Randomizing Scalar Multiplication using Exact Covering Systems of Congruences

PIMS CRG on Explicit Methods for Abelian Varieties
Kick-off Workshop
Invited Talk

Laurent Imbert
Joint work with Eleonora Guerrini and Théo Winterhalter

LIRMM, CNRS, Univ. Montpellier, France

Abstract. Exponentiation over a finite group is a central operation for most public key cryptosystems. It is used extensively in the generation/verification of electronic signatures (e.g. using DSA or its elliptic curve variant) and in the encryption/decryption phases of RSA or (EC)DL-based algorithms. In general, data manipulated during these computations should be kept secret, as even a small amount of information may be maliciously exploited by an attacker, for example for forging one's signature or for acquiring some confidential information. Over the past fifteen years, an extensive variety of constant-time, highly regular exponentiation algorithms have been proposed. Combined together with various randomization techniques, these algorithms offer sound protections against differential, timing and simple side- channel attacks. Unfortunately, the ultimate, all-in-one, protection does not seem to exist. In order to protect an implementation against all known attacks, several countermeasures should often be carefully stacked together. In this talk, I will present a novel family of uniformly randomized scalar multiplication algorithms based on covering systems of congruences which offer good performances in terms of both speed and robustness against a wide class of side-channel attacks.

Keywords: Scalar multiplication, side-channel attacks, randomized algorithms, covering systems of congruences, mixed-radix number system