A Distinguisher for High Rate McEliece Cryptosystems

J.-C. Faugère[1] A. Otmani[2,3] L. Perret[1] J.-P. Tillich[2]

SALSA Team-Project – LIP6/UPMC/INRIA Paris-Rocquencourt
jean-charles.faugere@inria.fr, ludovic.perret@lip6.fr

SECRET Team-Project – INRIA Paris-Rocquencourt
ayoub.otmani@inria.fr, jean-pierre.tillich@inria.fr

GREYC - Université de Caen - Ensicaen

Rump Session – Eurocrypt'2010

McEliece's Cryptosystem & Algebraic Attack

- One of the oldest public-key cryptosystems (R.J. McEliece in 1978). Based on coding theory.
- Key-recovery attack against McEliece cryptosystem $\Longleftrightarrow$ Solving a highly structured polynomial system.

J.-C. Faugère, A. Otmani, L. Perret and J-P. Tillich. *Algebraic Cryptanalysis of McEliece Variants with Compact Keys.* Eurocrypt 2010.

McEliece's Cryptosystem & Algebraic Attack

$\mathcal{M}_{\mathrm{c}Eliece(k,n,r)}(\mathbf{X}, \mathbf{Y}) =$

$$\begin{cases} \vdots \\ g_{i,1}\, Y_1 X_1^j + \cdots + g_{i,n}\, Y_n X_n^j = 0, & \begin{matrix} i \in \{1, \ldots, k\} \\ j \in \{0, \ldots, t-1\} \end{matrix} \\ \vdots \end{cases}$$

- $\mathbf{X} := (\mathbf{X_1}, \ldots, \mathbf{X_{n-1}})$ and $\mathbf{Y} := (\mathbf{Y_1}, \ldots, \mathbf{Y_{n-1}})$ are unknowns.
- $g_{i,j}$'s are known coefficients of the public key.
- k is an integer which is at least equal to $n - t \cdot m$.
- McEliece (1978)
  $q = 2, m = 10, n = 1024, t = 50 \Rightarrow k \geqslant 524$.
  - #variables 2048, #equations 26 200.

Our Results

- We partially solved an important open problem in code-based cryptography
  - Can we distinguish the public key $\{g_{i,j}\}$ of a McEliece cryptosystem from a random matrix $\{\tilde{g}_{i,j}\}$?

Vs

  - Problem formally introduced by Courtois-Finiasz-Sendrier at Asiacrypt'01

$\Rightarrow$ Assumption widely used in security proofs for code-based cryptosystems.

Our Results

- We partially solved an important open problem in code-based cryptography
  - Can we distinguish the public key $\{g_{i,j}\}$ of a McEliece cryptosystem from a random matrix $\{\tilde{g}_{i,j}\}$?
  - Problem formally introduced by Courtois-Finiasz-Sendrier at Asiacrypt'01

  $\Rightarrow$ Assumption widely used in security proofs for code-based cryptosystems.

- Linearization of a tweaked version of $\mathcal{M}_{\mathrm{c}Eliece(k,n,r)}(\mathbf{X},\mathbf{Y})$
  - Rank is much smaller than expected
  - Combinatorial reasons to explain this phenomena
  - It is efficient (polynomial-time), i.e. we only have to perform a Gaussian elimination on the matrix of a linearized system.

Our Results

- We partially solved an important open problem in code-based cryptography
  - Can we distinguish the public key $\{g_{i,j}\}$ of a McEliece cryptosystem from a random matrix $\{\tilde{g}_{i,j}\}$?
  - Problem formally introduced by Courtois-Finiasz-Sendrier at Asiacrypt'01

  ⇒ Assumption widely used in security proofs for code-based cryptosystems.
- Linearization of a tweaked version of $\mathcal{M}_{\mathrm{c}Eliece(k,n,r)}(\mathbf{X},\mathbf{Y})$
  - Rank is much smaller than expected
  - Combinatorial reasons to explain this phenomena
  - It is efficient (polynomial-time), i.e. we only have to perform a Gaussian elimination on the matrix of a linearized system.
- Applies to codes with a high rate (k/n close to 1)
  - typically used in the code-based signature scheme CFS

M. Finiasz, N. Sendrier. *Security Bounds for the Design of Code-Based Cryptosystems*. ASIACRYPT 2009.

Why Should We Care?

- A first step toward a cryptanalysis

  V. Dubois, P.-A. Fouque, A. Shamir, J. Stern.
  Practical Cryptanalysis of SFLASH.
  CRYPTO 2007.

- Shed some light – a priori – on the choices of secure parameters

  O. Regev.
  The Learning With Errors Problem (LWE).
  Lattice Crypto Day (LCD).

- Open Question. How far this attack can be pushed to recover the private key of a McEliece cryptosystem?