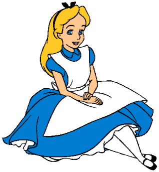
Code-Based, Post-Quantum Cryptography

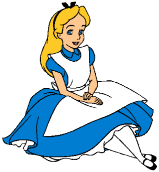
Valérie Gauthier Umaña

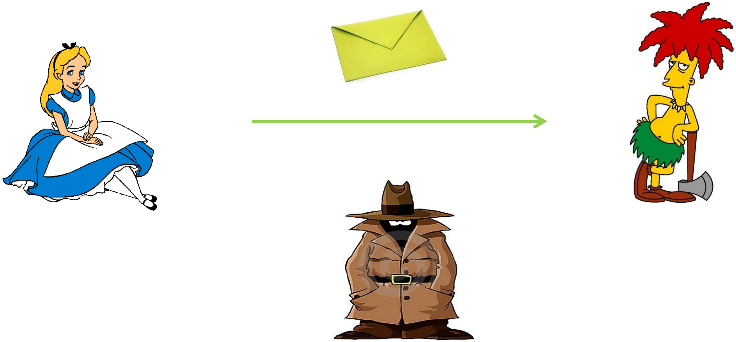
Departamento MACC - Universidad del Rosario

Seminario Quantil

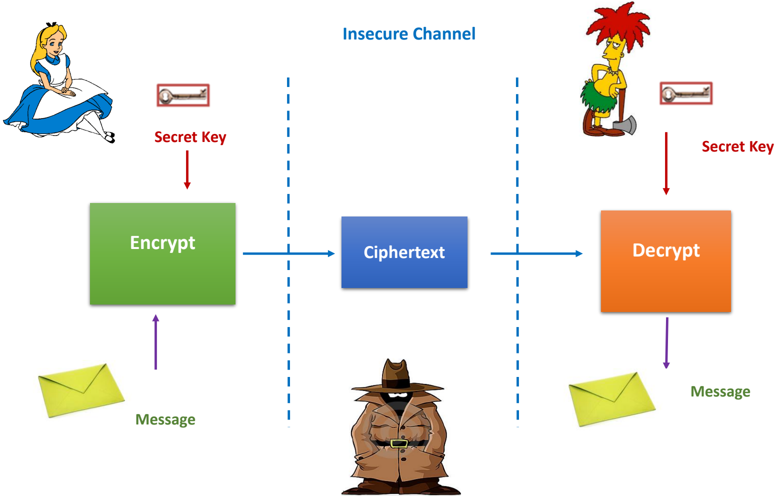
Cryptography: Classic to Post-Quantum







Secret Key Cryptosystem Scheme



Cesar Cryptosystem Scheme

ELHQYHQLGRVDOVHPLQDULR

Cesar Cryptosystem Scheme

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

ELHQYHQLGRVDOVHPLQDULR

Cesar Cryptosystem Scheme

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

↓

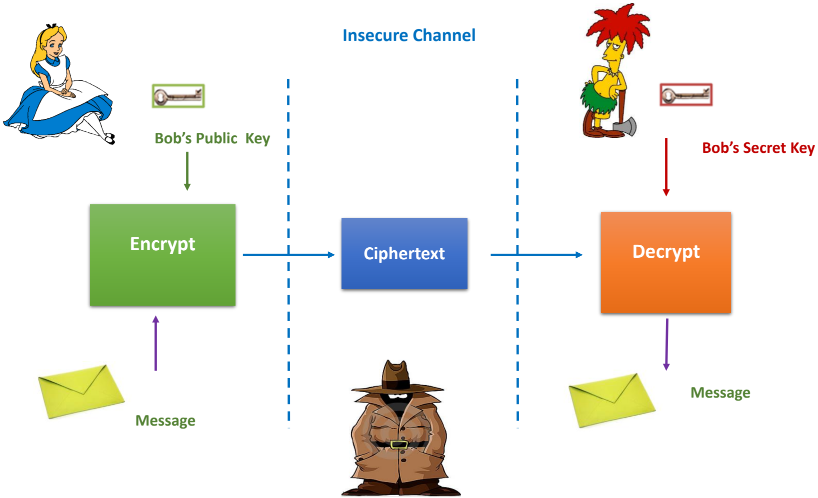
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

BIENVENIDOS AL SEMINARIO

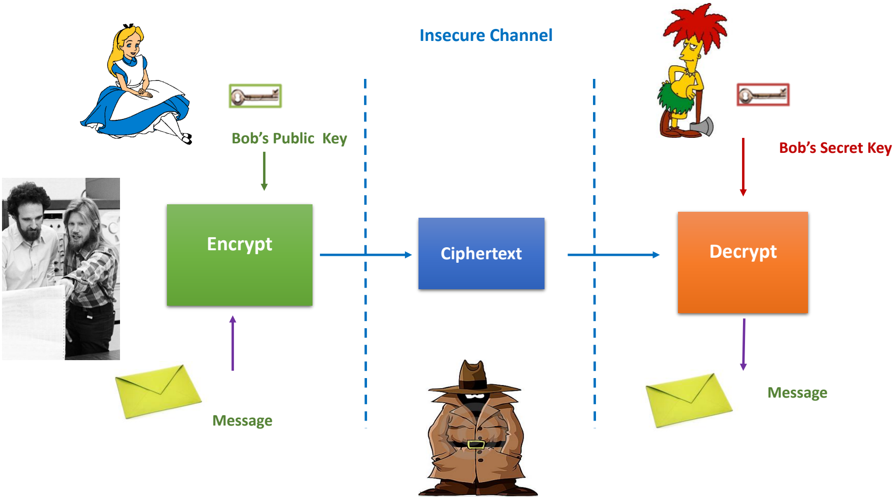
↕

ELHQYHQLGRVDOVHPLQDULR

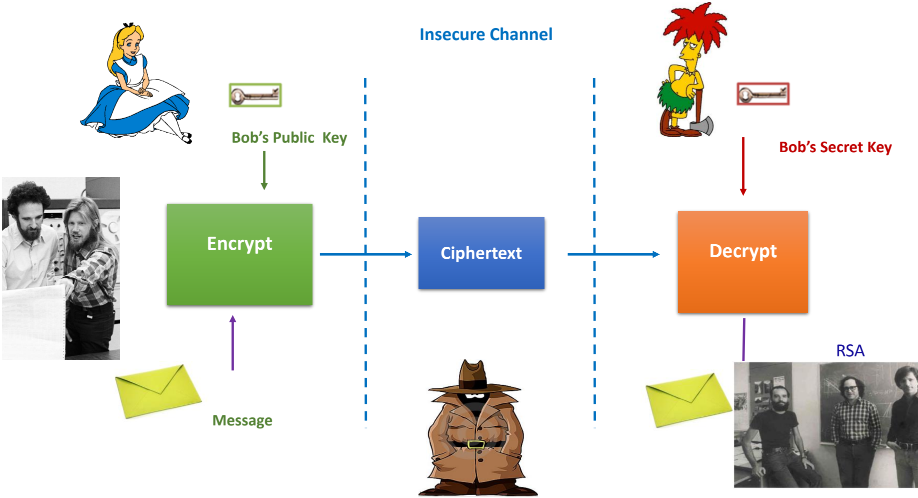
Public-Key Cryptosystem Scheme



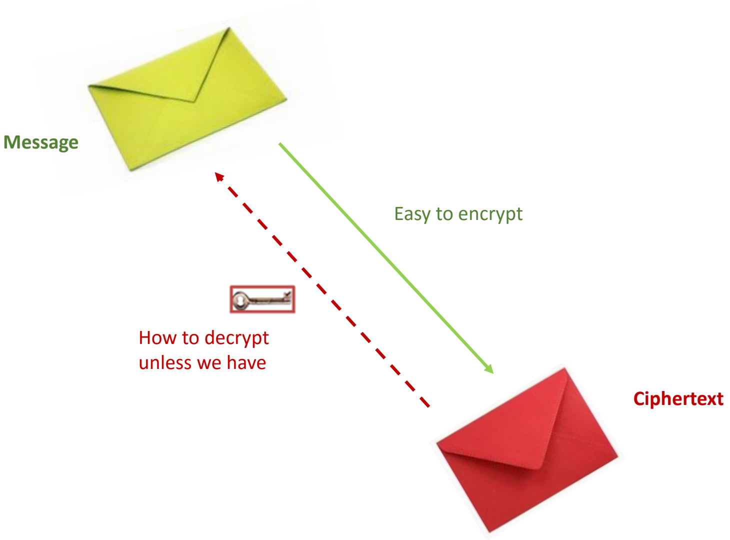
Public-Key Cryptosystem Scheme



Public-Key Cryptosystem Scheme



Trapdoor one-way function



Post-Quantum Cryptography

The sky is falling?

- When will a quantum computer be built?
  - 15 years, $1 billion USD, nuclear power plant (PQCrypto 2014, Matteo Mariantoni)
- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~Elliptic Curve Cryptography (ECDSA)~~
    - ~~Finite Field Cryptography (DSA)~~
    - ~~Diffie-Hellman key exchange~~
  - Symmetric key crypto:
    - AES — Need larger keys
    - Triple DES — Need larger keys
  - Hash functions:
    - SHA-1, SHA-2 and SHA-3 — Use longer output

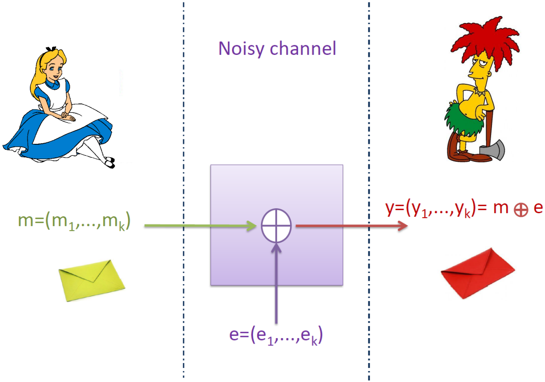
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Call for Proposals

- NIST is calling for quantum-resistant cryptographic algorithms for new public-key crypto standards
  - Digital signatures
  - Encryption/key-establishment
- We see our role as managing a process of achieving community consensus in a **transparent** and timely manner
- We do not expect to "pick a winner"
  - Ideally, several algorithms will emerge as 'good choices'
- We may pick one (or more) for standardization
  - Only algorithms publicly submitted considered

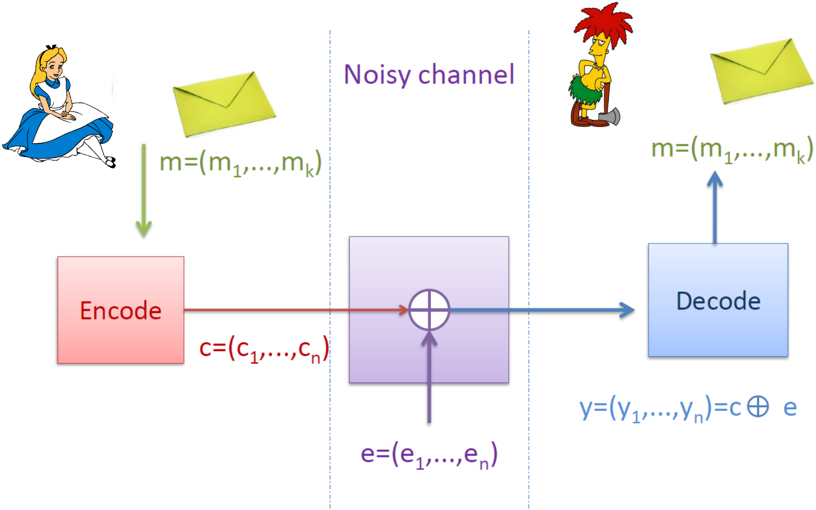
Coding Theory

Error-correcting codes



- Add redundancy to the message ($k < n$).
- Use the structure of the redundance to recover the message.

Encoding and Decoding Scheme



Definition: Let $\mathbb{F}_q$ be a finite field of q elements and $n, k \in \mathbb{N}$ such that $k < n$, the encoding function is

$$\begin{array}{rccc} f: & \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & \boldsymbol{m} & \longmapsto & \boldsymbol{c} \end{array}$$

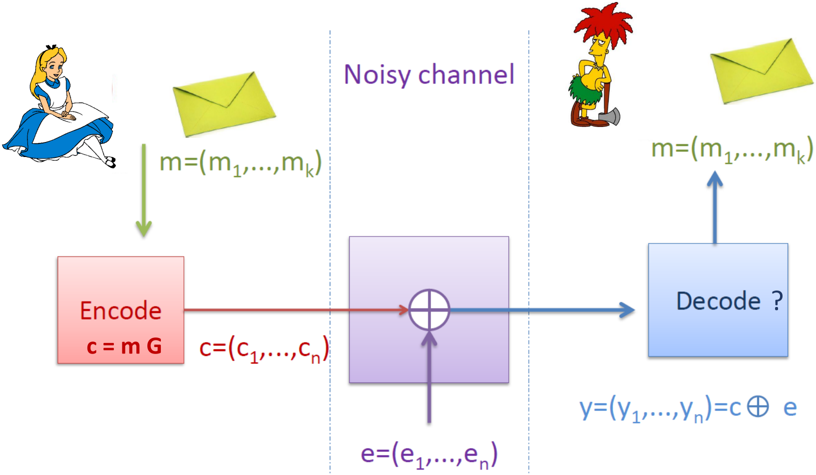
Definition: the code

$$\mathscr{C} \stackrel{\text{def}}{=} \left\{ \boldsymbol{c} \stackrel{\text{def}}{=} f(\boldsymbol{m}) \mid \boldsymbol{m} \in \mathbb{F}_q^k \right\}$$

$\mathscr{C}$ an (n, k)-linear code $\mathscr{C}$ defined over $\mathbb{F}_q$ if f is a linear function.

Remark: A linear *code* $\mathscr{C}$ of *length* n and *dimension* k over $\mathbb{F}_q$ is a subspace of dimension k of the full space $\mathbb{F}_q^n$.

Encoding and Decoding Scheme



Decoding Algorithm

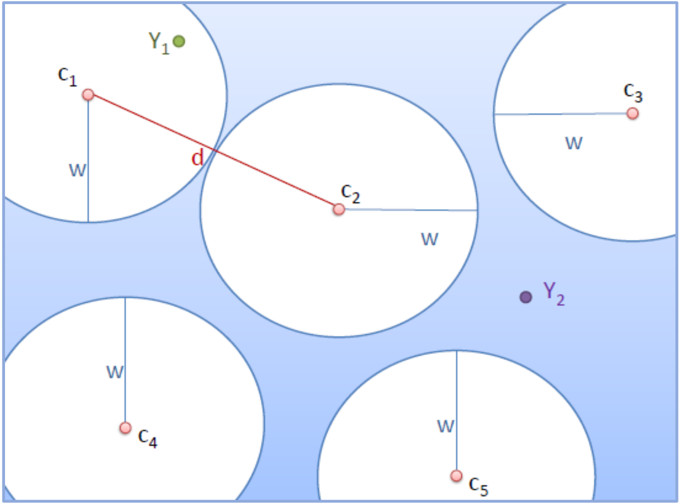
Let $\mathscr{C}$ be an (n, k, d)-linear code defined over $\mathbb{F}_q$ and generator matrix $\boldsymbol{G}$.

Definition: $\gamma_{\boldsymbol{G}}$ is a decoding algorithm for $\mathscr{C}$ that can correct up to w errors iff

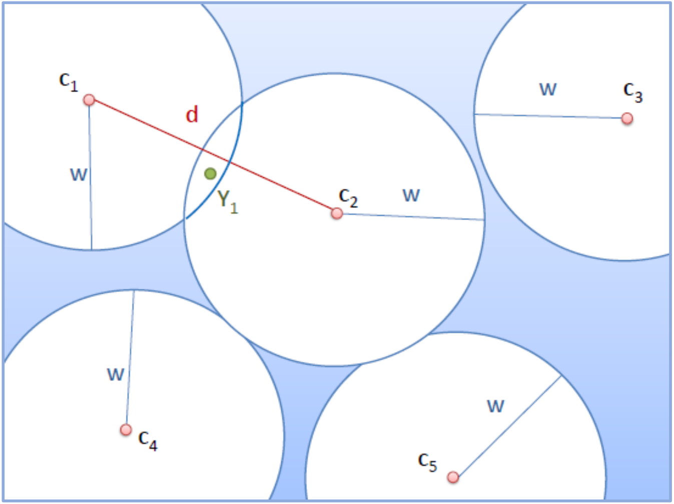
- $\forall \boldsymbol{e} \in \mathbb{F}_q^n$ with $w_H(\boldsymbol{e}) \leqslant w$
- $\forall \boldsymbol{m} \in \mathbb{F}_q^k$

$$\gamma_{\boldsymbol{G}} : \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^k \\ \boldsymbol{mG} \oplus \boldsymbol{e} & \longmapsto & \boldsymbol{m} \end{array}$$

Decoding



Decoding



Facts

1. 1978: Berlekamp, McEliece and van Tilborg showed that the associated decision problem of the *decoding a random linear code problem* is $\mathcal{NP}$-complete.

2. Structural case: there are codes that have efficient decoding algorithms.
   - Reed-Solomon codes.
   - Alternant codes.
   - Goppa codes, etc.

McEliece's Cryptosystem

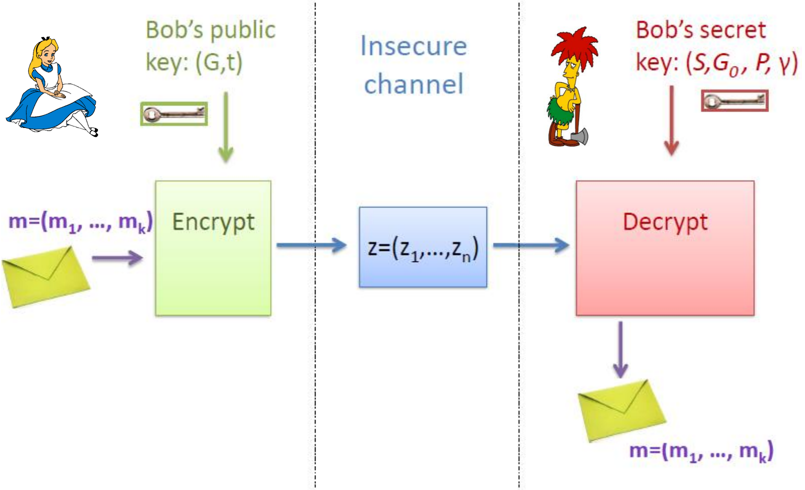
1978, Robert McEliece proposed the first PKC based on error-correcting codes.

Main idea:

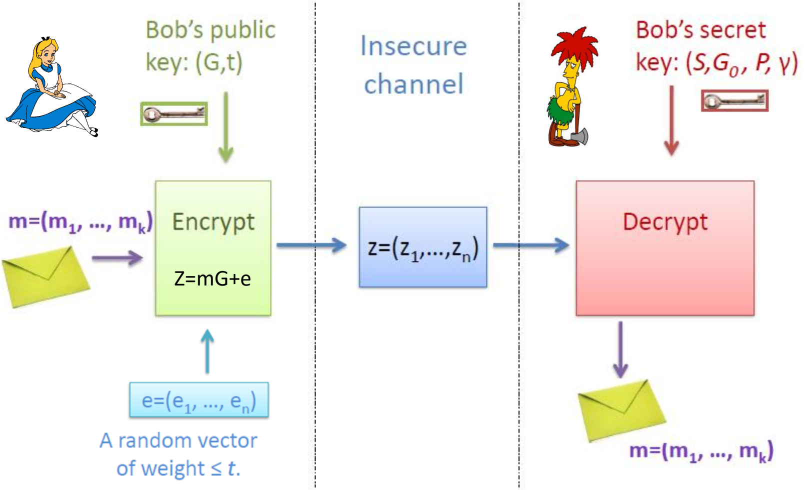
- Choose a code with generator matrix $\boldsymbol{G}_0$ and a polynomial time decoding algorithm γ that can correct up to t errors.
- Find a permutation matrix $\boldsymbol{P}$ and an invertible matrix $\boldsymbol{S}$ to disguise the algebraic structure of the code by computing

$$\boldsymbol{G} = \boldsymbol{S}\boldsymbol{G}_0\boldsymbol{P}.$$

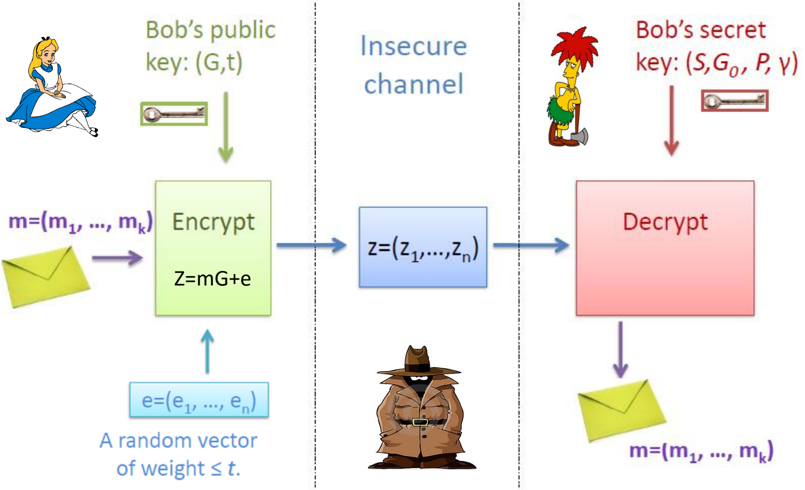
McEliece's PKC, $G = SG_0P$



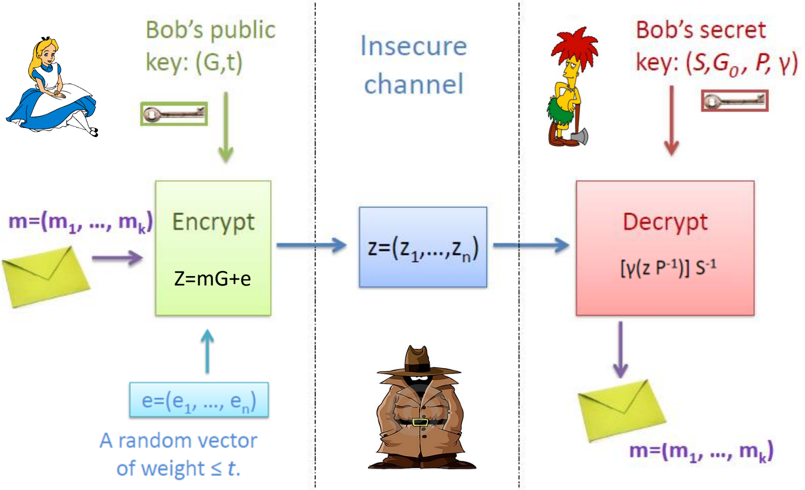
McEliece's PKC, $G = SG_0P$



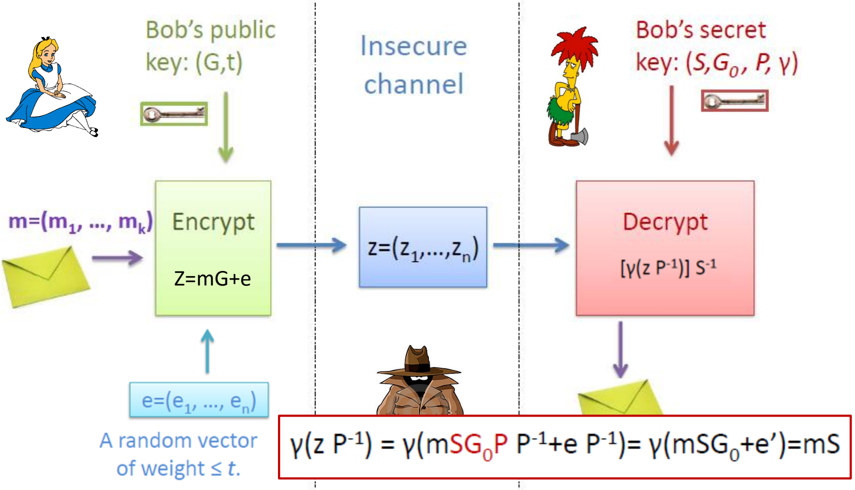
McEliece's PKC, $G = SG_0P$



McEliece's PKC, $G = SG_0P$



McEliece's PKC, $G = SG_0P$



Some Parameters of the McEliece cryptosystem using Goppa codes.

Security level	(n, k)	t	McEliece	RSA
80-bit	$(2048, 1751)$	27	520047	1248
128-bit	$(2960, 2288)$	56	1537536	3248
256-bit	$(6624, 5129)$	115	7667855	15424

- Fast encryption and decryption $\mathcal{O}(n^2 \log(n))$.
- Very big key size $k \times n$ or $(n - k) \times n$.

Attacks on McEliece's cryptosystem

There are mainly two guidelines:

1. Structural attacks: recover the secret key from the public key.
2. Decoding attacks: attack a single ciphertext using a generic decoding algorithm.

Security Proof / Distinguisher

Security proof

IF

$$\textit{Attack McEliece} \Longrightarrow \textit{Solve a problem } P$$

THEN

$$\textit{If } P \textit{ is hard to solve} \Longrightarrow \textit{McEliece is secure.}$$

Idea: use the fact that the associated decision problem of the *decoding a random-linear code problem* is $\mathcal{NP}$-complete.

Goppa Code Distinguishing problem

- Introduced in 2001 by Courtois, Finiasz, and Sendrier.
- Distinguishing problem:

  Is a decision problem that aims at distinguishing a generator matrix of a binary Goppa code from a randomly drawn binary matrix.
- Hypothesis:

  There is NO polynomial time algorithm that solvs the distinguishing problem.

Distinguisher for high-rate Goppa codes

- A Distinguisher for High Rate McEliece Cryptosystems, ITW 2011.
  Faugère, Gauthier, Otmani, Perret and Tillich.

Distinguisher for high-rate Goppa codes

- A Distinguisher for High Rate McEliece Cryptosystems, ITW 2011. Faugère, Gauthier, Otmani, Perret and Tillich.
- The distinguisher problem is solved in the range of parameters used in the CFS signature scheme.

Distinguisher for high-rate Goppa codes

- A Distinguisher for High Rate McEliece Cryptosystems, ITW 2011. Faugère, Gauthier, Otmani, Perret and Tillich.

- The distinguisher problem is solved in the range of parameters used in the CFS signature scheme.

- This is not an attack on the system, but it invalidates the hypothesis of the security proof.

Distinguisher for high-rate Goppa codes

- A Distinguisher for High Rate McEliece Cryptosystems, ITW 2011. Faugère, Gauthier, Otmani, Perret and Tillich.

- The distinguisher problem is solved in the range of parameters used in the CFS signature scheme.

- This is not an attack on the system, but it invalidates the hypothesis of the security proof.

- Error-correcting pairs for a public-key cryptosystem, Preprint 2012. Márquez-Corbella and Pellikaan.

Distinguisher for high-rate Goppa codes

- A Distinguisher for High Rate McEliece Cryptosystems, ITW 2011. Faugère, Gauthier, Otmani, Perret and Tillich.
- The distinguisher problem is solved in the range of parameters used in the CFS signature scheme.
- This is not an attack on the system, but it invalidates the hypothesis of the security proof.
- Error-correcting pairs for a public-key cryptosystem, Preprint 2012. Márquez-Corbella and Pellikaan.
- Does the distinguisher lead to a an attack of the McEliece PKC?

Bogdanov-Lee Cryptosystem

Key generation

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

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

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

Key generation - Example

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

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

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

Encryption

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

1. Pick $\boldsymbol{z} \in \mathbb{F}_q^k$ uniformly at random.

2. Pick $\boldsymbol{e} \in \mathbb{F}_q^n$ s.t. $Proba\left(e_i = 0 \ \forall i \in L\right)$ is close to one.

3. Compute

$$\boldsymbol{c} \stackrel{\text{def}}{=} \boldsymbol{z}\boldsymbol{P} + m\mathbf{1} + \boldsymbol{e}$$

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

Decryption

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

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

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

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

Correctness of the Decryption

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

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

Gauthier, Otmani and Tillich

Preliminary

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

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

Remarks:

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

$\Longrightarrow$ L is the only secret key.

Definitions

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

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

Main result:

Proposition

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

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

Example

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

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

Example

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

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

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

Example

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

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

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

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

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

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 $\dim(<\mathscr{C}_{I'}^2>) = 2k - 1 + |J|$.
2. Recover $L \setminus J$: exchange $i \in I \setminus J$ by $i' \in \{1, \ldots, n\} \setminus I$.
    - If $i' \in L$ then $\dim(<\mathscr{C}_{I'}^2>) = \Big(2k - 1 + |J|\Big) + 1$.
    - If $i' \notin L$ then $\dim(<\mathscr{C}_{I'}^2>) = \Big(2k - 1 + |J|\Big)$.

Similar attacks

1. 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]

Similar attacks

1. 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]
2. On C. Wieschebrink
   Two NP-complete Problems in Coding Theory with an Application in Code Based Cryptography. ISIT 2006
   - Couvreur, Gaborit, Gauthier, Otmani and Tillich
     Distinguisher-Based Attacks on Public-Key Cryptosystems Using Reed-Solomon Codes WCC 2013

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

THANK YOU!

Valérie Gauthier Umaña

Directora
Departamento MACC
Universidad del Rosario
valeriee.gauthier@urosario.edu.co

@MACC_URosario

@MACC_URosario