



On Constructing Quasi-Cyclic Subfield Subcodes of Dual Elliptic Codes with Known Parameters

Artyom Kuninets

Researcher

qapp.tech



Current status

- McEliece was proposed in 1978 $\rightarrow$ > 35 years of security research (Goppa codes)
- Extensive cryptanalysis $\rightarrow$ McEliece on Goppa codes is still secure
- "New" schemes (examples: BIKE, HQC)

Problems

- Public key is generator/parity-check matrix of the code ($|pk| \geq 255$ Kb in Classic McEliece)
- Structural attacks against McEliece on different codes
- Security problems in BIKE/HQC (DFR/Security proof/Side-channel attacks)

Solution (compromise)

- Find family of codes, secure against key-recovery attacks (with effective decoding algorithm)
- Use the quasi-cyclic structure to reduce public key size
- McEliece on structured QC-codes or subcodes (algebraic structure)

Families of codes for McEliece cryptosystem

- Goppa/alternant codes
- Codes modifications ($\mathcal{C}_1 \otimes \mathcal{C}_2$, Plotkin- $(u, u + v)$ construction) $\rightarrow$ quite impractical
- Subfield subcodes of algebraic geometry codes (SSAG) $\rightarrow$ QC-SSAG

Quasi-cyclic codes

Let n be an integer and $\ell \mid n$. The code $\mathcal{C} \subseteq \mathbb{F}^n$ is called ℓ -quasi-cyclic (ℓ -QC) if for every $c \in \mathcal{C}$, $\sigma(c) \in \mathcal{C}$, where σ is the quasi-cyclic shift

$$\sigma : \begin{cases} \mathbb{F}^n \rightarrow \mathbb{F}^n, \\ (\mathbf{b}_1 \mid \dots \mid \mathbf{b}_{\frac{n}{\ell}}) \mapsto (\sigma_\ell(\mathbf{b}_1) \mid \dots \mid \sigma_\ell(\mathbf{b}_{\frac{n}{\ell}})). \end{cases}$$

Here, σ_ℓ is cyclic shift of blocks $\mathbf{b}_i$ of length ℓ and ℓ is called the *quasi-cyclicity order* of the code

Block-circulant matrix

A matrix $\mathbf{M}$ is called ℓ -block-circulant if it consists of $\mathbf{M}_i$ circulant matrices of order ℓ :

$$\mathbf{M} = \begin{pmatrix} & & & \\ & & & \\ \dots & \mathbf{M}_i & \dots & \\ & & & \end{pmatrix}, \quad \text{where} \quad \mathbf{M}_i = \begin{pmatrix} a_0 & a_1 & \dots & a_{\ell-1} \\ a_{\ell-1} & a_0 & \dots & a_{\ell-2} \\ \vdots & \ddots & \ddots & \vdots \\ a_1 & \dots & a_{\ell-1} & a_0 \end{pmatrix}.$$

$$\mathbf{G} = \left(\mathbf{I}_k \mid \mathbf{M} \right) \Rightarrow |pk| = (n - k) \cdot \lceil \frac{k}{\ell} \cdot s \rceil, \text{ where } s = \lceil \log_2 p \rceil$$

- A code $\mathcal{C}$ with an ℓ -block-circulant generator matrix is an ℓ -QC code
- QC code of dimension k does not necessarily have an ℓ -block-circulant generator matrix

Cryptanalysis of QC-SSAG

- Key security reduction¹ $\longrightarrow$ affects QC-SSAG codes with large quasi-cyclicity order ℓ :
Affects even McEliece on QC-alternant codes² $\longrightarrow$ already broken in³
- ISD speedup by a factor of $\sqrt{\ell}$ with DOOM⁴
- Shur product distinguisher for high rate SSAG codes⁵

Conclusion

- Quasi-cyclicity order ℓ is small (exact value depends on the code family)
- Rate $R(C) < 0.95$

Under these conditions no structural attacks are known to date

[1] Elise Barelli. On the security of short McEliece keys from algebraic and algebraic geometry codes with automorphisms. 2018

[2] Thierry Berger et al. Reducing Key Length of the McEliece Cryptosystem. 2009

[3] Jean-Charles Faugère et al. Algebraic Cryptanalysis of McEliece Variants with Compact Keys. 2010

[4] Nicolas Sendrier. Decoding One Out of Many. 2011

[5] Sabira El Khalfaoui, Mathieu Lhotel и Jade Nardi. Goppa-Like AG Codes From $\mathcal{C}_{a,b}$ Curves and Their Behavior Under Squaring Their Dual. 2023

Definitions

- **Divisor** of the curve $\mathcal{X}$:

$$D = \sum_{P \in \mathcal{X}(\mathbb{F}_q)} n_P P, \text{ where } n_P \in \mathbb{Z} \text{ and } D \geq D' \iff n_P \geq n'_P \text{ for all } P \in \mathcal{X}(\mathbb{F}_q)$$

- **Support** of the divisor: $\text{supp}(D) = \{P : n_P \neq 0\}$
- **Principal divisor** of a function f on the curve $\mathcal{X}$ (function field):

$$(f) = (f)_0 - (f)_\infty,$$

where $(f)_0$ is the divisor of zeros and $(f)_\infty$ is the divisor of poles

- **Riemann-Roch space**: $\mathcal{L}(G) = \{f \in \mathbb{F}_q(\mathcal{X}) : (f) \geq -G\} \cup \{0\}$

Algebraic geometry code

AG code $\mathcal{C}_{\mathcal{L}}(D, G)$ associated with the divisors $D = \sum_{i=1}^n P_i$

and G , where $P_i \in \mathcal{X}(\mathbb{F}_q)$ are distinct and $\text{supp}(D) \cap \text{supp}(G) = \emptyset$:

$$\mathcal{C}_{\mathcal{L}}(D, G) = \{(f(P_1), \dots, f(P_n)) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n$$

Quasi-Cyclic Subfield Subcode of Dual Elliptic code

Construction (QC-SSDE)

1. Choose an elliptic curve $\mathcal{E}/\mathbb{F}_{p^m}$ and pick $\sigma \in \text{Aut}(\mathcal{E}/\mathbb{F}_{p^m})$ such that $\text{ord}(\sigma) = \ell$
2. Construct divisors D, G of the special form:

$$\text{Orb}_\sigma(P_i) = \{\sigma^j(P_i) : j \in \{0, \dots, \ell - 1\}\} \longrightarrow D = \sum_{i=1}^{n/\ell} \sum_{P \in \text{Orb}_\sigma(P_i)} P, \quad \text{supp}(D) = \coprod_{i=1}^{n/\ell} \text{Orb}_\sigma(P_i),$$

$$G = \sum_{i=1}^s t_i \sum_{Q \in \text{Orb}_\sigma(Q_i)} Q \longrightarrow \text{often } G = kP_\infty \Rightarrow \text{basis } \mathcal{L}_{\text{basis}}(kP_\infty) = \{x^i y^j \mid 2i + 3j \leq k, j = 0, 1\}$$

3. Build a generator matrix of the code $\mathcal{C}_{\mathcal{L}}(D, G) \Rightarrow \mathbf{G} = \begin{pmatrix} f_1(P_1) & f_1(P_2) & \dots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \dots & f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(P_1) & f_k(P_2) & \dots & f_k(P_n) \end{pmatrix}, f_i \in \mathcal{L}_{\text{basis}}$

4. Calculate $\mathcal{C}_{\text{QC-SSDE}}(D, G) = \mathcal{C}_{\mathcal{L}}(D, G)^\perp \cap \mathbb{F}_p$

If $\mathcal{C}_{\mathcal{L}}(D, G)$ is ℓ -quasi-cyclic, then quasi-cyclicity property holds for $\mathcal{C}_{\text{QC-SSDE}}(D, G) = \mathcal{C}_{\mathcal{L}}(D, G)^\perp \cap \mathbb{F}_p$

Open problems

- Lack of precise estimates for the **dimension** of subfield subcodes of elliptic codes
- Currently, **efficient construction** is only possible for $G = kP_\infty$ (the form of the Riemann-Roch space basis is explicitly known only in this case)
- No reliable results on **invariant points** of elliptic curves under automorphisms
- ...

Solution

The research successfully resolved all the identified problems

Theorem

Let $n = |\mathcal{E}(\mathbb{F}_{q^m})| - \varepsilon$ and $G = k_{\text{orig}}P_{\infty}$, where $\varepsilon \in \{0, 1\}$ and $0 \leq k_{\text{orig}} < n$. If $n > k_{\text{orig}} \cdot q^{m/2} + q^{m/2} + 1$, then the dimension of the subfield subcode is given by¹:

$$\dim \left(\mathcal{C}_{\mathcal{L}}^{\perp}(D, G) \Big|_{\mathbb{F}_p} \right) = n - (m(k_{\text{orig}} - \lfloor k_{\text{orig}}/q \rfloor) + 1) = n - mr - 1$$

Limitations

- Theorem holds in the case $R_{\text{orig}} = \frac{k_{\text{orig}}}{n} \approx 0$ (Example: $R_{\text{orig}} \leq 0.02$ for $\mathbb{F}_{2^m}$)
- Moreover, all rational points of the curve are involved in the code construction
($n = |\text{supp}(D)| = |\mathcal{E}(\mathbb{F}_{q^m})| - \varepsilon$)

Dimension of SSDE codes (practice)

Curve	Constraints $k_{\max\text{T}} \leq k_{\text{orig}} \leq k_{\max\text{P}}$	Code parameters $\mathcal{C}^\perp _{\mathbb{F}_p}$		$R(\mathcal{C}^\perp _{\mathbb{F}_p})$ $n = \mathcal{E}(\mathbb{F}_q) $	$R(\mathcal{C}^\perp _{\mathbb{F}_p})$ $n = n_{\min}$
		$n = \mathcal{E}(\mathbb{F}_q) - 1$ $k_{\text{orig}} = k_{\max\text{T}}/k_{\max\text{P}}$	$n = n_{\min}^*$ $k_{\text{orig}} = k_{\max\text{T}}/k_{\max\text{P}}$		
char($\mathbb{F}_q$) = 2					
$\mathcal{E}/\mathbb{F}_{2^{12}}$	64 $\leq k_{\text{orig}} \leq$ 126	[4224, 3839] [4224, 3467]	[2201, 1816] [2201, 1444]	0.908 0.820	0.825 0.656
$\mathcal{E}/\mathbb{F}_{2^{13}}$	91 $\leq k_{\text{orig}} \leq$ 256	[8373, 7774] [8373, 6708]	[4226, 3627] [6312, 4647]	0.928 0.801	0.858 0.736
char($\mathbb{F}_q$) = 3					
$\mathcal{E}/\mathbb{F}_{3^7}$	47 $\leq k_{\text{orig}} \leq$ 162	[2279, 2054] [2279, 1522]	[801, 576] [1563, 806]	0.901 0.667	0.719 0.515
$\mathcal{E}/\mathbb{F}_{3^8}$	81 $\leq k_{\text{orig}} \leq$ 163	[6723, 6290] [6723, 5850]	[2324, 1891] [2324, 1451]	0.935 0.870	0.813 0.624
char($\mathbb{F}_q$) = 7					
$\mathcal{E}/\mathbb{F}_{7^4}$	51 $\leq k_{\text{orig}} \leq$ 99	[2495, 2318] [2495, 2154]	[324, 147] [346, 5]	0.929 0.863	0.453 0.014
$\mathcal{E}/\mathbb{F}_{7^5}$	132 $\leq k_{\text{orig}} \leq$ 686	[17043, 16472] [17043, 14102]	[4784, 4213] [4784, 1843]	0.966 0.827	0.880 0.385

Note: $\star$ Minimal n for which $\dim(\mathcal{C}^\perp|_{\mathbb{F}_p}) = n - mr - 1$

Theorem (Orbit Structure under Automorphisms in Characteristics 2 and 3)

Let $\mathcal{E}/\mathbb{F}_q$ be an elliptic curve defined over a field of characteristic $\text{char}(\mathbb{F}_q) \in \{2, 3\}$, and let $\sigma \in \text{Aut}(\mathcal{E}/\overline{\mathbb{F}}_q, P_\infty)$ be a non-trivial automorphism of order $\ell = \text{ord}(\sigma)$. For any rational point $P_{x,y} \notin \mathfrak{S}$, where the excluded set $\mathfrak{S}$ is defined as:

$$\mathfrak{S} = \begin{cases} \mathcal{E}[2] & \text{if } \text{char}(\mathbb{F}_q) = 3, \\ \mathcal{E}[3] \cup \{P_{0,\beta_1}, P_{0,\beta_2}\} & \text{if } \text{char}(\mathbb{F}_q) = 2, \end{cases}$$

the orbit of $P_{x,y}$ under σ satisfies:

$$|\text{Orb}_\sigma(P_{x,y})| = \ell.$$

Here $\mathcal{E}[n]$ denotes the n -torsion subgroup.

We must choose $P \notin \mathfrak{S}$ while constructing QC-SSDE codes

Riemann-Roch space basis $G \neq kP_\infty$

Theorem

Let $\mathcal{E}/\mathbb{F}_{p^m}$ be an elliptic curve, $\sigma \in \text{Aut}(\mathcal{E}/\mathbb{F}_{p^m}, P_\infty)$, $\ell = \text{ord}(\sigma) \in \{2, 4, 6\}$ and $G = \sum_{z=1}^s t_z \sum_{Q \in \text{Orb}_\sigma(Q_z)} Q$, where $s \in \mathbb{N}$ and $Q_z \in \mathcal{E}(\mathbb{F}_{p^m}) \setminus (\{P_\infty, P_{0,\beta_1}, P_{0,\beta_2}, P_{\alpha_1,0}, P_{\alpha_2,0}, P_{\alpha_3,0}\} \cup \mathcal{E}[3])$. Also, denote $\mathcal{Q}_z = \text{Orb}_\sigma(Q_z)$. The basis of the Riemann-Roch space associated with the divisor G is defined as follows:

$$\mathcal{L}_b(G) = \left\{ \frac{X^i Y^j}{\prod_{z=1}^s \left[\prod_{\rho=1}^{\ell/2} (X - x(\mathcal{Q}_{z,\rho})) \right]^{t_z}} \mid 2i + 3j \leq \ell \cdot \sum_{z=1}^s t_z, j = \overline{0,1} \right\},$$

where $x(\mathcal{Q}_{z,\rho})$ is the x -coordinate of the point $\mathcal{Q}_{z,\rho}$ and $\deg(G) = \ell \cdot \sum_{z=1}^s t_z$.

Basis of the Riemann-Roch space for arbitrary divisors $G \neq kP_\infty$ is known

Parameters comparison

Target instance	q	n	k	t	Size (bytes)	Category
Classic McEliece (Niederreiter on Goppa codes)						
mceliece348864	2	3488	2720	64	261120	1
mceliece460896		4608	3360	96	524160	3
mceliece6688128		6688	5024	128	1044992	5
mceliece6960119		6960	5413	119	1047319	5
mceliece8192128		8192	6528	128	1357824	5
ECC ² (McEliece on Elliptic codes)						
ECC ² -128	134807	521	150	196	125214	1
ECC ² -192	301831	781	225	294	297112	3
ECC ² -256	561307	1031	322	364	570745	5
Niederreiter on QC-SSDE codes						
QC-SSDE-128 ₂	2	3364	2492	66	67907	1
QC-SSDE-128 ₃	3	2250	1542	75	45489	1
QC-SSDE-192 ₂	2	4972	3528	110	159201	3
QC-SSDE-192 ₇	7	3234	2508	84	113801	3
QC-SSDE-256 ₂	2	7472	5820	126	300457	5
QC-SSDE-256 ₇	7	4440	3474	112	209743	5

Conclusion

QC-SSDE key size reduction

Field characteristic	Classic McEliece	ECC ²
Security Level 1 (AES 128)		
$\text{char}(\mathbb{F}) = 2$	74 %	46 %
Security Level 3 (AES 192)		
$\text{char}(\mathbb{F}) = 2$	70 %	46 %
Security Level 5 (AES 256)		
$\text{char}(\mathbb{F}) = 2$	78 %	47 %

Niederreiter on QC-SSDE codes

- ✓ Public key size reduction ~ 70 % compared to Classic McEliece
- ✓ Encryption speed is similar to Classic McEliece
- ✗ Loss in key generation speed due to the construction of a block-circulant matrix



Artyom Kuninets

Researcher

akuninec@qapp.tech

@Arkraft



qapp.tech

