# Lest We Remember: Cold-boot Attacks on Encryption-Keys [8]

**Équipes d'accueil** : PolSys (`http://www-polsys.lip6.fr/`) équipe commune INRIA/UPMC et RO `http://www.lip6.fr/recherche/team.php?id=320`
**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 :**

— B. Escoffier (`bruno.escoffier@lip6.fr`)
— J.-C. Faugère (`Jean-Charles.Faugere@inria.fr`)
— L. Perret (`ludovic.Perret@lip6.fr`)

## 1 Contexte Cryptographique

Dans [8], les auteurs introduisent une technique de cryptanalyse (*cold-boot attack*) permettant à un attaquant de retrouver les clefs secrètes stockées sur toute machine. La technique nécessite d'une part de faire une manipulation physique de la machine cible, et d'autre part de résoudre un système d'équations non-linéaires avec du bruit (`MaxPoSSo`). L'objet du stage est de proposer des algorithmes pour résoudre `MaxPoSSo`.

## 2 Description du Stage

Le problème `MaxPoSSo` est une variante du problème `PoSSo`. Le problème `PoSSo` consiste à trouver les solutions d'un système d'équations non-linéaires. Plus précisément, nous allons étudier le problème sur $\mathbb{F}_2$ :
`PoSSo`$(n, m, d)$
**Entrée.** des polynômes non-linéaires $f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$ de degré de $d > 1$, en $n$ variables sur $\mathbb{F}_2$.
**Question.** Trouver – s'il existe – un vecteur $\mathbf{z} = (z_1, \ldots, z_n) \in \mathbb{F}_2^n$ tel que :

$$f_1(\mathbf{z}) = 0, \ldots, f_m(\mathbf{z}) = 0.$$

Il est bien connu que `PoSSo`$(n, m, d)$ est NP-dur. Dans [2], les auteurs présentent le premier algorithme pour `PoSSo`$(n, n, 2)$ ayant une complexité en dessous de la recherche exhaustive $\big($i.e. $< O(2^n)\big)$. Dans sa version déterministe, l'algorithme a une complexité de $O(1.79^n)$ (et en $O(1.73^n)$ dans une version probabiliste, type Las-Vegas).

Dans le stage, on souhaite étudier une variante du problème `PoSSo` dans laquelle on cherche une solution qui annule le plus grand nombre de polynômes $f_1, \ldots, f_m$. C'est le problème `MaxPoSSo`$(n, m, d)$. En plus des *cold-boot attacks* ([8]), le problème est sous-jacent à la sécurité d'un schéma d'authentification de Gouget et Patarin [7] et d'un chiffrement homorphique proposé dans [1]. On retrouve

également MaxPoSSo$(n, m, d)$ dans les *cold-boot attacks*, un type d'attaque par canaux auxiliaires [8].

Un algorithme naïf pour résoudre MaxPoSSo$(n, m, d)$ consiste à évaluer les polynômes $f_1, \ldots, f_m$ sur l'ensemble des $\mathbf{z} \in \mathbb{F}_2^n$. Cela donne un algorithme qui retourne la solution optimale mais nécessite $4 \log_2(n)\, 2^n$ opérations [4]. Un objectif naturel est de chercher un algorithme d'une meilleure complexité. Pour cela, nous allons relâcher la contrainte sur l'optimalité de la solution. On souhaite proposer des algorithmes qui ne retournent pas obligatoirement la solution optimale mais une *bonne* approximation.

Dans [9], J. Hastad donne un algorithme (polynomial) simple permettant d'approximer MaxPoSSo avec un facteur d'approximation de $1/2^d$. C'est à dire, l'algorithme retourne en temps polynomial une solution de MaxPoSSo qui annule au moins $\mathrm{OPT}/2^d$ équations, avec OPT le nombre maximal d'équations s'annulant simultanément pour un $\mathbf{z} \in \mathbb{F}_2^n$. L'idée de l'algorithme consiste à remarquer qu'un polynôme $f \in \mathbb{F}_2[x_1, \ldots, x_n]$ de degré $d$ s'annule sur $\mathbf{z}$ avec probabilité $\leq 1 - 1/2^d$. Il montre également qu'il est NP-dur d'approximer MaxPoSSo avec un facteur d'approximation de $1/2^d + \epsilon$, pour tout $\epsilon > 0$. Ainsi, ceci indique que tout algorithme qui approxime MaxPoSSo avec un facteur légèrement meilleur que $1/2^d$ est nécessairement exponentiel dans le pire cas.

L'objectif du stage est de combiner les techniques de [5] et l'algorithme [2] pour dériver – si possible – un algorithme modérément exponentiel pour approximer MaxPoSSo.

Le stage débutera par un travail de bibliographie pour se familiariser avec les algorithmes permettant de résoudre PoSSo et MaxPoSSo ainsi que les techniques d'approximations pour MaxSat. Le stage nécessitera aussi de valider les idées développées par des implantations dans un système de calcul formel comme MAPLE ou MAGMA [3] sur des instances de MaxPoSSo provenant d'applications comme [7, 8].

# Références


[1] Martin R. Albrecht, Pooya Farshim, Jean-Charles Faugère, and Ludovic Perret. Polly cracker, revisited. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 179–196. Springer, 2011.

[2] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Pierre-Jean Spaenlehauer. On the complexity of solving quadratic boolean systems. *J. Complexity*, 29(1) :53–75, 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] Charles Bouillaguet, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, and Bo-Yin Yang. Fast exhaustive search for quadratic systems in $\mathbb{F}_2$ on FPGAs. In Tanja Lange, Kristin E. Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada*, volume 8282 of *Lecture Notes in Computer Science*, pages 205–222. Springer, 2013.

[5] Bruno Escoffier, Vangelis Th. Paschos, and Emeric Tourniaire. Approximating MAX SAT by moderately exponential and parameterized algorithms. In Manindra Agrawal, S. Barry Cooper, and Angsheng Li, editors, *Theory and Applications of Models of Computation - 9th Annual Conference, TAMC 2012, Beijing, China, May 16-21, 2012. Proceedings*, volume 7287 of *Lecture Notes in Computer Science*, pages 202–213. Springer, 2012.

[6] 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.

[7] Aline Gouget and Jacques Patarin. Probabilistic multivariate cryptography. In Phong Q. Nguyen, editor, *Progressin Cryptology - VIETCRYPT 2006, First International Conferenceon Cryptology in Vietnam, Hanoi, Vietnam, September 25-28, 2006, Revised Selected Papers*, volume 4341 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2006.

[8] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember : cold-boot attacks on encryption keys. *Commun. ACM*, 52(5) :91–98, 2009.

[9] Johan Håstad. Satisfying degree-d equations over $\mathbb{F}_2^n$. *Theory of Computing*, 9 :845–862, 2013.