HAL
open science

Faster cofactorization with ECM using mixed representations

Cyril Bouvier, Laurent Imbert

To cite this version:

Cyril Bouvier, Laurent Imbert. Faster cofactorization with ECM using mixed representations. WRAC'H 2019 - Workshop on Randomness and Arithmetics for Cryptography on Hardware, Apr 2019, Roscoff, France. lirmm-02309390

HAL Id: lirmm-02309390

https://hal-lirmm.ccsd.cnrs.fr/lirmm-02309390

Submitted on 9 Oct 2019

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.

Faster cofactorization with ECM using mixed representations

WRAC'H 2019

Workshop on Randomness and Arithmetics for Cryptography on Hardware

Invited Talk

Laurent Imbert

Joint work with Cyril Bouvier

LIRMM, CNRS, Univ. Montpellier, France

Abstract. In this talk, we introduce a novel implementation of the elliptic curve factoring method specifically designed for medium-size integers such as those arising by billions in the cofactorization step of the Number Field Sieve. In this context, our algorithm requires fewer modular multiplications than any other publicly available implementation. The main ingredients are: the use of batches of primes, fast point tripling, optimal double-base decompositions and Lucas chains, and a good mix of Edwards and Montgomery representations.

Keywords: Elliptic curve method, cofactorization, double-base representation, twisted Edwards curve, Montgomery curve, CADO-NFS

More info: `http://eco.lirmm.net/double-base_ECM/`