情報通信研究機構

NICT 先端研究 ⑮

効率的な暗号技術 構成に成功

サイバーセキュリティ研究所・セキュリティ基盤研究室主任研究員 大久保 美也子

NTTから2010年4月に入所。暗号アルゴリズム・暗号プロトコルの研究に従事。00年暗号と情報セキュリティシンポジウム論文賞受賞。15年市村学術賞功績賞受賞。12―13年スイス連邦工科大学（EPFL）滞在。博士（工学）。

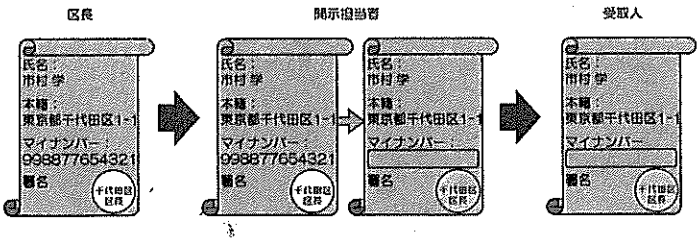
ほとんどの情報システムはさまざまな暗号技術を接続して構成される。一方、おのおのの暗号技術は、従来、それぞれ単体で安全であるように設計されており、入出力の形態（データ形式）も異なる。このインターフェースの不一致が暗号技術の相互接続を困難にしており、開発コストの増大、現実的でない安全性仮定の導入、さらには複雑なミドルウエアの挿入による脆弱性をもたらす。

この研究では、おのおのの暗号技術のインターフェースを統一（数学的構造としてペアリング群の要素で統一）した新たな設計コンセプト「群構造維持（Structure—Preserving：SP）暗号系」を提唱し、それに基づくSPディジタル署名をはじめとするさまざまな暗号技術を開発した。本質的に新しい研究課題が生じた。本研究では、ペアリングが持つ一方向性を統一された群要素のみで利用できるよう工夫することで効率的なSP暗号技術を構成することに成功した。

SP暗号系では個々に応じて担当者が必要な部分のみを開示し、再度公印を付与することなく検証可能な証明書を発行する。

このシステムを従来の暗号技術で構成する場合、それぞれを接続するためのミドルウエアが必要となる。一方、SP暗号系の技術を用いれば直接接続が可能となり、単純な構造で比較的容易に開発が可能となる。

本研究で提唱している群構造維持暗号系は、安全で効率的な暗号システムの開発を容易にし、クラウドなどを活用した大規模な情報システムの安全な設計に資する技術である。（火曜日に掲載）



応用の一例として、部分的に開示可能な証明書を挙げる。さまざまな個人情報が含まれる公印付きの証明書が作成された後、申請者の要求