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　　滝澤　修　ほか８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20年度の成果

⑴　暗号理論と代数系

「安全性が離散対数問題に依存する暗号プロトコルの強度評価に関する研究」に関して、公立大学法人はこだて未来大学システム情報科学部・情報アーキテクチャ学科高木剛教授との共同研究を開始した。

⑵　暗号プロトコルの設計・安全性検証

利用者のプライバシに配慮した資格認証方式をペアリング技術を用いて開発し、実システムへの応用を検討している。本方式は従来の方式と比較して、匿名での複数回の利用や利用履歴の秘匿を可能にし、資格を他人に譲渡することが不可能であるという特徴がある。さらに、公開鍵基盤とIDベース暗号の両方の利点を合わせ持つプロキシ暗号システムをペアリング技術を利用して構成した。これは代理人の権限が有効である期間であっても、代理人を交代することができるという機能を有する。平成20年11月には、国際交流プログラム海外個別招へい研究者として、上海交通大学曹珍富教授を招へいし、第二回国際暗号プロトコルワークショップを開催した。

量子暗号に関する共同研究を開始した。また、平成20年12月には、第二回国際量子暗号会議を開催した。フォトニックインターネットフォーラムのセキュリティ分科会と量子ICT運営委員会に参画し、量子暗号の標準化に貢献している。

⑶　暗号技術の解析手法

一般的な楕円曲線暗号を中心として、各種楕円曲線間の鍵長と強度の比較や、RSA暗号等他の暗号要素技術との強度比較をより精密に行った。この研究は、鍵長の寿命を予測することにより、鍵更新時期などの運用方針に役立てるとともに、複数の異なる暗号要素技術を組み合わせて使用するシステム等での強度バランスを明確にすることを目的としている。

暗号危殆化対策の一環として、安全性や利便性、危殆化対策に係るコスト低減を十分考慮しつつ、電子署名の更新及び暗号化データの再暗号化を可能とし、それらの有効性を継続的に保証するための技術を確立するための研究開発を行った。

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

IT機器へのサイドチャネル攻撃へのソフトウェア的対策手法の最適化についての研究に関し、PCからの電磁雑音の取得からモニタ表示画像再現に至る信号処理方法に関する定量的手法を提案した。ITU-T　SG5 Q15 “Security of telecommunication and information systems regarding electromagnetic environment”

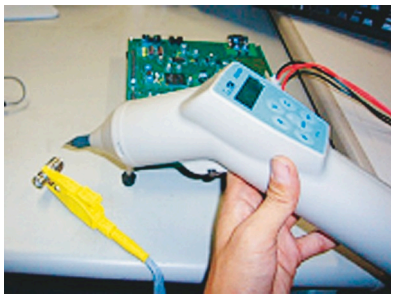
に副ラポータとして貢献した。

暗号が組込まれたICカードなどのモジュールに対して、電磁気的な回路の誤動作を利用した攻撃手法とその安全性評価手法を検討した。回路に外部から電磁気的信号を照射させるシステムを構成し、誤動作メカニズム及び回路内素子の故障メカニズムの解析を行った。暗号モジュールでは、外部からの電磁気的な攻撃に対してその暗号処理が正常に行われない、または処理信号の一部が改竄されても暗号処理が継続する可能性がある。このような誤動作（故障）を利用した故障利用攻撃の実行について検証した。

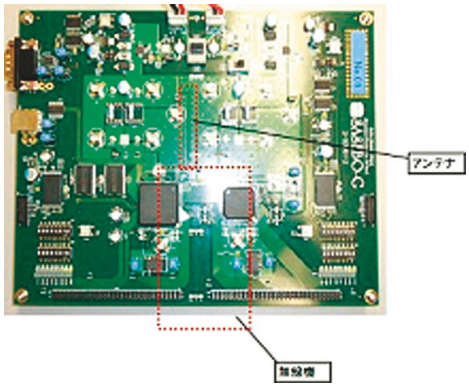
連続電磁妨害波照射によるネットワーク機器の誤動作電界強度（または注入電流値）を調査するとともに、試験方法における要素技術について検討を行った。インパルス電磁妨害照射実験システムの開発を行い、対策技術についての検討を行った。

PC等の電磁雑音に起因する情報漏洩や高出力電磁照射による通信妨害等の電磁環境に起因する情報セキュリティ脅威に対処するための技術調査を目的として、平成19年４月に電磁波・情報セキュリティ技術調査専門委員会を設立し運営を担当し、今年度は電磁波・情報セキュリティに関する技術調査報告書の作成を開始した。

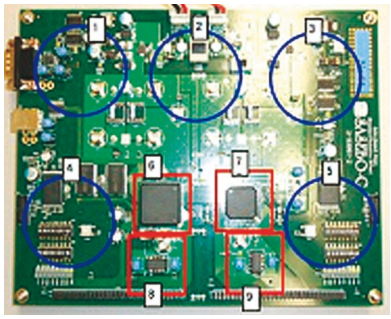
〈故障利用攻撃の電磁波照射装置〉



〈電磁波照射実験の対象（SASEBOボード）及び結果〉



a）リコンフィグが発生する電磁波照射位置



b）電磁波照射を行った位置

a）電磁波照射によりリコンフィグもしくはランダムな誤り発生が確認された。

b）この位置で誤り発生の観測を行った。最適な照射場所は４であることが実験的に確認された。

SASEBO：JCMVP認証を取得した暗号技術実装評価用FPGAボード。INSTAC-8準拠暗号技術実装評価ボードに加えて、今年度新たに実験対象とした。

⑸　CRYPTREC活動を通して電子政府暗号への貢献

新たにIDベース暗号調査ワーキンググループを発足し、IDベース暗号技術をはじめとするペアリング関連の技術について、電子政府推奨暗号リストへのカテゴリ追加を検討するための調査を開始した。今年度は、平成25年度に行われる電子政府推奨暗号リスト改訂に向けての第一歩を踏み出した。平成20年８月に「電子政推奨暗号リストの改訂に関する骨子（案）」に対する意見募集を実施し、平成21年２月には、「CRYPTRECシンポジウム2009～電子政府推奨暗号リスト改訂に向けて～」を開催した。半年に渡る審議の結果、暗号技術公募要項が確定し、平成21年10月から、128ビットブロック暗号、ストリーム暗号、メッセージ認証コード、暗号利用モード、エンティティ認証の五つのカテゴリにおいて、実際の公募が始まる。