International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 12 Issue 02 February 2024, Page no. – 4008-4014

Index Copernicus ICV: 57.55, Impact Factor: 8.316

DOI: 10.47191/ijmcr/v12i2.02

Signature Scheme Based on Alternant Codes

Peter Arnaud Kidoudou[1], Regis Freguin Babindamana[2], Bossoto[3], Benjamin Mampassi[4]

[1,2,3,4]Faculté des Sciences et Techniques, Université Marien NGOUABI

ARTICLE INFO	ABSTRACT
Published on: 07 February 2024	In this paper, we present a version of the signature on subcodes of generalized Reed-Solomon codes defined on a subfield. We show that the use of alternating codes reduces the key size and the use of subcodes has the caracteristic of hiding the code structure. This makes the system more secure.
Corresponding Author: **Regis Freguin Babindamana**	**General Terms** MSC Classification 2020: 68P30, 94B05, 94A60

KEYWORDS: code-based cryptography, GRS, Signature, subfield, subcodes, alternant codes.

INTRODUCTION

Cryptography based on error-correcting codes [2][16][17] is an alternative to modern cryptography based on number theory. The McEliece cryptosystem is one of the best-known and most robust error-correcting cryptosystems.

This McEliece cryptosystem is based on binary Goppa codes [13][15] which are subcodes of generalized Reed-Solomon codes [14]. The enormous key size generated by the McEliece cryptosystem makes it unusable in practice.

This is why we need to look for other code families that can reduce key size.

One of the criteria guaranteed by modern cryptography is the non-repudiation of transactions, which is ensured by the signature. A signature verifies that a message has been sent by the holder of a public key.

The first code-based signature scheme was developed by Courtois-Finiasz-Sendrier [9][7] using binary Goppa codes.

In this paper, we describe a signature scheme based on the subcodes of GRS codes[18][20] on a subfield.

The use of alternating codes has the advantage of reducing key size and hiding the code structure to avoid structural attacks.

This paper is organized as follows:

- In the first section we present a background of generalized Reed-Solomon codes and subfield.
- In the second section, we propose a new signature protocol.

1. BACKGROUND ON GENERALIZED REED SOLOMON SUB-CODES AND SUBFIELD

1.1. Error correcting codes

Definition 1.1. Let be $F_{q^m}^n$ a finite field. A linear code C of length n and of dimension k is a vector subspace of $F_{q^m}^n$.

We denote by d its minimum distance, defined as follows:

$$d=min\ \{d_H\ (c, c')\ |c, c' \in \mathsf{C}\ , c \neq c'\} = min\ \{wt(\ c)\ |c\ \in \mathsf{C}\ \{0\}\}$$

One notes $[n, k, d]$ the code parameters. If C is an $[n, k, d]$ code then any matrix $\mathbf{G}\ \in F_q^{k\times n}$ such that:

$$\mathsf{C}= \{m\mathbf{G}, m \in\ F_q^k\}$$

is called the generating matrix of C.The rows of $\mathbf{G}$ form a basis of C. From another point of view, any matrix $H \in F_q^{(n-k)\times n}$ such that:

$$\mathsf{C}= \{\ c \in\ F_q^k\ H\ c^T\ = 0^T\}$$

is called the parity matrix, or control matrix, of C. A parity equation is any vector h such that $< h, c >= 0$ for all $c \in \mathsf{C}$.

The rows of H therefore form a basis of the orthogonal space to C.

Definition 1.2. Let C an $[n, k, d]$ code. We denote by $\mathsf{C}^{\perp}$ the space of vectors of F_q^n which are orthogonal to those of C. The space $C^{\perp}$ is called the dual code of C.

It is a code of length n and of dimension n-k. Its minimum distance is denoted by d^T.

Note that a generating matrix of $\mathsf{C}^{\perp}$ is a parity matrix of C and inversely $(\mathsf{C}^{\perp})^{\perp}$ unlike R ou C the intersection $\mathsf{C} \cap \mathsf{C}^{\perp}$ not always zero (non-zero isotropic vectors may exist in F_q^n). For example (1,1) $\in F_2^2$

Definition 1.3. Let C be an $[n, k, d]$ code and $I \subset [1, n]$ such that $|I|=i$ with cardinal then $1 \leq i \leq n-1$ then

1. Punctured C on I is:

$$\mathrm{Punct}_I(\mathsf{C}) = \{ \pi_{[1,n]\setminus I^{(c)}|c\in\mathsf{C}} \} \subseteq F_q^{n-i}$$

2. Shortened C on I is:

$$\mathrm{Short}_I(\mathsf{C}) = \{ \pi_{[1,n]\setminus I^{(c)}|c\in\mathsf{C}} \} \subseteq F_q^{n-i}$$

1.2. Property [12] For any code C and any subset $I \subset [1, n]$ with cardinal $1 \leq |I| \leq n-1$ on has

$$\mathrm{Punct}_I(\mathsf{C})^{\perp} = \mathrm{Short}_I(\mathsf{C}^{\perp})$$

Definition 1.4. Let $\mathsf{C} \subseteq F_q^n$ be a k-dimensional code. The information set of C is a subset $I \subset [1, n]$ of cardinal k such that $\pi_I(\mathsf{C})$is of dimension k. In short, I contains all the information of the code words.

1.3. Cyclic code

Definition 1.5. Cyclic codes are widely used in data communication because their structure makes encoder and decoder circuitry simple. Hill in 1986 defined code C as cyclic $[n, k]$-code if is a linear code of length n over a finite field and if any cyclic shift of a codeword is also a codeword. Thus, for a cyclic code C,

$$(c_0, \ldots, c_{n-1}) \in \mathsf{C} \Rightarrow (c_n, c_1, .., c_{n-1}) \in \mathsf{C}$$

The permutation σ

$\sigma(c_0, \ldots, c_n) = (c_n, .., c_{n-1})$ is called "shift".

1.4. Bose-Chaudhuri-Hocquenghem (BCH) Codes

Definition 1.6. A BCH code is a cyclic polynomial code over a finite field with a particularly chosen generator polynomial. Hamming codes are the subset of BCH codes with $k= 2^m-1-m$ and an error correction of 1. Generally, a family of t-error correcting codes defined over finite fields F_q where $2t+1<q$, are BCH codes or RS codes [11]. The main advantage of BCH codes is the ease with which they can be decoded using syndrome and many good decoding algorithms exist. A well-known decoding algorithm is the Berlekamp-Massey algorithm. This allows very simple electronic hardware to perform the task, making the need for a computer unnecessary. This implies that a decoding device may be small and consume little power. BCH codes allow control over block length and acceptable error thresholds, which makes them very flexible. This indicates that code can be designed to meet custom requirements. Another reason they are important is that there exist good decoding algorithms that correct multiple errors. Hocquenghem, as well as Bose and Ray-Chaudhuri, discovered the class of BCH codes, but not the decoding.

Peterson developed the first decoding algorithm in 1960 followed by refinement from Berlekamp, Massey and many others [19]

1.5. Theorem

A Reed-Solomon code of length q-1 and of constructed distance d $(2 \leq d \leq q-1)$is a cyclic code such that its generator polynomial is written as:

$$g(x) = (x-\delta^r)(x-\delta^{r+1}).\ldots.(x-\delta^{r+d-2})$$

Where δ is a primitive element of F_q.Its parameters are $[q-1, q-d, d]$. It is therefore an MDS code. For further details and proof, please refer to [9].

1.6. Reed-Solomon codes.

Reed-Solomon codes are block-based error correcting codes with a wide range of applications in digital communications and storage. Reed-Solomon codes are used to correct errors in many systems including:

- Storage devices (including tape, Compact Disk, DVD, barcodes, etc)
- Wireless or mobile communications (including cellular telephones, microwave links, etc)
- Satellite communications
- High-speed modems such as ADSL, xDSL, etc.

1.7. Generalized Reed Solomon Code (GRS).

Definition 1.7. Consider nonzero elements $(v_0, \ldots, v_{n-1}) \in F_q^n$ and distinct elements $(\delta_0, \ldots, \delta_{n-1}) \in F_q^n$. Set $S = (v_1, \ldots, v_n)$ and $\Delta = (\delta_0, \ldots, \delta_n)$. For $1 \leq k \leq n$ let define the generalized Reed-Solomon codes

$$\mathrm{GRS}_{n,k}(S, \Delta) := \{(v_1 f(\delta_1), \ldots, v_n f(\delta_n)) | f(x) \in F_q^n[x]_k\}$$

Here we write $F_q^n[x]_k$ for the set of polynomials $\in F_q^n[x]$ of degree less than k $(F_q^n[x]_k$ is a vector space of dimension k over $F_q^n)$.For fixed n, S and Δ the various GRS codes enjoy the nice embedding property $\mathrm{GRS}_{n,k-1}(S, \Delta) \leq \mathrm{GRS}_{n,k}(S, \Delta)$.

If $f(x)$ is a polynomial, then we shall usually write $\boldsymbol{f}$ for its associated codeword. This codeword also depends upon S and Δ; so at times we prefer to write unambiguously

$$\mathrm{es}_{s,\Delta}(f(x)) = \{(v_1 f(\delta_1), \ldots, v_n f(\delta_n))\}.$$

1.7. 1.Theorem

Any basis $(f_1(x),\ldots,f_n(x))$ of $F_q^n[x]_k$ gives rise to a basis $(\boldsymbol{f}_1,\ldots..,\boldsymbol{f}_n)$ of the code. A particularly nice polynomial basis is the set of monomials $1,x,\ldots,x^i,\ldots,x^{k-1}$.The corresponding generator matrix, whose i^{th}.row (numbering rows from 0 to *k-1*) is:

$$\mathrm{es}_{s,\Delta}(x^i)=\{(v_1\delta_1^i,\ldots v_j\delta_j^i.,v_n\delta_n^i)\}.$$

is the canonical generator matrix for $\mathrm{GRS}_{n,k}(\mathrm{S},\Delta)$:

$$\begin{pmatrix} \mathrm{v}_1 & . & .\mathrm{v}_J & . & \mathrm{v}_n \\ \mathrm{v}_1\delta_1. & . & .\mathrm{v}_\mathrm{j}\delta_\mathrm{j} & . & \mathrm{v}_n\delta_n \\ \mathrm{v}_1\delta_1^i. & . & .\mathrm{v}_\mathrm{j}\delta_\mathrm{j}^i & . & \mathrm{v}_n\delta_n^i \\ \mathrm{v}_1\delta_1^{k-1} & . & .\mathrm{v}_j\delta_\mathrm{j}^{k-1} & . & \mathrm{v}_n\delta_n^{k-1} \end{pmatrix}$$

1.8. Notion of subcodes on a subfield of a code

The subfield subcode C^* over F_q. of a F_{q^m} linear code C defined is the set of words of C that have components over F_q.

1.8.1. Construction of a subfield C^* on $\boldsymbol{F_q}$ by using a generator matrix

Suppose that the code C on F_{q^m} is defined by a parity matrix *H*. Let $H=(H_{ij})$ with $(H_{ij})\in F_{q^m}$ $1\le i\le r, 1\le j\le n$. H is a^T therefore an $r\times n$ matrix._The code C^* on F_q. consists of all the vectors $\mathrm{a}=(\mathrm{a}_0,\ldots,\mathrm{a}_n)$,with each $\mathrm{a}_i\in F_q$ such that $H=0$

1.8.2. Another construction

Let $(\alpha_1,\ldots,\alpha_n)$ be a basis of F_{q^m} over F_q. And

$$h_{ij}=\sum_{i=1}^{n} h_{ijl}\,\alpha_l \quad h_{ijl}\in F_q$$

One defines a matrix H^* of size $rm\times n$ obtained by replacing each entry in h_{ij} by the corresponding column vector $(h_{ij1},\ldots,h_{ijm})^T$ of F_q and so

$$H^*=\begin{pmatrix} h_{111} & . & .h_{121} & . & h_{1n1} \\ h_{112} & . & .h_{122} & . & h_{1n2} \\ h_{11n}. & . & .h_{12m} & . & h_{1nm} \\ h_{r1n}. & . & .h_{r2m} & . & h_{rnm} \end{pmatrix}$$

Then a $\in$ C^*

$$\begin{cases} <=> \sum_{i=1}^{n} h_{ij}\,a_i \;for\; i=1,\ldots,r \\ <=> \sum_{i=1}^{n} h_{ijl}\,a_i \;for\; i=1,\ldots,r\; l=1,\ldots,m \\ <=> H^*a^T=0 \end{cases}$$

The rank of H^* over F_{q^m} is at most equal to rm.Thus C^* is an [*n*, *k* ≥ *n-rm*] code assuming $rm\le n$.

Definition 1.8. Let $\beta=\{\beta_0,\ldots,\beta_{n-}\}\in F_{q^m}$ and denote by θ_β: F_{q^m}->F_q^m.

θ_β can be extended in the space $F_{q^m}^n$

if $\mathrm{C}=(\mathrm{c}_1,\ldots,\mathrm{c}_n)\in F_{q^m}^n$ then $\theta_\beta(\mathrm{C})=(\theta_\beta(\mathrm{c}_1),\ldots,\theta_\beta(\mathrm{c}_n))$.The q-ary image of a code C in relation to the base β is the image:

$\mathrm{I}_{mq}(\mathrm{C})=\theta_\beta(\mathrm{C})$

$\mathrm{I}_{mq}(\mathrm{C})$ is a linear code of length nm.This code depends on the choice of the base β

In order to construct a generator matrix g of $\mathrm{I}_{mq}(\mathrm{C})$ on F_{q^m} with $\mathrm{I}_{mq}(\mathrm{C})\neq F_{q^m}$,it is necessary to take all the multiples of $\mathbf{G}$ simply take n, a multiple of F_q linear).

Proposition 1.1.[12]

If $g=\alpha_{ij}$ is a generator matrix of size $k\times m$ then $mk\times nm$ a matrix $\mathbf{G}$ obtained by replacing each α_{ij} by matrix $m\times n$ corresponding $\boldsymbol{M}_{\alpha_{ij}}$.We denote by $\boldsymbol{M}_\alpha$ the matrix of the corresponding endomorphism: with obvious notations, if $\theta_\beta(\mathrm{x})=(\mathrm{x}_1,\ldots,\mathrm{x}_m)$ then $\theta_\beta(\alpha\mathrm{x})=(\mathrm{x}_1,\ldots,\mathrm{x}_m)\,\boldsymbol{M}_\alpha$.

1.9. Subcodes on generalized subspaces

Definition 1.9. let C be a linear m-block of length *n*. Let *k* be an integer smaller than *m*. Let $(\mathrm{v}_1,\ldots,\mathrm{v}_n)$ a set of *k*-dimensional subspaces of $\mathrm{E}=F_q^m$ .We have $\bar{V}=(\mathrm{v}_1,\ldots,\mathrm{v}_n)$ with n-tuple.

Generalization of a *k*-subspace on the subcodes of C in relation to $\bar{V}$ is $\mathrm{C}_{|\bar{V}}=\mathrm{C}\cap\bar{V}$

Proposition 1.2.[6]

A subcode on the generalized subspaces of an *m*-block code C is a subcode subspace of a code C' which is multiplicatively equivalent to C.

However, the parameter limits obtained by considering the $\mathrm{CSS}_v(\mathrm{C})$ code as a shortened code apply to the subcodes of the generalized subspaces.

We propose an algorithm (**Algorithm 1**) to efficiently compute a generating matrix of a subcode on generalized subspaces.

Algorithm 1: Generator matrix GSS

Input G: an m-block generator matrix of the code $\mathcal{C}$ with $i \in [1,..,n]$
G is a generator matrix of size $k \times m$
Let $\beta \doteq (b_1, \cdots, b_m)$ a basis of $\mathbb{F}_q^m$
Output : $\mathcal{G}$ generator matrix
(1) $\mathcal{G} \doteq (\beta_{ij})$
(2) Compute the systematic matrix $\mathcal{G}_{sys}$
(3) construction of the q-ary image $\mathrm{Im}(\mathcal{G}_{sys})$
(4) Replace each entry β_{ij} with the matrix $M_{\beta_{ij}}$ of size $m \times m$
(5) compute the generator matrix $\mathcal{G}$ of GSS
(6) return $\mathcal{G}$

1.10.Alternant codes

Definition 1.10. An alternant code is a subfield subcode of a GRS code. It inherits the decoding algorithm of the underlying Reed-Solomon code.

1.11. Example: let *n=7*, *k=6*, *d=3* α a root of $\alpha^3 + \alpha^2 + 1$.

$$\mathcal{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^2+\alpha+1 & \alpha^2+\alpha & \alpha & \alpha^2+1 & \alpha+1 \\ 1 & \alpha^3 & \alpha^2+\alpha & \alpha^2 & \alpha+1 & \alpha & \alpha^2 \\ 1 & \alpha^4 & \alpha & \alpha+1 & \alpha^2 & \alpha^2+\alpha & \alpha^2+1 \\ 1 & \alpha^5 & \alpha^2+1 & \alpha & \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha^2 \end{pmatrix}.$$

The systematic matrix is:

$$\mathcal{G}_{sys} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \alpha^6 \\ 0 & 1 & 0 & 0 & 0 & 0 & \alpha^5 \\ 0 & 0 & 1 & 0 & 0 & 0 & \alpha^5 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \alpha^6 \\ 0 & 0 & 0 & 0 & 0 & 1 & \alpha^7 \end{pmatrix}$$

The q-ary image (binary image) of the generator matrix G in the basis
$\{1 = (100), \alpha = (010), \alpha^2 = (001)\}$ is:

$$Im_2(\mathcal{G}_{sys}) \doteq \begin{pmatrix} M_1 & M_0 & M_0 & M_0 & M_0 & M_0 & M_{\alpha^6} \\ M_0 & M_1 & M_0 & M_0 & M_0 & M_0 & M_{\alpha^5} \\ M_0 & M_0 & M_1 & M_0 & M_0 & M_0 & M_{\alpha^5} \\ M_0 & M_0 & M_0 & M_1 & M_0 & M_0 & M_0 \\ M_0 & M_0 & M_0 & M_0 & M_1 & M_0 & M_{\alpha^6} \\ M_0 & M_0 & M_0 & M_0 & M_0 & M_1 & M_{\alpha^7} \end{pmatrix}$$

$$Im_2(\mathcal{G}) \doteq \left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc} 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ \hline 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ \hline 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&1 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0 \\ \hline 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ \hline 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0 \\ \hline 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1 \end{array}\right)$$

With

$$M_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} M_{\alpha^i} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \text{for all } i \in \{1,\ldots,6\}$$

1.12. Remark

As we can see, we have a so-called hollow matrix with many zero elements and a few non-zero elements. This makes difficult to structure the original code used. We have thus the following generator matrix:

$$\mathcal{G} \doteq \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&1 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1 \end{pmatrix}.$$

2. SIGNATURE SCHEME

2.1. Description

A signature verifies that a message has been sent by the holder of a "public key". This cryptographic process enables anyone to verify the identity of the author of a document and to ensure that it has not been altered.

This cryptographic process enables anyone to verify the identity of the author of a document and guarantee that it has not been altered. The process is based on a pair of keys: one is private and known only to its holder, the other is public and accessible to all. The signature is generated using the private key. The public key is used to verify the signature. This verification can therefore be carried out by anyone with access to the public key.

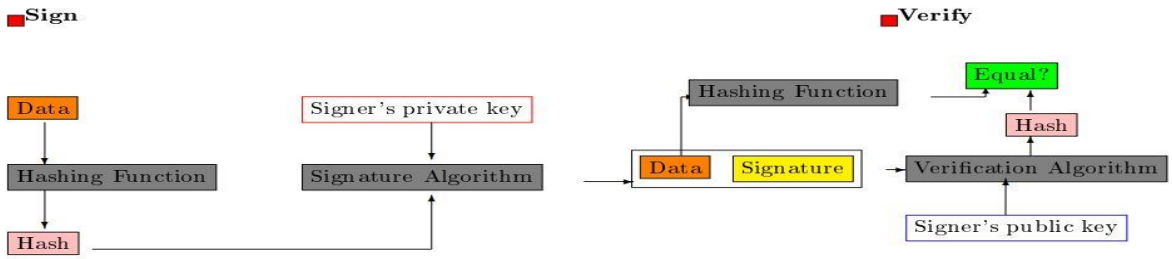

FIGURE 1. Signature scheme

A signature scheme is composed of two algorithms:

- a signature algorithm
- a verification algorithm

Signature scheme is a quintuplet (ρ, A, K, δ, V)

- ρ: Set of messages
- A: *Signature set*
- K: *Key signature set*
- δ: *signature algorithm*
- V: *verification algorithm*

for $k \in K$ there is a signature algorithm $\mathrm{Sgn}_k \in \delta$ and a verification algorithm Verify $\in V$

2.2. Signature scheme based on the subcodes of generalized subspaces

Fiat-Shamir obtains signatures by transforming the zero-knowledge identification scheme. We use the Fiat-Shamir transformation [10] to implement the new signature scheme based on the subcodes of generalized subspaces. We propose the following algorithms.

Algorithm 2: Key generation algorithm

Key generation:
Input:
Let integer k, m, n and with $k < n \leq m$
data :
$\mathcal{G}$ generator matrix of a alternant Codes
h hash function,
$\mathcal{S}$ invertible matrix of size $k \times k$
$\mathcal{P}$ permutation matrix of size $n \times n$
$\mathcal{G}_{pub} \doteq \mathcal{SGP}$
$l \in \mathbb{F}_{q^m}^k$, ϑ: number of round
private key: $l \in \mathbb{F}_{q^m}^k$ and $e \in \mathbb{F}_{q^m}^n$
public key: $x' = l\mathcal{G}_{pub} + e$, $r = wt(e) = \frac{n-k}{2}$

Algorithm 3: Signature algorithm

Signature:
$i = 0$
While$(i \leq \vartheta - 1)$
(1) $u_i \leftarrow\$\ \mathbb{F}_2^k$, $\sigma_i \leftarrow\$\ \{1, .., k\}$
(2) $c_{1i} \leftarrow \mathrm{h}(\sigma_i)$
(3) $c_{2i} \leftarrow \mathrm{h}(\sigma_i(u_i + l) \cdot \mathcal{G}_{pub})$
(4) $c_{3i} \leftarrow \mathrm{h}(\sigma_i(u_i \cdot \mathcal{G}_{pub} + x'))$
(5) cmt$=(c_{1i}|c_{2i}|c_{3i}|...|c_{1\vartheta-1}|c_{2\vartheta-1}|c_{3\vartheta-1})$
ch=h(cmt,msg)
$b \leftarrow\$\ \{0, 1, 2\}$
$i = 0$
while $(i \leq \vartheta - 1)$
(1) **if** $b_i = 0$
$\mathrm{rep}_{1i} \leftarrow \sigma$, $\mathrm{rep}_{2i} \leftarrow u_i + l$
(2) **if** $b_i = 1$
$\mathrm{rep}_{1i} \leftarrow \sigma_i((u_i + l) \cdot \mathcal{G}_{pub})$ $\mathrm{rep}_{2i} \leftarrow \sigma_i(e)$
(3) **if** $b_i = 2$
$\mathrm{rep}_{1i} \leftarrow \sigma_i$, $\mathrm{rep}_{2i} \leftarrow u_i$
rep$=(\mathrm{rep}_{1i}, \mathrm{rep}_{2i}, ..., \mathrm{rep}_{1,\vartheta-1}, \mathrm{rep}_{2,\vartheta-1})$
return Sgn $\leftarrow$ (cmt,rep)

Algorithm 4: Verification algorithm

1 Verification:
2 ch=h(cmt,msg)
3 extracts cmt
4 $i = 0$
5 While$(i \leq \vartheta - 1)$
(1) $c_{1i} \leftarrow \mathrm{h}(cmt_i)$
(2) $c_{2i} \leftarrow \mathrm{h}(cmt_i)$
(3) $c_{3i} \leftarrow \mathrm{h}(cmt_i)$
(4) **if** $b_i = 0$ then
$c_{1i} = \mathrm{h}(\mathrm{rep}_{1i})$ and $c_{2i} = \mathrm{h}(\mathrm{rep}_{1i}(\mathrm{rep}_{2i} \cdot \mathcal{G}_{pub})$
(5) **if** $b_i = 1$ then
$c_{2i} = \mathrm{h}(\mathrm{rep}_{1i})$ and $c_{3i} = \mathrm{h}(\mathrm{rep}_{1i} + \mathrm{rep}_{2i})$
and $\mathtt{wt}(\mathrm{rep}_{2i}) = r$
(6) **if** $b_i = 2$ then
$c_{1i} = \mathrm{h}(\mathrm{rep}_{1i})$ and $c_{3i} = \mathrm{h}(\mathrm{rep}_{1i}(\mathrm{rep}_{2i} \cdot \mathcal{G}_{pub} + x'))$
if cmt$=(c_{1i}|c_{2i}|c_{3i}|...|c_{1\vartheta-1}|c_{2\vartheta-1}|c_{3\vartheta-1})$ then the signature is valid.

2.2.1. Example: Let : G be an |21,18,3], code $P \in F_{q^m}^n$ *and* $S \in F_{q^m}^k$
The public generator matrix $G_{pub} = SGP$

$$\begin{pmatrix}
1&1&1&0&0&1&0&1&0&1&0&1&1&0&1&1&1&1&0&0&0\\
1&1&0&0&0&1&0&1&0&1&1&1&1&0&0&1&1&0&1&1&1\\
0&0&0&1&0&0&0&0&1&1&1&1&1&1&0&1&1&0&1&1&1\\
0&0&1&0&0&1&0&0&0&0&1&0&0&0&1&0&1&0&0&0&1\\
0&1&0&1&1&1&1&0&1&1&1&1&0&0&1&0&1&1&1&0&0\\
1&1&0&1&1&0&1&0&1&1&1&1&1&0&0&1&0&0&0&1&0\\
0&0&1&1&0&0&0&0&0&1&0&0&0&0&0&1&1&1&0&0&0\\
0&0&0&0&1&0&0&1&1&0&0&0&1&0&0&1&1&1&0&0&1\\
1&1&0&0&1&0&1&0&1&1&1&0&0&1&1&0&0&1&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1&0\\
0&0&0&0&1&1&1&0&1&1&0&1&1&0&1&0&0&0&1&0&0\\
1&0&1&1&1&1&0&1&0&1&1&0&0&1&1&1&0&1&1&1&0\\
1&1&0&0&0&1&1&0&0&1&0&0&1&0&1&1&1&0&0&1&1\\
1&1&1&1&1&0&0&1&1&0&0&1&1&0&0&1&0&0&1&1&0\\
0&1&1&0&1&1&0&1&1&0&1&0&0&0&1&1&1&1&1&0&0\\
0&1&1&0&1&1&1&1&0&1&1&1&0&0&1&0&1&1&1&1&0\\
0&0&0&1&1&0&1&0&0&0&0&0&0&1&1&1&1&1&0&1&1\\
0&0&1&1&0&1&0&1&0&1&1&1&0&1&0&0&1&0&0&1&1
\end{pmatrix}$$

The private key is: *sk= (e, l)* with

e= (0 0 0 0 0 0 0 1 01 0 0 0 0 1 0 0 0 0 0 0) *l*= (1 1 0 1 1 0 1 1 0 1 1 0 0 1 0 0 11).

The public key is: *pk*= (1 11 0 0 01 0 0 0 0 1 10 1 0 0 0 0 11).

We use a hash function: hash let:
commitments *ch:*

3635780394363946408480713917344480713650181-8787340603405549986480713650243-922337155614112558

the answers rep:
'[12, 9, 14, 10, 1, 5, 17, 16, 3, 11, 8, 6, 18, 15, 2, 7, 4, 13](0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)[3, 1, 14, 5, 13, 11, 15, 9, 8, 2, 7, 10, 4, 17, 18, 12, 16, 6](0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)'.

The final signature is composed of :(ch, rep)

'3635780394363946408480713917344480713650181-8787340603405549986480713650243-922337155614112558[12, 9, 14, 10, 1, 5, 17, 16, 3, 11, 8, 6, 18, 15, 2, 7, 4, 13](0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)[3, 1, 14, 5, 13, 11, 15, 9, 8, 2, 7, 10, 4, 17, 18, 12, 16, 6](0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)'.

Proposed parameters

Size of secret key	$m \times k + m \times n$
Public key size	$m \times n + log_2(r)$
Matrix size	$m \times n \times k$
Total number of bits exchanged	$\delta(3\mathrm{h} + 2 + \frac{2}{3}(mk + k))$

2.3. Security parameter
The main strength of this system is that it is used to mount structural attacks against code-based cryptosystems.
In our zero-knowledge system [8] [1] [5][15] the Veron scheme [3][4] (with several rounds) probability of cheating is 2/3 for the security of 2^{80}, 150 rounds are required. The

number of rounds reduces the probability of identity theft according to our needs. In general, to achieve a level of security with a probability of identity theft, the number of rounds $\delta = log_q(1/2^l)$ is determined.

ISO/IEC-9798-5 specifies two probability values: 2^{-16} and 2^{-32} or 28 and 56 rounds.

CONCLUSION

Alternant codes are generalized Reed Solomon codes, like the Goppa codes used in code-based cryptography schemes. The use of these codes in cryptography results in secure cryptosystems with reasonable key sizes. Our signature scheme presents within its generalized subdomains leads to the theory and hiding of codes. it has an advantage in terms of low communication cost and resilience against quantum computer attacks. No secret information can be deduced in polynomial time during scheme execution thanks to zero-knowledge.

REFERENCES

1. Aguilar, C., Gaborit, P., Schrek, J.: A new zero-knowledge code based identification scheme with reduced communication. In: 2011 IEEE Information Theory Workshop. pp. 648–652. IEEE (2011))
2. Aragon, N., Blazy, O., Gaborit, P., Hauteville, A., Zémor, G.: Durandal: a rank metric based signature scheme. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 728–758. Springer (2019
3. Aragon, N.: Cryptographie à base de codes correcteurs d'erreurs en métrique rang et application. Ph.D. thesis, Université de Limoges (2020)
4. Bellini, E., Caullery, F., Hasikos, A., Manzano, M., Mateu, V.: Code-based signature schemes from identification protocols in the rank metric. In: International Conference on Cryptology and Network Security. pp. 277–298. Springer (2018).
5. Bellini, E., Gaborit, P., Hasikos, A., Mateu, V.: Enhancing code based zero-knowledge proofs using rank metric. In: Cryptology and Network Security: 19th International Conference, CANS 2020, Vienna, Austria, December 14–16, 2020, Proceedings 19. pp. 570–592. Springer (2020)
6. Berger, T.P., Gueye, C.T., Klamti, J.B.: Generalized subspace subcodes with application in cryptology. IEEE Transactions on Information Theory 65(8), 4641–4657 (2019)
7. Cayrel, P.L., Alaoui, S.: Dual construction of stern-based signature scheme 63,98–103 (03 2010).
8. Cayrel, P.L., Véron, P., El Yousfi Alaoui, S.M.: A zero-knowledge identification scheme based on the q-ary syndrome decoding problem. In: International Workshop on Selected Areas in Cryptography. pp. 171–186. Springer (2010)
9. Courtois, N.T., Finiasz, M., Sendrier, N.: How to achieve a mceliece-based digital signature scheme. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 157–174. Springer (2001)
10. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Conference on the theory and application of cryptographic techniques. pp. 186–194. Springer (1986)
11. Hill, R.: A first course in coding theory. Oxford University Press (1986)
12. Huffman, W.C., Pless, V.: Fundamentals of error-correcting codes. Cambridge university press (2010)
13. Loidreau, P.: Etude et optimisation de cryptosystèmes à clé publique fondés sur la théorie des codes correcteurs. Ph.D. thesis (5 2001)
14. McWilliams, F., Sloane, N.: The theory of error correcting codes, north mathematical library, vol. 16 (1983)
15. Misoczki, R., Barreto, P.S.: Compact mceliece keys from goppa codes. In: International Workshop on Selected Areas in Cryptography. pp. 376–392. Springer (2009)
16. Moufek, H.: Les codes correcteurs pour la cryptographie. Ph.D. thesis, Faculté de Mathématiques (2017)
17. Richmond, T. : Implantation sécurisée de protocoles cryptographiques basés sur les codes correcteurs d'erreurs. (secure implementation of cryptographic protocols based on error-correcting codes) (2016)
18. Sidelnikov, V.M., Shestakov, S.O.: On insecurity of cryptosystems based on generalized reed-solomon codes (1992)
19. Trappe, W.: Introduction to cryptography with coding theory. Pearson Education India (2006)
20. Wieschebrink, C.: Cryptanalysis of the niederreiter public key scheme based on grs subcodes. In: Post-Quantum Cryptography: Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings 3. pp. 61–72. Springer (2010)