Code-Based Cryptography

McEliece Cryptosystem

I. Márquez-Corbella

2. McEliece Cryptosystem

Security-Reduction Proof

Problem Reduction: To prove that a cryptosystem Π is secure:

1. Select a problem $\mathcal{P}$ which is known to be hard to solve.
2. Reduce the problem $\mathcal{P}$ to the security of Π.

Since $\mathcal{P}$ is hard to solve, the cryptosystem Π is hard to break.

Security-Reduction Proof

Security Reduction $\Longrightarrow$ An **adversary** able to attack the scheme is able to solve some **hard** computational problems with a similar effort.

Problem Reduction: To prove that a cryptosystem Π is secure:

1. Select a problem $\mathcal{P}$ which is known to be hard to solve.
2. Reduce the problem $\mathcal{P}$ to the security of Π.

Since $\mathcal{P}$ is hard to solve, the cryptosystem Π is hard to break.

A Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

For given parameters n, k

Let $\mathcal{G} \subset \mathcal{K} \subset \{0,1\}^{k \times n}$

A Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

For given parameters n, k

Let $\mathcal{G} \subset \mathcal{K} \subset \{0,1\}^{k \times n}$

Public-Key Space

A Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

For given parameters n, k

Let $\underbrace{\mathcal{G}}_{\text{Public-Key Space}} \subset \underbrace{\mathcal{K}}_{\text{“apparent” Public-Key Space}} \subset \{0,1\}^{k \times n}$

A Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

For given parameters n, k

Binary matrices
of size $k \times n$

Let $\mathcal{G} \subset \mathcal{K} \subset \{0,1\}^{k \times n}$

Public-Key
Space

"apparent" Public-Key
Space

A Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

For given parameters n, k

In McEliece:
$\mathcal{K}_{\text{Goppa}}$

Binary matrices
of size $k \times n$

Let $\mathcal{G} \subset \mathcal{K} \subset \{0,1\}^{k\times n}$

Public-Key Space

"apparent" Public-Key Space

A Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

For given parameters n, k

In McEliece:

$\mathcal{K}_{\text{Goppa}}$

$\{0,1\}^{k \times n}$

Binary matrices of size $k \times n$

Let $\mathcal{G} \subset \boxed{\mathcal{K}} \subset \{0,1\}^{k \times n}$

Public-Key Space

"apparent" Public-Key Space

A Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

For given parameters n, k

In McEliece:

$\mathcal{K}_{\text{Goppa}}$

$\{0,1\}^{k \times n}$

Binary matrices
of size $k \times n$

Let $\mathcal{G} \subset \mathcal{K} \subset \{0,1\}^{k \times n}$

Public-Key
Space

"apparent" Public-Key
Space

A **distinguisher** $\mathcal{D}$ is a mapping $\mathcal{D} : \{0,1\}^{k \times n} \longrightarrow \{\texttt{True}, \texttt{false}\}$

A Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

For given parameters n, k

In McEliece:

$\mathcal{K}_{\text{Goppa}}$

$\{0,1\}^{k \times n}$

Binary matrices
of size $k \times n$

Let $\mathcal{G} \subset \mathcal{K} \subset \{0,1\}^{k \times n} \longrightarrow$ **Sample Space (Ω)**

Public-Key
Space

"apparent" Public-Key
Space

A **distinguisher** $\mathcal{D}$ is a mapping $\mathcal{D} : \{0,1\}^{k \times n} \longrightarrow \{\texttt{True}, \texttt{false}\}$

A Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

For given parameters n, k

In McEliece:

$\mathcal{K}_{\text{Goppa}}$

$\{0,1\}^{k\times n}$

Binary matrices of size $k \times n$

Let $\mathcal{G} \subset \mathcal{K} \subset \{0,1\}^{k\times n}$ $\longrightarrow$ **Sample Space (Ω)**

Public-Key Space

"apparent" Public-Key Space

A **distinguisher** $\mathcal{D}$ is a mapping $\quad \mathcal{D} : \{0,1\}^{k\times n} \longrightarrow \{\texttt{True}, \texttt{false}\}$

We define the event **"distinguishable"**

$$T_{\mathcal{D}} = \{G \in \Omega \mid \mathcal{D}(G) = \texttt{true}\}$$

A Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

The **Advantage** of $\mathcal{D}$ for $\mathcal{G} \subset \mathcal{K}$ is:

$$\mathrm{Adv}(\mathcal{D}) = \left| \Pr_{\Omega}(\mathcal{T}_{\mathcal{D}}) - \Pr_{\Omega}(\mathcal{T}_{\mathcal{D}} \mid \mathcal{G}) \right|$$

A Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

The **Advantage** of $\mathcal{D}$ for $\mathcal{G} \subset \mathcal{K}$ is:

$$\mathrm{Adv}(\mathcal{D}) = \left| \Pr_{\Omega}(\mathcal{T}_{\mathcal{D}}) - \Pr_{\Omega}(\mathcal{T}_{\mathcal{D}} \mid \mathcal{G}) \right|$$

(T, ε)-Distinguisher (for $\mathcal{G}$ against $\mathcal{K}$)

A program $\mathcal{D}$ is a (T, ε)-distinguisher for $\mathcal{G} \subset \mathcal{K}$ if:

1. **Running time:** $|\mathcal{D}| \leq T$
2. **Advantage:** $\mathrm{Adv}\left(\mathcal{D}\right) \geq \varepsilon$

A Decoder (for $\mathcal{K}$)

For given parameters n, k, t

We define the following sample space

$$\Omega = \{0,1\}^k \times \{0,1\}^{k \times n} \times \mathrm{W}_{n,t}$$

A Decoder (for $\mathcal{K}$)

For given parameters n, k, t

We define the following sample space

$$\Omega = \underbrace{\{0,1\}^k}_{\text{Message Space}} \times \{0,1\}^{k \times n} \times \mathrm{W}_{n,t}$$

A Decoder (for $\mathcal{K}$)

For given parameters n, k, t

We define the following sample space

$$\Omega = \underbrace{\{0,1\}^k}_{\text{Message Space}} \times \underbrace{\{0,1\}^{k \times n}}_{\text{“apparent” Public-Key Space}} \times \mathrm{W}_{n,t}$$

A Decoder (for $\mathcal{K}$)

For given parameters n, k, t

We define the following sample space

Error-vector Space

$\{\mathbf{e} \in \mathbb{F}_2^n \mid \mathrm{w}_H(\mathbf{e}) \leq t\}$

$$\Omega = \underbrace{\{0,1\}^k}_{\text{Message Space}} \times \underbrace{\{0,1\}^{k \times n}}_{\text{“apparent” Public-Key Space}} \times \boxed{\mathrm{W}_{n,t}}$$

A Decoder (for $\mathcal{K}$)

For given parameters n, k, t

We define the following sample space

$$\Omega = \underbrace{\{0,1\}^k}_{\text{Message Space}} \times \underbrace{\{0,1\}^{k\times n}}_{\text{“apparent” Public-Key Space}} \times \overbrace{\mathrm{W}_{n,t}}^{\substack{\text{Error-vector Space} \\ \{\mathbf{e}\in\mathbb{F}_2^n \mid \mathrm{w}_H(\mathbf{e})\le t\}}}$$

A **decoder** $\mathcal{A}$ is a mapping $\mathcal{A}: \{0,1\}^n \times \{0,1\}^{k\times n} \longrightarrow \mathrm{W}_{n,t}$

A Decoder (for $\mathcal{K}$)

For given parameters n, k, t

We define the following sample space

$$\Omega = \underbrace{\{0,1\}^k}_{\text{Message Space}} \times \underbrace{\{0,1\}^{k\times n}}_{\text{“apparent” Public-Key Space}} \times \overbrace{\mathrm{W}_{n,t}}^{\substack{\text{Error-vector Space} \\ \{\mathbf{e}\in\mathbb{F}_2^n \mid \mathrm{w}_H(\mathbf{e})\le t\}}}$$

A **decoder** $\mathcal{A}$ is a mapping $\mathcal{A}: \{0,1\}^n \times \{0,1\}^{k\times n} \longrightarrow \mathrm{W}_{n,t}$

We define the event **“successful decoding”**

$$\mathcal{S}_{\mathcal{A}} = \{(\mathbf{x}, G, \mathbf{e}) \in \Omega \mid \mathcal{A}(\mathbf{x}G + \mathbf{e}, G) = \mathbf{e}\}$$

A Decoder (for $\mathcal{K}$)

The **success probability** of $\mathcal{A}$ for $\mathcal{K}$ is:

$$\mathrm{Succ}\left(\mathcal{A}\right) = \Pr_{\Omega}(\mathcal{S}_{\mathcal{A}})$$

A Decoder (for $\mathcal{K}$)

The **success probability** of $\mathcal{A}$ for $\mathcal{K}$ is:

$$\mathrm{Succ}\left(\mathcal{A}\right) = \Pr_{\Omega}(\mathcal{S}_{\mathcal{A}})$$

Generic (T, ε)-decoder

A program $\mathcal{A}$ is a (T, ε)-decoder for $\mathcal{K}$ if:

1. **Running time:** $|\mathcal{A}| \leq T$
2. **Success Probability:** $\mathrm{Succ}\left(\mathcal{A}\right) \geq \varepsilon$

An Adversary (against the McEliece scheme)

For given parameters n, k, t

We keep the same sample space

$$\Omega = \{0,1\}^n \times \{0,1\}^{k \times n} \times \mathrm{W}_{n,t}$$

An Adversary (against the McEliece scheme)

For given parameters n, k, t

We keep the same sample space

$$\Omega = \underbrace{\{0,1\}^n}_{\text{Ciphertext Space}} \times \{0,1\}^{k \times n} \times \mathrm{W}_{n,t}$$

An Adversary (against the McEliece scheme)

For given parameters n, k, t

We keep the same sample space

$$\Omega = \underbrace{\{0,1\}^n}_{\text{Ciphertext Space}} \times \underbrace{\{0,1\}^{k \times n}}_{\text{“apparent” Public-Key Space}} \times W_{n,t}$$

An Adversary (against the McEliece scheme)

For given parameters n, k, t

We keep the same sample space

$$\Omega = \underbrace{\{0,1\}^n}_{\text{Ciphertext Space}} \times \underbrace{\{0,1\}^{k\times n}}_{\text{“apparent” Public-Key Space}} \times \overbrace{\boxed{W_{n,t}}}^{\text{Error-vector Space}}$$

An Adversary (against the McEliece scheme)

For given parameters n, k, t

We keep the same sample space

Error-vector Space

$$\Omega = \{0,1\}^n \times \{0,1\}^{k\times n} \times W_{n,t}$$

Ciphertext Space

"apparent" Public-Key Space

A **adversay (against McEliece)** measures the efficiency of a decoder when the generator matrix is a valid public-key.

An Adversary (against the McEliece scheme)

We define the event **"successful adversary"**

$$\mathcal{S}_{\mathcal{A}} \mid \mathcal{K}_{\text{Goppa}} = \left\{ \mathcal{A}(\mathbf{x}G + \mathbf{e}, G) = \mathbf{e} \mid G \in \mathcal{K}_{\text{Goppa}} \right\}$$

An Adversary (against the McEliece scheme)

We define the event **"successful adversary"**

$$\mathcal{S}_{\mathcal{A}} \mid \mathcal{K}_{\text{Goppa}} = \left\{ \mathcal{A}(\mathbf{x}G + \mathbf{e}, G) = \mathbf{e} \mid G \in \mathcal{K}_{\text{Goppa}} \right\}$$

The **success probability** of $\mathcal{A}$ against McEliece scheme is:

$$\text{Succ}\left(\mathcal{A} \mid \mathcal{K}_{\text{Goppa}} \right) = \Pr_{\Omega}(\mathcal{S}_{\mathcal{A}} \mid \mathcal{K}_{\text{Goppa}})$$

An Adversary (against the McEliece scheme)

We define the event **"successful adversary"**

$$\mathcal{S}_{\mathcal{A}} \mid \mathcal{K}_{\mathrm{Goppa}} = \{\mathcal{A}(\mathbf{x}G + \mathbf{e}, G) = \mathbf{e} \mid G \in \mathcal{K}_{\mathrm{Goppa}}\}$$

The **success probability** of $\mathcal{A}$ against McEliece scheme is:

$$\mathrm{Succ}\left(\mathcal{A} \mid \mathcal{K}_{\mathrm{Goppa}}\right) = \Pr_{\Omega}(\mathcal{S}_{\mathcal{A}} \mid \mathcal{K}_{\mathrm{Goppa}})$$

(T, ε)-adversary against McEliece

A program $\mathcal{A}$ is a (T, ε)-adversary (against a PK scheme) if:

1. **Running time:** $|\mathcal{A}| \leq T$
2. **Success Probability:** $\mathrm{Succ}\left(\mathcal{A} \mid \mathcal{K}_{\mathrm{Goppa}}\right) \geq \varepsilon$

An Adversary (against the McEliece scheme)

Proposition [Sendrier (2009)]

Let $\mathcal{G} \subset \mathcal{K}$. If there exists a (T, ε)-**adversary** against McEliece, then there exists either:

- ➜ A $(T, \frac{\varepsilon}{2})$-**decoder** (for $\mathcal{K}$)
- ➜ Or a $(T + \mathcal{O}\left(n^2\right), \frac{\varepsilon}{2})$-**distinguisher** (for $\mathcal{G}$ against $\mathcal{K}$)

Proof:

An Adversary (against the McEliece scheme)

Proposition [Sendrier (2009)]

Let $\mathcal{G} \subset \mathcal{K}$. If there exists a (T, ε)-**adversary** against McEliece, then there exists either:

- A $(T, \frac{\varepsilon}{2})$-**decoder** (for $\mathcal{K}$)
- Or a $\left(T + \mathcal{O}\left(n^2\right), \frac{\varepsilon}{2}\right)$-**distinguisher** (for $\mathcal{G}$ against $\mathcal{K}$)

Proof:

Let $\mathcal{A}: \{0,1\}^n \times \{0,1\}^{k \times n} \longrightarrow \mathrm{W}_{n,t}$ be a (T, ε)-adversary against McEliece.

An Adversary (against the McEliece scheme)

Proposition [Sendrier (2009)]

Let $\mathcal{G} \subset \mathcal{K}$. If there exists a (T, ε)-**adversary** against McEliece, then there exists either:

- A $(T, \frac{\varepsilon}{2})$-**decoder** (for $\mathcal{K}$)
- Or a $\left(T + \mathcal{O}\left(n^2\right), \frac{\varepsilon}{2}\right)$-**distinguisher** (for $\mathcal{G}$ against $\mathcal{K}$)

Proof:

Let $\mathcal{A} : \{0,1\}^n \times \{0,1\}^{k \times n} \longrightarrow W_{n,t}$ be a (T, ε)-adversary against McEliece. We define the following distinguisher:

$$\begin{array}{rccl} \mathcal{D} : & \{0,1\}^{k \times n} & \longrightarrow & \{\texttt{True}, \texttt{False}\} \\ & G & \longmapsto & \begin{array}{l} \text{If } \mathcal{A}(\mathbf{x}G + \mathbf{e}, G) = \mathbf{e} \text{ return } \texttt{True} \\ \text{else return } \texttt{False} \end{array} \end{array}$$

An Adversary (against the McEliece scheme)

Proposition [Sendrier (2009)]

Let $\mathcal{G} \subset \mathcal{K}$. If there exists a (T, ε)-**adversary** against McEliece, then there exists either:

- A $(T, \frac{\varepsilon}{2})$-**decoder** (for $\mathcal{K}$)
- Or a $(T + \mathcal{O}\left(n^2\right), \frac{\varepsilon}{2})$-**distinguisher** (for $\mathcal{G}$ against $\mathcal{K}$)

Proof:

Let $\mathcal{A} : \{0,1\}^n \times \{0,1\}^{k \times n} \longrightarrow \mathrm{W}_{n,t}$ be a (T, ε)-adversary against McEliece.
We define the following distinguisher:

$$\begin{array}{rcl} \mathcal{D} : \{0,1\}^{k\times n} & \longrightarrow & \{\texttt{True}, \texttt{False}\} \\ G & \longmapsto & \begin{array}{l} \text{If } \mathcal{A}(\mathbf{x}G + \mathbf{e}, G) = \mathbf{e} \text{ return } \texttt{True} \\ \text{else return } \texttt{False} \end{array} \end{array}$$

Then, $\mathrm{Adv}(\mathcal{D}, \mathcal{K}_{\mathrm{Goppa}}) = |\mathrm{Succ}(\mathcal{A} \mid \mathcal{K}_{Goppa}) - \mathrm{Succ}(\mathcal{A})| \ldots$

2. McEliece Cryptosystem