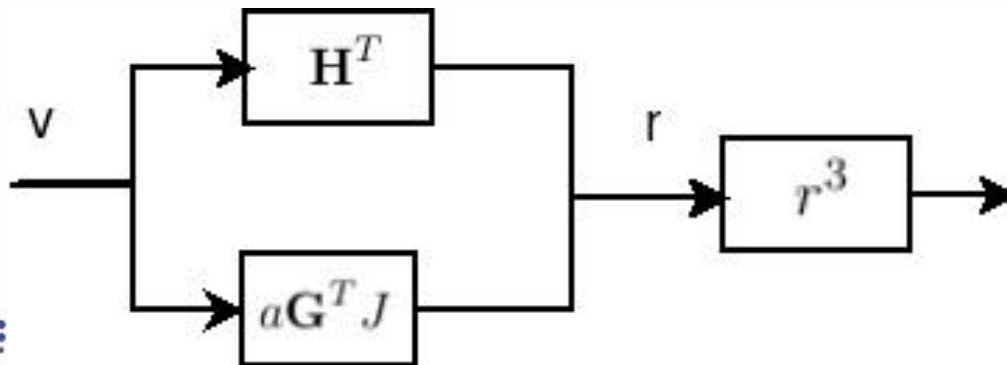
$$C_L = (x, v) \mid x \in GF(2^k), v = (Px)^3 \in GF(2^r)$$

Proposed Robust Code Scheme

by taking multiplicative inverse in $GF(2^r)$ of r redundant bits:



by calculation the cube in $GF(2^r)$ of r redundant bits:



Benefits of wavelet codes

Code	$Q(e)$	Undetectable errors
Hamming linear code	1	2^k
Partially robust Hamming code	1	2^{k-r}
Robust quadratic systematic code [2]	2^{-r}	0
Robust duplication code [2]	2^{-k}	0
Wavelet linear code	1	2^k
Wavelet robust code with encoding function $1/x$	2^{-k}	0
Wavelet robust code with encoding function x^3	2^{-k}	0

Spline-wavelet codes

Theorem 2. For the second-order spline-wavelet decomposition of the space $\Omega(X)$, formulas of the reconstruction are:


$$c_j = a_j + b_j \quad \text{for } j \leq k - 3,$$

$$c_{k-2} = a_{k-3}(\bar{x}_k - \xi)(\bar{x}_k - \bar{x}_{k-2})^{-1} +$$

$$+ a_{k-2}(\xi - \bar{x}_{k-2})(\bar{x}_k - \bar{x}_{k-2})^{-1} + b_{k-2},$$

$$c_{k-1} = a_{k-2}(\bar{x}_{k+1} - \xi)(\bar{x}_{k+1} - \bar{x}_{k-1})^{-1} +$$

$$+ a_{k-1}(\xi - \bar{x}_{k-1})(\bar{x}_{k+1} - \bar{x}_{k-1})^{-1} + b_{k-1},$$

 ITMO UNIVERSITY $c_j = a_{j-1} + b_j \quad \text{for } j \geq k.$



Theorem 3. For the second-order spline-wavelet decomposition of the space $\Omega(X)$, formulas of the decomposition are:

$$a_i = c_i \quad \text{for } i \leq k - 3,$$

$$a_{k-2} = -(\bar{x}_k - \xi)(\xi - \bar{x}_{k-2})^{-1}c_{k-3} +$$

$$+(\bar{x}_k - \bar{x}_{k-2})(\xi - \bar{x}_{k-2})^{-1}c_{k-2},$$

$$a_i = c_{i+1} \quad \text{for } i \geq k - 1,$$

$$b_j = 0 \quad \text{for } j \neq k - 1,$$

$$b_{k-1} = \left[(\bar{x}_{k+1} - \xi)(\bar{x}_k - \xi)c_{k-3} - (\bar{x}_{k+1} - \xi)(\bar{x}_k - \bar{x}_{k-2})c_{k-2} + \right.$$

$$\left. + (\bar{x}_{k+1} - \bar{x}_{k-1})(\xi - \bar{x}_{k-2})c_{k-1} - (\xi - \bar{x}_{k-1})(\xi - \bar{x}_{k-2})c_k \right] \times$$

$$\times (\bar{x}_{k+1} - \bar{x}_{k-1})^{-1}(\xi - \bar{x}_{k-2})^{-1}.$$

$$b_{k-1} = [(\overline{x_{k+1}} - \xi)(\overline{x_k} - \xi)c_{k-3} - (\overline{x_{k+1}} - \xi)(\overline{x_k} - \overline{x_{k-2}})c_{k-2} - (\overline{x_{k+1}} - \overline{x_{k-1}})(\xi - \overline{x_{k-2}})c_{k-1} - (\xi - \overline{x_{k-1}})(\xi - \overline{x_{k-2}})c_k] \cdot (\overline{x_{k+1}} - \overline{x_{k-1}})(\xi - \overline{x_{k-2}})$$

$$f(c_{k-3}, c_{k-2}, c_{k-1}, c_k) = b_{k-1} = [(c_{k-3} \oplus c_k)(\overline{x_k} \oplus c_k)c_{k-3} \oplus \oplus (c_{k-3} \oplus c_k)(\overline{x_k} \oplus c_{k-2})c_{k-2} \oplus (c_{k-3} \oplus c_{k-1})(c_k \oplus c_{k-2})c_{k-1} \oplus \oplus (c_k \oplus c_{k-1})(c_k \oplus c_{k-2})c_k](c_{k-3} \oplus c_{k-1})(c_k \oplus c_{k-2})$$

Theorem 4. *Encoding function $f(c_{k-3}, c_{k-2}, c_{k-1}, c_k) = c_k c_{k-1} \oplus c_k c_{k-3} \oplus c_{k-1} c_{k-3} \oplus c_{k-2} c_{k-3}$ is a bent function and its nonlinearity coefficient is $1/2$.*

Theorem 5. *Spline-wavelet code with encoding function $f(c_{k-3}, c_{k-2}, c_{k-1}, c_k) = c_k c_{k-1} \oplus c_k c_{k-3} \oplus c_{k-1} c_{k-3} \oplus c_{k-2} c_{k-3}$ is optimal robust code.*

Implementation in ADV612

Table 1. Comparison of the maximum error masking probability $Q(e)$ and number of undetected errors for the ADV612 computer model.

Wavelet code parameters	$\max Q(e)$	Number of the undetected errors
System without codes	1	All errors
(32, 16)-linear wavelet code	1	2^{16}
(32, 16)-robust wavelet code	2^{-15}	0

Implementation in ADV612

Compared constructions	Encoding rate in system without wavelets	Encoding rate in ADV612 computer model
System without codes	3, 14 c	2, 93 c
Linear wavelet code	3, 32 c	3, 18 c
Robust wavelet code with w^{-1} nonlinear part	3, 51 c	3, 36 c

AMD codes

2008 Ronald Cramer AMD code



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 $E : S \rightarrow G$ and deterministic decoding function $D : G \rightarrow S \cup \perp$, such that $D(E(s)) = s$ with probability 1 for each s .

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 $\delta \in G \setminus \{0\}$ and $s \in S$, the probability that $D(E(s) + \delta) \neq \perp$ less than ε .

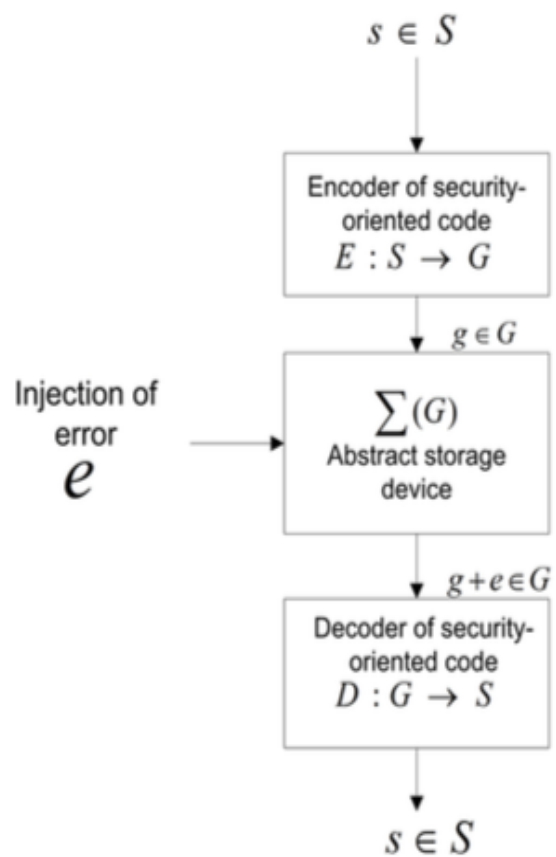
3) AMD code is called *systematic* if the set S is a group and encoding function E has the following form

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

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

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

Original information (input codewords). In practice, s is nonuniform distributed



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

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

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.

Wavelet AMD codes

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

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

BF on wavelet transformation

$$f = c_0c_1 + c_2c_3.$$

$$f = c_1c_2 + bc_4$$

$$f = c_1c_2 + c_3c_4 + c_4 \quad f = c_1c_2 + c_3c_4 + c_4c_2: \quad f = c_1c_2 + c_3c_4$$



Thank you for your attention!



SCALab

SCA Research Lab

