Double-and-Add with Relative Jacobian Coordinates

Björn Fay

2015-09-15

NXP

SECURE CONNECTIONS FOR A SMARTER WORLD

Introduction

- EC double & add algorithm for short Weierstrass curves
- Based on:
  - Nicolas Meloni. New point addition formulae for ecc applications. In Claude Carlet and Berk Sunar, editors, WAIFI, volume 4547 of Lecture Notes in Computer Science, pages 189–201. Springer, 2007.
  - Patrick Longa and Ali Miri. New composite operations and precomputation scheme for elliptic curve cryptosystems over prime fields (full version). IACR Cryptology ePrint Archive, 2008:51, 2008.
  - Patrick Longa and Ali Miri. New multibase non-adjacent form scalar multiplication and its application to elliptic curve cryptosystems (extended version). IACR Cryptology ePrint Archive, 2008:52, 2008.
  - Matthieu Rivain. Fast and regular algorithms for scalar multiplication over elliptic curves. IACR Cryptology ePrint Archive, 2011:338, 2011.
- Already 18 field multiplications per double & add step
- But affine pre-computed points needed
  - -> extra inversion (expensive)

Features

- Usage of relative Jacobian coordinates
- $P_0 = (X_0 : Y_0 : Z_0)$
- $P_1 = (X_1 : Y_1 : Z_1')$ (accumulated point)
- $Z_1 = Z_0 \cdot Z_1'$
- Common z coordinates (Z_0) for precomputed points (no affine coordinates needed)
- Double & Add
- $P_1 := P_0 + P_1 + P_1$
- Needs 13 M + 5 S + 14 A per double & add step
- Only 4 auxiliary registers are needed (field elements)
- Compatibel with generic double & add algorithms as e.g. window method and comb method
- Paper available: `http://eprint.iacr.org/2014/1014`