

セキュリティパラダイムの革命 -ペアリング暗号

Revolution of Security Technology - Pairing Based CryptoSystems

氏名
Name野田坂 祥史
Nodasaka Shoji
久岡 直史
Hisaoka Naofumi藤田 真可
Fujita Manaka
丹羽 弘和
Niwa Hirokazu中西 真起子
Nakanishi Makiko
宮崎 行規
Miyazaki Yukinori本間 匠
Honma Takumi
宮本 義弘
Miyamoto Yoshihiro伊藤 拓也
Ito Takuya
古林 靖規
Kobayashi Yasunori真田 淳史
Sanada Atsushi
佐々木 勇太
Sasaki Yuta

活動

Actibity

April

みんなが会い、
これからの1年について話し合う。
We talk about one year
of the future.

May

数学の基礎を固める。

I learned a base of mathematics.

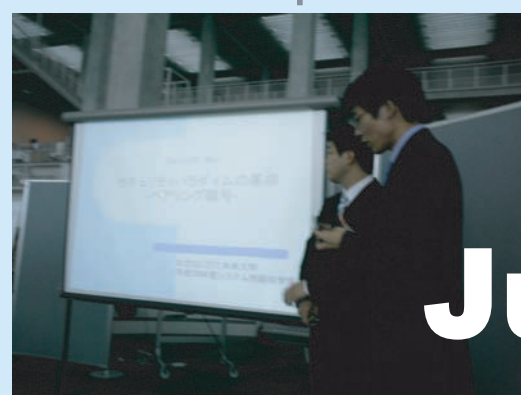
有限体班、拡大体班、楕円曲線班
に分かれる。

We made Finite Field Group, Extension
Field Group and Elliptic Curve Group.

June

基本プログラムの実装、改良
Implementation and improvement
of a basic
program.

中間発表
(7/21)



July

August

夏休み SUMMER VACATION

英語論文を読む

We read an English article
about application.

September

後期のグループに分かれる。
(墨塗り署名、透かし暗号、
タイムカプセル署名)

We made three Group.

October

プログラムの実装とアプリ作成。
Implementation of program
and make application.

November

アプリ完成、シュミレーション。
We complete application and test.

最終発表

Final Presentation

December

概要

Outline

ペアリング暗号とは公開鍵暗号の一種である。ペアリングと
いう演算を用いたこの暗号方式は従来では実現不可能であった
様々な技術が実装できる。
私たちは、ペアリングを用いたアプリケーションの作成を行った。

Paring Based CryptoSystems is one of the Public Key Cryptosystem.
This Encryption using Pairing can implement the various technologies
that were not able to achieve conventionally.
We made an application with Pairing.



ペアリング Pairing

楕円曲線に点P, 点Qをとって、 $e(P, Q)$ とする。
P点のa倍点のaP, Q点のb倍点のbQに対して、
写像を行った時、

$$e(aP, bQ) = e(P, Q)^{ab} = e(bP, aQ)$$

となる性質。

成果

Result

墨塗り署名

A Sanitize Signature

署名の指定単語に墨を塗ることができ、
さらにその状態で署名を検証することができる。

We can sanitize appointment word of signature.
Furthermore, we are verifiable the signature
in the state.



透かし暗号

Keyword Search

ファイルを暗号化して、復号化
せずにファイル名を検索できる。

We can search a coded file name
without decoding.



タイムカプセル署名

Time Capsule
Signature

暗号化するときに解除時刻を指定する
ことができる。

また、署名を検証することができる。

To do encryption, if it can't elapse of the time
which it assigns defeasibletime, it can't verify signing.

