Probable security in asymmetric cryptography

Speaker: Damien VERGNAUD

Provable (or reductionnist) security is a set of mathematical techniques by means of which cryptographers analyze a cryptographic system and demonstrate its security. The recent formalization of security notions for cryptosystems allows one to formulate security by relating resistance to attacks to so-called intractability assumptions. Initially of theoretical interest, reductionnist security has become over the past few years an extremely popular, practical and powerful tool for both the design and evaluation of cryptographic systems. This presentation will give an overview on the methods and the pitfalls of applying reductionnist security for cryptographic schemes.