Code-Based Cryptography

McEliece Cryptosystem

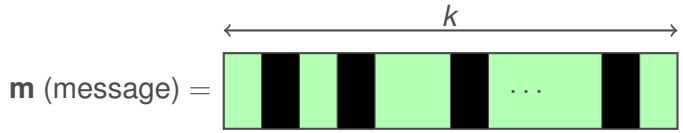
I. Márquez-Corbella

informatiques mathématiques

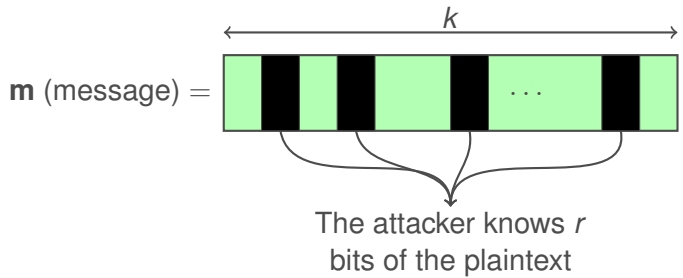
2. McEliece Cryptosystem

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

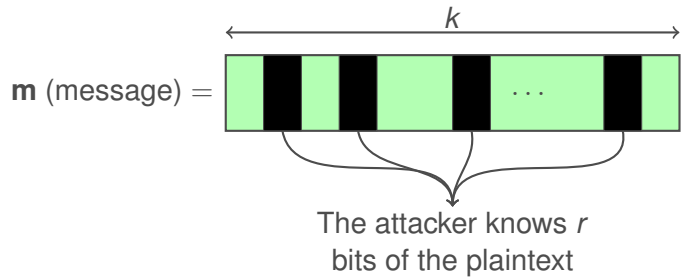
Critical Attacks: Partial knowledge on the plaintext



Critical Attacks: Partial knowledge on the plaintext



Critical Attacks: Partial knowledge on the plaintext



Recovering the rest of $k - r$ **bits** in the McEliece scheme **with parameters** $[n, k]$

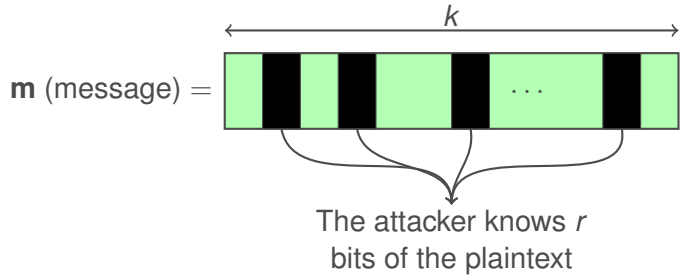
$\equiv$

Recovering a **plaintext** in the McEliece scheme **with parameters** $[n, k - r]$

Critical Attacks: Partial knowledge on the plaintext

$I =$ Known positions

$\{1, \ldots, n\} \setminus I = \overline{I} :=$ Unknown positions



Recovering the rest of $k - r$ **bits** in the McEliece scheme **with parameters** $[n, k]$

$\equiv$

Recovering a **plaintext** in the McEliece scheme **with parameters** $[n, k - r]$

Critical Attacks: Partial knowledge on the plaintext

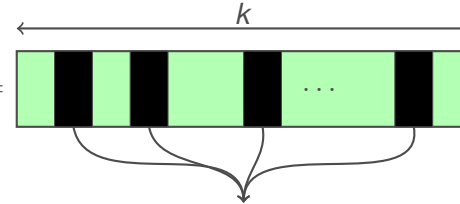
$I =$ Known positions

$\{1, \ldots, n\} \setminus I = \overline{I} :=$ Unknown positions

$$\begin{aligned} \mathbf{y} &= \mathbf{m}G + \mathbf{e} \\ &= m_I G_I + m_{\overline{I}} G_{\overline{I}} + \mathbf{e} \end{aligned}$$

Restriction of the matrix G to the columns indexed by $i \in I$

$\mathbf{m}$ (message) =



The attacker knows r bits of the plaintext

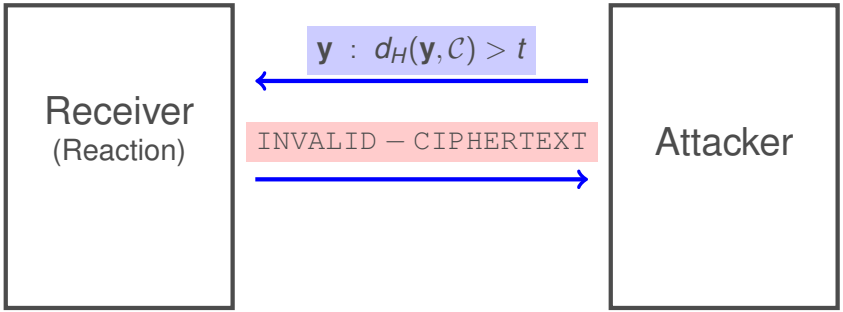
Recovering the rest of $k - r$ **bits** in the McEliece scheme **with parameters** $[n, k]$

$\equiv$

Recovering a **plaintext** in the McEliece scheme **with parameters** $[n, k - r]$

Critical Attacks: Reaction Attack

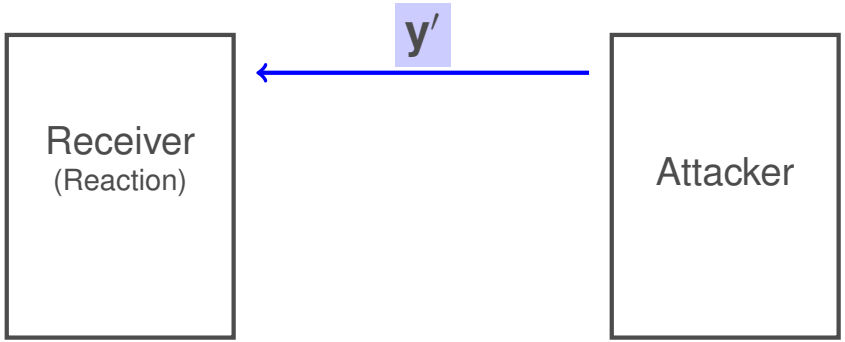
This attack can be classified as CCA but with a weaker assumption



"A decoder of an $[n, k]_q$ code will not attempt to correct a vector which has $t + 1$ or more errors "

Critical Attacks: Reaction Attack

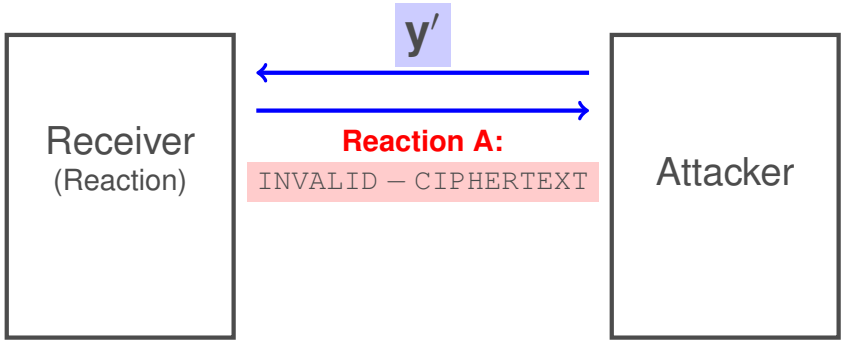
We flip the i-th bit of the ciphertext $\mathbf{y}$: $\mathbf{y} \longrightarrow \mathbf{y}'$



K. Kobara and H. Imai
New Chosen-Plaintext Attacks on the One-Wayness of the Modified McEliece PKC.
Proposed at Asiacrypt 2000.

Critical Attacks: Reaction Attack

We flip the i-th bit of the ciphertext $\mathbf{y}$: $\mathbf{y} \longrightarrow \mathbf{y}'$



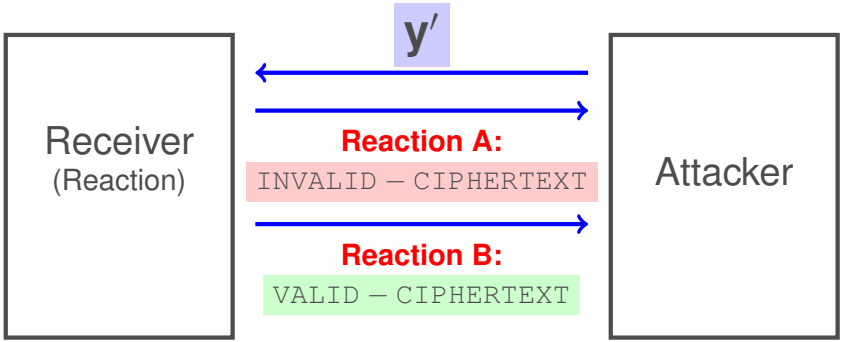
Reaction A: i **is an error-free position,** $d_H(\mathbf{y}', \mathcal{C}) = t + 1$

K. Kobara and H. Imai

New Chosen-Plaintext Attacks on the One-Wayness of the Modified McEliece PKC.
Proposed at Asiacrypt 2000.

Critical Attacks: Reaction Attack

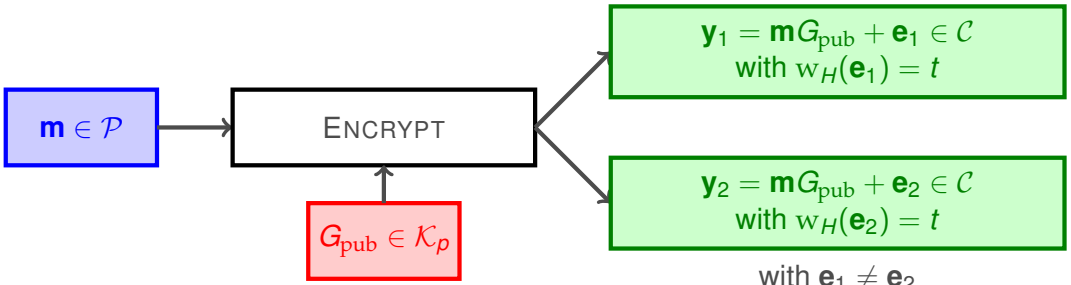
We flip the i-th bit of the ciphertext $\mathbf{y}$: $\mathbf{y} \longrightarrow \mathbf{y}'$



Reaction A: i **is an error-free position,** $d_H(\mathbf{y}', \mathcal{C}) = t + 1$
Reaction B: i **is an error position,** $d_H(\mathbf{y}', \mathcal{C}) = t - 1$

K. Kobara and H. Imai
New Chosen-Plaintext Attacks on the One-Wayness of the Modified McEliece PKC.
Proposed at Asiacrypt 2000.

Critical Attacks: Resend-message Attack



Message-Resend Condition:

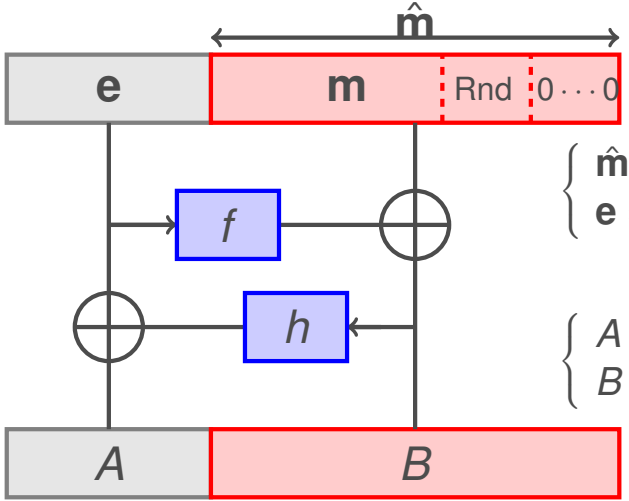
$$\mathrm{w}_H(\mathbf{y}_1 + \mathbf{y}_2) = \mathrm{w}_H(\mathbf{e}_1 + \mathbf{e}_2) = 2(t - \nu)$$

In practice ν is very small

Thomas A. Berson

Failure of the McEliece public-key cryptosystem under message-resend and related-message attack.
Advances in Cryptology - CRYPTO'97, LNCS, volume 1294, 1997, pp. 213-220.

Semantic Secure Conversions (Example)



$$\begin{cases} \hat{\mathbf{m}} = A + h(B) \\ \mathbf{e} = B + f(A + h(B)) \end{cases}$$

$$\Updownarrow$$

$$\begin{cases} A = \mathbf{e} + h(\hat{\mathbf{m}} + f(\mathbf{e})) \\ B = \hat{\mathbf{m}} + f(\mathbf{e}) \end{cases}$$

Under random **oracle assumption** on f and h this conversions provides semantic security (non malleability and indistinguishability)

Semantic Secure Conversion

➜ OAEP Conversion

M. Bellare and P. Rogaway.
Optimal Asymmetric Encryption.
Eurocrypt 1994, pp. 92-111.

Semantic Secure Conversion

- **OAEP Conversion**

M. Bellare and P. Rogaway.
Optimal Asymmetric Encryption.
Eurocrypt 1994, pp. 92-111.

- **Kobara-Imai conversion**

K. Kobara and H. Imai
Semantically secure McEliece public-key cryptosystems-conversions for McEliece PKC.
PKC 2001, 19-35.

Under Kobara-Imai Conversion:

Break **indistinguishability of encryption** of the **specific** conversion of McEliece in an **CC2** scenario

$=$

Break the **original McEliece** without any decryption oracles and any knowledge on the plaintext

Semantic Secure Conversion

- **OAEP Conversion**

M. Bellare and P. Rogaway.
Optimal Asymmetric Encryption.
Eurocrypt 1994, pp. 92-111.

- **Kobara-Imai conversion**

K. Kobara and H. Imai
Semantically secure McEliece public-key cryptosystems-conversions for McEliece PKC.
PKC 2001, 19-35.

Under Kobara-Imai Conversion:

Break **indistinguishability of encryption** of the **specific** conversion of McEliece in an **CC2** scenario

=

Break the **original McEliece** without any decryption oracles and any knowledge on the plaintext

- **An IND-CPA conversion without random oracles also exists**

R. Nojima, H. Imai, K. Kobara and K. Morozov
Semantic Security for the McEliece Cryptosystem without Random Oracles.
International Workshop on Coding and Cryptography WCC 2007, pp.289-305.

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