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

Boosting Linearly-Homomorphic Encryption

Dario Fiore (speaker)[1], **Dario Catalano**[2]

We show a technique to transform a linearly-homomorphic encryption into a homomorphic encryption scheme capable of evaluating degree-2 computations on ciphertexts. Our transformation is surprisingly simple and requires only one very mild property on the underlying linearly-homomorphic scheme: the message space must be a public ring in which it is possible to sample elements uniformly at random. This allows us to instantiate our transformation with virtually all existing number-theoretic linearly-homomorphic schemes, such as Goldwasser-Micali, Paillier, or ElGamal. Our resulting schemes achieve circuit privacy and are compact when considering a subclass of degree-2 polynomials where the number of additions of degree-2 terms is bounded by a constant. As an additional contribution we extend our technique to build a protocol for outsourcing computation on encrypted data using two (non-communicating) servers. Somewhat interestingly, in this case we can boost a linearly-homomorphic scheme to support the evaluation of any degree-2 polynomial while achieving full compactness.

Referencias

[1] D. Catalano, D. Fiore: *Boosting Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data*. Cryptology ePrint Archive, Report 2014/813, 2014. `http://eprint.iacr.org/2014/813`

[1]IMDEA Software Institute, Madrid
`dario.fiore@imdea.org`

[2]Dipartimento di Matematica e Informatica
Università di Catania
Catania, italy
`catalano@dmi.unict.it`