# On the Implementation Challenges of Multi-Scalar-Multiplication for SNARKs

RAPHAËL COMPS, VLADIMÍR MARCIN, TIBOR TRIBUS*,

MAYA-ZK, PRAGUE, Czechia

VIKTOR FISCHER, CARLOS ANDRES LARA-NINO,

Université Jean Monnet Saint-Etienne, CNRS, Institut d'Optique Graduate School, Laboratoire Hubert Curien UMR 5516, F-42023, SAINT-ETIENNE. France

A zero-knowledge proof (ZKP) is a cryptographic method that allows a prover to convince a verifier of the truth of a statement without revealing any additional information other than the fact that the statement is true. The verifier gains no knowledge about the underlying secret, and the proof cannot be reused by a third party to convince others. The application scope for such protocols includes identity verification with anonymity, electronic voting systems, and enhancing the privacy of block-chain. In the latter, distributed computing approaches can also mitigate the need for any certifying authority.

At the time of writing, a significant share of the market is using Succinct Non-Interactive Argument of Knowledge (SNARKS). For universal SNARKs, such as PLONK or Marlin, a polynomial commitment scheme is needed. An example of an efficient one is the Kate-Zaverucha-Goldberg (KZG) scheme. The verifier needs to verify some polynomial openings using bilinear pairings. So far, the verification algorithms boil down mainly to pairing computations.

The bottleneck in the proving algorithm of most elliptic-curve-based SNARK proof systems is the Multi-Scalar-Multiplication (MSM). This algorithm solves the accumulation of a large number of scalar multiplications; currently, $2^{26}$ scalar multiplications are used. Computing such a large volume of data requires a lengthy processing time, which we aim to reduce. In this talk, we describe our approach for solving this problem.

*Authors appear in alphabetical order.

Authors' addresses: Raphaël Comps, Vladimír Marcin, Tibor Tribus,
MAYA-ZK, PRAGUE, Czechia, maya-zk.com; Viktor Fischer, Carlos Andres Lara-Nino,
Université Jean Monnet Saint-Etienne, CNRS, Institut d'Optique Graduate School, Laboratoire Hubert Curien UMR 5516, F-42023, 18 rue du Professeur Benoît Lauras 42000, SAINT-ETIENNE. France, {fischer,carlos.lara}@univ-st-etienne.fr.