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 11 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っている。

⑴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: 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は離散対数問題の解法を改良し計算機実験により強度評価を行う。

⑵コヒーレント光通信の通信路容量評価と量子秘匿変調方式の安全性評価手法: 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（データを固定長の文字列に変換する関数）の暗号プロトコル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に関しては ISO での標準化活動に寄与する。量子プロトコルに関して量子 ICT の観点からも研究を行い、通信路容量の評価なども行う。

⑶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。

⑷ CRYPTREC（Cryptography Research and Evaluation Committees の略であり、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト）活動による電子政府暗号への貢献: 暗号技術の安全性評価に関する研究を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評価へ昇華する。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 21 年度の成果

⑴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

多くの暗号プロトコルで利用されている公開鍵暗号は暗号文を作成するための公開鍵と暗号文を復号するための秘密鍵の 2 種類の鍵で構成されている。文字通り公開鍵は一般に公開し、秘密鍵はユーザのみが利用できる秘密の情報である。このように鍵に性格付けすることで暗号通信に必要な鍵の交換の手間が必要なくなり利便性が高まる。一方、自由に選んだ平文を公開鍵で暗号化し、得られた暗号文の組み合わせを解析することで秘密鍵が逆算される攻撃リスクが発生する。公開鍵暗号では秘密鍵を求めるための手段を数学的難問の解法と同等であることを証明することで安全性を保証している。良く知られている RSA 暗号は素因数分解問題と同等であることが示されており、その安全性は素因数のサイズによって評価される。

例えば 3 ケタの数字の素因数分解は簡単に計算できるが、300 ケタになるとかなり時間がかかる。そこで、現在知られている最も有効な解法と最速のコンピュータの組み合わせで解くことができるサイズよりも大きな値を利用することで十分な安全性を実現する。逆にいえば、現在どこまでのサイズを解くことができるかを確認することが、その暗号の強度評価や鍵サイズの適正値を考察するうえで重要なポイントとなる。

本研究では、離散対数問題に安全性が帰着されている公開鍵暗号に着目し、公立はこだて未来大学と共同研究を行った。その結果、18 台の計算機（Intel Xeon 96 コア）を用いて約 33 日間で、世界記録である 676 ビットのサイズの問題を解くことに成功した。これまでは、2005 年のフランス国防省とレンヌ数学研究所のグループにより計算した 613 ビットが世界記録であったが、これを上回ることに成功した。また、離散対数問題の解法は「多項式選択」、「関係探索」、「線形代数計算」、「離散対数計算」の 4 ステップからなるとともに、関係探索ステップを従来よりも 8 倍、線形代数計算を従来よりも 36 倍高速に行うことができる効果的なアルゴリズムを開発した。

⑵コヒーレント光通信の通信路容量評価と量子秘匿変調方式の安全性評価手法

コヒーレント光とはレーザー光のように波長と位相が揃っている光である。そのようなコヒーレント光を使った通信の代表的なものとして光ファイバ通信が挙げられる。当グループでは、コヒーレント光通信の研究

として主に 2 つのテーマに取り組んでいる。

位相変調（Phase Shift Keying: PSK）及び位相振幅変調（Quadrature Amplitude Modulation: QAM）において多値変調数と通信路容量の関係の評価を行った。これらは光ファイバの使用を前提として送信電力及び帯域幅の制限を与え、シャノン限界との比較をまとめたもので、その結果が国際論文誌 Optical Science of America B に採択された。本結果は利用状況に応じた多値変調数の設定を可能にするものである。

PSK 及び QAM の変調パラメータを秘密にすることで実現できる量子秘匿変調方式に関する安全性評価を行った。従来は共通鍵暗号方式の 1 手法であるストリーム暗号との比較により安全性の議論がなされてきた。本テーマでは、新たに共通鍵暗号方式の別手法であるブロック暗号の利用モードに対する安全性評価の視点を加え構造的な安全性評価を実施し、安全な構成を実現するための必要条件を導いた。

⑶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

電子機器はその動作時に必ず電磁波を放射する。電磁波の強さは人体への影響や他の電子機器の機能障害を起こさないように制限され、VCCI（情報処理装置等電波障害自主規制協議会）などにより認定されたものが製品として流通している。しかしながら微弱とはいえ電磁波は放射され、その電磁波は電子機器が内部で制御している情報に応じた放射をするため、情報セキュリティへの新たな脅威となっている。代表的な脅威の例として、モニタに表示されている文字や画像などが電磁波を傍受し処理を施すことで再現できる、TEMPEST が知られている。また、最近ではネットワーク機器やケーブルに電磁波を照射することで通信に誤りを発生させ、あたかも DoS 攻撃（サービス不能攻撃）を受けているような状況を作りだす脅威も考えられている。これまで当グループでは「放射電磁波から情報漏洩させないための規格及びその対策技術の評価手法」、「ネットワークインフラに対する電磁的脅威への対策手法」について研究を進めて来たが、平成 21 年度はこれらを標準化文書としてまとめ、ITU-T SG5Q.15“Security of telecommunication and information system regarding electromagnetic environment”において勧告案として提案し了承された。

・ITU-T K.78（HEMP 評価防護指針）勧告
・ITU-T K.78（HPEM 評価防護指針）勧告

これらの標準化作業に関し、アソシエイトラポータ（とりまとめ副責任者）としても貢献した。さらに特許を 2 件出願した。

⑷ CRYPTREC 活動による電子政府暗号への貢献

当グループでは暗号技術の安全性評価に関して、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の監視活動を担当することで公的機関としての役割を果たしている。電子政府推奨暗号リストは平成 25 年度に次期リストとして組み替えられることが決定しており、平成 21 年度は新たに策定された技術カテゴリを含めて以下に関する公募を行った。

・128 ビットブロック暗号
・ストリーム暗号
・暗号利用モード　　--- 新設カテゴリ
・メッセージ認証コード　--- 新設カテゴリ
・エンティティ認証　　--- 新設カテゴリ

平成 22 年度から具体的な安全性評価が開始され、アルゴリズム安全性が確認されたものに対して平成 23 年度にハードウェア及びソフトウェアの実装評価がなされる。当グループは応募暗号を管理する事務局としての運営も行いつつ、これらの安全性評価に貢献していく。

さらに ID ベース暗号や擬似乱数生成に関するリストガイドの整備を行った。ID ベース暗号は今後普及が見込まれる公開鍵暗号技術であり、特に電子政府用途を考えた場合のセキュリティ要件整理、評価手法整理と現状の安全性評価の実状、製品化及び標準化動向に関して調査を行った。

また、代表的な擬似乱数生成アルゴリズムに関して調査を行い、特に実装面での安全性に問題がないかの確認を行った。

CRYPTREC 活動に関してはホームページ（http://www.cryptrec.go.jp）から全ての報告書、応募暗号の仕様や評価書及び評価状況、今後の活動予定が公開され参照できる。