3.6.3　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　　田中秀磨　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った。

(1)　数学理論と数学的構造：離散対数に基づく加法準同型暗号に関する研究、ブレイド群など非可換群に基づく手法など耐量子計算機暗号技術に関する研究を行った。

(2)　暗号・認証プロトコルの設計と評価：省リソース機器向け認証プロトコル、墨塗りやメッセージ構造保持型など高機能署名技術の開発、ID ベース暗号や Proxy 型暗号技術を開発し暗号文を復号せずに内容を処理できる手法を開発した。

(3)　暗号技術の解析手法：米国で行われている次世代ハッシュ関数（SHA-3）選定プロジェクトに貢献した。また、量子暗号通信の評価のための基礎技術としてコヒーレント光通信の通信路容量の評価を行った。さらに量子秘匿変調方式の安全性評価に関する研究を行った。

(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情報漏えい対策（TEMPEST）に関しては ITU-T の標準化活動の継続のみを実施し、電磁波を用いた故障利用攻撃に関する研究を行った。

(5)　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した。また、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った。

【平成 22 年度の成果】

1　数学理論と数学的構造

【離散対数に基づく加法準同型暗号に関する研究】

Paillier の素因数分解に基づく加法準同型方式より効率が高い離散対数に基づく加法準同型暗号を提案した。

【耐量子計算機暗号技術に関する研究】

(1)　非可換代数構造に基づく暗号に関する研究

安全性が CSP（Conjugator Search Problem）問題に帰着できる非可換 Semi-group に基づく暗号プロトコルを提案した。Standard Model で IND-CPA/CCA 安全を満たすブレイド群に基づく新しい署名方式を提案した。既存の量子攻撃とブレイド群 CSP 仮説の関係を明らかにし、提案方式が既存量子攻撃に対して安全あることを示した。

(2)　多変数公開鍵暗号の安全性評価に必要な解読アルゴリズムの高速化

多変数公開鍵暗号の有力な解読方法にグレブナー基底攻撃がある。この攻撃では多変数多項式剰余環上の多項式演算を頻繁に行う。本研究ではこの演算コストを少なくする手法を提案した(攻撃アルゴリズムの向上)。この結果、安全性評価の効率を高めると共に適切なパラメータ選択を可能にした。

2　暗号・認証プロトコルの設計と評価

【省リソース機器向け認証プロトコルの研究】

計算能力とメモリの限られた RFID のようなデバイスで、セキュリティを確保しプライバシを保護する認証プロトコルを提案した。セキュリティに関してサイドチャネル攻撃をモデル化した Leakage-Resilient の性質を満たす世界初の方式である。

【メッセージの構造を保存したまま署名生成可能な署名方式】

署名とゼロ知識証明を組み合わせた匿名性を有する署名方式に関して、従来手法はメッセージ構造を保つことができないという問題があった。本研究では、ペアリング技術を導入することでこの欠点を解決し、メッセージの構造を保存したまま署名生成可能な署名方式を提案した。さらに、メッセージ構造を保ちつつ任意長の

メッセージに対する署名生成が可能な手法へ発展させた。

【スタンダードモデルで効率のよい墨塗り署名方式の研究】

公的機関での利用も見込まれる墨塗り署名において、これまでのランダムオラクルモデルと呼ばれる強い仮定を必要としないスタンダードモデルでありながら最小の署名長に抑えた方式の提案を行った。

【新たな署名技術に関する研究】

一般の署名は不特定多数が検証可能である。それ故に利害が衝突するようなケースでは、利用が適さない場合があり、これを解決するために検証者に制限を付ける必要がある。そのようなセキュリティ要件を満たす変換可能な否認不可署名を提案した。

【暗号プロトコル安全性評価手法の研究】

フォーマルメソッドを用いた暗号プロトコルの安全性評価の信頼性を保つフレームワークを確立した。このフレームワークについては、ISO/IEC JTC1 SC27/WG3 において、ISO29128（Verification of Cryptographic Protocols）のエディタとして標準化活動を実施した。

3　暗号技術の解析手法

【ハッシュ関数の評価基準の策定】

現在米国で行われている次世代ハッシュ関数の評価において、日本の電子政府用途における安全性及び実装性の評価基準を反映することを目的に、実際のシステムでの利用形態に応じた評価基準の導出を行った。

【コヒーレント光通信の通信路容量の評価】

コヒーレント光の変調法や測定法を設定し各種パラメータを与え、通信路容量の評価を行った。増幅器のない光ファイバーを使用した前提において帯域幅やコヒーレント光の変調法を与え通信路容量の評価を行った。本結果は量子通信を仮定した暗号通信において、機器性能が実現すべき性能、及び盗聴者が盗聴に成功する可能性を見積もるための基礎理論拡充へ応用していく。

【量子秘匿変調方式の安全性評価に関する研究】

光通信における位相変調方式を応用した秘匿通信方式（Y-00 など）に対する安全性評価を行った。従来のストリーム暗号に対する安全性評価だけでなく、暗号利用モードに対する評価手法を適用し、構造的な欠点と克服すべき課題についてまとめた。

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

暗号モジュール評価標準ボード（SASEBO）に対する電磁波を用いた故障利用攻撃に関する研究を行った。局所的に電磁波を照射し、メモリ内容を書き換える、信号線上のデータを書き換えることが可能かどうかの検証を行った。電磁波照射装置はアマチュア無線機、EMC 用サージ照射機、強電界照射装置を使用した。また、直接信号線に接続し過電圧をかけることでデータを書き換える専用装置を作成し、検証実験を行った。その結果、電磁波を使った場合は基盤上の特定照射位置ではデータの書き換えは容易に行えるが、任意のデータへの書き換えは不能であった。また、照射位置によっては電源部分を破壊してしまうことを明らかにした。専用装置では任意のデータへの書き換えが可能であり、例えば暗号モジュールに対する選択平文攻撃の脅威が現実的なものであることを明らかにした。

5　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た。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、そのために技術公募を行い応募された新提案技術の安全性評価を行った（128 ビットブロック暗号 2 件、ストリーム暗号 2 件、メッセージ認証コード 1 件、エンティティ認証 1 件）。その結果、128 ビットブロック暗号 1 件に対し、鍵が違うにも関わらず同じ暗号化処理をしてしまう等価鍵を発見したので、評価終了と判断した。また、エンティティ認証 1 件についても安全性不備のため、評価終了と判断した。残りの技術に関しては、ソフトウェア及びハードウェアの実装評価を平成 23 年度に行い、既存の推奨暗号技術との有意性を確認した上で、リストに掲載するか否かを判断する。