Randomizing Scalar Multiplication using Exact Covering Systems of Congruences

Laurent Imbert

Randomizing Scalar Multiplication
using Exact Covering Systems of Congruences

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