# Faster cofactorization with ECM using mixed representations

Cyril Bouvier, Laurent Imbert

# 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/`