CONGRESO DE JÓVENES INVESTIGADORES
Real Sociedad Matemática Española
Universidad de Murcia, del 7 al 11 de Septiembre de 2015

Criptografía basada en códigos correctores: alternativa a los clásicos criptosistemas de clave pública

Irene Márquez-Corbella[1]

En un mundo en que la utilización de datos electrónicos es imprescindible tanto en la vida personal como en la institucional, el uso de la criptografía ya no es opcional: es imperativo. Sin embargo, se está convirtiendo en una tarea ardua encontrar primitivas criptográficas eficientes que sobrevivan a ataques criptoanalíticos. Por ejemplo, la seguridad de casi todos los criptosistemas de clave pública -aquellos que no requieren un intercambio inicial de secretos- se basa hoy en día sólo en dos problemas: la factorización y el logarítmo discreto. Por lo tanto, avances en estos problemas o la construcción de ordenadores cuánticos cambiarán de forma drástica el panorama actual.

La criptografía basada en códigos correctores junto con la criptografía basada en retículos (en inglés: lattice based cryptography), la criptografía multivariable o la criptografía basada en funciones hash son las principales técnicas de las que disponemos para resistir a ataques por ordenador cuántico. McEliece en 1978 [3] propone el primer criptosistema basado en la teoría de códigos correctores, definiendo uno de los sistemas de cifrado más eficientes que existen y que, además, resiste (hasta el momento) cualquier tipo de criptoanálisis.

El principio de estos criptosistemas se basa en la siguiente función *"trapdoor one-way"*: es fácil y rápido codificar mensajes utilizando transformaciones lineales; pero el problema general de decodificación se ha demostrado que es un problema NP-completo para la métrica de Hamming. La "puerta trampa" consiste en que existen ciertas familias de códigos que poseen algoritmos específicos eficientes de decodificación. En su artículo original, McEliece propone utilizar códigos Goppa binarios, y esta opción sigue siendo segura. Pero otras familias de códigos han sido propuestas en un intento de reducir el tamaño de las claves, por ejemplo (y esta lista está lejos de ser exhaustiva): los códigos Reed-Solomon Generalizados [6], los códigos Reed-Muller binarios [8] o los códigos geométricos [2]. Todas estas propuestas han sido atacadas en tiempo polinomial o sub-exponencial [7, 4, 1]. La principal desventaja de estos criptosistemas es el gran tamaño de sus claves. Sin embargo, se han realizado grandes avances en este área (reduciendo la longitud de la clave pero manteniendo el mismo nivel de seguridad). Los nuevos resultados admiten claves muy compactas [5] (alrededor de 5000 bits para alcanzar 80 bits de seguridad), lo que permite comparar estos criptosistemas con el clásico criptosistema RSA.

En esta charla presentaremos con detalle el estado de la criptografía basada en códigos correctores y los progresos que ha hecho la comunidad con el fin de estar preparada para el proceso de estandarización.

Referencias

[1] A. Couvreur and I. Márquez-Corbella and R. Pellikaan. A Polynomial Time Attack against Algebraic Geometry Code Based Public Key Cryptosystems. En *IEEE International Symposium on Information Theory (ISIT)*, 1446–1450. Honolulu, June 2014.

[2] H. Janwa and O. Moreno. McEliece public cryptosystem using algebraic-geometric codes. *Des. Codes Cryptogr.* **8** (1996) 293–307.

[3] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report* **42-44**, (1978) 114–116.

[4] L. Minder and A. Shokrollahi. Cryptanalysis of the Sidelnikov cryptosystem. En *Advances in Cryptology - EUROCRYPT 2007*, Lecture Notes in Computer Science, vol. 4515 (2007) 347-360.

[5] R. Misoczki, J.P. Tillich, N. Sendrier and P. Barreto. MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes En *IEEE International Symposium on Information Theory (ISIT)*, 2069-2073. Istanbul, July 2013.

[6] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory* **15** (2) (1986) 159–166.

[7] V. M. Sidelnikov and S. O. Shestakov. On the insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Math. Appl.* **2** (1992) 439–444.

[8] V.M. Sidelnikov. A public-key cryptosytem based on Reed-Muller codes. *Discrete Math. Appl.***4** (3) (1994) 191-207.

[1]Project-team SECRET, INRIA Rocquencourt
78153 Le Chesnay Cedex, France
irene.marquez-corbella@inria.fr