Cryptographie Multivariée
Un Second Regard sur HFE

Équipe d'accueil : PolSys (http://www-polsys.lip6.fr/) équipe commune INRIA/UPMC.
Lieu : Le stage se déroulera au Laboratoire d'Informatique de Paris 6 (LIP6) sur le campus de Jussieu.
Adresse : 4, place Jussieu, F-75252 Paris Cedex 05.
Encadrants :
- J.-C. Faugère (Jean-Charles.Faugere@inria.fr)
- L. Perret (ludovic.Perret@lip6.fr)

1 Description du Stage

La cryptographie à clef publique repose sur des problèmes mathématiques réputés *difficiles* dans lesquels il est possible d'introduire une *trappe*. Les problèmes les plus connus sont ceux du logarithme discret et de la factorisation d'entiers. Aujourd'hui, ces deux problèmes sont utilisés dans plus de 99% des applications pratiques de la cryptographie (https, IPSEC, VPN, ...). Si la difficulté de ses problèmes était remise en cause, l'impact sur la société serait extrêmement important. C'est le scénario de la *cryptocalypse* ; le chaos cryptographique.
Nous sommes encore loin de cette situation. En revanche, il est important d'anticiper dès aujourd'hui un tel scénario. En effet, il n'y a finalement que de rares problèmes qui offrent assez de garanties pour être des alternatives crédibles aux problèmes de la théorie des nombres.
L'objet du stage est de nous pencher sur une alternative crédible : la *cryptographie multivariée*. Ces schémas ont vu le jour au milieu des années 80 [5]. La particularité des *cryptosytèmes multivariés* est d'utiliser la difficulté du problème PoSSo : étant donnés des polynômes non-linéaires $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, le problème consiste à trouver, s'il existe, une zéro commun des $f_1, \ldots, f_m$.
Le schéma multivariée à clef publique le plus populaire est sans doute le HFE (Hidden Field Equations), proposé par J. Patarin [6]. La clef secrète de HFE est donnée par une paire $(S, U) \in \mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{GL}_n(\mathbb{F}_q)$ de matrices inversibles et un ensemble de polynômes quadratiques $\mathbf{f} = (f_1, \ldots, f_n) \in (\mathbb{F}_q[x_1, \ldots, x_n])^n$ avec une structure très particulière. Les polynômes $f_1, \ldots, f_m$ sont les composantes d'un polynôme univarié $F(X)$ défini sur une extension $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$. La clef publique est alors donnée par :

$$\mathbf{p} = (p_1, \ldots, p_n) = U \times \mathbf{f}(\mathbf{x} \cdot S), \text{ avec } \mathbf{x} = (x_1, \ldots, x_n).$$

Pour chiffrer $\mathbf{m} \in \mathbb{F}_q^n$, on calcule $\mathbf{c} = \mathbf{p}(\mathbf{m})$. Le déchiffrement (avec la clef secrète) revient essentiellement à trouver les racines d'une équation univarié sur $\mathbb{F}_{q^n}$ de la forme

$$F_C(X) = F(X) - C = 0,$$

avec $C \in \mathbb{F}_{q^n}$ qui dépend du chiffré $\mathbf{c}$ et de la matrice U.

L'efficacité de HFE, comme sa sécurité, dépend crucialement du choix du polynôme F. La famille de polynôme F proposé initialement par J. Patarin rendait HFE vulnérable à des attaques par bases Gröbner très efficaces [4, 1].
Dans le stage, on souhaite explorer de nouvelles pistes sur le choix de F dans HFE. Par exemple, on pourra évaluer la sécurité d'une proposition des auteurs de [7] qui utilise un polynôme F de très haut degré, mais qui se factorise en des polynômes creux. Une autre piste consiste à utiliser des résultats récents sur la factorisation des polynômes univariés creux [2] pour proposer éventuellement d'autres choix pour le polynôme F.

Le stage débutera par un travail de bibliographie pour se familiariser avec les bases de Gröbner et les algorithmes récents pour factoriser des polynômes creux. Le stage nécessitera aussi de valider les idées développées par des implantations dans un système de calcul formel comme MAPLE ou MAGMA [3].

Références

[1] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of HFE, Multi-HFE and variants for odd and even characteristic. *Designs, Codes and Cryptography*, 69(1) :1 – 52, 2013.

[2] Jingguo Bi, Qi Cheng, and J. Maurice Rojas. Sub-linear root detection, and new hardness results, for sparse polynomials over finite fields. In Manuel Kauers, editor, *International Symposium on Symbolic and Algebraic Computation, ISSAC'13, Boston, MA, USA, June 26-29, 2013*, pages 61–68. ACM, 2013.

[3] Wieb Bosma, John J. Cannon, and Catherine Playoust. The Magma algebra system I : The user language. *Journal of Symbolic Computation*, 24(3-4) :235–265, 1997.

[4] Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases. In *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *LNCS*, pages 44–60. Springer, 2003.

[5] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Advances in Cryptology – EUROCRYPT '88*, volume 330 of *LNCS*, pages 419–453. Springer, 1988.

[6] Jacques Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP) : two new families of asymmetric algorithms. In *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *LNCS*, pages 33–48. Springer, 1996.

[7] Jaiberth Porras, John Baena, and Jintai Ding. ZHFE, a new multivariate public key encryption scheme. In Michele Mosca, editor, *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings*, volume 8772 of *Lecture Notes in Computer Science*, pages 229–245. Springer, 2014.