

Cryptanalysis of McEliece cryptosystem on elliptic codes: a review of known methods and a new structural attack with hints

Artyom Kuninets

Researcher QApp

PhD student



- The McEliece cryptosystem possesses high speed and post-quantum security, but requires huge public keys, which limits its practical application
- To reduce key sizes, elliptic codes were proposed, among other approaches. They gave more compact keys compared to Goppa codes, and the scheme was considered secure against known attacks
- Existing cryptanalysis methods either required exponential search for minimum weight codewords, or worked only for the special case $G = kP_\infty$

Our contribution

We present the first polynomial-time structural attack that works for arbitrary effective divisors and for any number of errors

Attempts to embed codes into the McEliece scheme

- 1978: McEliece cryptosystem
- 1986: Niederreiter cryptosystem [GRS codes]
- 1992: **Attack** by Sidelnikov–Shestakov [GRS codes]
- 1996: Reed–Muller codes (Sidelnikov)
- 2001: AG codes and their subfield subcodes (Janwa, Moreno)
- 2001: Subcodes of GRS codes (Berger, Loidreau)
- 2005: QC-BCH codes (Gaborit)
- 2008: **Attack** [AG codes of genus ≤ 2] (Faure, Minder)
- 2008: QC-alternant codes (Berger, Cayrel, Gaborit, Otmani)
- 2010: “Wild” Goppa codes over $\mathbb{F}_q$ (Bernstein, Lange, Peters)
- 2010: Algebraic **attacks** [QC codes] (Otmani, Tillich, Dallot, Faugère, Perret)
- 2010: **Attack** based on Schur product [subcodes of GRS codes] (Wieschebrink)
- 2012: MDPC codes
- 2014: **Attack** [Reed–Muller codes] (Borodin, Chizhov)
- 2014: **Attack** [AG codes] (Couvreur, Márquez-Corbella, Pellikaan)
- 2014: **Attack** [“wild” Goppa codes for $m = 2, 3$] (Faugère, Perret, Portzamparc)
- 2014: **Attack** [QC and QD codes] (Faugère, Otmani, Perret, Portzamparc, Tillich)
- 2017: NIST competition $\Rightarrow$ launch of standardization initiatives worldwide

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

$$D = \sum_{P \in \mathcal{X}(\mathbb{F}_q)} n_P P, \quad \text{where } n_P \in \mathbb{Z} \text{ and } D \geq D - P_1 \iff n_P \geq n'_P \text{ for all } P \in \mathcal{X}(\mathbb{F}_q)$$

- **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, $(f)_\infty$ is the divisor of poles

- **Function field of the curve:**

$$\mathbb{F}_q(\mathcal{X}) = \left\{ \frac{g(x,y)}{h(x,y)} \mid g, h \in \mathbb{F}_q[x,y], h \neq 0 \right\} / \sim,$$

where $\frac{g}{h} \sim \frac{g'}{h'} \iff (gh' - g'h)(P) = 0 \forall P \in \mathcal{X}$

- **Riemann–Roch space:**

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

Key Generation in ECC2 (Simplified)

Input: finite field $\mathbb{F}_q$; code parameters $n, k, t \in \mathbb{N}$

Output: public key $(\mathbf{G}_{\text{pub}}, t > \frac{d-1}{2})$; private key (D, a_4, a_6)

- 1: Choose an elliptic curve $\mathcal{E}/\mathbb{F}_q : y^2 = x^3 + a_4x + a_6$
- 2: $D \leftarrow P_0 + \cdots + P_{n-1}$ with $P_i \neq P_j$ for $i \neq j$, and $P_i \in \mathcal{E}(\mathbb{F}_q)$
- 3: $G \leftarrow kP_\infty$
- 4: $\mathcal{L}_b(G) \leftarrow \{x^i y^j \mid 2i + 3j \leq k, j = \overline{0, 1}\}$
- 5: $\mathbf{G} \leftarrow \begin{pmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n) \end{pmatrix}$, where $f_i \in \mathcal{L}_b(G)$ $\triangleright \mathcal{C}_{\mathcal{L}}(D, G) \leftarrow \{\text{ev}_D(f) : f \in \mathcal{L}(G)\}$
- 6: Transform matrix $\mathbf{G}$ to systematic form $(\mathbf{I}_k \mid \mathbf{G}')$
- 7: $\mathbf{G}_{\text{pub}} \leftarrow \mathbf{G}'$
- 8: **return** $\text{pk} = (\mathbf{G}_{\text{pub}}, t)$, $\text{sk} = (D, a_4, a_6)$

[1] Zhang F., Zhang Z., Guan P. ECC2: Error correcting code and elliptic curve based cryptosystem // Information Sciences, 2020

Drawbacks of known attacks

Attack	Limitation
Minder's attack ¹	Requires finding minimum weight codewords
Attack recovering isomorphic code representation ²	No polynomial-time decoding algorithm is known
Attack based on error-correcting pairs/arrays ³	The attack does not recover the code structure and depends on the number of errors $t \leq \lfloor \frac{d-1}{2} \rfloor$

The ECC2 scheme⁴ is secure against all presented attacks

[1] Minder L. Cryptography based on error correcting codes : PhD thesis. – Verlag nicht ermittelbar, 2007

[2] Márquez-Corbella I., Martínez-Moro E., Pellikaan R. On the unique representation of very strong algebraic geometry codes // Designs, Codes and Cryptography

[3] Couvreur A., Márquez-Corbella I., Pellikaan R. Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and Their Subcodes // IEEE Transactions on Information Theory, 2017

[4] Zhang F., Zhang Z., Guan P. ECC2: Error correcting code and elliptic curve based cryptosystem // Information Sciences, 2020

Parameters of the ECC2 scheme

Target instance	q	n	k	t	Size (bytes)
Classic McEliece					
mceliece348864	2	3488	2720	64	261120
mceliece460896	2	4608	3360	96	524160
mceliece6688128	2	6688	5024	128	1044992
mceliece6960119	2	6960	5413	119	1047319
mceliece8192128	2	8192	6528	128	1357824
ECC2					
ECC2-128	134807	521	150	196	125214
ECC2-192	301831	781	225	294	297112
ECC2-256	561307	1031	322	364	570745

Drawback — low decryption speed

Idea

- The ideas from works^{2,3} are adapted to compute an isomorphic representation of the code
- It is based on computing the sequence of codes from work²

$$\mathcal{V}_i = \mathcal{C}_{\mathcal{L}}(D - P_1, G + iP_1), \quad \mathcal{U}_i = \mathcal{C}_{\mathcal{L}}(D - P_1, iP_1), \quad \text{for } i = 0, \dots, t-1$$

- Unlike work², where the sequence is computed for $i = 0, \dots, t-1$, attack¹ proposes to stop at $\mathcal{U}_2, \mathcal{U}_3$ and recover the code structure using them

[1] Shkuratov Yu. D. Attack on the ECC2 cryptosystem and the McEliece cryptosystem built on elliptic codes // PDM. Supplement. – 2025. – No. 18. – Pp. 188-194. – URL: <http://mi.mathnet.ru/pdma710>.

[2] Couvreur A., Márquez-Corbella I., Pellikaan R. Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and Their Subcodes // IEEE Transactions on Information Theory, 2017

[3] I. V. Chizhov, "Hadamard closure of general Reed–Solomon codes and filtration attack on the original Niederreiter cryptosystem", Diskr. Mat., 37:1 (2025), 130–150

Advantages of the attack

- The code structure is recovered
- The attack does not depend on finding minimum weight codewords or the parameter t
- Complexity: $\mathcal{O}((k^2 + q^2)n^2)$ operations in $\mathbb{F}_q$

Limitation

- The attack uses knowledge of the second divisor $G = kP_\infty$
- Generalizing the attack to an arbitrary divisor $G = \sum Q_i$, where $Q_i \in \mathcal{E}/\mathbb{F}_q$, seems difficult to achieve
- The McEliece scheme on arbitrary "elliptic codes" with $G \neq kP_\infty$ was considered secure

Considered variant of the scheme

KeyGen

Input: finite field $\mathbb{F}_q$; code parameters $n, k, t \in \mathbb{N}$

Output: public key $(\mathbf{G}_{\text{pub}}, t > \frac{d-1}{2})$; private key (D, G)

- 1: Choose an elliptic curve $\mathcal{E}/\mathbb{F}_q^n : y^2 = x^3 + a_4x + a_6$
- 2: $D \leftarrow P_0 + \dots + P_{n-1}$ with $P_i \neq P_j$ for $i \neq j$, and $P_i \in \mathcal{E}(\mathbb{F}_q)$
- 3: $G \leftarrow k_1Q_1 + \dots + k_sQ_s$, where $\deg(G) = \sum k_i$
- 4: $\mathbf{G} \leftarrow$ Generator matrix of the code $\mathcal{C}_{\mathcal{L}}(D, G) = \{\text{ev}_D(f) : f \in \mathcal{L}(G)\}$
- 5: Transform matrix $\mathbf{G}$ to systematic form $(\mathbf{I}_k \mid \mathbf{G}')$
- 6: $\mathbf{G}_{\text{pub}} \leftarrow \mathbf{G}'$
- 7: **return** $\text{pk} = (\mathbf{G}_{\text{pub}}, t)$, $\text{sk} = (D, G)$

- $G = kP_{\infty} \longrightarrow G = \sum k_i Q_i$
- $\text{sk} = (D, \mathcal{E}) \longrightarrow \text{sk} = (D, G)$

In contrast to the ECC2 scheme, here the curve is not part of the private key

Divisor D recovery

- Do not construct the entire chain of codes

$$\mathcal{V}_i = \mathcal{C}_{\mathcal{L}}(D - P_1, G + iP_1), \quad \mathcal{U}_i = \mathcal{C}_{\mathcal{L}}(D - P_1, iP_1), \quad \text{for } i = 0, \dots, t-1$$

- Compute $\mathcal{U}_2$ and recover the divisor D using a basis of the Riemann-Roch space $\mathcal{L}(2P_1)$

Divisor G recovery

- Recover the divisor G using the results of work¹
- In work¹, a basis of the Riemann-Roch space for arbitrary divisors $G = \sum Q_i$ is derived
- Therefore, we can recover the second divisor by enumerating functions (polynomial complexity)

[1] Kuninets A., Malygina E. Bases of Riemann-Roch spaces associated with arbitrary elliptic curve divisors and their application in constructing various elliptic codes families // arXiv:2508.04340. – URL: <https://arxiv.org/abs/2508.04340>.

Theorem 1

Let $\mathcal{C}_{\mathcal{L}}(D, G)$ be an elliptic code associated with the curve $\mathcal{E}/\mathbb{F}_q$. If $3 \leq \deg(G) \leq \frac{n}{2} - 2$, then **knowing** the curve $\mathcal{E}$, the generator matrix $\mathbf{G}_{\text{pub}}$ and 3 distinct points $P_1, P_2, P_3 \in D$, the entire **divisor D can be recovered in $\mathcal{O}(k^2 n^2 + |\mathcal{E}(\mathbb{F}_q)| + n)$ operations in $\mathbb{F}_q$ with probability exceeding $1 - \frac{3}{(|\mathcal{E}(\mathbb{F}_q)|)^2} + \frac{2}{(|\mathcal{E}(\mathbb{F}_q)|)^3}$.**

Theorem 2

Let $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ be an elliptic code associated with the elliptic curve $\mathcal{E}/\mathbb{F}_q$, where $\text{char}(\mathbb{F}_q) \neq 3$, $n = |\text{supp}(D)|$ and $G = \sum_i k_i Q_i$, $k_i > 0$. Then given the elliptic curve $\mathcal{E}$, the generator matrix $\mathbf{G}_{\text{pub}}$ and the divisor D , the second divisor G **can be recovered in $\mathcal{O}((|\mathcal{E}(\mathbb{F}_q)| - n)^2 \cdot n^2 + \deg(G) \cdot (n + n^2))$ operations in $\mathbb{F}_q$.**

If 3 points are unknown: complexity $\mathcal{O}(|\mathcal{E}(\mathbb{F}_q)|^3 \cdot (T_1 + T_2))$

Attack complexity for the McEliece scheme with $G = kP$

Attack complexity given known curve

Parameters [n, k, t]	q	Number of known points	ISD complexity	Our attack	$ pk $ bytes
[521, 150, 196]	134807	3	147	47	125214
		2		64	
		1		81	
		0		98	
[781, 225, 294]	301831	3	212	50	297114
		2		68	
		1		86	
		0		105	
[1031, 322, 364]	561307	3	279	52	570745
		2		71	
		1		90	
		0		109	

New parameters

Parameters $[n, k, t]$	q	Number of known points	ISD complexity	Our attack	$ pk $ bytes
$[480, 123, 189]$	2147483647	3	128	50	170155
		2		81	
		1		112	
		0		143	
$[760, 224, 284]$	460099999999993	3	209	62	690368
		2		108	
		1		153	
		0		199	
$[1020, 300, 376]$	2305843009213693951	3	273	79	1647000
		2		140	
		1		201	
		0		262	

- For security 192 and 256 bits, the public key sizes are larger than in the McEliece scheme with Goppa codes
- **We lose the advantage of using "elliptic codes"**

Part 1: recovering the divisor D

1. Compute the code $\mathcal{U}_2 = \mathcal{C}_{\mathcal{L}}(D - P_1, 2P_1)$ using the results of work¹
2. We know the form of the basis of the Riemann-Roch space

$$\mathcal{L}_b(2P_1) = \left\{ 1, f_2 = \frac{y - \beta' - \gamma(x - \alpha)}{(x - \alpha)^2} \right\}, \text{ for } P_1 = (\alpha, \beta) \text{ and } -P_1 = (\alpha, \beta'),$$

$$\text{where } \beta \neq 0 \text{ and } \gamma = \begin{cases} \frac{\alpha^2 + a_4 + a_1\beta'}{a_1\alpha + a_3} & \text{if } \text{char}(\mathbb{F}_q) = 2; \\ \frac{3\alpha^2 + a_4}{2\beta'} & \text{if } \text{char}(\mathbb{F}_q) \geq 3. \end{cases}$$

We can move to a known basis:

$$\mathbf{G}_{\mathcal{U}_2} = \begin{pmatrix} g_{1,2} & g_{1,3} & \cdots & g_{1,n} \\ g_{2,2} & g_{2,3} & \cdots & g_{2,n} \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & \cdots & 1 \\ f_2(P_2) & f_2(P_3) & \cdots & f_2(P_n) \end{pmatrix}.$$

We know: f_2 and $f_2(P)$ for all $P_i \in D$. **Goal:** find P

3. It is proven that the value of the function f can be the same only at two points P and $\tilde{P}$

$$\tilde{D} = \left\{ \{P_2, \tilde{P}_2\}, \dots, \{P_n, \tilde{P}_n\} \right\} \longrightarrow \text{Repeat for } \mathcal{U}'_2 = \mathcal{C}_{\mathcal{L}}(D - P_2, 2P_2)$$

[1] Couvreur A., Márquez-Corbella I., Pellikaan R. Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and Their Subcodes // IEEE Transactions on Information Theory, 2017

Part 2: recovering the divisor G

- The form of the basis of the Riemann-Roch space for an arbitrary divisor $G \neq kP_\infty$ has been obtained¹

$$\mathcal{L}_b = \{1\} \cup \{f_{i,s} \mid 1 \leq i \leq z, 2 \leq s \leq k_i\} \cup \{g_i \mid 1 \leq i \leq z-1\},$$

where the functions are defined as follows:

$$f_{i,s}(X, Y) = \frac{Y + A_{i,s}(X)}{(X - \alpha_i)^s}, \quad 2 \leq s \leq k_i, \quad g_i(X, Y) = \frac{Y + B_i(X)}{(X - \alpha_i)(X - \alpha_{i+1})}, \text{ or } g_i(X, Y) = \frac{1}{X - \alpha_i}.$$

Here, $A_{i,s}(X) \in \mathbb{F}_{p^m}(\mathcal{E})$ has degree $\deg(A_{i,s}) \leq s-1$ and

$$B_i(X) = \left(\frac{\beta_{i+1} - \beta_i}{\alpha_{i+1} - \alpha_i} + a_1 \right) X + \left((\beta_i + a_1 \alpha_i + a_3) - \left(\frac{\beta_{i+1} - \beta_i}{\alpha_{i+1} - \alpha_i} + a_1 \right) \alpha_i \right)$$

- Knowing the divisor D , we can enumerate functions, construct codewords, and check membership in the code
- Complexity given a known divisor D : $\mathcal{O}\left((|\mathcal{E}(\mathbb{F}_q)| - n)^2 \cdot n^2 + \deg(G) \cdot (n + n^2)\right)$

[1] Kuninets A., Malygina E. Bases of Riemann-Roch spaces associated with arbitrary elliptic curve divisors and their application in constructing various elliptic codes families // arXiv:2508.04340. – URL: <https://arxiv.org/abs/2508.04340>.

Divisor D recovery complexity

- The first part of the attack requires enumerating three points P_1, P_2, P_3
- **Question:** is it possible to use only two points?
- This has only been shown in the case when there are 2-torsion points or when the matrix contains a minimum weight codeword

Divisor G recovery complexity

- In the worst case, the complexity is $\mathcal{O}\left((|\mathcal{E}(\mathbb{F}_q)| - n)^2 \cdot n^2 + \deg(G) \cdot (n + n^2)\right)$
- We can achieve linear complexity in $|\mathcal{E}(\mathbb{F}_q)|$ in some special scenarios

Why consider the model with a known curve?

The elliptic code $\mathcal{C}_{\mathcal{L}}(D, G)$ is **ℓ -quasi-cyclic** if the divisors D and G are of the form:

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

$$G = \sum_{i=1}^s t_i \sum_{Q \in \text{Orb}_{\sigma}(Q_i)} Q.$$

- QC codes can be used to reduce the public key size
- **The most efficient and practical schemes with a fixed curve**
- Attack complexity for QC elliptic codes:

$$\mathcal{O}(|\mathcal{E}(\mathbb{F}_q)| (k^2 n^2 + |\mathcal{E}(\mathbb{F}_q)| + n + (|\mathcal{E}(\mathbb{F}_q)| - n) \cdot n^2 + \deg(G) \cdot (n + n^2))) \sim \mathcal{O}(|\mathcal{E}(\mathbb{F}_q)|^2 n^2)$$

Why consider only effective divisors?

The paper considers divisors of the form $G = \sum_i k_i P_i$, where $k_i \geq 0$ for all i .

- Let $G = \sum_{i=1}^z k_i P_i - \sum_{j=1}^r \ell_j Q_j$, where $k_i, \ell_j > 0$
- In this case, the Riemann-Roch space consists of functions of the following form:

$$\mathcal{L}(G) = \{f \in \mathcal{L}(G^+) : v_{Q_j}(f) \geq \ell_j \text{ for all } j\}, \text{ where } G^+ = \sum_{i=1}^z k_i P_i$$

- Consequently, the space $\mathcal{L}(G)$ is obtained from $\mathcal{L}(G^+)$ by imposing $\sum_{j=1}^r \ell_j$ linear conditions $\rightarrow$ additional structure?
- **Points with negative valuations should be avoided?**
- In the Goppa code, only one point with negative valuation is used: $\Gamma(L, g) = \mathcal{C}_{\mathcal{L}}(D, G_0 - P_{\infty})^{\perp} \cap \mathbb{F}_p^n$

- Computing the "code filtration" does not work in the case of a subfield subcode

$$\mathcal{V}_{-i-1} = \left\{ \mathbf{z} \in \mathcal{V}_{-i} \mid \mathbf{z} \star \mathcal{V}_{-i+1} \subseteq \mathcal{V}_{-i}^{(2)} \right\}, \text{ where } \deg(G) - \frac{n-4}{2} \leq i \leq \deg(G) - 2g + 1,$$

$$\mathcal{U}_i = \{ \mathbf{z} \in \mathbb{F}_q^{n-1} \mid \mathbf{z} \star \mathcal{V}_j \subseteq \mathcal{V}_\ell \}, \quad \text{where } \deg(G) + j > 2g$$

- The attack is applicable if $\mathcal{C} = \left(\mathcal{C} \star (\mathcal{C}^{(2)})^\perp \right)^\perp$
- If $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G) \cap \mathbb{F}_p^n$, then this property does not hold
- **The attack is not applicable in the case of subfield subcodes**

Conclusions and future work

- Finally, we present the first polynomial-time structural attack on McEliece scheme with elliptic codes, working for arbitrary effective divisors and any number of errors. This closes the long-standing question of their security
- The attack does not extend to subfield subcodes → they can be considered as an alternative to Goppa codes

Future work

- Can/should the attack complexity be reduced to $\mathcal{O}(|\mathcal{E}(\mathbb{F}_q)|^2)$?

Co-authors of the talk



Artyom Kuninets

Researcher
PhD student



Ekaterina Malygina

Researcher
Cand. Phys.-Math. Sci.



Evgeniy Melnichuk

Researcher



Artyom Kuninets

Researcher QApp

PhD student

akuninec@qapp.tech

@Arkaft



qapp.tech