# A Distinguisher-Based Attack of a Homomorphic Encryption Scheme Relying on Reed-Solomon Codes

Valérie Gauthier[1], Ayoub Otmani[1] and Jean-Pierre Tillich[2]

GREYC - Université de Caen - Ensicaen

SECRET Project - INRIA Rocquencourt

Code-based Cryptography Workshop, May 2012

# Homomorphic encryption schemes

- Proposed by Rivest, Adleman and Dertouzos in 1978.

# Homomorphic encryption schemes

- Proposed by Rivest, Adleman and Dertouzos in 1978.
- Gentry proposed the first homomorphic scheme based in lattices in 2009.

# Homomorphic encryption schemes

- Proposed by Rivest, Adleman and Dertouzos in 1978.
- Gentry proposed the first homomorphic scheme based in lattices in 2009.
- Challenge: find Homomorphic schemes based in coding therory.

# Homomorphic encryption schemes

- Proposed by Rivest, Adleman and Dertouzos in 1978.
- Gentry proposed the first homomorphic scheme based in lattices in 2009.
- Challenge: find Homomorphic schemes based in coding therory.
- Two proposals
  - *On Constructing homomorphic Encryption Schemes from Coding Theory.* IMACC 2011. Armkent, Augot, Perret and Sadeghi.
  - *Homomorphic encryption from codes* (Accepted to STOC 2012) Bogdanov and Lee.

# Distingushing problem

- Introduced in 2001 by Courtois, Finiasz, and Sendrier to formalize a security proof of the McEliece cryptosystem.

# Distingushing problem

- Introduced in 2001 by Courtois, Finiasz, and Sendrier to formalize a security proof of the McEliece cryptosystem.
- *A Distinguisher for High Rate McEliece Cryptosystems* (ITW 2011). Faugère, Gauthier, Otmani, Perret and Tillich

# Distingushing problem

- Introduced in 2001 by Courtois, Finiasz, and Sendrier to formalize a security proof of the McEliece cryptosystem.
- *A Distinguisher for High Rate McEliece Cryptosystems* (ITW 2011). Faugère, Gauthier, Otmani, Perret and Tillich
- *Error-correcting pairs for a public-key cryptosystem.* Preprint 2012. Márquez-Corbella and Pellikaan.

# Distingushing problem

- Introduced in 2001 by Courtois, Finiasz, and Sendrier to formalize a security proof of the McEliece cryptosystem.
- *A Distinguisher for High Rate McEliece Cryptosystems* (ITW 2011). Faugère, Gauthier, Otmani, Perret and Tillich
- *Error-correcting pairs for a public-key cryptosystem.* Preprint 2012. Márquez-Corbella and Pellikaan.
- Two independent attacks
  - *Cryptanalysis of the Bogdanov-Lee Cryptosystem* by Gottfried Herold
  - *When Homomorphism Becomes a Liability* by Zvika Brakerski. (Cryptology ePrint Archive: Report 2012/225)

# Outline

# Outline

# Key generation

- A subset $L$ of $\{1, \ldots, n\}$ of cardinality $3\ell$.
- Generate at random $n$ distinct $x_i \in \mathbb{F}_q$.

$$\mathbf{G}_i^T \stackrel{\text{def}}{=} \begin{cases} (x_i, x_i^2, \ldots, x_i^\ell, 0, \ldots, 0) & \text{if } i \in L \\ (x_i, x_i^2, \ldots, x_i^\ell, x_i^{\ell+1}, \ldots, x_i^k) & \text{if } i \notin L \end{cases}$$

- Secret key: $L$, $\mathbf{G}$.
- Public key: $\mathbf{P} \stackrel{\text{def}}{=} \mathbf{SG}$ where $\mathbf{S}$ is a random invertible over $\mathbb{F}_q$.

# Key generation - Example

- A subset $L$ of $\{1, \ldots, n\}$ of cardinality $3\ell$.
- Generate at random $n$ distinct $x_i \in \mathbb{F}_q$.

$$\mathbf{G} = \begin{pmatrix} x_1 & \ldots & x_{3\ell} & x_{3\ell+1} & \ldots & x_n \\ \vdots & & \vdots & & \vdots & \\ x_1^\ell & \ldots & x_{3\ell}^\ell & x_{3\ell+1}^\ell & \ldots & x_n^\ell \\ 0 & \ldots & 0 & x_{3\ell+1}^{\ell+1} & \ldots & x_n^{\ell+1} \\ \vdots & & \vdots & & \vdots & \\ 0 & \ldots & 0 & x_{3\ell+1}^k & \ldots & x_n^k \end{pmatrix}$$

- Secret key: $L$, $\mathbf{G}$.
- Public key: $\mathbf{P} \stackrel{\text{def}}{=} \mathbf{SG}$ where $\mathbf{S}$ is a random invertible over $\mathbb{F}_q$.

# Encryption

$$m \in \mathbb{F}_q \longrightarrow \mathbf{c} \in \mathbb{F}_q^n$$

1. Pick $\mathbf{z} \in \mathbb{F}_q^k$ uniformly at random.
2. Pick $\mathbf{e} \in \mathbb{F}_q^n$ s.t. $Proba\big(e_i = 0 \ \forall i \in L\big)$ is close to one.
3. Compute

$$\mathbf{c} \stackrel{\text{def}}{=} \mathbf{zP} + m\mathbf{1} + \mathbf{e}$$

where $\mathbf{1} \in \mathbb{F}_q^n$ is the all-ones row vector.

# Decryption

1. Find $\mathbf{y} \stackrel{\text{def}}{=} (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ that solves:

$$\begin{cases} \mathbf{G}\mathbf{y}^T &= 0 \\ \sum_{i \in L} y_i &= 1 \\ y_i &= 0 \text{ for all } i \notin L. \end{cases} \tag{1}$$

2. For any solution $\mathbf{y}$ of (1):

$$m = \mathbf{c}\mathbf{y}^T$$

# Correctness of the Decryption

$$
\begin{aligned}
\mathbf{c}\mathbf{y}^T &= (\mathbf{z}\mathbf{P} + m\mathbf{1} + \mathbf{e})\mathbf{y}^T \\
&= (\mathbf{z}\mathbf{P} + m\mathbf{1})\mathbf{y}^T \quad (\text{since } e_i = 0 \text{ if } i \in L \text{ and } y_i = 0 \text{ if } i \notin L) \\
&= \mathbf{z}\mathbf{S}\mathbf{G}\mathbf{y}^T + m\sum_{i=1}^{n} y_i \\
&= m \quad (\text{since } \mathbf{G}\mathbf{y}^T = 0 \text{ and } \sum_{i=1}^{n} y_i = 1)
\end{aligned}
$$

# Outline

# Preliminary

Find $\mathbf{y} \in \mathbb{F}_q^n$ s.t.

$$\begin{cases} \mathbf{P}\mathbf{y}^T & = & 0 \\ \sum_{i \in L} y_i & = & 1 \\ y_i & = & 0 \text{ for all } i \notin L. \end{cases} \quad (2)$$

Remarks:

- $\mathbf{P}\mathbf{y}^T = 0 \Leftrightarrow \mathbf{S}\mathbf{G}\mathbf{y}^T = 0$ then system (2) $\Leftrightarrow$ system (1).
- For any $\mathbf{y}$ solution of (2): $m = \mathbf{c}\mathbf{y}^T$.

$\Longrightarrow$ $L$ is the only secret key.

# Definitions

- Star product: $\mathbf{a} \star \mathbf{b} \stackrel{\text{def}}{=} (a_1 b_1, \ldots, a_n b_n)$.
- Star product of two codes: $< \mathscr{A} \star \mathscr{B} >$ is the vector space spanned by all products $\mathbf{a} \star \mathbf{b}$ where $\mathbf{a} \in \mathscr{A}$ and $\mathbf{b} \in \mathscr{B}$.
- Square code: $< \mathscr{A}^2 > = < \mathscr{A} \star \mathscr{A} >$
- Restriction of a code $\mathscr{A}$, $I \subset \{1, \ldots, n\}$

$$\mathscr{A}_I \stackrel{\text{def}}{=} \left\{ \mathbf{v} \in \mathbb{F}_q^{|I|} \mid \exists \mathbf{a} \in \mathscr{A}, \mathbf{v} = (a_i)_{i \in I} \right\}.$$

# Main result:

- Proposition:
  - Choose $I \subset \{1, \ldots, n\}$.
  - Denote $J \stackrel{\text{def}}{=} I \cap L$ and $\mathscr{C}$ the code generated by $\mathbf{G}$.

$$\text{if } \begin{cases} |J| \leqslant \ell - 1 \\ |I| - |J| \geqslant 2k \end{cases} \implies \dim(<\mathscr{C}_I^2>) = 2k - 1 + |J|$$

## Recover $L$: $dim(< \mathscr{C}_I^2 >) = 2k - 1 + |J|$

1. Recover $J = L \cap I$: choose $i \in I$, consider $I' \stackrel{\text{def}}{=} I \setminus \{i\}$.
   - If $i \in L$ then $\dim(< \mathscr{C}_{I'}^2 >) = \Big(2k - 1 + |J|\Big) - 1$.
   - If $i \notin L$ then $\dim(< \mathscr{C}_{I'}^2 >) = 2k - 1 + |J|$.

# Recover $L$: $dim(<\mathscr{C}_I^2>) = 2k - 1 + |J|$

1. Recover $J = L \cap I$: choose $i \in I$, consider $I' \stackrel{\text{def}}{=} I \setminus \{i\}$.
   - If $i \in L$ then $\dim(<\mathscr{C}_{I'}^2>) = \left(2k - 1 + |J|\right) - 1$.
   - If $i \notin L$ then $\dim(<\mathscr{C}_{I'}^2>) = 2k - 1 + |J|$.
2. Recover $L \setminus J$: exchange $i \in I \setminus J$ by $i' \in \{1, \dots, n\} \setminus I$.
   - If $i' \in L$ then $\dim(<\mathscr{C}_{I'}^2>) = \left(2k - 1 + |J|\right) + 1$.
   - If $i' \notin L$ then $\dim(<\mathscr{C}_{I'}^2>) = \left(2k - 1 + |J|\right)$.

# Explanation

- Example: If $L = (1, \dots, 3\ell)$

$$\mathbf{G} = \begin{pmatrix} x_1 & \dots & x_{i_1} & \dots & x_{3\ell} & x_{3\ell+1} & \dots & x_{i_{|I|}} & \dots & x_n \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots & & \vdots \\ x_1^\ell & \dots & x_{i_1}^\ell & \dots & x_{3\ell}^\ell & x_{3\ell+1}^\ell & \dots & x_{i_{|I|}}^\ell & \dots & x_n^\ell \\ 0 & \dots & 0 & \dots & 0 & x_{3\ell+1}^{\ell+1} & \dots & x_{i_{|I|}}^{\ell+1} & \dots & x_n^{\ell+1} \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & 0 & x_{3\ell+1}^k & \dots & x_{i_{|I|}}^k & \dots & x_n^k \end{pmatrix}$$

# Explanation

- Example: If $L = (1, \ldots, 3\ell)$

$$\mathbf{G} = \begin{pmatrix} x_1 & \ldots & x_{i_1} & \ldots & x_{3\ell} & x_{3\ell+1} & \ldots & x_{i_{|I|}} & \ldots & x_n \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots & & \vdots \\ x_1^\ell & \ldots & x_{i_1}^\ell & \ldots & x_{3\ell}^\ell & x_{3\ell+1}^\ell & \ldots & x_{i_{|I|}}^\ell & \ldots & x_n^\ell \\ 0 & \ldots & 0 & \ldots & 0 & x_{3\ell+1}^{\ell+1} & \ldots & x_{i_{|I|}}^{\ell+1} & \ldots & x_n^{\ell+1} \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \ldots & 0 & x_{3\ell+1}^k & \ldots & x_{i_{|I|}}^k & \ldots & x_n^k \end{pmatrix}$$

- Define:
  - $I \stackrel{\text{def}}{=} \{i_1, \ldots, i_{|I|}\} \subset \{1, \ldots, n\}$

# Explanation

- Example: If $L = (1, \ldots, 3\ell)$

$$\mathbf{G} = \begin{pmatrix} x_1 & \ldots & x_{i_1} & \ldots & x_{3\ell} & x_{3\ell+1} & \ldots & x_{i_{|I|}} & \ldots & x_n \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots & & \vdots \\ x_1^\ell & \ldots & x_{i_1}^\ell & \ldots & x_{3\ell}^\ell & x_{3\ell+1}^\ell & \ldots & x_{i_{|I|}}^\ell & \ldots & x_n^\ell \\ 0 & \ldots & 0 & \ldots & 0 & x_{3\ell+1}^{\ell+1} & \ldots & x_{i_{|I|}}^{\ell+1} & \ldots & x_n^{\ell+1} \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \ldots & 0 & x_{3\ell+1}^k & \ldots & x_{i_{|I|}}^k & \ldots & x_n^k \end{pmatrix}$$

- Define:
  - $I \stackrel{\text{def}}{=} \{i_1, \ldots, i_{|I|}\} \subset \{1, \ldots, n\}$
  - $J \stackrel{\text{def}}{=} I \cap L.$

# Explanation

$$\mathbf{G}_I = \begin{pmatrix} \overbrace{x_{i_1} & \cdots & x_{3\ell}}^{|J|} & \overbrace{x_{3\ell+1} & \cdots & x_{i_{|I|}}}^{|I|-|J|} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{i_1}^{\ell} & \cdots & x_{3\ell}^{\ell} & x_{3\ell+1}^{\ell} & \cdots & x_{i_{|I|}}^{\ell} \\ 0 & \cdots & 0 & x_{3\ell+1}^{\ell+1} & \cdots & x_{i_{|I|}}^{\ell+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & x_{3\ell+1}^{k} & \cdots & x_{i_{|I|}}^{k} \end{pmatrix}$$

# Explanation

$$
\mathbf{G}_I = \left(\begin{array}{ccc|ccc}
\multicolumn{3}{c}{\overbrace{\hphantom{x_{i_1} \quad \cdots \quad x_{3\ell}}}^{|J|}} & \multicolumn{3}{c}{\overbrace{\hphantom{x_{3\ell+1} \quad \cdots \quad x_{i_{|I|}}}}^{|I|-|J|}} \\
x_{i_1} & \cdots & x_{3\ell} & x_{3\ell+1} & \cdots & x_{i_{|I|}} \\
\vdots & A & \vdots & \vdots & & \vdots \\
x_{i_1}^{\ell} & \cdots & x_{3\ell}^{\ell} & x_{3\ell+1}^{\ell} & \cdots & x_{i_{|I|}}^{\ell} \\
0 & \cdots & 0 & x_{3\ell+1}^{\ell+1} & \cdots & x_{i_{|I|}}^{\ell+1} \\
\vdots & & \vdots & \vdots & & \vdots \\
0 & \cdots & 0 & x_{3\ell+1}^{k} & \cdots & x_{i_{|I|}}^{k}
\end{array}\right)
$$

# Explanation

$$
\mathbf{G}_I = \begin{pmatrix}
\overbrace{\begin{matrix} x_{i_1} & \dots & x_{3\ell} \\ \vdots & \mathbf{A} & \vdots \\ x_{i_1}^{\ell} & \dots & x_{3\ell}^{\ell} \end{matrix}}^{|J|} & \overbrace{\begin{matrix} x_{3\ell+1} & \dots & x_{i_{|I|}} \\ \vdots & \mathbf{B} & \vdots \\ x_{3\ell+1}^{\ell} & \dots & x_{i_{|I|}}^{\ell} \end{matrix}}^{|I|-|J|} \\
\begin{matrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{matrix} & \begin{matrix} x_{3\ell+1}^{\ell+1} & \dots & x_{i_{|I|}}^{\ell+1} \\ \vdots & & \vdots \\ x_{3\ell+1}^{k} & \dots & x_{i_{|I|}}^{k} \end{matrix}
\end{pmatrix}
$$

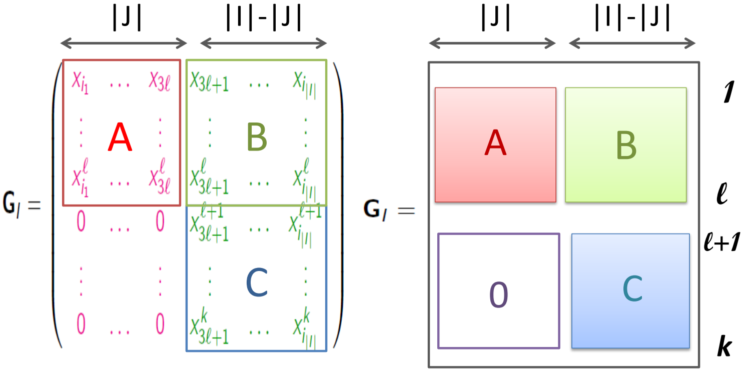
# Explanation

|J|     |I|-|J|

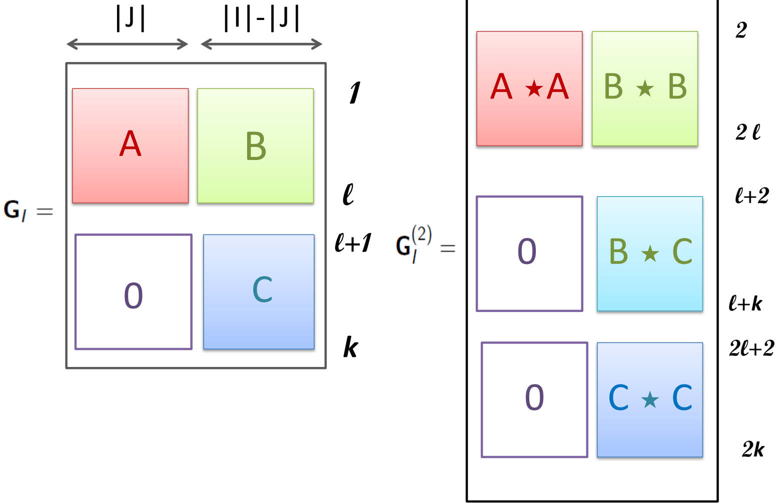
A     B     C

$$\mathbf{G}_I = \begin{pmatrix} x_{i_1} & \cdots & x_{3\ell} & x_{3\ell+1} & \cdots & x_{i_{|I|}} \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{i_1}^{\ell} & \cdots & x_{3\ell}^{\ell} & x_{3\ell+1}^{\ell} & \cdots & x_{i_{|I|}}^{\ell} \\ 0 & \cdots & 0 & x_{3\ell+1}^{\ell+1} & \cdots & x_{i_{|I|}}^{\ell+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & x_{3\ell+1}^{k} & \cdots & x_{i_{|I|}}^{k} \end{pmatrix}$$

# Explanation

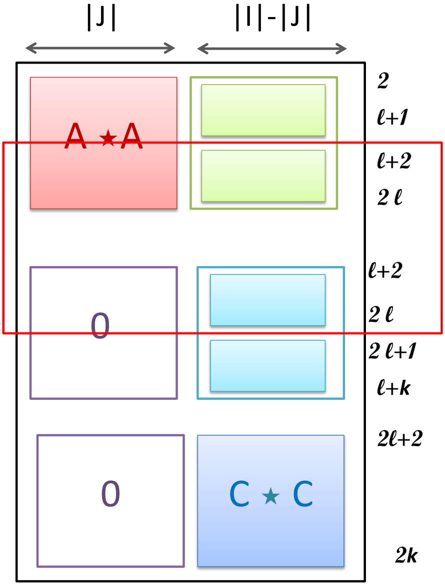


# Explanation

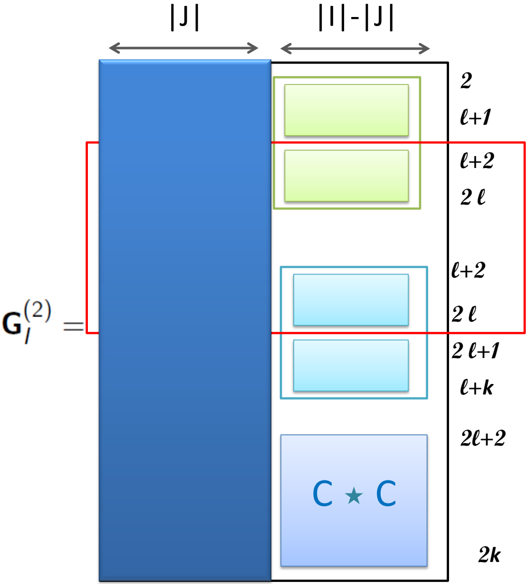


# Explanation

$\mathbf{G}_I^{(2)} =$

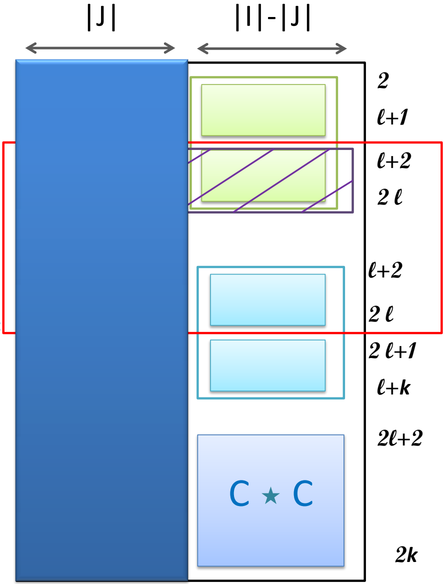


# Explanation: If $|J| = 0$



# Explanation: If $|J| = 0$ then $\dim(< \mathscr{C}_I^2 >) = 2k - 1$

$\mathbf{G}_I^{(2)} =$



# Fact

Consider $t$ independent vectors:

$$\left.\begin{matrix} (v_{1,1} & \cdots & v_{1,|J|} & v_{1,|J|+1} & \cdots & v_{1,n}) \\ \vdots & & \vdots & \vdots & & \vdots \\ (v_{t,1} & \cdots & v_{t,|J|} & v_{t,|J|+1} & \cdots & v_{t,n}) \end{matrix}\right\}$$

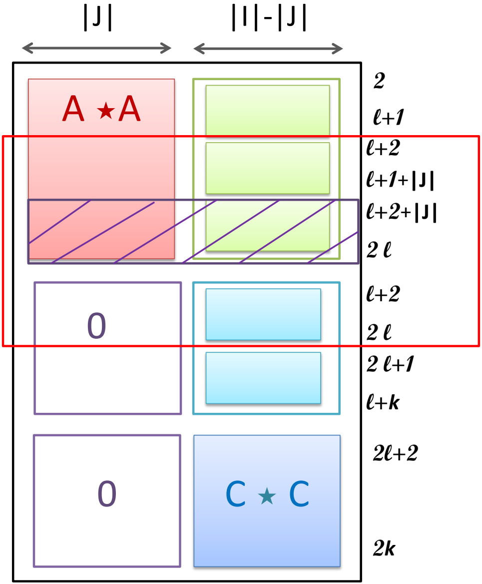
# Fact

Consider $t$ independent vectors $v_1, \ldots, v_t$:

$$\left.\begin{array}{cccccc}
(v_{1,1} & \ldots & v_{1,|J|} & v_{1,|J|+1} & \ldots & v_{1,n}) \\
\vdots & & \vdots & \vdots & & \vdots \\
(v_{t,1} & \ldots & v_{t,|J|} & v_{t,|J|+1} & \ldots & v_{t,n}) \\
(0 & \ldots & 0 & v_{1,|J|+1} & \ldots & v_{1,n}) \\
\vdots & & \vdots & \vdots & & \vdots \\
(0 & \ldots & 0 & v_{|J|,|J|+1} & \ldots & v_{|J|,n})
\end{array}\right\} t + |J| \text{ independent vectors.}$$

# Explanation: If $|J| > 0$ then $\dim(< \mathscr{C}_I^2 >) = 2k - 1 + |J|$

$\mathbf{G}_I^{(2)} =$



# Outline

# Conclusions and futur work

- Similar attack on M. Baldi *et. al.* proposition
  - *Enhanced public key security for the McEliece cryptosystem.* arxiv:1108.2462v2[cs.IT]
  - *A Distinguisher-Based Attack on a Variant of McEliece's Cryptosystem Based on Reed-Solomon Codes.* arXiv:1204.6459v1 [cs.CR]

# Conclusions and futur work

- Similar attack on M. Baldi *et. al.* proposition
  - *Enhanced public key security for the McEliece cryptosystem.* arxiv:1108.2462v2[cs.IT]
  - *A Distinguisher-Based Attack on a Variant of McEliece's Cryptosystem Based on Reed-Solomon Codes.* arXiv:1204.6459v1 [cs.CR]
- Can we derive an attack for McEliece cryptosystem from a distinguisher?

# Conclusions and futur work

- Similar attack on M. Baldi *et. al.* proposition
  - *Enhanced public key security for the McEliece cryptosystem.* arxiv:1108.2462v2[cs.IT]
  - *A Distinguisher-Based Attack on a Variant of McEliece's Cryptosystem Based on Reed-Solomon Codes.* arXiv:1204.6459v1 [cs.CR]
- Can we derive an attack for McEliece cryptosystem from a distinguisher?
- Can we build a homomorphic public key cryptosystem based in codes?

Thank you for your attention

# Thank you for your attention