

**Workshop on Elliptic Curve Cryptography Standards
Accepted Presentations**

Adobe Digital Signatures and Elliptic Curve Cryptography

Steve Gottwals

Symantec's view on the current state of ECC

Rick Andrews

Efficient ephemeral elliptic curve cryptographic keys

Arjen Lenstra, Andrea Miele

Ed448-Goldilocks, a new elliptic curve

Mike Hamburg

Vehicle to Vehicle Safety Application using Elliptic Curve PKI

Bill Anderson, William Whyte

Elliptic Curves: A Hardware Perspective

Joppe Bos

Requirements for Elliptic Curves for High-Assurance Applications

Manfred Lochter, Johannes Merkle, Jörn-Marc Schmidt, Torsten Schütze

Diversity and Transparency for ECC

Jean-Pierre Flori, Jérôme Plût, Jean-René Reinhard, Martin Ekerå

A random zoo: sloth, unicorn, and trx

Arjen Lenstra, Benjamin Wesolowski

FourQ: four dimensional decompositions on a Q-curve over the Mersenne prime

Craig Costello, Patrick Longa

An Efficient Certificate Format for ECC

Warwick Ford, Yuri Poeluev

A brief discussion on selecting new elliptic curves

Craig Costello, Patrick Longa, Michael Naehrig

Curve41417: fast, highly secure and implementation-friendly curve

Daniel Bernstein, Chitchanok Chuengsatiansup, Tanja Lange

Simplicity

Daniel Bernstein, Tanja Lange

Fastest Curve25519 Implementation Ever

Tung Chou

Efficient and Secure Elliptic Curve Cryptography Implementation of Curve P-256

Mehmet Adalier

An Analysis of High-Performance Primes at High-Security Levels

Craig Costello, Patrick Longa

Efficient Side-Channel Attacks on Scalar Blinding on Elliptic Curves with Special Structure

Werner Schindler, Andreas Wiemers