Randomizing Scalar Multiplication using Exact Covering Systems of Congruences

Laurent Imbert

To cite this version:

Laurent Imbert. Randomizing Scalar Multiplication using Exact Covering Systems of Congruences. Explicit Methods for Abelian Varieties: Kick-off Workshop, May 2015, Calgary, Canada. lirmm-01340683v1

HAL Id: lirmm-01340683

https://hal-lirmm.ccsd.cnrs.fr/lirmm-01340683v1

Submitted on 11 Oct 2019 (v1), last revised 11 Oct 2019 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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. A set of congruence relations is a $\mathbb{Z}$-covering if each integer belongs to at least one congruence class from that set. In this paper, we first show that most existing scalar multiplication algorithms can be formulated in terms of covering systems of congruences. Then, using a special form of covering systems called exact n-covers, we present a novel uniformly randomized scalar multiplication algorithm with built-in protections against most passive side-channel attacks. Our algorithm randomizes the addition chain using a mixed-radix representation of the scalar. Its reduced overhead and purposeful robustness could make it a sound replacement to several conventional countermeasures. In particular, it is significantly faster than Coron's scalar blinding technique for elliptic curves when the choice of a particular finite field tailored for speed compels to double the size of the scalar, hence the cost of the scalar multiplication.

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