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

Algebraic Attack to the Noise-Free Version of Aaronson-Christiano's Quantum Money Scheme

Marta Conde Pena[1], **Jean-Charles Faugère**[2], **Ludovic Perret**[2]

As physical devices are involved in the generation of cash, forgery is (at least theoretically) possible. However, Wiesner proposed in [1] to take advantage of the non-cloning theorem of quantum mechanics to construct (quantum) money that is theoretically impossible to counterfeit (or more precisely, the probability of successful forging is exponentially small). This work was followed by several papers [3, 4, 2] that improved Wiesner's idea, and today's main efforts in quantum money research are put into constructing what is called public-key quantum money: quantum money that can be verified by anyone with a quantum device and not only by the bank that issued it as it was the case in [1].

The main proposal for public-key quantum money is Aaronson-Christiano's scheme [5] both in its noise-free and noisy version. We focus only in the noise-free version. Whereas the security of other proposals (for example [6]) is not well understood, Aaronson-Christiano's scheme is the first one that is proved to be cryptographically secure under a new non-quantum hardness assumption. This assumption states that, once we 'hide' two orthogonal subspaces by encoding each of them as the common zeros of a set of appropriate random multivariate polynomials of degree d over a finite field of prime size q, it is not possible to efficiently recover the subspaces hidden. The problem is hence called the hidden subspaces problem (or HSP_q for short).

We study of the hardness of HSP_q. We present a randomized polynomial-time algorithm that solves HSP_q for $q > d$ with success probability $approx 1 - \frac{1}{q}$, which proves that the quantum money scheme over $\mathbb{F}_q$ is not secure for big q, solving the open question in [5] of whether their scheme (defined over $\mathbb{F}_2$) can be extended to $\mathbb{F}_q$ or not. Finally we show that there is also a heuristic randomized polynomial-time algorithm solving HSP_2 with high probability and so their original noise-free scheme is conjectured to be broken too.

Work partially supported by Ministerio de Economía y Competitividad under the project TIN2014-55325-C2-1-R (ProCriCiS).

Referencias

[1] S. Wiesner: Conjugate coding, *ACM SIGACT News* **15** (1) (1983), 78–88.

[2] Mosca, M., Stebila, D.: Quantum coins. *Error-Correcting Codes, Finite Geometry and Cryptography* **523** (2010), 35–47.

[3] Bennett, C.H., Brassard, G., Breidbard, S., Wiesner, S.: Quantum cryptography, or unforgeable subway tokens. En *Proceedings of CRYPTO*, David Chaum and Ronald L. Rivest and Alan T. Sherman (eds.), 267–275. Plenum Press New York, Santa Barbara, California, USA, 1982.

[4] Gavinsky, D.: Quantum money with classical verification. En *Proceedings of the 27th Conference on Computational Complexity, CCC*, nombres de los editores/editors names (eds.), 42–52. IEEE, Porto, Portugal, 2012.

[5] Aaronson, S., Christiano, P.: Quantum money from hidden subspaces. En *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC*, Howard J. Karloff and Toniann Pitassi (eds.), 41–60. ACM, New York, USA, 2012.

[6] Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A., Shor, P.W.: Quantum money from knots. En *Proceedings of Innovations in Theoretical Computer Science, ITCS*, Shafi Goldwasser (eds.), 276–289, Cambridge, MA, USA, 2012.

[1]Instituto de Tecnologías Físicas y de la Información (ITEFI)
Consejo Superior de Investigaciones Científicas (CSIC)
Calle Serrano, 144, 28006, Madrid, Spain
marta.conde@iec.csic.es

[2]Sorbonne Universités, UPMC Univ Paris 06, POLSYS, UMR 7606, LIP6, F-75005, Paris, France
INRIA, Paris-Rocquencourt Center
CNRS, UMR 7606, LIP6, F-75005, Paris, France
jean-charles.faugere@inria.fr, ludovic.perret@lip6.fr