3.2.7　セキュリティ基盤グループ

中期計画期間全体

目　　標

公開鍵暗号、共通鍵暗号、暗号プロトコルの理論的な研究を行い、その成果を新しい提案として生かすとともに、電子政府システムの安全性を確保することに利用する。

目標を達成するための内容と方法

安全で安心な通信を実現するセキュリティ基盤技術の研究開発を行うことを課題とする。代数系とそのアルゴリズムについて理論的研究を行い、新しい数理原理に基づく公開鍵暗号・プロトコルを構成する。共通鍵暗号アルゴリズムの理論的解析と漏えい電磁波等のサイドチャネルを利用した攻撃の研究を行う。これらの理論的な研究において培った秘術を背景にして電子政府推奨暗号監視活動 (CRYPTREC) において主導的に支援を行う。漏えい電磁波セキュリティについてはセキュアネットワークグループ、EMC センターと協力して活動を進める。

特　　徴

新しい数理原理を利用した暗号プリミティブの理論的研究を推進し、新規の技術を構築する。また、暗号強度評価研究で培った技術力を最大限に利用して、セキュリティ評価や調査研究を公平・中立な立場で行い、電子政府システムのセキュリティ要素技術の安全性評価を行うことができる。暗号・認証技術の安全性評価研究や漏えい電磁波セキュリティの研究など民間や大学で研究することが困難であることに積極的に取り組むことは、NICT で取り扱う課題としてふさわしい。

今年度の計画及び報告

今年度の計画

新しい数理原理に安全性の根拠を持つ暗号要素技術及び高機能暗号プロトコルの開発を目指し、代数系のアルゴリズム (特に Lattice) とそれを応用した暗号について理論的研究を行う。一方で、暗号アルゴリズム解析手法を発展させ既存の暗号アルゴリズムの解析に適用し安全性評価研究を行い電子政府暗号の評価に貢献する。また、物理的なエネルギー放射による情報漏えいの問題点を明らかにするために、電磁波の放射による暗号アルゴリズム解析手法を調査し、テンペスト攻撃対策として日本語テンペストフォントを設計・構築する。

今年度の成果

(1) 準同型暗号化関数に関する安全性について部分群メンバーシップ問題との関連を調べ、多くの準同型暗号化関数の安全性を解明し、効率的な暗号プロトコルを構成した。また、順序構造が導入されたグラフ上の偏作用とそれに対応する代数系の構造を逆半群表示の形で特徴付け、代数系の新しい知見を得ることができた。
(2) ブロック暗号の鍵スケジュールまで含めて解析し、高階差分攻撃を拡張してブロック暗号 Misty1 の安全性評価を行った。また、代数的解読方法の一つと考えられる線形化攻撃を提案し、LFSR を複数個組み合わせた非線形コンバイナ型擬似乱数生成器に対して適用することにより、ストリーム暗号の強度評価に応用した。
(3) パスワード認証型鍵共有システムについて調査を行い、新しい利用方法について検討した。
(4) 暗号プロトコルの形式的手法 (特に Spi 計算) について調査を行った。
(5) ソフトウェア的 TEMPEST 対策技術である Tempest fonts について傍受実験 (図 1) を行い、その有効性と限界を評価し技術的問題点を明らかにした。さらにその弱点を克服する方法について提案した (図 2)。外部展示、掲載記事を通して漏えい電磁波セキュリティの問題点を広く一般に紹介した。
(6)2004 年夏以降に相次いで発見された幾つかのハッシュ関数の問題点について、監視委員会暗号利用モードワーキンググループ (CRYPTREC) において主導的に調査を行った。

図 1　Tempest 傍受実験

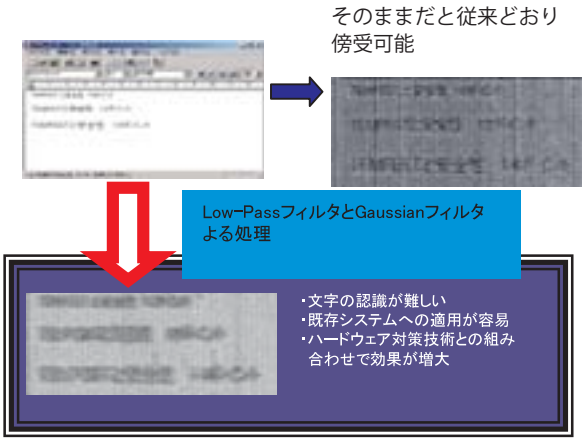

図 2　Tempest fonts