Courses
2018-19

Post-quantum Cryptography

Iván Blanco Chacón (University College Dublin), Ignacio Luengo Velasco
(Universidad Complutense Madrid) & Irene Marquez Corbella
(Universidad de La Laguna)

10-14 September 2018 (5 sessions) l 09:30 - 11:30 (a total of 10 hours)

Post-quantum Cryptography is the Public Key Cryptography (PKC) secure against quantum computers. The future quantum computers will break RSA and ECC thanks to the celebrated Shor's algorithm, rendering Internet and electronic commerce insecure. The american institute of standards (NIST) launched an open contest to select and standardize quantum safe (post-quantum) PKC schemes. The open call ended in November 2017, most of the surviving candidates being based on lattices, error correcting codes and polynomial maps.

OBJECTIVES:
The objective of this course is to present the state of the art of cryptosystems based on those three technologies, and at the same time introduce the audience into the main ideas and methods of modern cryptography.

The course does not assume much mathematical background, and the main concepts and ideas will be introduced along it. It should be accessible to master students.

PROGRAMME:
1. Introduction to PKC. Complexity. Finite fields.

2. Code bases Cryptography
In the late seventies, McEliece introduced the first code based public-key cryptosystem (PKC) whose security reposes on the hardness of decoding a random linear code. Compared to public- key schemes based on integer factorization (like RSA) or discrete logarithm, McEliece not only is resistant, so far, to attacks by quantum computers, but also presents faster encryption and decryption schemes. However, due to the large size of the keys required to have a good security level, it is rarely used in practice. Nevertheless, note that recent proposals makes such proposals competitive with RSA. This course will start with a short introduction and in-depth look at all the ingredients required for constructing code-based public key encryption systems, we will study in detail the security reduction of McEliece and Niederreiter systems (which are the principal PKC based on Error correcting codes) and how to reduce the size of its keys, then we will devoted to the best known attack against these cryptosystems (generic decoding of linear codes) and we will finish with Key attacks (those attacks that try to

retrieve the code structure rather than attempting to use an unspecific decoding algorithm.

3. Lattice Cryptography

Lattice based PQC is based on the (proved or conjectured) unfeasibility of the problem of finding the shortest vector in a lattice. In particular, the Learning With Errors (LWE) cryptosystem is backed on the proved NP-hardness of this problem on generic lattices, but it has the drawback of the quadratic overhead in the key sizes. The Ring Learning With Errors (RLWE) cryptosystem solves the quadratic overhead but is built on the conjectured NP-hardness of the problem but restricted to ideal lattices. We will focus in RLWE and discuss how arithmetic invariants of algebraic number fields determine the expected security of the cryptosystem.

4. Multivariate Cryptography

Multivariate Cryptography Public Key Cryptography (MPKC) uses as public keys (usually quadratic) multivariate polynomials maps F=(F1,..,Fn) (with a trapdoor) that looks generics because solve a generic system of non linear polynomials is an NP-complete problem. They encryption (evaluation) is fast and are considered secure agains quantum computers. For efficiency reasons mainly quadratic maps are used as Public Key and all NIST candidates are quadratics except one (DME) that uses high degree polynomials in few variables. We will describe the main constructions in MPKC and its security against algebraic attacks.

REFERENCES:

[1] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press 10996.
[2] D. Bernstein, J. Buchmann, and E.Dahmen, Post-Quantum Cryptography, 2009, Springer-Verlag, Berlin-Heidleberg.
[3] J.Ding, J. Gower, D. Schmidt, Multivariate Public Key Cryptosystems Advances in Information Security 25, Springer 2006.
[4] J Ding, A. Petzoldt: Current State of Multivariate Cryptography. IEEE Security & Privacy 15(4): 28-36 (2017).
[5] W. C. Huffman and V. Pless. Fundamentals of error-correcting codes. Cambridge University Press, Cambridge, 2003.
[6] R. Overbeck and N. Sendrier. Code-based cryptography. In D.J. Bernstein, J. Buchmann, and E. Dahmen, editors, Post-Quantum Cryptography, pages 95-145. Springer, 2009.
[7] V. Lyubashevsky, C. Peikert, O. Regev: On ideal lattices and learning with errors over rings: https://eprint.iacr.org/2012/230.pdf
[8] M. Rosca, D. Stehlé, A. Wallet: On the R-LWE and Polynomial-LWE problems. In EUROCYPT 2018 J.B. Nielsen, V. Rijmen (Eds) IACR 2018.

***Registration is free, but inscription is required before 5th September:** So as to inscribe go to https://bit.ly/2zdi5FF and fill the registration form. Student grants are available. Please, let us know if you need support for travel and accommodation expenses when you fill the form.