КРИПТОНИТ

On self-duality of quasi-cyclic algebraic geometric codes associated with elliptic curve

Yuri Shkuratov

JSRPC ”Kryptonite”

CTCrypt 2024

Table of contents

Introduction

Code-based cryptosystems

- The first of them is proposed by Robert J. McEliece in 1978.
- Security is provided by the difficulty of certain problems in the theory of error-correcting codes.
- The size of the public key is generally equal to the size of the code generator matrix.
- The decryption speed depends on the linear code decoding speed.

Are there any options?

- ✓ Self–duality: allows to reduce key size without compromising security[1].
- ✓ Quasi-cyclicity: allows to optimize the memory spent on storing the public key[2].
- ✓ Elliptic curves: algebraic geometric codes associated with elliptic curve has large minimum code distance and effective decoding algorithms.

Let's combine it!

---

[1] Mariot L., Picek S., Yorgova R. On McEliece-type cryptosystems using self-dual codes with large minimum weight //IEEE Access. – 2023.

[2] Aguilar-Melchor C. et al. Efficient encryption from random quasi-cyclic codes //IEEE Transactions on Information Theory. – 2018. – Т. 64. – №. 5. – С. 3927-3943

Linear codes

Linear codes

Definition

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear $[n, k, d]$—code over field $\mathbb{F}_q$. Its *dual* code $\mathcal{C}^\perp$ is linear code

$$\mathcal{C}^\perp = \{b \in \mathbb{F}_q^n \mid \forall a \in \mathcal{C}\ a \cdot b = 0\}.$$

If $\mathcal{C} = \mathcal{C}^\perp$ then $\mathcal{C}$ is *self–dual*.

Definition

Let $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a cyclic shift operator one position to the right of $a = (a_0, a_1 ..., a_{n-1})$, i.e. $T(a) = (a_{n-1}, a_0, ..., a_{n-2})$. A linear code $\mathcal{C}$ is *ℓ—quasi–cyclic* if

$$\forall a \in \mathcal{C} \quad T^\ell(a) \in \mathcal{C}.$$

Algebraic geometric codes

Algebraic function fields

Definition

An *algebraic function field* F/K of one variable over K is an extension field $F \supset K$ such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K.

Definition

A *valuation ring* of the function field F/K is a ring $\mathcal{O} \subseteq F$ with the following properties:

1. $K \subsetneq \mathcal{O} \subsetneq F$ and
2. $\forall z \in F \quad z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Definition

A function field *point* P is a maximal ideal of $\mathcal{O}$. We denote set of points as $\mathbb{P}_F$.

Divisors

Definition

A *divisor* is a formal sum

$$D = \sum_{P \in \mathbb{P}_F} n_P P,$$

where $n_P \in \mathbb{Z}$ and $\#\{n_P \in \mathbb{Z} \mid n_P \neq 0,\ P \in \mathbb{P}_F\} < \infty$.

If $D = \sum n_P P$ and $D' = \sum n'_P P$ then sum of divisors D and D' is

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

A partial ordering of divisors defined by

$$D \leq D' \Leftrightarrow \forall P \in \mathbb{P}_F\ n_P \leq n'_P.$$

Divisors

Definition

Let $0 \neq f \in F$ and let $Z \subseteq \mathbb{P}_F$ (resp. $N \subseteq \mathbb{P}_F$) is the set of zeros (resp. poles) of f. Then

- $(f)_0 = \sum_{P \in Z} n_P P$ is the zero divisor of f,
- $(f)_\infty = -\sum_{P \in N} n_P P$ is the pole divisor of f and
- $(f) = (f)_0 - (f)_\infty$ is the *principal divisor* of f.

AG codes

Definition

Let G is a divisor. *The Riemann—Roch space* associated to G is

$$\mathcal{L}(G) = \{f \in F \mid (f) + G \geq 0\} \cup \{0\}.$$

Definition

Let G and $D = \sum_{i=0}^{n-1} P_i$ are divisors. The *algebraic geometric code* (or *AG code*) associated to G and D is

$$\mathcal{C}_{\mathcal{L}}(D, G) = \{f(P_0), ..., f(P_{n-1}) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Elliptic codes

Elliptic curves

We fix $\mathrm{char}(\mathbb{F}_q) = 2$. Any elliptic curve over $\mathbb{F}_q$ is isomorphic to one of two curves:

$$\varepsilon_0 : y^2 + cy = x^3 + ax + b \quad \text{or} \quad \varepsilon_1 : y^2 + xy = x^3 + ax^2 + b,$$

where $a, b \in \mathbb{F}_q$ and $0 \neq c \in \mathbb{F}_q$.

Curves isomorphic to ε_0 are called *supersingular*.

Curves isomorphic to ε_1 are called *nonsupersingular*.

Further we will denote the set of points of an elliptic curve ε over $\mathbb{F}_q$ as $\varepsilon(\mathbb{F}_q)$.

Code distance. Known facts

The Singleton bound and Corollary 2.2.3[3] imply an estimate for parameters of AG codes associated with elliptic curve:

Statement

A linear $[n, k, d]$–code $\mathcal{C}_{\mathcal{L}}(D, kP_\infty)$ associated with elliptic curve over $\mathbb{F}_q$ has such parameters that

$$n - k \leq d \leq n - k + 1.$$

And there is the following theorem[4]

Theorem

If $q \geq 13$, there are no codes with $d = n - k + 1$ and $n > q + 1$.

[3] Stichtenoth H. Algebraic function fields and codes. – Springer Science & Business Media, 2009. – T. 254.

[4] Влэдуц С. Г., Ногин Д. Ю., Цфасман М. А. Алгеброгеометрические коды. Основные понятия. – 2003.

Our results I

Theorem

Let $\mathrm{char}(\mathbb{F}_q) = 2$ *and* $\varepsilon_0 : y^2 + cy = x^3 + ax + b$ *is elliptic curve over* $\mathbb{F}_q$. *Let* $M \subseteq \varepsilon_0(\mathbb{F}_q) \setminus \{P_\infty\}$ *such that if* $P \in M$, *then* $-P \notin M$. *Denote* $m = \#M$.

If $m \equiv 0 \pmod 2$ *and*

$$\exists T \in \mathbb{F}_q : \forall (x, y) \in M \quad x \cdot \prod_{\substack{(x', y') \in M \\ x \neq x'}} (x + x') = T$$

then there is self–dual m*—quasi-cyclic AG* $[2m, m, d]$*—code associated with* ε_0.

Our results II

Theorem

Let $\mathrm{char}(\mathbb{F}_q) = 2$ *and* $\varepsilon_1 : y^2 + xy = x^3 + ax^2 + b$ *is elliptic curve over* $\mathbb{F}_q$. *Let* $M \subseteq \varepsilon_1(\mathbb{F}_q) \setminus \{P_\infty\}$ *such that if* $P \in M$, *then* $-P \notin M$. *Denote* $m = \#M$.

If

$$\exists T \in \mathbb{F}_q : \forall (x, y) \in M \quad \prod_{\substack{(x', y') \in M \\ x \neq x'}} (x + x') = T$$

then there is self–dual m*—quasi-cyclic AG* $[2m, m, d]$*—code associated with* ε_1.

Generalization of AG codes

Generalization of AG codes

Similar to the definition of the Generalized Reed—Solomon code, we introduce the following generalization of AG codes:

$$\mathcal{C}_{\mathcal{L}}(D, G, u) = \{u_0 f(P_0), ..., u_{n-1} f(P_{n-1}) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n,$$

where $u = (u_0, ..., u_{n-1}) \in (\mathbb{F}_q^\star)^n$.

Remark

Linear $[n, k, d]$—code $\mathcal{C}_{\mathcal{L}}(D, G, u)$ associated with elliptic curve ε has the same parameters as «classic» AG code $\mathcal{C}_{\mathcal{L}}(D, G)$ associated with ε.

Our results III

Theorem

Let $\mathrm{char}(\mathbb{F}_q) = 2$ *and* $\varepsilon_0 : y^2 + cy = x^3 + ax + b$ *is elliptic curve over* $\mathbb{F}_q$. *Let integer* $m \leq \frac{\#\varepsilon_0(\mathbb{F}_q)-1}{2}$ *such that* $m \equiv 0 \pmod 2$. *Then there exists vector* $u \in (\mathbb{F}_q^\star)^n$ *such that self–dual* m*—quasi-cyclic AG* $[2m, m, d]$*—code* $\mathcal{C}_\mathcal{L}(D, G, u)$ *associated with* ε_0 *exists.*

Theorem

Let $\mathrm{char}(\mathbb{F}_q) = 2$ *and* $\varepsilon_1 : y^2 + xy = x^3 + ax^2 + b$ *is elliptic curve over* $\mathbb{F}_q$. *Let integer* $m \leq \frac{\#\varepsilon_1(\mathbb{F}_q)-1}{2}$. *Then there exists a vector* $u \in (\mathbb{F}_q^\star)^n$ *such that self–dual* m*—quasi-cyclic AG* $[2m, m, d]$*—code* $\mathcal{C}_\mathcal{L}(D, G, u)$ *associated with* ε_1 *exists.*

КРИПТОНИТ

Thanks for your attention!

The report was prepared by

Yuri Shkuratov:
JSRPC ”Kryptonite”, y.shkuratov@kryptonite.ru