セキュリティパラダイムの革命 ーペアリング暗号ー

Revolution of security paradigm -pairing encrypt system-

ブロードキャスト暗号班：石黒 司 小松 康平
Broadcast cryptosystem group: Ishiguro Tsukasa Komatsu Kouhei

概要 Outline

Dan Boneh, Craig Gentry, Brent Watersによって2005年に提案された、ペアリングを用いたブロードキャスト暗号を実装し、それを用いた応用アプリケーションをC++を用いて開発する。
また、この暗号方式の実装は本プロジェクトが初めてである。

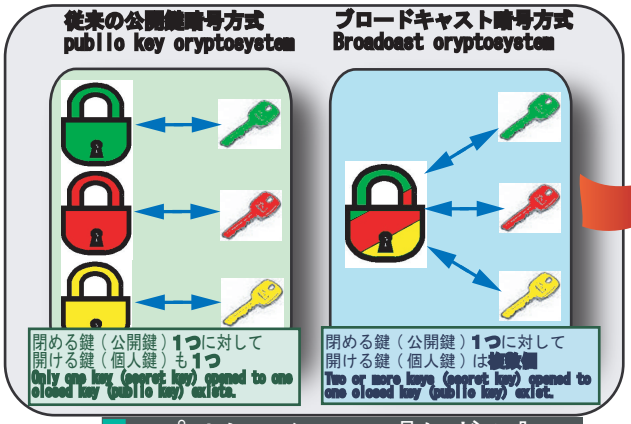
We implement broadcast cryptosystem that uses the pairing. It's proposed by Dan Boneh, Craig Gentry and Brent Waters in 2005.
This project is the first time in implementation this cryptosystem.

ブロードキャスト暗号とは

What is the broadcast encrypt system?

従来の公開鍵暗号方式と違い、閉める鍵（公開鍵）１つに対して複数個の開ける鍵（個人鍵）を割り当てることができる。この性質によって鍵管理が楽などの利点が得られる。

This is different from the public key cryptosystem used so far. It can allocate two or more opened keys (private key) to one closed key (public key). There is an advantage such as becoming of it easiness to manage the key by this character.



・受信者の数によらず公開鍵が１つで良いため鍵管理が楽。
・暗号化したデータも１つで良く、保存する容量が少なくて済む。
・どの個人鍵によって復号化可能にするか簡単に限定できる。
・ペアリングを利用しているため、個人鍵の長さが短い。

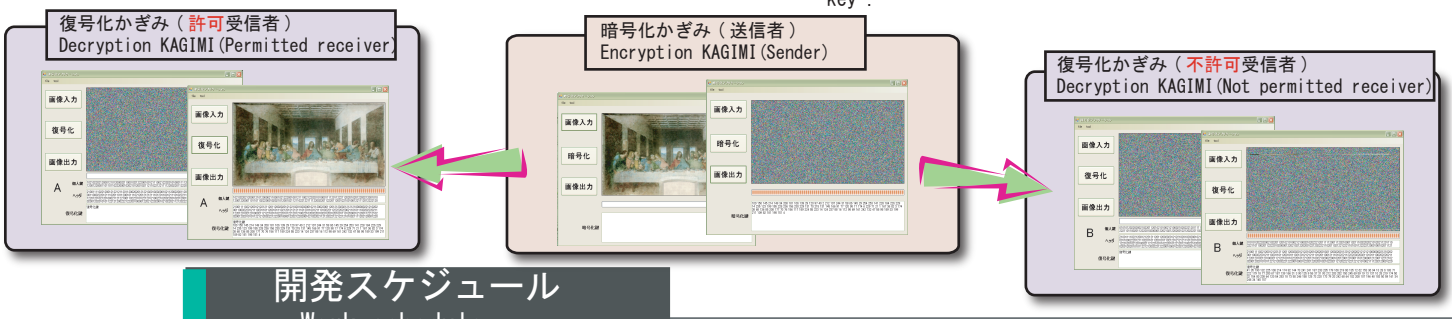
・Because it doesn't depend on the number of addressees and the public key is unnecessary only by one, the key management is easy.
・The encrypted data can be unnecessary only by one, and the preserved capacity be a little.
・We can easily specify whether to make the data can decrypted by which individual key.
・Because the pairing is used, the length of an individual key is short.

アプリケーション『かぎみ』

Application “KAGIMI”

応用アプリケーションとして、画像を安全にコンテンツ配信できるアプリケーション『かぎみ』を開発した。この『かぎみ』を使い、１つの暗号化したデータだけを作れば、そのデータは複数の個人鍵で復号化できる。『かぎみ』の名前は、「限られた受信者のみが鍵を使って画像を見ることができる」という性質からきている。

We developed the application 'KAGIMI' as application. It can safely send the image data. If we use this 'KAGIMI', and we make only one encrypted data, it can be decrypted with two or more individual keys. The name of 'KAGIMI' comes from the character "Only the limited addressee can see the image with a key".



開発スケジュール

Work schedule

前期の活動
Work at the first term

楕円曲線上のペアリングを計算するプログラムの作成
Making of program that calculates pairing on elliptic curve.

4～7月

後期の活動 Work at latter term

8,9月	10月	11月	12月	1月
・ブロードキャスト暗号についての論文を読み個人学習 ・The thesis of the broadcast code was read.	・鍵生成部分（C言語）プログラミング ・Programming in the C language as for the key generation part.	・応用アプリケーション設計 ・アプリケーション（C++）プログラミング ・Applied application design. ・Programming in the C++ language as for the application.	・最終発表会準備 ・報告書作成 ・Preparation of the final symposium.	・Write a report.

感想・考察

Impression and consideration

石黒 司（担当：基本アルゴリズム、応用アプリケーション、ポスター）
２人という少人数での開発ということもあり、妥協しなければいけないことも沢山あったが、それでも一つのアプリケーションを開発できたのは良い経験になった。
There were a lot of things that had to compromise because it was development by the few members. Still, being able to develop one application became a good experience for me.

小松 康平（担当：基本アルゴリズム、応用アプリケーション、パワーポイント）
私はこれが初の実装であることにやりがいを感じた。そして成し遂げることができたことを大変うれしく思う。
As for me, putting felt that it was in the first mounting this. And, I think accomplishing to be a very glad.