Efficient Code Based Encryption Without Hidden Structure

Jean-Christophe Deneuville
<jean-christophe.deneuville@xlim.fr>

November the 9th, 2016
Séminaire Cryptologie et Sécurité

Joint work with:

C. Aguilar Melchor — IRIT Toulouse
O. Blazy, P. Gaborit — **XLIM-DMI**
G. Zémor — University of Bordeaux

Outline

Outline

Maths (1/2)

Notations:

- $\mathbb{Z}$: ring of integers
- $\mathbb{F}$: finite (hence commutative) field
- $\mathbb{F}_q$: for prime q for Hamming Codes
- $\mathbb{F}_{q^m}$: for Rank Metric codes
- $\mathcal{V}$: vector space of dimension n over $\mathbb{F}$ for some positive n

Vectors:

Row vector $\mathbf{v} \in \mathcal{V}$ can be seen as a polynomial in $\mathcal{R} = \mathbb{F}[X]/(X^n - 1)$ (or $\mathcal{R}_q$ or $\mathcal{R}_{q^m}$).

Operations:

For any two elements $\mathbf{x}, \mathbf{y} \in \mathcal{V}$, we define their product similarly as in $\mathcal{R}$, *i.e.* $\mathbf{x} \cdot \mathbf{y} = \mathbf{c} \in \mathcal{V}$ with

$$c_k = \sum_{i+j \equiv k \mod n} x_i y_j, \text{ for } k \in \{0, 1, \ldots, n-1\}. \quad (1)$$

Maths (2/2)

Definition (Circulant Matrix)

Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}^n$. The *circulant matrix* induced by $\mathbf{x}$ is defined and denoted as follows:

$$\mathbf{rot}(\mathbf{x}) = \begin{pmatrix} x_1 & x_n & \cdots & x_2 \\ x_2 & x_1 & \cdots & x_3 \\ \vdots & \vdots & \ddots & \vdots \\ x_n & x_{n-1} & \cdots & x_1 \end{pmatrix} \in \mathbb{F}^{n \times n} \tag{2}$$

As a consequence, we introduce the $\mathbf{rot}(\cdot)$ operator as:

$$\mathbf{x} \cdot \mathbf{y} = \mathbf{x} \cdot \mathbf{rot}(\mathbf{y})^\top = \left(\mathbf{rot}(\mathbf{x}) \cdot \mathbf{y}^\top\right)^\top = \mathbf{y} \cdot \mathbf{rot}(\mathbf{x})^\top = \mathbf{y} \cdot \mathbf{x}. \tag{3}$$

Outline

General Problems

Cryptography needs different difficult problems

- Factorization
- Discrete Logarithm
- Shortest/Closest Vector problem
- Syndrome Decoding problem

For Code-based Cryptography, the security of cryptosystems is usually related to the problem of *decoding a syndrome* for a particular metric.

Post-Quantum Cryptography

Consider the simple linear system problem :
H a random $(n-k) \times n$ matrix over some field $\mathbb{K}$ ($\mathbb{R}$, $\mathbb{F}_q$, $\mathbb{F}_{q^m}$, ...)

Given $\mathbf{s} \in \mathbb{K}^{n-k}$, find $\mathbf{x} \in \mathbb{K}^n$ such that $\mathbf{xH} = \mathbf{s}$?

Post-Quantum Cryptography

Consider the simple linear system problem :
H a random $(n-k) \times n$ matrix over some field $\mathbb{K}$ ($\mathbb{R}$, $\mathbb{F}_q$, $\mathbb{F}_{q^m}$, ...)

Given $\mathbf{s} \in \mathbb{K}^{n-k}$, find $\mathbf{x} \in \mathbb{K}^n$ such that $\mathbf{xH} = \mathbf{s}$?

$\rightarrow$ Easy problem:

1. Choose $n-k$ columns of **H**, obtain $(n-k) \times (n-k)$ submatrix **A** of **H**
2. **A** invertible with good probability, then $\mathbf{x} = (0, \ldots, 0, \mathbf{sA}^{-1}, 0, \ldots, 0)$.

Post-Quantum Cryptography

Consider the simple linear system problem :
H a random $(n-k) \times n$ matrix over some field $\mathbb{K}$ ($\mathbb{R}$, $\mathbb{F}_q$, $\mathbb{F}_{q^m}$, ...)

Given $\mathbf{s} \in \mathbb{K}^{n-k}$, find $\mathbf{x} \in \mathbb{K}^n$ such that $\mathbf{xH} = \mathbf{s}$?

$\rightarrow$ Easy problem:

1. Choose $n-k$ columns of **H**, obtain $(n-k) \times (n-k)$ submatrix **A** of **H**
2. **A** invertible with good probability, then $\mathbf{x} = (0, \ldots, 0, \mathbf{sA}^{-1}, 0, \ldots, 0)$.

$\rightarrow$ **How to make this problem difficult ?**

Difficult Probrems for PQ-Crypto

(1) add a constraint to x: **x** small for some metric

- Hamming distance $\rightarrow$ **Code-based Crypto**
- Euclidean distance $\rightarrow$ **Lattice-based Crypto**
- Rank distance $\rightarrow$ **Rank-based Crypto**

$\Rightarrow$ only difference : the metric considered, and its associated properties

(2) consider rather a multivariable non linear system: quadratic, cubic, etc...
$\rightarrow$ **Mutivariate Crypto**

General interest of post-quantum cryptogrphy

Advantages

- A priori resistant to a quantum computer
- Usually faster than number-theory based cryptography
- Easier to protect against side-channel attacks

General interest of post-quantum cryptogrphy

Advantages

- A priori resistant to a quantum computer
- Usually faster than number-theory based cryptography
- Easier to protect against side-channel attacks

Drawback

- Key sizes may be larger

Outline

Encryption Scheme

Encryption Scheme. An encryption scheme is a tuple of four polynomial time algorithms (Setup, KeyGen, Encrypt, Decrypt):

- Setup(1^λ), where λ is the security parameter, generates the global parameters param of the scheme;

- KeyGen(param) outputs a pair of keys, a (public) encryption key pk and a (private) decryption key sk;

- Encrypt(pk, $\boldsymbol{\mu}$, ρ) outputs a ciphertext $\mathbf{c}$, on the message $\boldsymbol{\mu}$, under the encryption key pk, with the randomness ρ;

- Decrypt(sk, $\mathbf{c}$) outputs the plaintext $\boldsymbol{\mu}$, encrypted in the ciphertext $\mathbf{c}$ or $\perp$.

Outline

Rank Metric (1/3)

The rank metric is defined in finite extensions.

$\mathbb{F}_q$ a finite field with q a power of a prime.

$\mathbb{F}_{q^m}$ an extension of degree m of $\mathbb{F}_q$.

$\mathbf{B} = (b_1, ..., b_m)$ a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

$\mathbb{F}_{q^m}$ can be seen as a vector space on $\mathbb{F}_q$.

$\mathcal{C}[n, k]$ a linear code over $\mathbb{F}_{q^m}$ of dimension k and length n.

$\mathbf{G}$ a $k \times n$ generator matrix of the code $\mathcal{C}$.

$\mathbf{H}$ a $(n-k) \times n$ parity check matrix of $\mathcal{C}$: $\mathbf{G}\mathbf{H}^\top = \mathbf{0}$.

$\mathbf{H}$ a dual matrix, $\mathbf{x} \in \mathbb{F}_{q^m}^n \rightarrow$ syndrome of $\mathbf{x}$: $\mathbf{H}\mathbf{x}^\top \in \mathbb{F}_{q^m}^{n-k}$.

Rank metric (2/3)

Words of the code $\mathcal{C}$ are n-uplets with coordinates in $\mathbb{F}_{q^m}$.

$$\mathbf{v} = (v_1, \ldots, v_n)$$

with $v_j \in \mathbb{F}_{q^m}$.
Any coordinate $v_j = \sum_{i=1}^{m} v_{ij} b_i$ with $v_{ij} \in \mathbb{F}_q$.

$$\mathbf{v} = (v_1, ..., v_n) \rightarrow \mathbf{V} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}$$

Rank metric (3/3)

Definition (Rank weight of word)

$\mathbf{v}$ has rank $r = \mathrm{rank}(\mathbf{v})$ iff the rank of $\mathbf{V} = (v_{ij})_{ij}$ is r.
Equivalently $\mathrm{rank}(\mathbf{v}) = r \Leftrightarrow v_j \in V_r \subset \mathbb{F}_{q^m}^n$ with $\dim(V_r)$=r.

The determinant of $\mathbf{V}$ does not depend on the basis

Definition (Rank distance)

Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^m}^n$, the rank distance between $\mathbf{x}$ and $\mathbf{y}$ is defined by $\mathrm{d}_R(\mathbf{x}, \mathbf{y}) = \mathrm{rank}(\mathbf{x} - \mathbf{y})$.

Analogy: counting subspaces

Counting the number of possible supports for length n and dimension t

Analogy: counting subspaces

Counting the number of possible supports for length n and dimension t

Hamming : number of sets with t elements in sets of n elements: Newton binomial $\binom{n}{t}$ $(\leq 2^n)$

Analogy: counting subspaces

Counting the number of possible supports for length n and dimension t

Hamming : number of sets with t elements in sets of n elements: Newton binomial $\binom{n}{t}$ $(\leq 2^n)$

Rank : number of subspaces of dimension t over $\mathbb{F}_q$ in the space of dimension n over $\mathbb{F}_{q^m}$: Gaussian binomial $\begin{bmatrix} n \\ t \end{bmatrix}_q (\sim q^{t(n-t)})$

Analogy: counting subspaces

Counting the number of possible supports for length n and dimension t

Hamming : number of sets with t elements in sets of n elements: Newton binomial $\binom{n}{t}$ $(\leq 2^n)$

Rank : number of subspaces of dimension t over $\mathbb{F}_q$ in the space of dimension n over $\mathbb{F}_{q^m}$: Gaussian binomial $\begin{bmatrix} n \\ t \end{bmatrix}_q (\sim q^{t(n-t)})$

Bottom line: **Rank metric** attacks have **quadraticly** exponential $2^{\mathcal{O}(n^2)}$ complexity, against **simply** exponential $2^{\mathcal{O}(n)}$ for **Hamming metric**

Outline

Code-Based Encryption (1/3) : McEliece

Key Generation :

$\mathcal{C}[n,k]$ linear code, generated by $\mathbf{G} \in \mathbb{F}_q^{k\times n}$, decoding up to t errors

$\mathbf{S} \xleftarrow{\$} \mathbb{F}_q^{k\times k}$ invertible, $\mathbf{P} \xleftarrow{\$} \mathbb{F}_2^{n\times n}$ permutation

$$\rightarrow \mathsf{pk} = (\tilde{\mathbf{G}} = \mathbf{SGP}, t),\ \mathsf{sk} = (\mathbf{S}, \mathbf{G}, \mathbf{P})$$

Encryption (of $\mu \in \mathbb{F}_q^k$) :

$\mathbf{e} \xleftarrow{\$} \mathbb{F}_q^n$, with $\omega(\mathbf{e}) = t$

$$\rightarrow \mathbf{c} = \mu\tilde{\mathbf{G}} + \mathbf{e}$$

Decryption :

$\tilde{\mu} = \mathcal{C}.\mathsf{Decode}(\mathbf{cP}^{-1})$

$$\rightarrow \tilde{\mu}\mathbf{S}^{-1}$$

Code-Based Encryption (2/3) : MDPC

Key Generation :

$\mathcal{C}[n,k]$ MDPC code, parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{k \times n}$, decoding up to t errors

$\mathbf{G} \in \mathbb{F}_q^{(n-k) \times n}$ generator matrix in reduced echelon form

$$\rightarrow \mathsf{pk} = (\mathbf{G}, t),\ \mathsf{sk} = \mathbf{H}$$

Encryption (of $\mu \in \mathbb{F}_2^{n-k}$) :

$\mathbf{e} \xleftarrow{\$} \mathbb{F}_2^n$, with $\omega(\mathbf{e}) = t$

$$\rightarrow \mathbf{c} = \mu\mathbf{G} + \mathbf{e}$$

Decryption :

$\tilde{\mu} = \mu\mathbf{G} \leftarrow \mathcal{C}.\mathrm{Decode}_{\mathbf{H}}(\mu\mathbf{G} + \mathbf{e})$

$\rightarrow$ extract μ from $(n-k)$ first positions of $\tilde{\mu}$

Code-Based Encryption (3/3) : LRPC

Key Generation :

$\mathcal{C}[n,k]$ LRPC code, of support $\mathcal{S}$ of small rank r

parity-check matrix $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$, generator matrix $\mathbf{G} \in \mathbb{F}_{q^m}^{k\times n}$

$$\rightarrow \mathsf{pk} = (\mathbf{G}, r),\ \mathsf{sk} = \mathbf{H}$$

Encryption (of $\mu \in \mathbb{F}_{q^m}^k$) :

$\mathbf{e} \xleftarrow{\$} \mathbb{F}_{q^m}^n$, with $\mathrm{rank}(\mathbf{e}) \leq r$

$$\rightarrow \mathbf{c} = \mu\mathbf{G} + \mathbf{e}$$

Decryption :

$\mathbf{e} = \mathcal{C}.\mathrm{Decode}(\mathbf{cH})$

$$\rightarrow \mu\mathbf{G} = \mathbf{c} - \mathbf{e},\ \text{return } \mu$$

Outline

Comparisons / Motivations

	McEliece	MDPC	LRPC
Key Sizes			
Decryption Fail. proba			
Hidden Structure			
Security			
Overall Practicality			

Outline

Presentation

Intuition

Encryption
- Message is encoded through a code $\mathcal{C}$
- An error term is added to this coding using Public Key

Decryption
- Secret Key used to remove errors
- Code $\mathcal{C}$ used for decoding back to the message

Notation $\rightarrow$ Secret data - Public data - One-time Randomness

Presentation

- Setup(1^λ): generates $n = n(\lambda)$, $k = k(\lambda)$, $\delta = \delta(\lambda)$, and $w = w(\lambda)$. Plaintext space is $\mathbb{F}^k$. param$= (n, k, \delta, w)$.

Presentation

- Setup(1^λ): generates $n = n(\lambda)$, $k = k(\lambda)$, $\delta = \delta(\lambda)$, and $w = w(\lambda)$. Plaintext space is $\mathbb{F}^k$. param$= (n, k, \delta, w)$.

- KeyGen(param): generates $\mathbf{q}_r \xleftarrow{\$} \mathcal{V}$, the parity matrix $\mathbf{Q} = (\mathbf{I}_n \mid \mathbf{rot}(\mathbf{q}_r))$ of $\mathcal{C}$ and its associated generator matrix $\mathbf{G} \in \mathbb{F}^{k \times n}$, $\mathsf{sk} = (\mathbf{x}, \mathbf{y}) \xleftarrow{\$} \mathcal{V}^2$ such that $\omega(\mathbf{x}), \omega(\mathbf{y}) \leq w$, sets $\mathsf{pk} = \left(\mathbf{G}, \mathbf{H}, \mathbf{s} = \mathsf{sk} \cdot \mathbf{Q}^\top, w\right)$, and returns $(\mathsf{pk}, \mathsf{sk})$.

Presentation

- Setup(1^λ): generates $n = n(\lambda)$, $k = k(\lambda)$, $\delta = \delta(\lambda)$, and $w = w(\lambda)$. Plaintext space is $\mathbb{F}^k$. param$= (n, k, \delta, w)$.

- KeyGen(param): generates $\mathbf{q}_r \xleftarrow{\$} \mathcal{V}$, the parity matrix $\mathbf{Q} = (\mathbf{I}_n \mid \mathbf{rot}(\mathbf{q}_r))$ of $\mathcal{C}$ and its associated generator matrix $\mathbf{G} \in \mathbb{F}^{k \times n}$, $\mathsf{sk} = (\mathbf{x}, \mathbf{y}) \xleftarrow{\$} \mathcal{V}^2$ such that $\omega(\mathbf{x}), \omega(\mathbf{y}) \leq w$, sets $\mathsf{pk} = \left(\mathbf{G}, \mathbf{H}, \mathbf{s} = \mathsf{sk} \cdot \mathbf{Q}^\top, w\right)$, and returns $(\mathsf{pk}, \mathsf{sk})$.

- Encrypt($\mathsf{pk} = (\mathbf{G}, \mathbf{Q}, \mathbf{s}), \boldsymbol{\mu}, \theta$): uses randomness θ to generate $\boldsymbol{\epsilon} \xleftarrow{\$} \mathcal{V}$, $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2) \xleftarrow{\$} \mathcal{V}^2$ such that $\omega(\boldsymbol{\epsilon}), \omega(\mathbf{r}_1), \omega(\mathbf{r}_2) \leq w$, sets $\mathbf{v}^\top = \mathbf{Q}\mathbf{r}^\top$ and $\boldsymbol{\rho} = \boldsymbol{\mu}\mathbf{G} + \mathbf{s} \cdot \mathbf{r}_2 + \boldsymbol{\epsilon}$. It finally returns $\mathbf{c} = (\mathbf{v}, \boldsymbol{\rho})$, an encryption of $\boldsymbol{\mu}$ under pk.

Presentation

- Setup(1^λ): generates $n = n(\lambda)$, $k = k(\lambda)$, $\delta = \delta(\lambda)$, and $w = w(\lambda)$. Plaintext space is $\mathbb{F}^k$. param$= (n, k, \delta, w)$.

- KeyGen(param): generates $\mathbf{q}_r \xleftarrow{\$} \mathcal{V}$, the parity matrix $\mathbf{Q} = (\mathbf{I}_n \mid \mathbf{rot}(\mathbf{q}_r))$ of $\mathcal{C}$ and its associated generator matrix $\mathbf{G} \in \mathbb{F}^{k \times n}$, $\mathsf{sk} = (\mathbf{x}, \mathbf{y}) \xleftarrow{\$} \mathcal{V}^2$ such that $\omega(\mathbf{x}), \omega(\mathbf{y}) \leq w$, sets $\mathsf{pk} = \left(\mathbf{G}, \mathbf{H}, \mathbf{s} = \mathsf{sk} \cdot \mathbf{Q}^\top, w\right)$, and returns $(\mathsf{pk}, \mathsf{sk})$.

- Encrypt($\mathsf{pk} = (\mathbf{G}, \mathbf{Q}, \mathbf{s}), \boldsymbol{\mu}, \theta$): uses randomness θ to generate $\boldsymbol{\epsilon} \xleftarrow{\$} \mathcal{V}$, $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2) \xleftarrow{\$} \mathcal{V}^2$ such that $\omega(\boldsymbol{\epsilon}), \omega(\mathbf{r}_1), \omega(\mathbf{r}_2) \leq w$, sets $\mathbf{v}^\top = \mathbf{Q}\mathbf{r}^\top$ and $\boldsymbol{\rho} = \boldsymbol{\mu}\mathbf{G} + \mathbf{s} \cdot \mathbf{r}_2 + \boldsymbol{\epsilon}$. It finally returns $\mathbf{c} = (\mathbf{v}, \boldsymbol{\rho})$, an encryption of $\boldsymbol{\mu}$ under pk.

- Decrypt($\mathsf{sk} = (\mathbf{x}, \mathbf{y}), \mathbf{c} = (\mathbf{v}, \boldsymbol{\rho})$): returns $\mathcal{C}$.Decode$(\boldsymbol{\rho} - \mathbf{v} \cdot \mathbf{y})$.

Correctness

Correctness Property

$$\text{Decrypt}\left(\mathsf{sk}, \text{Encrypt}\left(\mathsf{pk}, \mu, \theta\right)\right) = \mu$$

$\mathcal{C}$.Decode correctly decodes $\rho - \mathbf{v} \cdot \mathbf{y}$ whenever

the error term is **not too big**

$$\omega\left(\mathbf{s} \cdot \mathbf{r}_2 - \mathbf{v} \cdot \mathbf{y} + \boldsymbol{\epsilon}\right) \leq \delta$$

$$\omega\left(\left(\mathbf{x} + \mathbf{q}_r \cdot \mathbf{y}\right) \cdot \mathbf{r}_2 - \left(\mathbf{r}_1 + \mathbf{q}_r \cdot \mathbf{r}_2\right) \cdot \mathbf{y} + \boldsymbol{\epsilon}\right) \leq \delta$$

$$\omega(\mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y} + \boldsymbol{\epsilon}) \leq \delta$$

Error distribution analysis $\rightarrow$ Decryption failure probability better understood

Outline

Theorem

Definition (SD Distribution)

For positive integers, n, k, and w, the *SD(n, k, w) Distribution* chooses $\mathbf{H} \xleftarrow{\$} \mathbb{F}^{(n-k)\times n}$ and $\mathbf{x} \xleftarrow{\$} \mathbb{F}^n$ such that $\omega(\mathbf{x}) = w$, and outputs $(\mathbf{H}, \mathbf{H}\mathbf{x}^\top)$.

Definition (Decisional s-QCSD Problem)

For positive integers n, k, w, s, a random parity check matrix $\mathbf{H}$ of a QC code $\mathcal{C}$ and $\mathbf{y} \xleftarrow{\$} \mathbb{F}^n$, the *Decisional s-Quasi-Cyclic SD Problem s-DQCSD(n, k, w)* asks to decide with non-negligible advantage whether $(\mathbf{H}, \mathbf{y}^\top)$ came from the s-QCSD(n, k, w) distribution or the uniform distribution over $\mathbb{F}^{(n-k)\times n} \times \mathbb{F}^{n-k}$.

Theorem

The scheme presented above is IND-CPA *under the* 2*-DQCSD and* 3*-DQCSD assumptions.*

Quick Recall

- KeyGen:
  - $\mathsf{sk} = (\mathbf{x}, \mathbf{y}) \xleftarrow{\$} \mathcal{V}^2$ such that $\omega(\mathbf{x}), \omega(\mathbf{y}) \leq w$
  - $\mathsf{pk} = \left(\mathbf{G}, \mathbf{Q}, \mathbf{s} = \mathsf{sk} \cdot \mathbf{Q}^\top, w\right)$

- Encrypt$(\mathsf{pk}, \boldsymbol{\mu})$: $\boldsymbol{\epsilon} \xleftarrow{\$} \mathcal{V}$, $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2) \xleftarrow{\$} \mathcal{V}^2$ such that $\omega(\mathbf{r}_1), \omega(\mathbf{r}_2) \leq w$, and $\omega(\boldsymbol{\epsilon}) = 3w$
  - $\mathbf{v}^\top = \mathbf{Q}\mathbf{r}^\top$
  - $\boldsymbol{\rho} = \boldsymbol{\mu}\mathbf{G} + \mathbf{s} \cdot \mathbf{r}_2 + \boldsymbol{\epsilon}$

- Decrypt$(\mathsf{sk}, \mathbf{c} = (\mathbf{v}, \boldsymbol{\rho}))$: returns $\mathcal{C}.\mathsf{Decode}(\boldsymbol{\rho} - \mathbf{v} \cdot \mathbf{y})$.

Intuition

Usual Game :

$\mathbf{Exp}^{\mathsf{ind}-b}_{\mathcal{E},\mathcal{A}}(\lambda)$
1. $\mathsf{param} \leftarrow \mathsf{Setup}(1^\lambda)$
2. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{param})$
3. $(\boldsymbol{\mu}_0, \boldsymbol{\mu}_1) \leftarrow \mathcal{A}(\texttt{FIND} : \mathsf{pk})$
4. $\mathbf{c}^* \leftarrow \mathsf{Encrypt}(\mathsf{pk}, \boldsymbol{\mu}_b, \theta)$
5. $b' \leftarrow \mathcal{A}(\texttt{GUESS} : \mathbf{c}^*)$
6. $\texttt{RETURN}\ \ b'$

Intuition

Usual Game :

$\mathbf{Exp}^{\mathsf{ind}-b}_{\mathcal{E},\mathcal{A}}(\lambda)$
1. $\mathsf{param} \leftarrow \mathsf{Setup}(1^\lambda)$
2. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{param})$
3. $(\boldsymbol{\mu}_0, \boldsymbol{\mu}_1) \leftarrow \mathcal{A}(\texttt{FIND} : \mathsf{pk})$
4. $\mathbf{c}^* \leftarrow \mathsf{Encrypt}(\mathsf{pk}, \boldsymbol{\mu}_b, \theta)$
5. $b' \leftarrow \mathcal{A}(\texttt{GUESS} : \mathbf{c}^*)$
6. $\texttt{RETURN}\ \ b'$

Alternative : Hybrid Argument

Intuition

Usual Game :

$\mathbf{Exp}^{\mathsf{ind}-b}_{\mathcal{E},\mathcal{A}}(\lambda)$
1. $\mathsf{param} \leftarrow \mathsf{Setup}(1^\lambda)$
2. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{param})$
3. $(\mu_0, \mu_1) \leftarrow \mathcal{A}(\texttt{FIND} : \mathsf{pk})$
4. $\mathbf{c}^* \leftarrow \mathsf{Encrypt}(\mathsf{pk}, \mu_b, \theta)$
5. $b' \leftarrow \mathcal{A}(\texttt{GUESS} : \mathbf{c}^*)$
6. $\texttt{RETURN}\ \ b'$

Alternative : Hybrid Argument

Build a sequence of game from an adversary receiving an encryption of message μ_0 to an adversary receiving an encryption of a message μ_1.

Intuition

Usual Game :

$\mathbf{Exp}^{\mathsf{ind}-b}_{\mathcal{E},\mathcal{A}}(\lambda)$
1. $\mathsf{param} \leftarrow \mathsf{Setup}(1^\lambda)$
2. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{param})$
3. $(\boldsymbol{\mu}_0, \boldsymbol{\mu}_1) \leftarrow \mathcal{A}(\texttt{FIND} : \mathsf{pk})$
4. $\mathbf{c}^* \leftarrow \mathsf{Encrypt}(\mathsf{pk}, \boldsymbol{\mu}_b, \theta)$
5. $b' \leftarrow \mathcal{A}(\texttt{GUESS} : \mathbf{c}^*)$
6. $\texttt{RETURN}\ \ b'$

Alternative : Hybrid Argument

Build a sequence of game from an adversary receiving an encryption of message $\boldsymbol{\mu}_0$ to an adversary receiving an encryption of a message $\boldsymbol{\mu}_1$.

If the adversary can tell them apart, we use it to construct a simulator breaking the DQCSD assumption for QC codes of order 2 and 3.

Game 0

Real game:

- honest KeyGen algorithm
- receive (μ_0, μ_1) from $\mathcal{A}$
- produce a valid encryption of μ_0.

Game 1

Game 1:

- forget the decryption key sk
- take **s** at random
- proceed honestly

Under the DQCSD this game is indistinguishable from game 0.

Game 2

Game 2:

- we don't know the decryption key
- we can start generating random ciphertexts
- instead of picking correctly weighted $\mathbf{r}_1, \mathbf{r}_2, \epsilon$
- the simulator now picks random vectors in the full space

The adversary view is:

$$\begin{pmatrix} \mathbf{v} \\ \boldsymbol{\rho} - \boldsymbol{\mu}_0 \mathbf{G} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{rot}(\mathbf{q}_r) \\ \mathbf{0} & \mathbf{I}_n & \mathbf{rot}(\mathbf{s}) \end{pmatrix} \cdot (\mathbf{r}_1, \epsilon, \mathbf{r}_2)^\top$$

When $\mathbf{r}_1, \mathbf{r}_2, \epsilon$ are picked at random, $\mathbf{v}$, $\boldsymbol{\rho}$ look random. Hence honestly generated ciphertexts are indistinguishable from invalid ones under the DQCSD assumption (applied on a $2n \times 3n$ quasi-cyclic matrix of order 3).

Game 3

We now proceed in reverse. Given,

- $\mathbf{r}_1, \mathbf{r}_2, \epsilon$ random
- messages μ_0, μ_1
- $\mathbf{v}, \rho$ computed as before

Game 3:

- find values $\mathbf{r}'_1, \mathbf{r}'_2, \epsilon'$ such that $\mathbf{v}^\top = \mathbf{Q}\mathbf{r}'^\top$ and $\rho = \mu_1 \mathbf{G} + \mathbf{s} \cdot \mathbf{r}'_2 + \epsilon'$

Hence, the previous invalid encryption of μ_0 is perfectly indistinguishable from a fake encryption of μ_1.

Game 4

Same game as Game 3, but

- pick $\mathbf{r}'_1, \mathbf{r}'_2, \epsilon'$ with the correct weight

Under DQCSD this is indistinguishable from the previous game.

Game 5

End of proof:

- switch pk to an honestly generated one

Similarly to Game 1, this game is indistinguishable from the previous one, under DQCSD.

Proof Conclusion

We manage to build a sequence of games allowing a simulator to transform a ciphertext of a message μ_0 to a ciphertext of a message μ_1. Hence the advantage of an adversary against the IND-CPA experiment is bounded:

$$\mathbf{Adv}^{\text{ind}}_{\mathcal{E},\mathcal{A}}(\lambda) \leq 2 \cdot \left(\mathbf{Adv}^{\text{2-DQCSD}}(\lambda) + \mathbf{Adv}^{\text{3-DQCSD}}(\lambda) \right). \tag{4}$$

□

Outline

Simple Codes (1/3)

Lemma

Consider two independent random variables $X, Y \sim \mathcal{B}(\frac{w}{n})$. *Then*

$$\Pr[X \cdot Y = c] = \begin{cases} \left(\frac{w}{n}\right)^2 \text{ if } c = 1, \\ (1 - \frac{w}{n})^2 + 2\frac{w}{n}(1 - \frac{w}{n}) = 1 - \left(\frac{w}{n}\right)^2 \text{ if } c = 0, \\ 0 \text{ otherwise.} \end{cases} \quad (5)$$

Lemma

Let $S_k = \left\{(i,j) \in \{0,\ldots,n-1\}^2 \text{ such that } i + j \equiv k \mod n\right\}$ *for* $k \in \{0,\ldots,n-1\}$. *Then* $\#S_k = n$.

Simple Codes (2/3)

Proposition

Let $\mathbf{x}, \mathbf{y} \xleftarrow{\$} \mathcal{V}$ *be two n-dimensional vectors of weight w, and let* $\mathbf{z} = \mathbf{x} \cdot \mathbf{y}$. *Then*

$$\Pr[z_k = c] = \begin{cases} \sum_{0 \leq i \leq n, i \text{ odd}} \binom{n}{i} \cdot \left(\left(\frac{w}{n}\right)^2\right)^i \cdot \left(1 - \left(\frac{w}{n}\right)^2\right)^{n-i} & \text{if } c = 1, \\ \sum_{0 \leq i \leq n, i \text{ even}} \binom{n}{i} \cdot \left(\left(\frac{w}{n}\right)^2\right)^i \cdot \left(1 - \left(\frac{w}{n}\right)^2\right)^{n-i} & \text{if } c = 0, \\ 0 \text{ otherwise.} \end{cases} \tag{6}$$

Proposition

Let $\mathbf{x}, \mathbf{y}, \mathbf{r}_1, \mathbf{r}_2 \xleftarrow{\$} \mathbb{F}_2^n$ *be n-dimensional vectors of weight w, and let* $\mathbf{t} = \mathbf{x}\mathbf{r}_2 - \mathbf{r}_1\mathbf{y}$. *Then*

$$\Pr[t_k = c] = \begin{cases} 2\tilde{p}(1-\tilde{p}) \text{ if } c = 1, \\ (1-\tilde{p})^2 + \tilde{p}^2 \text{ if } c = 0, \\ 0 \text{ otherwise.} \end{cases} \tag{7}$$

Simple Codes (3/3)

Theorem

Let $\mathbf{x}, \mathbf{y}, \mathbf{r}_1, \mathbf{r}_2 \xleftarrow{\$} \mathbb{F}_2^n$ *be n-dimensional vectors of weight* w, $\boldsymbol{\epsilon} \xleftarrow{\$} \mathbb{F}_2^n$ *of weight* ϵ, *and let* $\mathbf{e} = \mathbf{x}\mathbf{r}_2 - \mathbf{r}_1\mathbf{y} + \boldsymbol{\epsilon}$. *Then*

$$\Pr[e_k = c] = \begin{cases} 2\tilde{p}(1-\tilde{p})(1-\frac{\epsilon}{n}) + \left((1-\tilde{p})^2 + \tilde{p}^2\right)\frac{\epsilon}{n} \text{ if } c = 1, \\ \left((1-\tilde{p})^2 + \tilde{p}^2\right)(1-\frac{\epsilon}{n}) + 2\tilde{p}(1-\tilde{p})\frac{\epsilon}{n} \text{ if } c = 0, \\ 0 \text{ otherwise.} \end{cases} \tag{8}$$

$$\Pr[\omega(\mathbf{e}) = d] = \binom{n}{d} \cdot (p^\star)^d \cdot (1-p^\star)^{(n-d)}. \tag{9}$$

Tensor Product Codes (1/2)

$$\bar{p}_\gamma = \bar{p}_\gamma(n_1, n_2) = \sum_{i=\lfloor \frac{n_2-1}{2} \rfloor + 1}^{n_2} \binom{n_2}{i} \left(\frac{\gamma}{n_1 n_2}\right)^i \left(1 - \frac{\gamma}{n_1 n_2}\right)^{n_2 - i}. \tag{10}$$

$$\mathcal{P} = \mathcal{P}(\delta_1, n_1, n_2, \gamma) = \sum_{i=\delta_1+1}^{n_1} \binom{n_1}{i} (\bar{p}_\gamma)^i (1 - \bar{p}_\gamma)^{n_1 - i}. \tag{11}$$

Tensor Product Codes (2/2)

Theorem

Let $\mathcal{C} = \mathrm{BCH}(n_1, k, \delta) \otimes \mathbb{1}_{n_2}$, $(pk, sk) \leftarrow \mathsf{KeyGen}$, $\boldsymbol{\mu} \xleftarrow{\$} \mathbb{F}_2^k$, *and some randomness* $\theta \in \{0,1\}^*$, *then with the notations above, the decryption failure is*

$$p_{\mathsf{fail}} = \Pr[\mathsf{Decrypt}(\mathsf{sk}, \mathsf{Encrypt}(\mathsf{pk}, \boldsymbol{\mu}, \theta)) \neq \boldsymbol{\mu}.] \tag{12}$$

$$= \sum_{\gamma=0}^{\min\left(2w^2+\epsilon, n_1 n_2\right)} \Pr[\omega(\mathbf{e}) = \gamma] \cdot \mathcal{P}(\delta_1, n_1, n_2, W) \tag{13}$$

Outline

Parameters (1/2)

Hamming Metric instantiation (HQC)

		Cryptosystem Parameters								
	Instance	n_1	n_2	$n' \approx n_1 n_2 = n$	k'	δ	w	$\epsilon = 3w$	security	p_{fail}
Classical	Toy	255	25	6,379	63	30	36	108	64	$< 2^{-64}$
	Low	255	37	9,437	79	27	45	135	80	$< 2^{-80}$
	Medium	255	53	13,523	99	23	56	168	100	$< 2^{-100}$
	Strong	511	41	20,959	121	58	72	216	128	$< 2^{-128}$
Quantum	Toy	255	65	16,603	63	87	72	216	64	$< 2^{-64}$
	Low	511	47	24,019	76	85	89	267	80	$< 2^{-80}$
	Medium	255	141	35,963	99	23	112	336	100	$< 2^{-100}$
	Strong	511	109	55,711	121	58	143	429	128	$< 2^{-128}$

Key sizes : $2n$ or $n + \lambda$ bits by giving a seed

Outline

Parameters (2/2)

Rank Metric instantiation (RQC)

	Cryptosystem Parameters								
Instance	n	k'	m	q	w	ϵ	plaintext	key size	security
RQC-I	37	13	37	4	3	3	962	2,738	90
RQC-II	53	13	53	2	4	4	689	2,809	95
RQC-III	61	3	61	2	5	4	183	3,721	140
RQC-IV	83	3	83	2	6	4	249	6,889	230
RQC-V	61	3	61	4	5	4	366	7,442	264

Outline

Comparison (1/2)

Parameters for different code-based cryptosystems as a function of the security parameter λ

Cryptosystem		Code Length	Public Key Size	Ciphertext Size	Hidden Structure
Goppa-McEliece	[ME78]	$\mathcal{O}(\lambda \log \lambda)$	$\mathcal{O}\left(\lambda^2 (\log \lambda)^2\right)$	$\mathcal{O}(\lambda \log \lambda)$	Strong
MDPC	[BMTS13]	$\mathcal{O}\left(\lambda^2\right)$	$\mathcal{O}\left(\lambda^2\right)$	$\mathcal{O}\left(\lambda^2\right)$	Weak
LRPC	[GMRZ13]	$\mathcal{O}\left(\lambda^{\frac{2}{3}}\right)$	$\mathcal{O}\left(\lambda^{\frac{4}{3}}\right)$	$\mathcal{O}\left(\lambda^{\frac{4}{3}}\right)$	Weak
HQC		$\mathcal{O}\left(\lambda^2\right)$	$\mathcal{O}\left(\lambda^2\right)$	$\mathcal{O}\left(\lambda^2\right)$	No
RQC		$\mathcal{O}\left(\lambda^{\frac{2}{3}}\right)$	$\mathcal{O}\left(\lambda^{\frac{4}{3}}\right)$	$\mathcal{O}\left(\lambda^{\frac{4}{3}}\right)$	No

Comparison (2/2)

	McEliece	MDPC	LRPC	HQC	RQC
Key Sizes					
Decryption Fail. proba					
Hidden Structure					
Security					
Overall Practicality					

Conclusion

Generic cryptosystem that can perform both **key exchange** and **encryption**

Conclusion

Generic cryptosystem that can perform both **key exchange** and **encryption**

HQC particularly well suited for KE

Conclusion

Generic cryptosystem that can perform both **key exchange** and **encryption**

HQC particularly well suited for KE

MDPC might be better for encryption due to their high rates

Conclusion

Generic cryptosystem that can perform both **key exchange** and **encryption**

HQC particularly well suited for KE

MDPC might be better for encryption due to their high rates

RQC good both for KE and Enc, but

Conclusion

Generic cryptosystem that can perform both **key exchange** and **encryption**

HQC particularly well suited for KE

MDPC might be better for encryption due to their high rates

RQC good both for KE and Enc, but

Rank metric deserves/needs **more scrutiny** from the community, so

Conclusion

Generic cryptosystem that can perform both **key exchange** and **encryption**

HQC particularly well suited for KE

MDPC might be better for encryption due to their high rates

RQC good both for KE and Enc, but

Rank metric deserves/needs **more scrutiny** from the community, so

Join the **rank metric** side
(we have small keys, and lots more...)

References

[Ale03] M. Alekhnovich, *More on Average Case vs Approximation Complexity*, FOCS 2003

[BMTS13] P. SLM Barreto, R. Misoczki, J.-P. Tillich, and N. Sendrier, *MDPC-McEliece: New McEliece variants from moderate density parity-check codes*, ISIT 2013

[GMRZ13] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor, *Low rank parity check codes and their application to cryptography*, WCC 2013

[GJS16] : Q. Guo, T. Johansson, and P. Stankovski. *A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors*, AsiaCrypt 2016

[ME78] R. J McEliece, *A public-key cryptosystem based on algebraic coding theory*, Deep Space Network Progress Report, 1978

[This work] Soon on ePrint...

Thank You !