担当教員　高木　剛 Takagi Tsuyoshi
宮本　衛市 Miyamoto Eiichi
小西　修 Konishi Osamu

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

加藤　陽介 Yosuke Kato
西山　孝輔 Kosuke Nishiyama
佐々木　廉 Ren Sasaki
田中　良彰 Yoshiaki Tanaka
中村　太 Futoshi Nakamura
坂本　恭一 Kyoichi Sakamoto
北村　晃輔 Kosuke Kitamura
井山　政志 Tadashi Iyama
早坂　健一郎 Kenichiro Hayasaka
青野　光 Hikaru Aono

概要

現代も発展し続けるネットワーク。セキュリティもそれと同等に発展を求められている。
我々のプロジェクトは、２０００年に開発された公開鍵暗号方式の一つである『ペアリング暗号』を学び、ペアリング暗号によって可能になった技術を用いアプリケーション作製を行う。

The Internet continue to develop. At the same time, security must continue to develop.In our project, we study pairing based cryptosystems developed in 2000 and is a sort of public key cryptosystems. And using new technologies are available by pairing based cryptsystems, we create application.

ペアリングとは

ペアリングとは２入力１出力関数のことである。
楕円曲線の写像による性質より次の式が成立する。

Pairing is a function have two input and one output.
By bilinearity, following mathematical expression is true.

２つの点 ＰとＱを代入
We substitute two points P and Q.

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

RSA など、他の暗号方式では困難であったことが容易に実現することが出来る。我々は３つのグループに別れ、それぞれにアプリケーションを作製した。

By using pairing based cryptosystems, It is possible to achieve existing difficulties.We divide into three groups, create application.

完成した三つのアプリケーション

Sniffer Dog

秘密鍵を不正に複製した人物を特定でき、さらにその不正な復号鍵の効力を無効にできる。

This application can identify the traitor makes an unauthorized copy of private key, and can expire it.

The Kis

秘密鍵を更新していくことで安全性が飛躍的に高まった電子署名を行うことができる。

Thanks to update of sercret key, we can use high- security digital signature.

ＵＰ太

ある人が復号化できる権利を他の人に譲渡することで、その人と暗号化された状態のままデータ共有ができる。

The Application is Aploder with Proxy Re-encryption Systems. It can share data.

年間スケジュール

April	May	June	July	August
プロジェクト開始 Project started.	有限体、拡大体、楕円曲線の班に分かれて活動 We made 3 groups and started works.	ペアリング班活動開始 We made the pairing cryptosystem group and started works.	中間報告 We got midterm presentation	不正利用者追跡暗号、鍵隔離署名、プロキシ再暗号化班に別れ自主活動 We made 3 groups and started works.
September	**October**	**November**	**December**	**January**
英論文を読む We read an E nglish article about application.	アプリケーションの構想を練る We devloped ideas.	プログラムの実装 We ran programs. アプリケーション完成 We achieved applications.	最終報告 We got final presentation.	報告書作成 We made final report.