Lining Wang
August 2, 2014
Edwards Curve ECC

1 Introduction

2 Elliptic Curves

Math background. Derive elliptic curves from algebraic geometry.

2.1 (Twisted) Edwards Curves

3 Elliptic Curve Cryptography

Cryptography background.

3.1 The Discrete Logarithm Problem

3.2 Encryption Schemes

3.3 Current Standards

4 Curve25519 and Ed25519

Current implementations by djb.

4.1 New Speed Records

4.2 Security Benefits

5 New Abstract Groups

Our contribution: Python abstract group interface.

5.1 Optimizations

6 Conclusions