TEPLA:
New C Library for Pairing-based Cryptosystems

Akira Kanaoka
(Univ. of Tsukuba, Japan)
Pairing-based Cryptosystems using $\eta_T$ pairing over $\text{GF}(3^{97})$ are broken.
Who was shot?
We were shot.
We were shot.
“Are you all right?”
We study...

Pairing Primitives
Fast Impl. on SW/HW
Framework of IBE/ABE/...
Framework of IBE/ABE/...
Interoperability

Middleware
Pairing Library

not just

Pairing Implementation
PBC
The Pairing-Based Cryptography Library
Diversity
University of Tsukuba Elliptic Curve and Pairing Library
TEPLA: Overview

- C Library
- Open Source
  - under BSD License
- Can be used in various platforms
  - Windows (Visual C++, MinGW)
  - Linux (gcc)
  - Mac OS X (gcc)
TEPLA: Functions

- Finite Field Arithmetic with 254-bit prime number:
  - addition, subtraction, multiplication, inversion, square, square root, exponentiation, frobenius map, random element
TEPLA: Functions

• Elliptic Curve Arithmetic on BN (Barreto-Naehrig) Curve:
  – addition, scalar multiplication, frobenius map, random point, map to point (mapping “ID” data to a point over the curve)
TEPLA: Functions

• Pairing Arithmetic using Optimal Ate Pairing over BN Curve

\[ \text{parameter } t = 2^{63} - 2^{54} + 2^{44} \]
Performance of TEPLA: Pairing

![Graph showing the relationship between Dlog security (bits) and Average Pairing Time (ms) for different pairing methods in TEPLA.]
Performance of TEPLA: Scalar Multiplication

![Graph showing performance comparison]

- pbc (a)
- pbc (d)
- pbc (e)
- pbc (f)
- pbc (g149)
- TEPLA (bn254)

---

[Logo: University of Tsukuba]
Release Date

• **January 22, 2013**
  – C Library
  – Documents: Specification, How to install
    • written in English and Japanese

http://www.cipher.risk.tsukuba.ac.jp/tepla/