

Code-Based Cryptography

McEliece Cryptosystem

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

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



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})

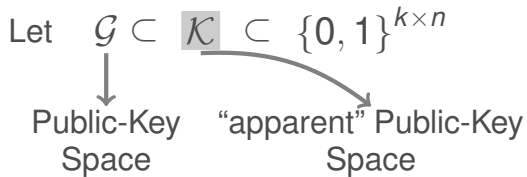
For given parameters n, k

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

↓
Public-Key
Space

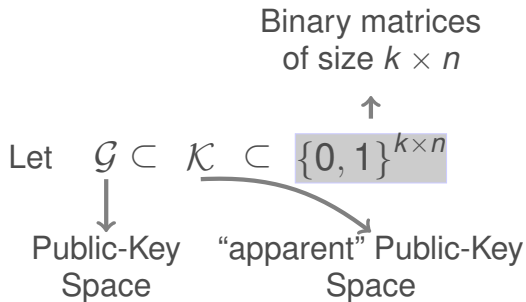
A Distinguisher (for \mathcal{G} against \mathcal{K})

For given parameters n, k



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

For given parameters n, k



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 “apparent” Public-Key
Space 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 (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

$$\mathcal{D} : \{0, 1\}^{k \times n} \longrightarrow \{\text{True}, \text{false}\}$$

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

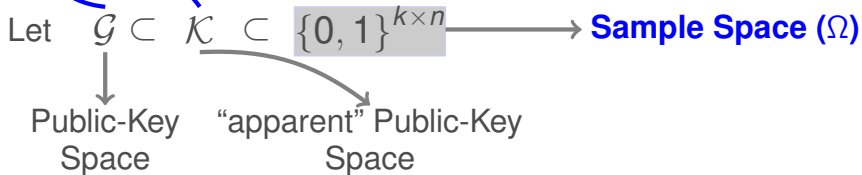
For given parameters n, k

In McEliece:

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

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

Binary matrices
of size $k \times n$



A **distinguisher** \mathcal{D} is a mapping

$$\mathcal{D} : \{0, 1\}^{k \times n} \longrightarrow \{\text{True}, \text{false}\}$$

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

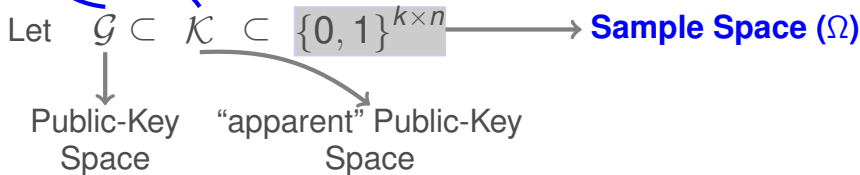
For given parameters n, k

In McEliece:

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

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

Binary matrices
of size $k \times n$



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

We define the event "**distinguishable**"

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

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

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

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

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

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

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

(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:** $\text{Adv}(\mathcal{D}) \geq \varepsilon$

A Decoder (for \mathcal{K})

For given parameters n, k, t

We define the following sample space

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

A Decoder (for \mathcal{K})

For given parameters n, k, t

We define the following sample space

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

\downarrow
Message
Space

A Decoder (for \mathcal{K})

For given parameters n, k, t

We define the following sample space

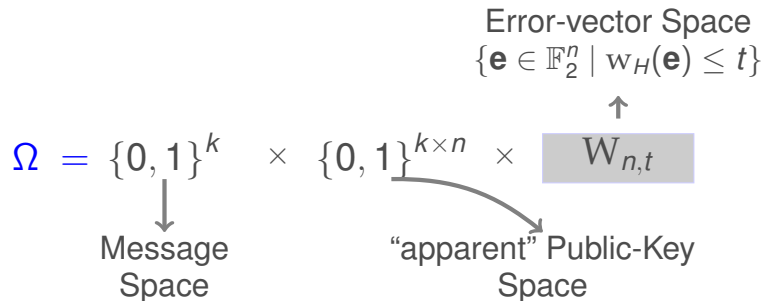
$$\Omega = \{0, 1\}^k \times \{0, 1\}^{k \times n} \times W_{n,t}$$

Message Space “apparent” Public-Key Space

A Decoder (for \mathcal{K})

For given parameters n, k, t

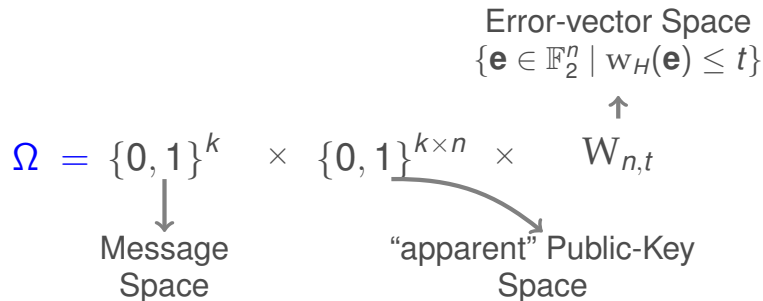
We define the following sample space



A Decoder (for \mathcal{K})

For given parameters n, k, t

We define the following sample space



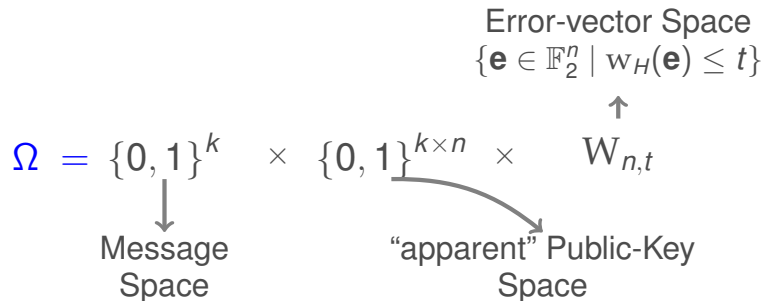
A **decoder** \mathcal{A} is a mapping

$$\mathcal{A}: \{0, 1\}^n \times \{0, 1\}^{k \times n} \longrightarrow W_{n,t}$$

A Decoder (for \mathcal{K})

For given parameters n, k, t

We define the following sample space



A **decoder** \mathcal{A} is a mapping

$$\mathcal{A}: \{0, 1\}^n \times \{0, 1\}^{k \times n} \longrightarrow W_{n,t}$$

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:

$$\text{Succ}(\mathcal{A}) = \Pr_{\Omega}(\mathcal{S}_{\mathcal{A}})$$

A Decoder (for \mathcal{K})

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

$$\text{Succ}(\mathcal{A}) = \Pr_{\Omega}(\mathcal{S}_{\mathcal{A}})$$

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:** $\text{Succ}(\mathcal{A}) \geq \varepsilon$

An Adversary (against the McEliece scheme)

For given parameters n, k, t

We keep the same sample space


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

An Adversary (against the McEliece scheme)

For given parameters n, k, t

We keep the same sample space

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

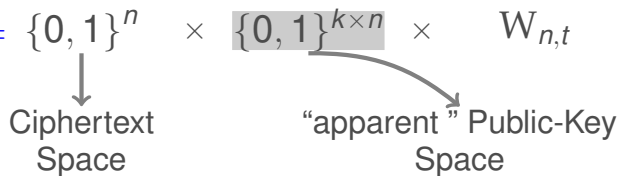

Ciphertext
Space

An Adversary (against the McEliece scheme)

For given parameters n, k, t

We keep the same sample space

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

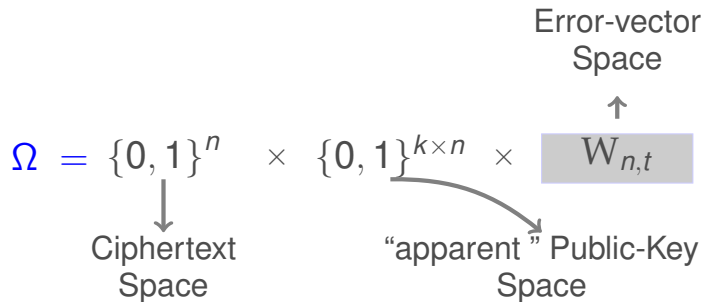


Ciphertext Space “apparent” Public-Key Space

An Adversary (against the McEliece scheme)

For given parameters n, k, t

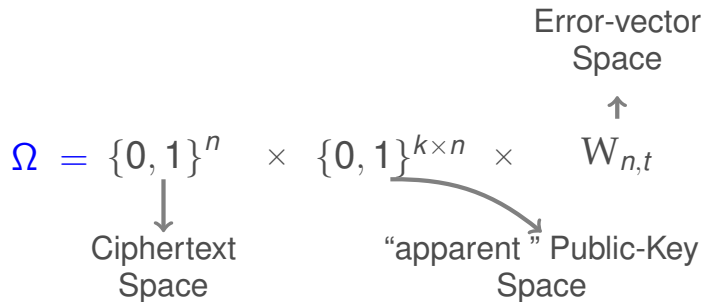
We keep the same sample space



An Adversary (against the McEliece scheme)

For given parameters n, k, t

We keep the same sample space



A **adversary (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**”

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

An Adversary (against the McEliece scheme)

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

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

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**”

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

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

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

(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:** $\text{Succ} \left(\mathcal{A} \mid \mathcal{K}_{\text{Goppa}} \right) \geq \varepsilon$

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 $(T + \mathcal{O}(n^2), \frac{\varepsilon}{2})$ -**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 $(T + \mathcal{O}(n^2), \frac{\varepsilon}{2})$ -**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.

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 $(T + \mathcal{O}(n^2), \frac{\varepsilon}{2})$ -**distinguisher** (for \mathcal{G} against \mathcal{K})

Proof:

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

We define the following distinguisher:

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

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 $(T + \mathcal{O}(n^2), \frac{\varepsilon}{2})$ -**distinguisher** (for \mathcal{G} against \mathcal{K})

Proof:

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

We define the following distinguisher:

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

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

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