Amélioration de la complexité de résolution du problème de décodage en métrique rang

P. Gaborit, O. Ruatta and J. Schrek

Université de Limoges, XLIM-DMI

Le problème du décodage en métrique rang à l'instar du problème classique de décodage en métrique de Hamming peut être utilisé en cryptographie. Par exemple le système GPT [2] est un analogue du cryptosystème de McEliece mais en métrique rang. Un des gros avantages de la métrique rang est que même pour des codes avec des paramètres petits, la complexité du problème de décodage d'un code rang aléatoire devient rapidement très importante. Soit C un code rang aléatoire $[n,k]$ sur $GF(q^m)$ et soit $y = x + e$ un mot reçu pour x un mot du code et e une erreur e de rang r, les meilleures attaques connues de Chabaud-Stern [1] ou de Ourivski-Johansson [5] donnent des complexités dont le terme exponentiel est de la forme $q^{(m-r)(r-1)}$ ou $q^{(k+1)(r-1)}$.

Dans cet exposé on propose deux nouvelles attaques sur le problème du décodage en métrique rang (problème RSD).

La première attaque que nous proposons est une attaque de type combinatoire qui généralise au cas de la métrique rang l'approche qui en métrique de Hamming consiste à retrouver un ensemble de positions qui contient l'erreur associée au syndrome qu'on veut décoder. Notre attaque a une complexité en moyenne de $min(O((n-k)^3 m^3 q^{r\lfloor \frac{km}{n} \rfloor}, O((n-k)^3 m^3 q^{(r-1)\lfloor \frac{(k+1)m}{n} \rfloor}))$ operations sur $GF(q)$. Cette attaque améliore clairement les complexités connues en introduisant dans la complexité la valeur de la longueur du code, ce qui n'était pas le cas des attaques précédentes.

La deuxième attaque est une attaque algébrique basée sur la théorie des q-polynomes de Ore [4]. On introduit une nouvelle mise en equations du problème RSD pour lequel les inconnues ne sont pas dans le petit corps $GF(q)$ mais directement dans l'extension $GF(q^m)$. Cette approche permet ainsi de réduire considérablement le nombre d'inconnues (mais augmente le degré des equations). On considère alors deux approches pour résoudre cette mise en equations. Les techniques de type linéarisation permettent de montrer que si $n \geq (k+1)(r+1) - 1$ alors le problème RSD peut être résolu en temps polynomial, plus généralement on montre en utilisant des techniques hybrides que si $\lceil \frac{(r+1)(k+1)-(n+1)}{r} \rceil \leq k$, alors le problème peut être résolu en $O(r^3 k^3 q^{r\lceil \frac{(r+1)(k+1)-(n+1)}{r} \rceil})$. On considère aussi la résolution directe à partir de bases de Gröbner (la version F4 de Magma) pour lesquelles on discute la complexité théorique. On considère aussi une résolution hybride de ces equations sur des paramètres concrets.

A titre d'exemple d'applications on montre que nos attaques permettent de casser tous les paramètres proposés pour les réparations récentes du système GPT [3, 7] contre les attaques d'Overbeck [6]. Certains paramètres annoncés avec une sécurité de 2^{80} sont même cassés concrétement en moins d'une seconde.

References

1. Florent Chabaud, Jacques Stern: The Cryptographic Security of the Syndrome Decoding Problem for Rank Distance Codes. ASIACRYPT 1996: 368-381
2. Ernst M. Gabidulin, A. V. Paramonov, O. V. Tretjakov: Ideals over a Non-Commutative Ring and thier Applications in Cryptology. EUROCRYPT 1991: 482-489
3. Pierre Loidreau: Designing a Rank Metric Based McEliece Cryptosystem. PQCrypto 2010: 142-152
4. O. Ore, On a special class of polynomials, Trans. American Math. Soc. (1933)
5. Ourivski, A. V. and Johansson, T., New Technique for Decoding Codes in the Rank Metric and Its Cryptography Applications,Probl. Inf. Transm.(38), 237–246 (2002)
6. Raphael Overbeck: Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes. J. Cryptology 21(2): 280-301 (2008)
7. Haitham Rashwan, Ernst M. Gabidulin, Bahram Honary: Security of the GPT cryptosystem and its applications to cryptography. Security and Communication Networks 4(8): 937-946 (2011)