Colloquium : Silvio Micali

Schedule for the 26th of May

[10:00 → 12:00] Masterclass (room 25-26/105)

Presentations by PhD students of their work. Each presentation (20 minutes) is followed by an open discussion with Silvio Micali (15 minutes):

- Virginie Lallemand (SECRET, Inria)

  Title : Cryptanalysis of Lightweight Block Ciphers

  Supervisor : María Naya-Plasencia

  abstract : In comparison to asymmetric cryptography, symmetric cryptography provides enormous performance and implementation advantages, which makes it essential in everyday applications. The most popular and widely deployed symmetric block cipher is the Advanced Encryption Standard (AES). Similarly to any symmetric cipher, the confidence accorded to the AES relies on empirical arguments, mainly based on analyses that test the resistance of the cipher against generic and dedicated attacks. The numerous years of analysis of the AES and of other primitives resul- ted in the formulation of criteria that ensure resistance against some known attacks (e.g. the Wide Trail Strategy) that simplify the task of cipher desi- gners. However, the recent emergence of embedded devices created a need for ciphers that are faster, smaller or less energy-consuming than existing ones, giving rise to a new generation of designs that deviate from common design strategies and have smaller security margins in the name of performance or compactness. In this respect, the work made by cryptanalysts appears essential since the security of those new primitives has to be studied carefully.

- Frédéric de Portzamparc (POLSYS, LIP6, UPMC)

  Title : Cryptanalyses of Compact McEliece Schemes

  Supervisors : Jean-Charles Faugère, Ludovic Perret and Aline Gouget

  abstract : Code-based cryptography, introduced by Robert McEliece in 1978, is a potential candidate to replace the asymmetric primitives which are threatened by quantum computers. More generally, it has been considered secure for more than thirty years, and allows very vast encryption primitives. Its major drawback lies in the size of the public keys. For this reason, several variants of the original McEliece scheme with keys easier to store were proposed in the last years.

  In this talk, we are interested in variants using alternant codes with symmetries and wild Goppa codes. We study their resistance to algebraic attacks, and reveal sometimes fatal weaknesses. In each case, we show the existence of hidden algebraic structures allowing to describe the secret key with non-linear systems

of multivariate equations containing fewer variables than in the previous modellings. Their resolutions with Grbner bases allow to find the secret keys for numerous instances out of reach until now and proposed for cryptographic purposes. For the alternant codes with symmetries, we show a more fundamental vulnerability of the key size reduction process.

- Cécile Pierrot (Almasty, LIP6, UPMC)

  Title : The discrete logarithm problem in medium characteristic finite fields

  Supervisor : Antoine Joux

  Abstract : Cryptography is the study of techniques for secure communication in the presence of third parties, also called adversaries. Such techniques are detailed in cryptosystems, explaining how to securely encode and decode messages. They are designed around computational hardness assumptions related to mathematical properties, making such algorithms hard to break in practice by any adversary. These protocols are based on the computational difficulty of various problems which often come from number theory, such as integer factorization or discrete logarithms computations.

  In this talk, we focus on the discrete logarithm problem in finite fields and more precisely we study the case where the characteristic of the field is of medium size. Combining two recent variants of the Number Field Sieve, namely the Conjugation Method and the Multiple variant, I design the best asymptotic algorithm to compute discrete logarithms in this case.

[17:15] Cocktail (in front of Amphi 25)

[18:00] Colloquium (Amphi 25)