Non commutative Goppa codes and their use in code-based cryptography

J. Gómez-Torrecillas
Universidad de Granada

F. J. Lobillo
Universidad de Granada

G. Navarro
Universidad de Granada

May 29, 2023

Abstract

A class of linear codes that extends classical Goppa codes to a non-commutative context is defined. An efficient decoding algorithm, based on the solution of a non-commutative key equation, is designed. We show how the parameters of these codes, when the alphabet is a finite field, may be adjusted to propose a McEliece-type cryptosystem.

1 Skew Goppa codes

The results of this talk can be found in [3, 4]. Let $R = L[x;\sigma,\partial]$ be an Ore extension of a field. Let $F \subseteq L$ be a subfield such that $[L : F] = m$. Let $g \in R$ be a nonzero twosided polynomial, $\alpha_0, \dots, \alpha_{n-1} \in L$ be P-independent elements such that $(x-\alpha_i, g)_\ell = 1$ for all $0 \leq i \leq n-1$, $h_i \in R$ such that $\deg(h_i) < \deg(g)$ and $(x-\alpha_i)h_i - 1 \in Rg$, and $\eta_0, \dots, \eta_{n-1} \in L^*$. A (generalized) skew differential Goppa code $\mathcal{C} \subseteq F^n$ is defined as

$$\mathcal{C} = \left\{ (c_0, \dots, c_{n-1}) \in F^n \mid \textstyle\sum_{i=0}^{n-1} h_i \eta_i c_i \in Rg \right\}.$$

We say that $\{\alpha_0, \dots, \alpha_{n-1}\}$ are the positional points, g is the skew differential Goppa polynomial and $h_0, \dots, h_{n-1}$ are the parity check polynomials.

For a received word $r = c + e \in F^n$, where $c \in \mathcal{C}$ and $e = \sum_{j=1}^{\nu} e_j \varepsilon_{k_j}$ with $e_j \neq 0$ for $1 \leq j \leq \nu$, The *syndrome polynomial* is defined and computed as

$$s = \sum_{i=0}^{n-1} h_i \eta_i r_i.$$

We define the *error locator polynomial* as

$$\lambda = \left[\{x - \alpha_{k_j} \mid 1 \leq j \leq \nu\} \right]_\ell .$$

Then $\deg(\lambda) \leq \nu$ and, for all $1 \leq j \leq \nu$, there exists $\rho_{k_j} \in R$ such that $\deg(\rho_{k_j}) \leq \nu - 1$ and

$$\lambda = \rho_{k_j}(x - \alpha_{k_j}).$$

The *error evaluator polynomial* is defined as

$$\omega = \sum_{j=1}^{\nu} \rho_{k_j} \eta_{k_j} e_j.$$

It follows that $\deg(\omega) < \nu$.

Theorem 1.1. *The error locator λ and the error evaluator ω polynomials satisfy the non-commutative key equation*

$$\omega = \kappa g + \lambda s, \tag{1}$$

for some $\kappa \in R$. Assume that $\nu \leq t = \left\lfloor \frac{\deg g}{2} \right\rfloor$. Let u_I, v_I and r_I be the Bezout coefficients returned by the left extended Euclidean algorithm (LEEA) with input g and s, where I is the index determined by the conditions $\deg r_{I-1} \geq t$ and $\deg r_I < t$. Then there exists $h \in R$ such that $\kappa = hu_I$, $\lambda = hv_I$ and $\omega = hr_I$.

This theorem allows to use the LEEA to solve the key equation. Decoding failures, which can appear when $(\lambda, \omega)_\ell \neq 1$, are solved in a similar way to [2].

2 A McEliece cryptosystem based on skew Goppa codes

When $\mathbb{F}_q = F \subseteq L = \mathbb{F}_{q^m}$ and $\partial = 0$, with $q = p^d$, we propose a key encapsulation mechanism based in McEliece and Niederreiter's cryptosystems (see [1, 5, 6]). Assume $\sigma(a) = a^{p^h}$ and let $\delta = (h, dm)$, $\mu = \frac{dm}{\delta}$. Then $K = \mathbb{F}_{p^\delta}$. Then it follows

$$\max\left\{\frac{n}{10t}, \frac{n\delta}{d(p^\delta - 1)}\right\} \leq m \leq \frac{n}{4t} \text{ and } \delta \mid dm. \tag{2}$$

Our proposal of a McEliece cryptosystem follows the dual version of Niederreiter [6], by means of a key encapsulations mechanism like the one proposed in [1].

2.1 Key schedule

The inputs are $n \gg t$ and $F = \mathbb{F}_q$ with $q = p^d$. In order to generate the public and private keys for a McEliece type cryptosystem, parameters m, δ, h have to be found. The values of m, δ can be computed randomly via an exhaustive search looking for pairs satisfying (2). We set $k = n - 2t \left\lfloor \frac{n}{4t} \right\rfloor$, the smaller possible dimension. Next pick randomly $h \leq dm$ such that $(h, dm) = \delta$, and let $\mu = \frac{dm}{\delta}$, $L = \mathbb{F}_{q^m}$, $K = \mathbb{F}_{p^\delta}$ and $\sigma = \tau^h : L \to L$. Fix a basis of L over F and denote $\mathfrak{v} : L \to F^m$ the map providing the coordinates with respect to this basis. Let also denote $R = L[x; \sigma]$.

Our set of positional points are going to be selected amongst the points in a maximal left P-independent set. We randomly pick a normal basis $\{\alpha, \sigma(\alpha), \ldots, \sigma^{\mu-1}(\alpha)\}$ and a primitive element γ of L. Let

$$\mathsf{P} = \left\{\gamma^i \frac{\sigma^{j+1}(\alpha)}{\sigma^j(\alpha)} \mid 0 \leq i \leq p^\delta - 2, 0 \leq j \leq \mu - 1\right\}$$

The list $\mathsf{E} = \{\alpha_0, \ldots, \alpha_{n-1}\}$ of positional points is obtained by a random selection of n points in P.

The skew Goppa polynomial is twosided, hence $g = \overline{g} x^a$ where $\overline{g} \in Z(R) = K[x^\mu]$. Since $0 \notin \mathsf{E}$, if $\overline{g}$ is irreducible as polynomial in $K[x^\mu]$, we get $(g, x - \alpha_i)_\ell = 1$ for all $\alpha_i \in \mathsf{E}$. Hence we randomly choose a monic irreducible polynomial $\overline{g} \in K[y]$ such that $\deg(\overline{g}) = \lfloor 2t/\mu \rfloor$ and set $g = \overline{g}(x^\mu) x^{2t \bmod \mu}$.

Finally, the right extended Euclidean algorithm allows to compute $h_0, \dots, h_{n-1} \in R$ such that, for each $0 \leq i \leq n-1$, $\deg(h_i) < 2t$ and

$$(x - \alpha_i)h_i - 1 \in Rg.$$

In fact $\deg(h_i) = 2t - 1$ by a degree argument.

A parity check matrix for our code is

$$H = \Big(\mathfrak{v}(\sigma^{-j}(h_{i,j})u_i)\Big)_{\substack{0 \leq j \leq 2t-1 \\ 0 \leq i \leq n-1}} \in F^{(2tm)\times n}$$

where $h_i = \sum_{j=0}^{2t-1} h_{i,j}x^j$. Once H is computed, the public key of our cryptosystem can be computed as follows: Let $r_H = \operatorname{rank}(H)$ and $R \in F^{(n-k-r_H)\times n}$ a random matrix. The H_{pub} consists in the non zero rows of the reduced row echelon form of the block matrix $\left(\begin{smallmatrix} H \\ R \end{smallmatrix}\right)$. If H_{pub} has less that $n-k$ rows, pick a new R. After this Key Schedule in the Key encapsulation mechanism, the different values remain as follows:

Parameters $t \ll n$, $q = p^d$ and $k = n - 2t \left\lfloor \frac{n}{4t} \right\rfloor$.

Public Key $H_{\text{pub}} \in F^{(n-k)\times n}$.

Private Key L, σ, $E = \{\alpha_0, \dots, \alpha_{n-1}\}$, g and $h_0, \dots, h_{n-1}$.

The other parameters and computed elements are not used in the encryption and decryption processes.

2.2 Encryption procedure: shared key derived by the sender

We pick a random vector, i.e. $e \in F^n$ such that $\mathrm{w}(e) = t$, with corresponding polynomial $e(x) = \sum_{j=1}^{\nu} e_j x^{k_j}$, $\nu \leq t$ and $0 \leq k_1 < k_2 < \cdots < k_\nu \leq n-1$. The sender can easily derive a shared secret key from e by means of a fixed and publicly known hash function $\mathcal{H}$. The cryptogram is

$$s = eH_{\text{pub}}^{\mathsf{T}} \in F^{n-k}.$$

2.3 Decryption procedure: shared key derived by the receiver

The receiver can easily compute $y \in F^n$ such that

$$s = yH_{\text{pub}}^{\mathsf{T}}$$

since H_{pub} is in row reduced echelon form. Let $y(x) = \sum_{i=0}^{n-1} y_i x^i$. The decoding algorithm in [2] can be applied to $y(x)$ in order to compute e. Then the shared secret key can be retrieved by the receiver as $\mathcal{H}(e)$.

References

[1] Martin R. Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varum Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlison, and Wen Wang. Classic McEliece: conservative code-based cryptography. Technical report, NIST's Post-Quantum Cryptography Standardization Project, 10 2020.

[2] J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro. A Sugiyama-like decoding algorithm for convolutional codes. *IEEE Transactions on Information Theory*, 63(10):6216–6226, 2017. arXiv:1607.07187.

[3] José Gómez-Torrecillas, F. J. Lobillo, and Gabriel Navarro. Procedimiento y dispositivo de cifrado/descifrado post-cuántico usando códigos lineales. OEPM, February 2022. patente solicitud número P202230118.

[4] José Gómez-Torrecillas, F. J. Lobillo, and Gabriel Navarro. Skew differential Goppa codes and their application to McEliece cryptosystem, 2022. URL: `https://arxiv.org/abs/2207.14270`,

[5] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical Report 42-44, National Aeronautics and Space Administration, January and February 1978.

[6] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory.*, 15:159–166, 1986.