
TEPLA: New C Library for Pairing-based Cryptosystems

Akira Kanaoka
(Univ. of Tsukuba, Japan)

Pairing-based Cryptosystems using

ηT pairing over $\text{GF}(3^{97})$

are broken.



Who was shot?





A large, intense fire dominates the background, with multiple bright orange and yellow flames rising from the ground. In the foreground, two small aircraft are visible on the ground. One is a red and white biplane, and the other is a grey jet-like plane. In the bottom left corner, three people are sitting on the ground, watching the fire. The sky above the fire is dark.

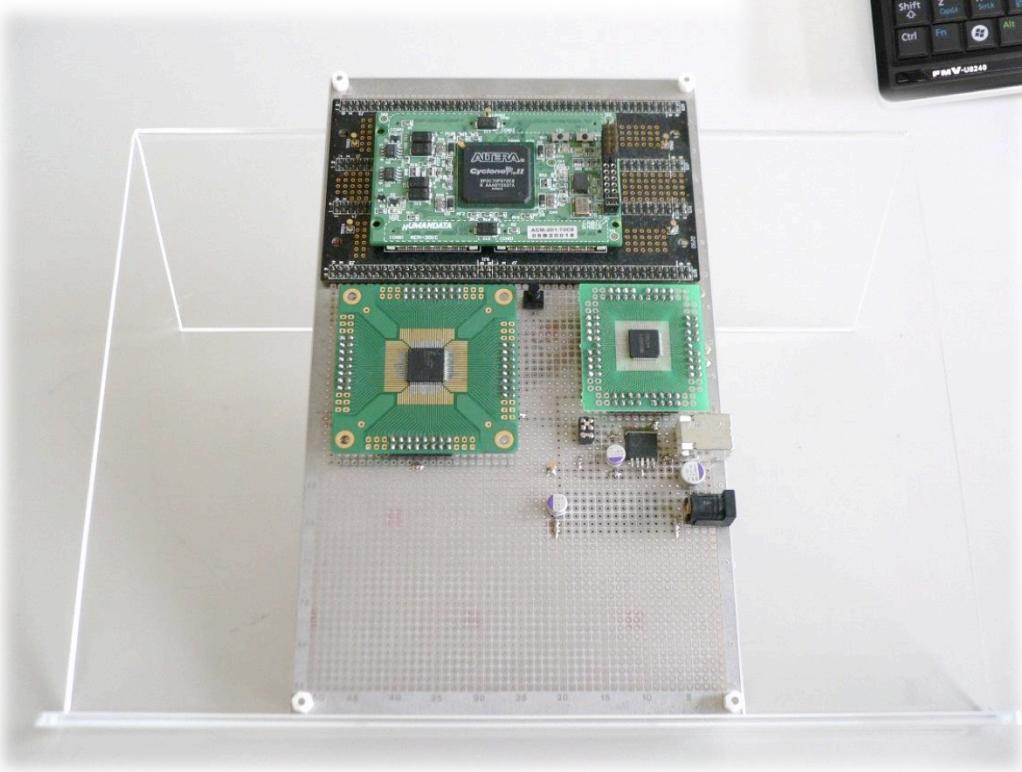
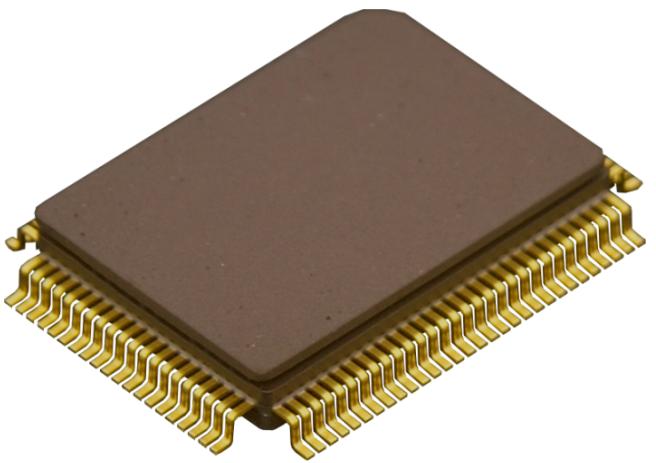
We were shot.





We were shot.





“Are you all right?”



DIE HARD

We study ...

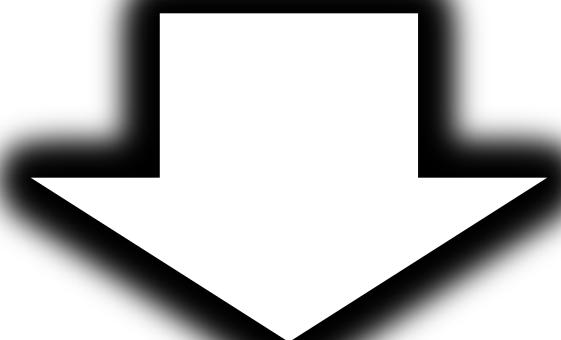
Pairing Primitives

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

TEPLA

University of Tsukuba **E**lliptic
Curve and **P**airing **L**ibrary

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

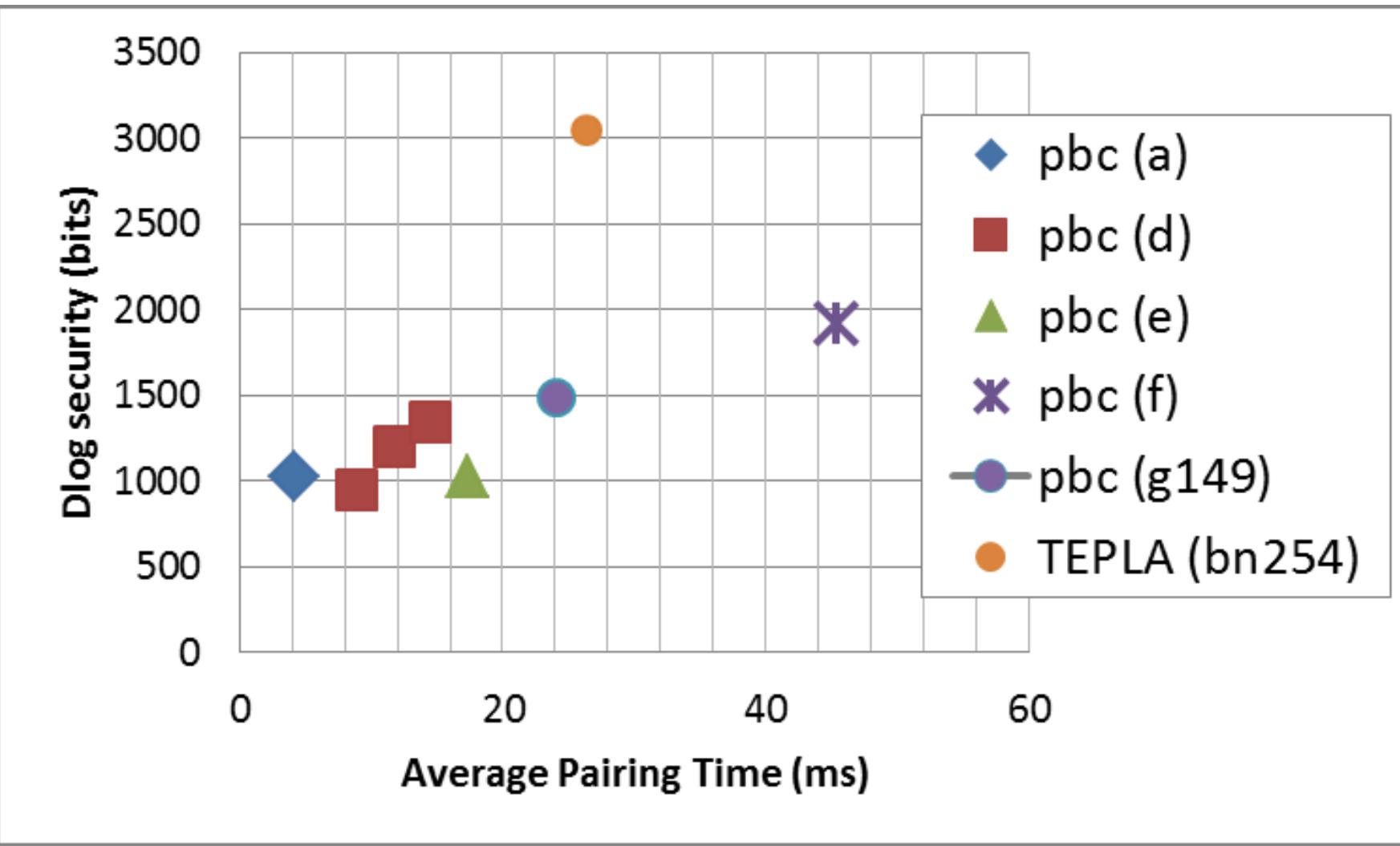
- **Elliptic Curve Arithmetic
on BN (Barreto-Naehrig)
Curve:**
 - addition, scalar multiplication,
frobenius map, random point,
map to point (mapping “ID”
data to a point over the curve)

TEPLA: Functions

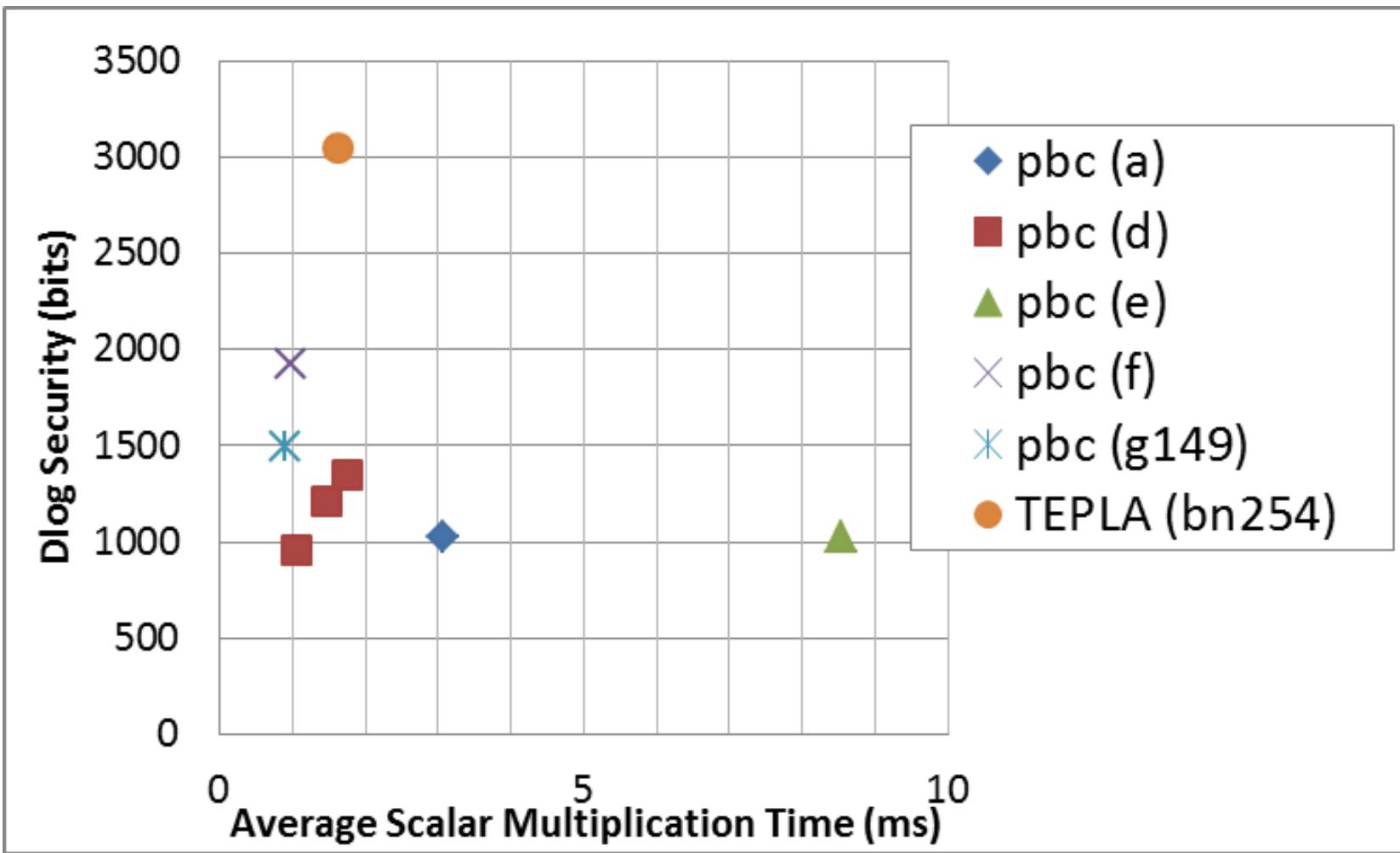
- **Pairing Arithmetic using
Optimal Ate Pairing
over BN Curve**

parameter $t = 2^{63} - 2^{54} + 2^{44}$

Performance of TEPLA: Pairing



Performance of TEPLA: Scalar Multiplication



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/>