Curso: THE MATHEMATICS OF SECURE COMPUTATION

Professor Ronald Cramer
(CWI, Amsterdam and Mathematical Institute, Leiden University)

Seminario 238, Departamento de Álgebra,
Facultad de Matemáticas,
Universidad Complutense de Madrid

Summary. This series of lectures focuses on novel interactions between secure computation on the one hand, and algebraic number theory, algebraic geometry, combinatorics and error correcting codes on the other hand.

Cryptology provides mathematical techniques for digital security in a malicious environment. It is crucial e.g. to computer security (firewalls), to financial Internet transactions, and, even back in the days of Julius Caesar, to national security.

Encryptions (secrecy) and digital signatures (authenticity, non-repudiation) provide unilateral security, i.e., they protect communication between legitimate parties against eavesdropping and tampering by *malicious outsiders*. Secure computation, initiated by Andrew Yao (1982), focuses instead on secure cooperation among *mutually distrusting* parties, i.e., multi-lateral security. It opened radically new vistas, its significance perhaps on a par with the very invention of secure communications in ancient times. Potential applications of secure computation are myriad, and include privacy protection, negotiations, and simulation of a trusted host computer where none exists. Following the massive deployment of public-key cryptography (e.g., the RSA crypto-system) in the late 1990s, secure computation may represent a next major wave in the future.

A series of ground-breaking works in the 1980s showed that "in principle, all multi-lateral security problems solvable with a trusted host are securely solvable without." Employing intricate cryptography, networked processors jointly perform computations on private data while maintaining secrecy and correctness even if a quorum of the processors are under full, malicious adversarial control.

Tentative Schedule:

Lecture 1: Introduction to Secret Sharing. The Black-Box Secret Sharing Problem. Optimal solutions based on algebraic number theory.

Lecture 2: Introduction to Secure Computation. Secure Multi-Party Multiplication with Linear Communication. An improvement of the classical solution.

Lecture 3: Linear Secret Sharing Schemes and Algebraic Combinatorics: The (Strong) Multiplication Problem. Constructions, open problems, relation to efficient error correction algorithms.

Lecture 4: Algebraic Geometric Constructions of Linear Secret Sharing Schemes with Strong Multiplication. Construction of ramp schemes with multiplication from error correcting codes.

Fechas y horarios:
Jueves 3 y Viernes 4 de Mayo a las 16h.
Martes 8, Jueves 10 y Viernes 11 de Mayo a las 16h (*).
(*) El horario de la segunda semana es provisional y se fijará con los asistentes.