高木　剛/Takagi Tsuyosi
宮本衛市/Miyamoto Eiiti
小西　修/Konisi Osamu

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 Technology - Pairing Based CryptoSystems

鈴木 康広 / Suzuki Yasuhiro　仁科 五月 / Nisina Satuki　山端 亮輔 / Yamahata Ryousuke　鳴海 寛之 / Narumi Hiroyuki　石黒 司 / Ishiguro Tsukasa
片山 貴充 / Katayama Takamitsu　林 卓也 / Hayasi Takuya　阿部 勇介 / Abe Yusuke　能戸 幸雄 / Noto Yukio　小松 康平 / Komatu Kouhei　信田 寿広 / Nobuta Tosihiro

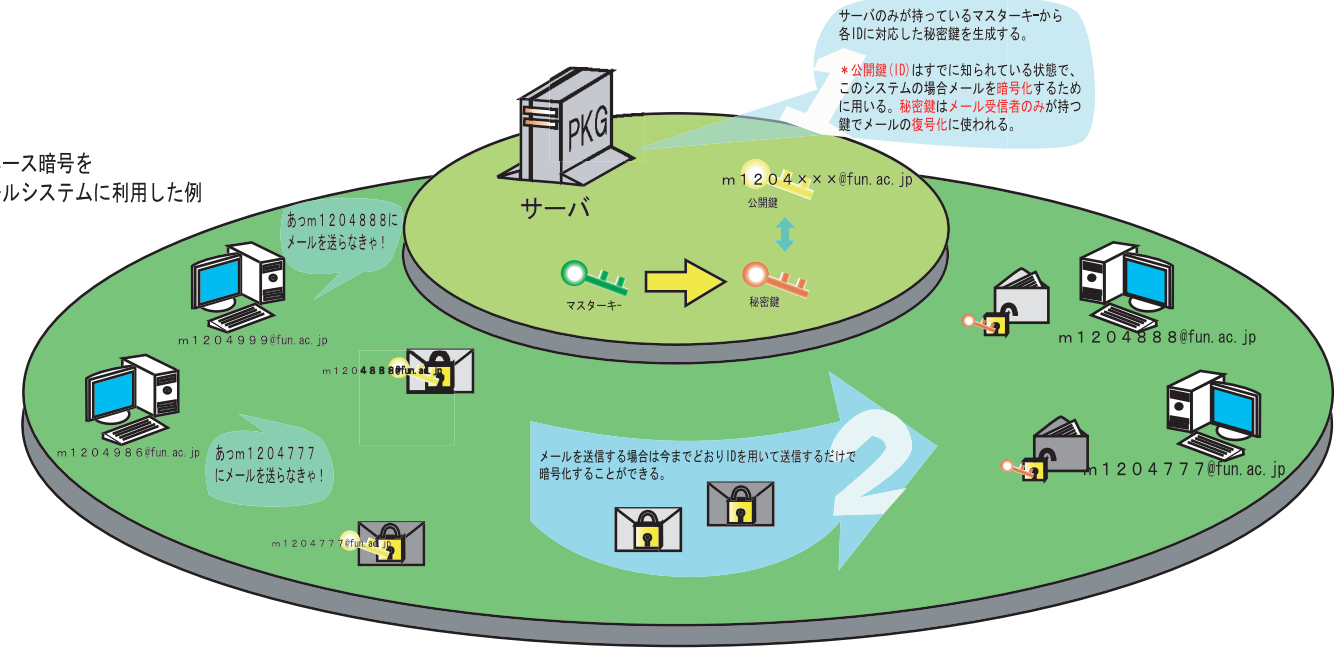
IDベース暗号プログラム概要

Identity-Based Crypto Program Outline

IDを公開鍵として用いることのできるIDベース暗号の実装に成功しました。暗号？と言われても、なんだかよくわからない世界ですよね。実際、暗号には複雑な計算をたくさん用いています。しかし、今回私たちが開発した「IDベース暗号」は企業から学校まで幅広い分野で応用可能です。従来使われてきた暗号に代わって使われる次世代の暗号となるでしょう。

We succeeded implementing of identity-based crypto system to be able to use ID public key. We think if you listen to crypto system many of man can't understand. In fact, crypto system use many complex caluculation. But, "identity-based crypto system" was devloped us can apply wide range of area from business organization to school. This system will be crypto system of following generation instead of crypto system of heretofore.

IDベース暗号を
メールシステムに利用した例



IDベース暗号を用いる利点として
・公開鍵の証明が必要ないことや、証明にかかる費用(年１００万円程度)の削減も可能です。
・IDを公開鍵として利用することができるので、広く一般に普及させることができます。

advantage to using identity-based crypto system
・This system is unnecessity authentication of public key and can cut down authentication of cost(This cost is about one million yen of year).
・As we can use ID public key, it will spreads widley in the generality.

従来のRSA暗号を
メールシステムに利用した例