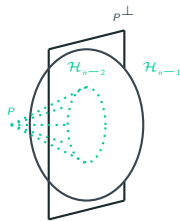


On the dimension of the subfield subcodes of 1-point Hermitian Codes

Sabira El Khalfaoui and Gábor P. Nagy

December 27, 2019

University of Szeged, Hungary
Bolyai Institute



Introduction

- Post-quantum cryptography

- McEliece cryptosystem

Generalities

- Quantum computing: attacks and McEliece instances

Subfield subcodes of Hermitian codes

- Hermitian codes

Post-quantum cryptography

- Post-quantum cryptography is the set of cryptographic schemes that are resistant against quantum computing attacks.
- In the existence of a quantum computers, most of the widely used public key cryptosystems will be broken employing **Shor Algorithm**(1994).
- The best understood post-quantum scheme is introduced by **McEliece** in 1978.

We need to plan for a post quantum-computing world if we want to keep long-term secrets!

Plan For Code-Based Cryptography!



McEliece Cryptosystem

McEliece scheme is the first code-based cryptosystem. Its security based on:

- The difficulty of decoding linear codes
- Indistinguishability of the chosen codes

How can we choose a family of codes for McEliece cryptosystem?

- with an efficient decoding algorithm
- indistinguishable from random codes

McEliece cryptosystem based on Binary Goppa codes is a good candidate for post-quantum cryptography.

But it is still suffering from having a large key size!

In December 2016 NIST launched a public competition to select one or more quantum-resistant public-key cryptographic algorithms.

Introduction

Post-quantum cryptography

McEliece cryptosystem

Generalities

Quantum computing: attacks and McEliece instances

Subfield subcodes of Hermitian codes

Hermitian codes

Attacks against code-based cryptography and ISD

There are two types of attacks against code-based cryptography:

- **Structural attack:** consists on reconstructing a decoding algorithm by studying the structure of the code generated by the public-key.
- **Decoding attack:** consists in decoding the intercepted ciphertext relatively to the public code generated by the public-key.

Information Set Decoding (ISD): is a generic decoding algorithm introduced by Prange 1962, most of well-known algorithm that do not imply any structure rely on ISD.

We base our security measurements on the complexity of ISD since it is assumed to be the lowest.

McEliece cryptosystem: original and proposed instance

The original McEliece cryptosystem is constructed on binary Goppa codes which are the subfield subcodes of the famous Reed-Solomon codes. Let C be a binary Goppa code of length n and dimension k , we denote the error capability by t .

- **Keys generation:** G generator matrix, H parity check matrix. $k \times k$ invertible matrix S , $n \times n$ permutation matrix P .
- **Secret Key:** G , S and P .
- **Public Key:** (SGP, t) .
- **Encryption:** $mSGP + e$ where e is a random error of weight t .
- **Decryption:** $(mSGP + e)P^{-1} = mSG + eP^{-1}$, then we decode to get mS . Thus $mSS^{-1} = m$.

The family of codes we suggest to use for McEliece scheme are "the subfield subcodes of Hermitian codes."

Introduction

Post-quantum cryptography

McEliece cryptosystem

Generalities

Quantum computing: attacks and McEliece instances

Subfield subcodes of Hermitian codes

Hermitian codes

Some facts on Algebraic Geometry (AG) codes: Hermitian codes

- AG codes are a generalizations of Reed-Solomon codes
- Constructed from a geometric object(line, curve...).

Example

As a classical example of codes from geometric object, Reed-Solomon codes are from a projective line.

Hermitian codes form a subclass of AG codes with Hermitian curve.

Hermitian curve over \mathbb{F}_{q^2} where $q = r^m$

The set of affine points of the Hermitian curve over \mathbb{F}_{q^2} is defined by the equation

$$\mathcal{H}_q : Y^q + Y = X^{q+1}.$$

The infinite point of the y -axis lies on \mathcal{H}_q ; it is denoted by P_∞ .

The projective closure of \mathcal{H}_q is $\bar{\mathcal{H}}_q = \mathcal{H}_q \cup \{P_\infty\}$.

Definition of 1-point Hermitian codes

- Let $x^i y^j$ be a monomial in $\mathbb{F}_{q^2}[x, y]$. The **weight** of $x^i y^j$ is defined as $qi + (q + 1)j$. It is denoted by $\rho(x^i y^j)$.
- $\mathcal{M}(s) := \{x^i y^j \mid 0 \leq i \leq q^2 - 1, 0 \leq j \leq q - 1, \rho(x^i y^j) \leq s\}$.
- $\mathcal{M}(s)$ is a basis of the **Riemann-Roch space** $\mathcal{L}(sP_\infty)$.
- $\langle \mathcal{M}(s) \rangle_{\mathbb{F}_{q^2}}$ is the vector space generated by the monomials in \mathcal{M} over \mathbb{F}_{q^2} .

1-point Hermitian codes

The **1-point Hermitian code** of weight s and length of n is defined as

$$H(s) = \left\{ (f(P_1), f(P_2), \dots, f(P_n)) \mid f \in \langle \mathcal{M}(s) \rangle_{\mathbb{F}_{q^2}} \right\}.$$

where P_1, P_2, \dots, P_n are the q^3 rational points of the Hermitian curve over \mathbb{F}_{q^2} . $H(s)$ has dimension of $k = s - g + 1$ if $2g - 2 < s < n$ where $g = q(q - 1)/2$ is the genus of \mathcal{H}_q .

The subfield subcode of 1-point Hermitian code

The subfield subcode of the Hermitian code defined over \mathbb{F}_{q^2} is the restricted space to \mathbb{F}_r :

$$H(s)|_{\mathbb{F}_r} = H(s) \cap \mathbb{F}_r^n.$$

Our study of the subfield subcodes of Hermitian codes has many goals, such as revealing some facts on the structure of such a class of codes and find good parameters for the McEliece cryptosystem. Our first result of this study is the following:

Theorem[SE Khalfaoui, GP Nagy]


Let $C_{q,r} = H(s)|_{\mathbb{F}_r}$ be the subfield subcodes of 1-point Hermitian codes, where $q = r^m$ is a prime power. Then

$$\dim C_{q,r}(s) = \begin{cases} 1 & \text{for } 0 \leq s < \frac{q^3}{r} \\ 2m + 1 & \text{for } s = \frac{q^3}{r} \end{cases}$$

Application of the subfield subcodes of 1-point Hermitian codes

The main application is to make McEliece cryptosystem practical. We summarise our methodology to produce appropriate parameters from the subfield subcodes of 1-point Hermitian codes:

- we implemented the subfield subcodes of 1-point Hermitian codes to compute the true dimension using **GAP** system.
- we computed the complexity of ISD using the parameters of the mentioned codes.
- we calculated the McEliece public key size with different parameters.

Let k be the dimension of $C_{q,r}(s)$ with length n . Let d be the Goppa designed minimum distance . We denote by $t = \lfloor \frac{d-1}{2} \rfloor$ the error capability and $R = k/n$ the rate. The McEliece public key size is $K = k(n - k)$.

Convenient parameters

The complexity formula of ISD is:

$$C(n, R) = p(n)2^{-t \log_2(1-R)} \approx 2^{-t \log_2(1-R)}$$

We consider the code $C_{8,2}(s)$ for $s \in \{256, \dots, 511\}$. The figure presents the computed values of $\log_2(C(n, R))$ with the parameters of $C_{8,2}(s)$ (y-axis) as a function of K (x-axis).

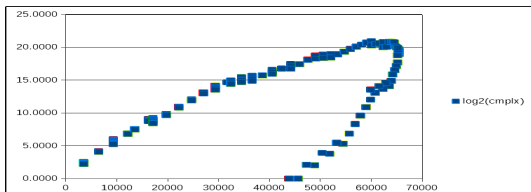


Figure 1: $\log_2(C(n, R))$ as a function of K .

The maximal value of $\log_2(C(n, R))$ is ≈ 20.91 , which is reached at key sizes 57 – 60 kbits.

- ▶ One of the motivations to determine the parameters of the subfield subcodes of **Hermitian codes** is their application in **post-quantum cryptography** in order to construct a codes-based cryptosystem as **McEliece cryptosystem**.
- ▶ Our contribution to the practicality progress of McEliece cryptographic scheme showed that the optimal parameters are still worse than those of binary Goppa codes.

As a further work, we analysed subfield subcodes for **broader classes of Hermitian codes**, in order to study their structure and select parameters for McEliece cryptosystem.

The efficient decoding algorithm can correct up to the half of **the Goppa designed minimum distance** of a functional AG codes, the reason for which we use this value without regarding the true minimum distance of the subfield subcodes of 1-point Hermitian codes which is greater. [▶ back](#)



The presented work was carried out within the project "**Security Enhancing Technologies for the Internet of Things**" 2018-1.2.1-NKP-2018-00004, supported by the National Research, Development and Innovation Fund of Hungary.

THANK YOU FOR YOUR ATTENTION!