Practical Key Recovery Attacks On Two Recent McEliece Variants

Valérie Gauthier, Gregor Leander

Danmarks Tekniske Universitet

PQCrypto, May 2010

In 1978 McEliece propose the first public-key cryptosystem based in error-correcting codes, until now no attack is known to represent a serious threat on the system, even on a quantum computer.

- Encryption: $c = m \times G \oplus e$
- Decryption: Decode c.

Main idea: choose a code such that we have a decoding algorithm, and disguise its algebraic structure.

Two promising variants have been proposed recently:

- In AfricaCrypt 2009 Berger, Cayrel, Gaborit and Otmani propose to use quasi-cyclic Alterant codes over a non-binary small field.
- In SAC 2009 Misoczki and Barreto propose to use binary Goppa codes in dyadic form.

However for many of the parameters choices, both schemes can be broken.

1. **Brief presentation of the quasi-cyclic variant**

2. General framework of the attack

3. Apply the framework to the quasi-cyclic variant

- Let $x_i, c_i \in \mathbb{F}_q$ where $q = 2^r$

$$\textbf{(secret key)} \quad H = \underbrace{\left(\begin{array}{ccccc} c_0 & c_1 & c_2 & \cdots & c_8 \\ c_0 x_0 & c_1 x_1 & c_2 x_2 & \cdots & c_8 x_8 \\ c_0 x_0^2 & c_1 x_1^2 & c_2 x_2^2 & \cdots & c_8 x_8^2 \\ c_0 x_0^3 & c_1 x_1^3 & c_2 x_2^3 & \cdots & c_8 x_8^3 \end{array} \right)}_{n=9} \Bigg\} t = 4$$

- Take the subfield subcode.

(public key) $P = SH$, where S is a secret invertible matrix.

The quasi-cyclic variant:

Let $y_j, a_j, \beta \in \mathbb{F}_q$, β has order ℓ ($\ell = 3$ in the example) and $1 \leq s \leq \ell - 1$ ($s = 2$ in the example).

$$H = \left(\begin{array}{ccc|c|c|c} a_0 & \beta^2 a_0 & \beta^4 a_0 & a_1 & \cdots & \cdots & \beta^4 a_2 \\ a_0 y_0 & \beta^2 a_0 \beta y_0 & \beta^4 a_0 \beta^2 y_0 & a_1 y_1 & \cdots & \cdots & \beta^4 a_2 \beta^2 y_2 \\ a_0 y_0^2 & \beta^2 a_0 \beta^2 y_0^2 & \beta^4 a_0 \beta^4 y_0^2 & a_1 y_1^2 & \cdots & \cdots & \beta^4 a_2 \beta^4 y_2^2 \\ a_0 y_0^3 & \beta^2 a_0 \beta^3 y_0^3 & \beta^4 a_0 \beta^6 y_0^3 & a_1 y_1^3 & \cdots & \cdots & \beta^4 a_2 \beta^6 y_2^3 \end{array}\right)$$

$$c_{\ell j+i} := \beta^{is} a_j \qquad \text{and} \qquad x_{\ell j+i} := \beta^i y_j$$

1. Brief presentation of the quasi-cyclic variant

2. **General framework of the attack**

3. Apply the framework to the quasi-cyclic variant

$$P = \mathbf{S} \times \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_8 \\ c_0 x_0 & c_1 x_1 & c_2 x_2 & \cdots & c_8 x_8 \\ c_0 x_0^2 & c_1 x_1^2 & c_2 x_2^2 & \cdots & c_8 x_8^2 \\ c_0 x_0^3 & c_1 x_1^3 & c_2 x_2^3 & \cdots & c_8 x_8^3 \end{pmatrix}$$

- Let (s_0, s_1, s_2, s_3) the first row of S, then:

$$P_{1,1} = s_0 c_0 + s_1 c_0 x_0 + s_2 c_0 x_0^2 + s_3 c_0 x_0^3 = c_0 g_0(x_0)$$

where $g_0(x) = s_0 + s_1 x + s_2 x^2 + s_3 x^3$.

$$P = \begin{pmatrix} c_0 g_0(x_0) & c_1 g_0(x_1) & c_2 g_0(x_2) & \cdots & c_8 g_0(x_8) \\ c_0 g_1(x_0) & c_1 g_1(x_1) & c_2 g_1(x_2) & \cdots & c_8 g_1(x_8) \\ c_0 g_2(x_0) & c_1 g_2(x_1) & c_2 g_2(x_2) & \cdots & c_8 g_2(x_8) \\ c_0 g_3(x_0) & c_1 g_3(x_1) & c_2 g_3(x_2) & \cdots & c_8 g_3(x_8) \end{pmatrix}$$

$$P = \begin{pmatrix} c_0 g_0(x_0) & c_1 g_0(x_1) & c_2 g_0(x_2) & \cdots & c_8 g_0(x_8) \\ c_0 g_1(x_0) & c_1 g_1(x_1) & c_2 g_1(x_2) & \cdots & c_8 g_1(x_8) \\ c_0 g_2(x_0) & c_1 g_2(x_1) & c_2 g_2(x_2) & \cdots & c_8 g_2(x_8) \\ c_0 g_3(x_0) & c_1 g_3(x_1) & c_2 g_3(x_2) & \cdots & c_8 g_3(x_8) \end{pmatrix}$$

- Let $\gamma = (\gamma_0, \gamma_1, \gamma_2, \gamma_3)$, where $\gamma_i \in \mathbb{F}q$ and

$$g_\gamma(x) = \gamma_0 g_0(x) + \gamma_1 g_1(x) + \gamma_2 g_2(x) + \gamma_3 g_3(x)$$

$$\gamma P = (c_0 g_\gamma(x_0), c_1 g_\gamma(x_1), c_2 g_\gamma(x_2), \cdots, c_8 g_\gamma(x_8))$$

- Main idea: control the polynomial g_γ such that γP reveals useful information on the secret values c_i, x_i.

$$\gamma P = (c_0 g_\gamma(x_0), c_1 g_\gamma(x_1), c_2 g_\gamma(x_2), \cdots, c_8 g_\gamma(x_8))$$

- Isolate: Choose a polynomial g_γ such that the redundancy (of c_i and x_i) allows us to efficiently recover the corresponding γ.

$$c_{\ell j+i} := \beta^{is} a_j \qquad \text{and} \qquad x_{\ell j+i} := \beta^i y_j$$

- Collect: Compute γP, find enough equations that will be solved in the next step.

- Solve: Extract the secret values x_i and c_i by solving a system of equations.

1. Brief presentation of the quasi-cyclic variant

2. General framework of the attack

3. **Apply the framework to the quasi-cyclic variant**

$$\gamma P = \left(a_0 g_\gamma(y_0), a_0\beta^2 g_\gamma(\beta y_0), \ldots, \beta^4 a_2 g_\gamma(\beta^2 y_2)\right)$$

Isolate: Consider $g_\gamma(x) = 1 \rightarrow$ compute γ:

$$\gamma P = \left(a_0, a_0\beta^2, a_0\beta^4, a_1, \cdots, a_2\beta^4\right)$$

$$\gamma P = a_0 \underbrace{(1, \beta^2, \beta^4, 0, \cdots, 0)}_{v_0} + a_1 \underbrace{(0, 0, 0, 1, \beta^2, \beta^4, 0, 0, 0)}_{v_1}$$

$$+ a_2 \underbrace{(0, \cdots, 0, 1, \beta^2, \beta^4)}_{v_2}$$

- To find γ we have to compute a basis for the space

$$\Gamma_0 = \{\gamma \mid \gamma P \in \langle v_0, v_1, v_2 \rangle\}$$

- Ideal case: $dim(\Gamma_0) = 1$, then

$$\{g_\gamma \mid \gamma \in \Gamma_0\} = \{\alpha \mid \alpha \in \mathbb{F}_q\}.$$

$$\gamma P = \alpha a_0 v_0 + \alpha a_1 v_1 + \alpha a_2 v_2$$

Given a_0 we will have the others constants.

- But let $g_\gamma(x) = \alpha_0 + \alpha_1 x^\ell$, here $g_\gamma(\beta x) = g_\gamma(x)$

$$\Rightarrow \gamma \in \Gamma_0 \text{ and } dim(\Gamma_0) \geq 2$$

Fact: $dim(\Gamma_0) = 2$

$$\{g_\gamma \mid \gamma \in \Gamma_0\} = \{\alpha_0 + \alpha_1 x^\ell \mid \alpha_0, \alpha_1 \in \mathbb{F}q\}.$$

$$\gamma P = \left(a_0 g_\gamma(y_0), a_0\beta^2 g_\gamma(\beta y_0), \ldots, \beta^4 a_2 g_\gamma(\beta^2 y_2)\right)$$

$$\gamma P = \alpha_0 \underbrace{(a_0, a_0\beta^2, \ldots, a_2\beta^4)}_{1^{st} \text{ row of H}} + \alpha_1 \underbrace{(a_0 y_0^\ell, a_0\beta^2 y_0^\ell, \ldots, a_2\beta^4 y_0^\ell)}_{\ell^{th} \text{ row of H}}$$

Collect:

$$\gamma P = \alpha_0(1^{st} \text{ row of H}) + \alpha_1(\ell^{th} \text{ row of H})$$

Let (γ_A, γ_B) a basis for Γ_0, such that $g_{\gamma_A}(x) = \alpha_{0A} + \alpha_{1A}x^\ell$ and $g_{\gamma_B}(x) = \alpha_{0B} + \alpha_{1B}x^\ell$.

$$\begin{pmatrix} \gamma_A \\ \gamma_B \end{pmatrix} P = \underbrace{\begin{pmatrix} \alpha_{0A} & \alpha_{1A} \\ \alpha_{0B} & \alpha_{1B} \end{pmatrix}}_{M} \times \begin{pmatrix} 1^{st} \text{ row of H} \\ \ell^{th} \text{ row of H} \end{pmatrix}$$

- Compare to the initial problem: $P = SH$, where S is an invertible $t \times t$ matrix.
- We broke the initial problem into (much) smaller subproblems.

$$\begin{pmatrix} \gamma_A \\ \gamma_B \end{pmatrix} P = \underbrace{\begin{pmatrix} \alpha_{0A} & \alpha_{1A} \\ \alpha_{0B} & \alpha_{1B} \end{pmatrix}}_{M} \times \begin{pmatrix} 1^{st} \text{ row of H} \\ \ell^{th} \text{ row of H} \end{pmatrix}$$

We are not really interested in the matrix M, but rather in the values x_i and c_i.

$$\underbrace{M^{-1} \begin{pmatrix} \gamma_A \\ \gamma_B \end{pmatrix} P}_{\text{linear in the components of } M^{-1}} = \begin{pmatrix} 1^{st} \text{ row of H} \\ \ell^{th} \text{ row of H} \end{pmatrix} \begin{matrix} (\text{linear part}) \\ (\text{high order term}) \end{matrix}$$

Solve:

- Find the values of the a_i by
  - guessing some constant values and solving the linear system.
  - using Gröbner basis.

- Doing a similar process with other values for g_γ, find the values of the y_i.

Table: Parameters proposed for the quasi-cyclic variant, running time and the complexity of our attacks.

q	q^m	ℓ	t	b	Assumed security	Complexity ($\log_2$)
2^8	2^{16}	51	100	9	80	74.9
		51	100	10	90	75.1
		51	100	12	100	75.3
		51	100	15	120	75.6
						Av. running time (sec)
2^{10}	2^{20}	75	112	6	80	47
		93	126	6	90	62
		93	108	8	100	75

- Faugère, Otmani, Perret and Tillich, will present an independent and faster attack in Eurocrypt 2010.

Thank you