Welcome Home Workshop 2014

NOME: Michela

COGNOME: Mazzoli

AFFILIAZIONE: Alpen-Adria-Universität Klagenfurt, Austria

POSIZIONE: dottoranda

EMAIL: michela.mazzoli@aau.at

LINGUA PER LA CONFERENZA: italiano

TITOLO: Computational Aspects of Hyperelliptic Curve Cryptography

COAUTORI:

Abstract

Public-key cryptography allows two entities to exchange a common secret and communicate privately over an insecure public channel. Many of these cryptographic schemes are based on the Discrete Logarithm Problem (DLP): given a cyclic group $G = \langle g \rangle$ and g^a, find the exponent a. The security of DLP-based public-key cryptography relies on the fact that no polynomial-time algorithm for the DLP is known.

Some groups suitable for cryptographic applications are, for instance, the group of points of an elliptic curve over a finite field, and the Jacobian of a hyperelliptic curve over a finite field. Elliptic and hyperelliptic curves must be carefully chosen to be secure against all known attacks. If these security constraints are fulfilled, the DLP in the corresponding groups is believed to be practically intractable. Nowadays elliptic curves are a well-established basis of standardised cryptographic protocols. On the other hand, security and efficient implementation of hyperelliptic curve cryptosystems is rather a novel field of research.

In this talk we first describe how an Abelian group (i.e. the Jacobian) can be obtained out of the set of points of a hyperelliptic curve. Secondly, we present an overview of the computational problems concerning hyperelliptic curve cryptography: 1) how to count the order of the Jacobian; 2) how to establish whether a curve is supersingular or not; 3) how to efficiently perform arithmetic, namely addition and scalar multiplication, in the Jacobian.