3.7.3　情報通信セキュリティ研究センター　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9名

セキュリティ基盤技術(暗号プリミティブ、暗号プロトコル)の評価手法・設計手法及び電磁波・情報セキュリティとサイドチャネル攻撃にかかわる研究開発

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。

⑴　暗号理論と代数系：安全性の根拠を新しい原理(ラティス等)に置く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。

⑵　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、暗号アルゴリズムの理論的解析手法を開発する。

⑶　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。

⑷　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：漏えい電磁波に含まれる情報の評価手法を確立する。これを国際標準(ITU-T)に提案し、対策手法等の研究開発成果を民間に技術移転する。

⑸　CRYPTREC活動による電子政府暗号への貢献：電子政府推奨暗号リストに掲載されている暗号技術の安全性に関する監視活動を行い、暗号技術監視委員会及び技術調査ワーキンググループを運営し、電子政府システムへの政策的アドバイスを行う。

平成19年度の成果

⑴　暗号理論と代数系

準同型暗号化関数の応用として、巡回群の直和構造を利用した、新しい準同型暗号化関数を提案し、電子投票システムに利用可能なn-暗号カウンターを構築した。国際学会発表1件を行った。

⑵　暗号プロトコルの設計・安全性検証

ペアリング(双線形写像)技術を利用した、他人への資格証明書譲渡を防止する匿名資格証明プロトコルを提案した。本方式は以下の機能を提供できる①資格証明書の他人への譲渡を防止。②資格検証時に検証者に対して匿名性を保証。③資格保有者のプライバシ(資格提示履歴など)を秘匿。④検証者を限定可能。⑤資格証明書を利用し特定の検証者と鍵共有が可能。本方式の応用として、利用者のプライバシを守る定額課金サービスへの利用が期待される。国際学会発表1件、特許出願1件、国内学会発表1件を行った。

また、利便性確保とプライバシ保護が両立可能であり、一般的な公開鍵基盤とIDベース暗号の両方の利点を合わせ持つCertificate-Based Proxy Cryptosystem with Revocabilityを提案した。Revocabilityは、代理人の権限が有効である期間であっても代理権を解除し、代理人を交代することができる機能を有する。国際学会発表1件を行った。

⑶　暗号技術の解析手法

解析対象を鍵拡大関数まで拡張した高階差分を用いた解析手法を提案した。本解析手法の特徴はブロック暗号の攻撃範囲を鍵拡大関数まで拡張した点にある。解析手法を64ビットブロック暗号MISTY1に適用し、解析結果としてはBest result（2007年現在)を示した。国際学会発表1件を行った。

線形化手法による線形複雑度の見積手法の提案を行った。既存手法と比較して計算量、データ量が小さいという特徴がある。学術論文発表1件を行った。

暗号プロトコルの安全性評価に定理自動証明手法を適用し、定理証明ツールによる形式的検証の実例を構成した。暗号プロトコルTLSを対象に、Paulsonの形式的モデルの定理証明支援ツールCoqへの移植を行い、安全性証明を行った。国際学会発表1件を行った。

⑷　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

漏えい電磁波に含まれる情報量の定量的評価指数に関して、通信路容量を利用した評価手法を提案し、測定実験により検証した。国際学会発表1件を行った。

PCモニタ表示文字の情報漏えい防止ソフトウェアを、株式会社ビヨンディットとの共同研究開発により

Microsoft Office Word上にプロトタイププログラムを実装した(図1参照)。リアルタイムで文字を表示可能であり、多国籍言語に対応可能である。関連特許を3件出願し、Microsoft Innovation Award（コマーシャル部門）2007 優秀賞を受賞した。

電磁雑音に含有する情報信号の測定方法を開発しITUへ貢献した。ITU-T SG5 課題15 “Draft of L.leakage: Test method and requirements against information leak through unintentional EM emission” に本研究で考案・開発した「電磁雑音に含有する情報信号の測定方法」を提案し、副ラポータとして審議の促進に寄与した。

(5)　CRYPTREC活動を通して電子政府暗号への貢献

内閣官房情報セキュリティセンター（NISC)、総務省、経済産業省及び情報処理推進機構と共同で、2013年の電子政府推奨暗号リストの改訂に向けて、新リスト作成(次期公募)に対する課題等についての検討を行った。

CRYPTRECでの調査・審議を踏まえ、NISC主催の「SHA-1等の安全性の低下等への対応に関する各府省庁連絡会」に対し、RSA1024ビット及びSHA-1の利用に関する政府統一的な方針について提言を行った。また、電子署名法を所管する総務省・法務省・経済産業省が開催した「電子署名及び認証業務に関する法律の施行状況に係る検討会」に対しても、同様の提言を行った。

「電子私書箱(仮称)による社会保障サービス等のIT化に関する検討会」に関しては、技術的課題である情報セキュリティを確保し、かつプライバシ保護を目的とした観点から検討した。現在想定できる社会保障関連の電子私書箱のサービスのみならず、将来の情報活用の様々な可能性を視野に入れた拡張性の高い仕組みを検討している。セキュリティ基盤グループにおける暗号・認証技術(特にシングルサインオンや認証プロトコル関連)の研究における知見を紹介し、審議に寄与した。

政府機関における安全な暗号利用の促進については、情報セキュリティ政策会議における、ハッシュ関数とRSA暗号の安全性の検討について、セキュリティ基盤グループが素因数分解問題の推定に関する知見などを提供することにより貢献した。

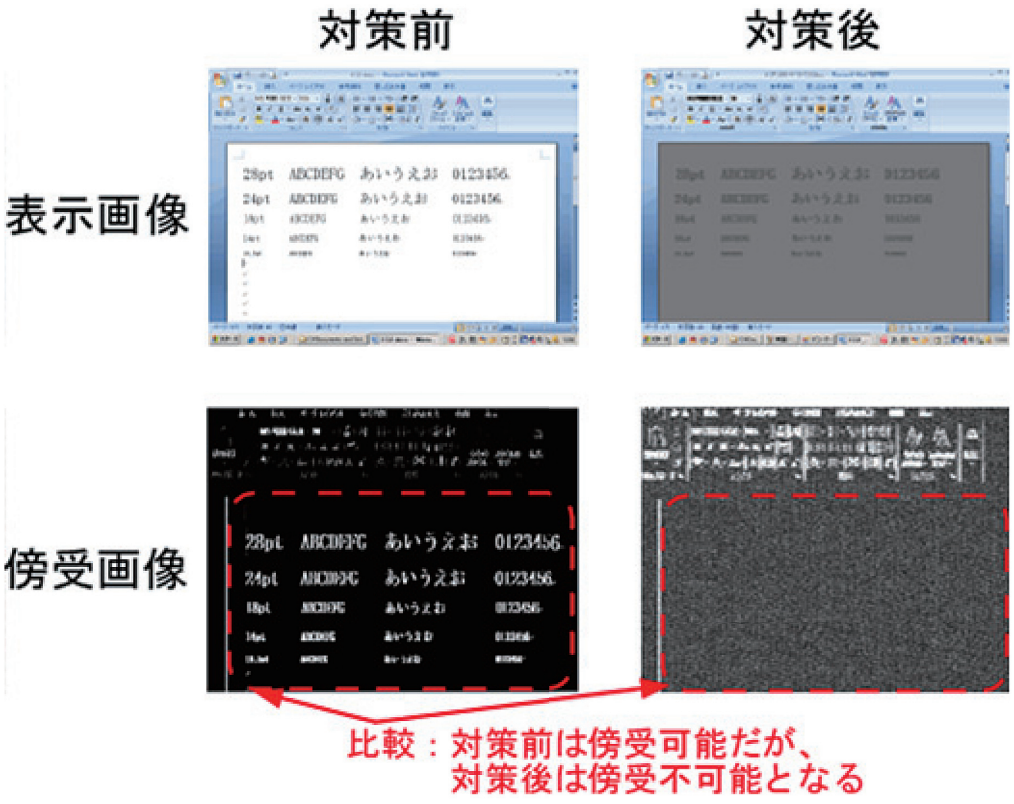

図1　情報漏えい防止ソフトウェア