Code-Based Cryptography

McEliece Cryptosystem

I. Márquez-Corbella

Code-Based Cryptography

1. Error-Correcting Codes and Cryptography
2. **McEliece Cryptosystem**
3. Message Attacks (ISD)
4. Key Attacks
5. Other Cryptographic Constructions Relying on Coding Theory

2. McEliece Cryptosystem

1. **Formal Definition**
2. Security-Reduction Proof
3. McEliece Assumptions
4. Notions of Security
5. Critical Attacks - Semantic Secure Conversions
6. Reducing the Key Size
7. Reducing the Key Size - LDPC codes
8. Reducing the Key Size - MDPC codes
9. Implementation

Formal definition of Public-Key Cryptography

$\mathcal{P}$ = Plaintext Space

$\mathcal{C}$ = Ciphertext Space

$\mathcal{K}_p$ = Public-Key Space

$\mathcal{K}_s$ = Secret-Key Space

Formal definition of Public-Key Cryptography

$\mathcal{P}$ = Plaintext Space

$\mathcal{C}$ = Ciphertext Space

$\mathcal{K}_\mathrm{p}$ = Public-Key Space

$\mathcal{K}_\mathrm{s}$ = Secret-Key Space

1. **Key generation algorithm:** KeyGen

$\mathfrak{K} \in \mathbb{N}$

Security parameter $\longrightarrow$ KeyGen $\longrightarrow$ $k_p \in \mathcal{K}_p$, $k_s \in \mathcal{K}_s$

➜ Run in expected polynomial time $\sim \mathcal{O}(\mathfrak{K}^c)$

Formal definition of Public-Key Cryptography

$\mathcal{P}$ = Plaintext Space

$\mathcal{C}$ = Ciphertext Space

$\mathcal{K}_{\mathrm{p}}$ = Public-Key Space

$\mathcal{K}_{\mathrm{s}}$ = Secret-Key Space

Formal definition of Public-Key Cryptography

$\mathcal{P}$ = Plaintext Space

$\mathcal{C}$ = Ciphertext Space

$\mathcal{K}_{\mathrm{p}}$ = Public-Key Space

$\mathcal{K}_{\mathrm{s}}$ = Secret-Key Space

2. **Encryption algorithm:** ENCRYPT

$$\begin{tikzcd}
\boxed{\mathbf{m} \in \mathcal{P}} \arrow[r] & \boxed{\textsc{Encrypt}} \arrow[r] & \boxed{\textsc{Encrypt}(\mathbf{m}, K_p) = \mathbf{y} \in \mathcal{C}} \\
& \boxed{K_p \in \mathcal{K}_p} \arrow[u] &
\end{tikzcd}$$

➜ Run in expected polynomial time $\sim \mathcal{O}(\mathfrak{K}^c)$

Formal definition of Public-Key Cryptography

$\mathcal{P}$ = Plaintext Space

$\mathcal{C}$ = Ciphertext Space

$\mathcal{K}_p$ = Public-Key Space

$\mathcal{K}_s$ = Secret-Key Space

Formal definition of Public-Key Cryptography

$\mathcal{P}$ = Plaintext Space

$\mathcal{C}$ = Ciphertext Space

$\mathcal{K}_p$ = Public-Key Space

$\mathcal{K}_s$ = Secret-Key Space

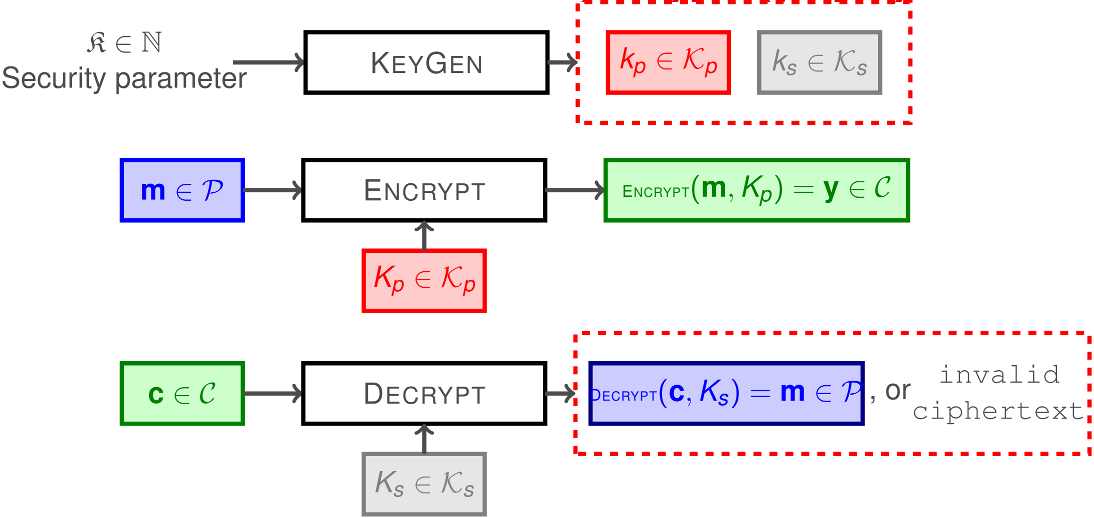
3. **Decryption algorithm:** DECRYPT

$\mathbf{c} \in \mathcal{C}$ → DECRYPT → $\text{DECRYPT}(\mathbf{c}, K_s) = \mathbf{m} \in \mathcal{P}$, or `invalid ciphertext`

$K_s \in \mathcal{K}_s$ → DECRYPT

→ Run in polynomial time

Formal definition of Public-Key Cryptography



- ➜ **It is required that:** $\text{Decrypt}\left(\text{Encrypt}(\mathbf{m}, K_p), K_s\right) = \mathbf{m}$
- ➜ Fasten known attack should requires $\geq 2^{\mathfrak{K}}$ bit operations

The McEliece Cryptosystem

McEliece introduced the first PKC based on Error-Correcting Codes in 1978.

R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.

The McEliece Cryptosystem

Security of the McEliece scheme is based on:

1. Hardness of decoding random linear codes
2. Distinguishing Goppa codes

McEliece introduced the first PKC based on Error-Correcting Codes in 1978.

R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.

The McEliece Cryptosystem

Advantages:

1. **Fast** ENCRYPT and DECRYPT.
2. **Post-quantum cryptosystem.**

Security of the McEliece scheme is based on:

1. Hardness of decoding random linear codes
2. Distinguishing Goppa codes

McEliece introduced the first PKC based on Error-Correcting Codes in 1978.

R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.

The McEliece Cryptosystem

Advantages:

1. **Fast** ENCRYPT and DECRYPT.
2. **Post-quantum cryptosystem.**

Drawback:

➢ Large key size.

Security of the McEliece scheme is based on:

1. Hardness of decoding random linear codes
2. Distinguishing Goppa codes

McEliece introduced the first PKC based on Error-Correcting Codes in 1978.

R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.

The McEliece Cryptosystem

Consider $\left(\mathcal{F}\right)$ family of codes

The McEliece Cryptosystem

Consider $\left(\mathcal{F}\right)$ family of codes

with an **efficient**
decoding algorithm

The McEliece Cryptosystem

Consider $\left(\mathcal{F} \right)$ family of codes

with an **efficient** decoding algorithm

Indistinguishable from random codes

The McEliece Cryptosystem

Consider $\left(\mathcal{F}\right)$ family of codes

with an **efficient** decoding algorithm

Indistinguishable from random codes

Key Generation Algorithm:

1. $G \in \mathbb{F}_q^{k \times n}$ a **generator matrix** for $\mathcal{C} \in \mathcal{F}$
2. $\mathcal{A}_\mathcal{C}$ an **“Efficient” decoding algorithm** for $\mathcal{C}$ which corrects up to t **errors**.

Public Key: $\mathcal{K}_{\mathrm{pub}} = (G, t)$
Private Key: $\mathcal{K}_{\mathrm{secret}} = (\mathcal{A}_\mathcal{C})$

The McEliece Cryptosystem

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ as

$$\textsc{Encrypt}(\mathbf{m}) = \mathbf{m}G + \mathbf{e} = \mathbf{y}$$

where $\mathbf{e}$ is a random error vector of weight at most t.

The McEliece Cryptosystem

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ as

$$\textsc{Encrypt}(\mathbf{m}) = \mathbf{m}G + \mathbf{e} = \mathbf{y}$$

where $\mathbf{e}$ is a random error vector of weight at most t.

Decryption Algorithm:

Using $\mathcal{K}_{secret}$, the receiver obtain $\mathbf{m}$.

$$\textsc{Decrypt}(\mathbf{y}) = \mathcal{A}_{\mathcal{C}}(\mathbf{y}) = \mathbf{m}$$

The McEliece Cryptosystem

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ as

$$\textsc{Encrypt}(\mathbf{m}) = \mathbf{m}G + \mathbf{e} = \mathbf{y}$$

where $\mathbf{e}$ is a random error vector of weight at most t.

Decryption Algorithm:

Using $\mathcal{K}_{secret}$, the receiver obtain $\mathbf{m}$.

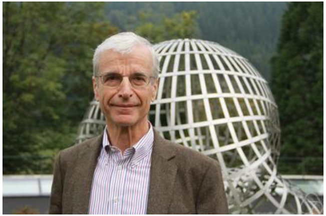
$$\textsc{Decrypt}(\mathbf{y}) = \mathcal{A}_{\mathcal{C}}(\mathbf{y}) = \mathbf{m}$$

Parameters	Key size	Security level
$[1024, 524, 101]_2$	67 ko	2^{62}
$[2048, 1608, 48]_2$	412 ko	2^{96}

The Niederreiter Cryptosystem

Niederreiter presents a dual version of McEliece (which is equivalent in terms of security) in 1986.

H. Niederreiter. (1986).
Knapsack-type crypto system and algebraic coding theory.
Problems of Control and Information Theory.

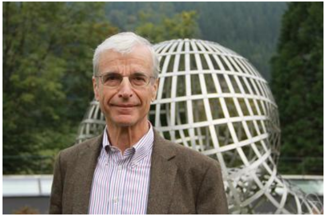


The Niederreiter Cryptosystem

Differences with the McEliece cryptosystem:

1. The public key is a parity check matrix. This improvement reduce the key size.
2. The secret key is an **efficient syndrome decoder**
3. The encryption mechanism

Niederreiter presents a dual version of McEliece (which is equivalent in terms of security) in 1986.



H. Niederreiter. (1986).
Knapsack-type crypto system and algebraic coding theory.
Problems of Control and Information Theory.

The Niederreiter Cryptosystem

Consider $\left(\mathcal{F}\right)$ family of codes

The Niederreiter Cryptosystem

Consider $\left(\mathcal{F}\right)$ family of codes

with an **efficient**
Syndrome decoding
algorithm

The Niederreiter Cryptosystem

Consider $\left(\mathcal{F}\right)$ family of codes

with an **efficient** Syndrome decoding algorithm

Indistinguishable from random codes

The Niederreiter Cryptosystem

Consider $\left(\mathcal{F}\right)$ family of codes

with an **efficient** Syndrome decoding algorithm

Indistinguishable from random codes

<u>**Key Generation Algorithm:**</u>

1. $H \in \mathbb{F}_q^{(n-k)\times n}$ a **parity check matrix** for $\mathcal{C} \in \mathcal{F}$
2. $\mathcal{D}_{\mathcal{C}}$ an **"Efficient" Syndrome Dec.** for $\mathcal{C}$ which corrects up to t **errors**.

Public Key: $\mathcal{K}_{\text{pub}} = (G, t)$
Private Key: $\mathcal{K}_{\text{secret}} = (\mathcal{D}_{\mathcal{C}})$

The McEliece Cryptosystem

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ of weight $\leq t$

$$\textsc{Encrypt}(\mathbf{m}) = \mathbf{m}H^T \in \mathbb{F}_2^{n-k}$$

The McEliece Cryptosystem

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ of weight $\leq t$

$$\textsc{Encrypt}(\mathbf{m}) = \mathbf{m}H^T \in \mathbb{F}_2^{n-k}$$

Decryption Algorithm:

Using $\mathcal{K}_{secret}$, the receiver obtain $\mathbf{m}$.

$$\textsc{Decrypt}(\mathbf{y}) = \mathcal{D}_{\mathcal{C}}(\mathbf{y}) = \mathbf{m}$$

The McEliece Cryptosystem

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ of weight $\leq t$

$$\textsc{Encrypt}(\mathbf{m}) = \mathbf{m}H^T \in \mathbb{F}_2^{n-k}$$

Decryption Algorithm:

Using $\mathcal{K}_{secret}$, the receiver obtain $\mathbf{m}$.

$$\textsc{Decrypt}(\mathbf{y}) = \mathcal{D}_{\mathcal{C}}(\mathbf{y}) = \mathbf{m}$$

Parameters	Key size	Security level
$[256, 128, 129]_{256}$	67 ko	2^{95}

Cryptanalysis - McEliece scheme

We have mainly 2 ways of cryptanalyzing the McEliece system:

Cryptanalysis - McEliece scheme

We have mainly 2 ways of cryptanalyzing the McEliece system:

1. **Message Attacks**
    - Address the problem of **decoding a random linear code**
    - More efficient **Message-Attacks** ➜ Larger codes

Cryptanalysis - McEliece scheme

We have mainly 2 ways of cryptanalyzing the McEliece system:

1. **Message Attacks**
   - Address the problem of **decoding a random linear code**
   - More efficient **Message-Attacks ➜** Larger codes

2. **Key Attacks**
   - Try to **retrieve the code structure**
   - Efficiently applied to: GRS codes, subcodes of GRS codes, Reed-Muller codes, AG codes, Concatenated codes, ...

2. McEliece Cryptosystem

1. Formal Definition
2. **Security-Reduction Proof**
3. McEliece Assumptions
4. Notions of Security
5. Critical Attacks - Semantic Secure Conversions
6. Reducing the Key Size
7. Reducing the Key Size - LDPC codes
8. Reducing the Key Size - MDPC codes
9. Implementation