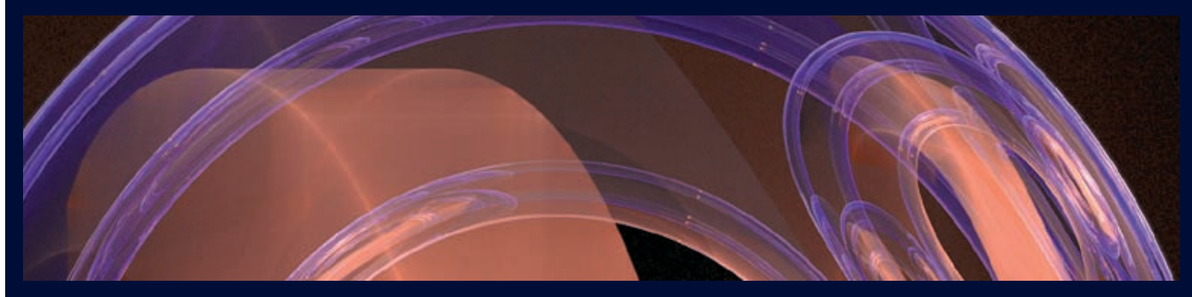
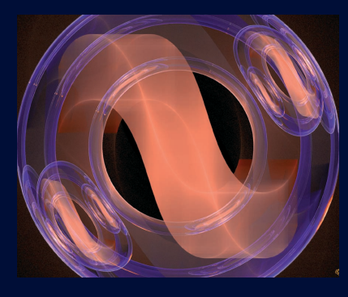


iMdea matemáticas



imdea seminar

February 13th, 2008

Dpto. de Matemáticas, sala 520
Facultad de Ciencias - UAM
Ciudad Universitaria de Cantoblanco
28049 Madrid
How to get there: www.imdea.org

Matemáticas, la llave para el conocimiento, el desarrollo y la innovación
Mathematics, the key for knowledge, development & innovation

12:00 · 13:00

Computing in the dark using algebraic geometry

Ronald CRAMER
CWI
Amsterdam & Mathematical Institute
Leiden University

Cryptology provides mathematical techniques for digital security in a malicious environment. Encryptions and digital signatures protect legitimate parties against eavesdropping and tampering by malicious outsiders, i.e., uni-lateral security. Secure computation focuses instead on multi-lateral security, i.e., secure cooperation among mutually distrusting parties or parties with conflicting interests. Potential applications are myriad, and include privacy protection, negotiations, and simulation of an incorruptible mediator. A fundamental theorem from the 1980s says in essence that ``all multi-lateral security problems solvable with a trusted host are securely solvable without."

It was proved (EUROCRYPT 2000) by Cramer, Damgaard and Maurer that information-theoretically secure multi-party computation can be realized from mathematical devices called linear secret sharing schemes with (strong) multiplication. It was shown (CRYPTO 2006) by Chen and Cramer that such devices can be constructed using algebraic function fields. Using in addition a well-known theorem of Garcia-Stichtenoth on curves with many rational points they showed how to perform secure computation with improved efficiency. This is the first non-trivial connection between secure computation and algebraic geometry. After an introduction to the concept of secure computation, some of the mathematical details behind this result are discussed. Recent extensions are due to Chen/Cramer/Goldwasser/deHaan/Vaikuntanatan (EUROCRYPT 2007) and Chen/Cramer/deHaan/CacudoPueyo (EUROCRYPT 2008), and we plan to discuss these results as well.

Meanwhile, these results have had remarkable application in the breakthrough work (STOC 2007) by Ishai/Kushilevitz/Ostrovsky/Sahai on *constant-rate* zero knowledge for circuit satisfiability, and by Harnik/Ishai/Kushilevitz/BuusNielsen (TCC 2008) on constant-rate robust combiners for Oblivious Transfer.