3.2.7　情報通信部門　セキュリティ基盤グループ

グループリーダー　山村明弘　ほか4名

情報通信危機管理基盤技術の研究開発

概　要

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。

(1)　暗号理論と代数系：新しい原理(ラティス等)に安全性の根拠を持つ暗号技術の提案を目指す。また、代数系とそのアルゴリズムについて研究を進め、セキュリティ技術への応用を目指す。数論的アルゴリズムについて通信複雑性の視点から調査する。

(2)　暗号プロトコルの設計・安全性検証：パスワードベースの認証手法を暗号プロトコルへ応用する。ハッシュ関数の暗号プロトコル(タイムスタンプ等)への影響を調査する。形式的手法による暗号プロトコルの検証を行い、カテゴリ論的方法により暗号プロトコルをモデル化する。

(3)　暗号技術の解析手法：ブロック暗号、ストリーム暗号とハッシュ関数の評価手法及び乱数検定法を提案し、暗号技術の応用システムの構成に利用する。

(4)　漏えい電磁波による情報セキュリティへの脅威とその対策：漏えい電磁波による画面情報又は打鍵情報の再現に関して、観測信号から情報を再現するプロセスを解析し、漏えい信号と再現情報の対応から情報漏えい問題を検討する。また、電磁波による情報漏えい対策として、ソフトウェア的な対策技術を提案・開発する。

(5)　CRYPTREC活動を通して電子政府暗号への貢献：電子政府推奨リストに掲載の暗号技術の安全性に関する監視活動を行い、署名・認証技術調査ワーキンググループ及びハッシュ関数・暗号利用モード調査ワーキンググループを運営し、ハッシュ関数の動向に対応して、電子署名法の指針の改訂といった対応を行う。

平成17年度の成果

(1)　準同形暗号化関数と部分群メンバーシップ問題について理論的研究を行い国際学会で発表した。代数系とそのアルゴリズムについては国際学会で発表し、代数系の応用についても論文を発表した。

(2)　平成17年度は匿名パスワード認証型グループ鍵交換(APAKE)スキームの概念を提案し、その実現手法としてプロトタイプを設計した。さらにその安全性概念を定義し、プロトタイプがその安全性を持っていることを証明した。APAKEの概念は世界で初めてNICTが提案した概念であり、既存のパスワード認証型鍵共有スキーム(PAKE)により高度な機能を付け加えた暗号プロトコルとなっている(図1)。形式的体系の意味論に関するカテゴリ論的構成について研究を行い国際会議で発表した。

(3)　認証型鍵共有手法における安全性について国内研究集会にて発表した。共通鍵暗号技術の安全性評価に関する論文、ハッシュ関数を利用した量子暗号の誤り訂正手法に関する論文を発表し、講演も行った。ハッシュ関数を利用した量子暗号の誤り訂正手法の特許が登録(韓国)された。

(4)　電磁波セキュリティの一問題であるPCからの雑音放出によるモニタ表示画像情報の漏えいに関しては、従来のアンテナや無線周波受信機を用いた画像再現手法に代わり、電流プローブとデジタルオシロスコープを利用した新しい画像再現手法を提案した。本提案手法は、従来手法では判断できなかった雑音中の情報含有率を定量的に評価することが可能であり、コストパフォーマンスにも優れている。また、電磁波による情報漏えいの脅威を啓発するため、PCモニタ表示画像情報の漏えいを視認可能な簡易型装置を市販の無線周波受信機及びモノポールアンテナを用いて構成し、展示会に出展してデモンストレーションを行った(図2)。

(5)　ハッシュ関数の安全性の評価について議論し、「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」における「特定認証業務に係る電子署名の基準」等について改正案を作成した。

図1

簡易型画面傍受装置

図2