“Symbolic Computations and Post-Quantum Cryptography” Online Seminar

Martin Albrecht

(Université Pierre et Marie Curie)

″Polly Cracker Revisited.″

May 25, 12:00pm (New York Time).

Abstract:

In this talk, we introduce the provable-security treatment of cryptographic constructions based on the hardness of computing a Groebner basis. We formalise and study the relation between various computational problems associated with Groebner bases, and revisit the (symmetric) polly cracker encryption scheme, proving that it achieves only bounded IND-CPA security under the ideal membership problem. Next, using results from computational commutative algebra, we show that no simple generic transformation can lead to a fully secure polly-cracker-type scheme. This then leads us to noisy variants of Groebner bases and related problems. After formalizing and justifying the hardness of the noisy assumptions we show that noisy encoding of messages results in a secure homomorphic scheme. Finally, through a symmetric-to-asymmetric conversion, we provide a positive answer to the long standing open problem proposed by Barkee et al. of using multivariate polynomials in public-key cryptography.
Joint work with C. Cid, P. Farshim, J-C. Faugere and L. Perret

Next presentation: **TBA**

Algebraic
Cryptography
Center