ICカード向け耐タンパーRSA暗号処理アルゴリズムの研究

東北学院大学工学部電気情報工学科　神永正博

[研究の背景・目的]

従来の磁気カードに代わり、JRのSuicaや、Mondex Moneyなどで、ICカードコンピュータが本格的に利用されるようになってきた。ICカードコンピュータは、個人情報や金額などといった重要な情報を格納するものであるが、ICチップにデータが密閉されているため、磁気ストライプカードに比べて高いセキュリティ性を持っている。

しかし、米国のセキュリティ研究者Kocherが発表した、ICチップ動作に伴う消費電力から内部情報を取り出す現実的な攻撃手法「消費電力解析」（参考文献[1]）が発表され、業界に衝撃を与えた。また、同じ頃、ケンブリッジ大学のAndersonらが、動作中に強制的に誤動作を引き起こして正常な結果と比較することにより、内部情報を取り出す「誤動作解析」に成功し（参考文献[2]）、これらの攻撃に対する対策技術（耐タンパー技術）が不可欠となった。本研究の目的は、電子マネーなどで用いられている代表的な公開鍵暗号であるRSA暗号に対し、既存の代表的な電流解析攻撃、誤動作解析攻撃に対する対策を実際のICカードに実装し、実際に既存の攻撃手法に対する耐性を、実験的に確認し、その安全性とコストの関係を明らかにすることである。

[研究の意義]

耐タンパー技術は、その必要性にも関わらず、従来の暗号理論では、重要視されていなかった「実装」に関わる技術である。耐タンパー技術に関しては、シミュレーションレベルで攻撃耐性の検討が行われることが多く、実験により、耐性を明らかにした研究は数少ない。問題の本質は、実装技術にあるため、シミュレーションによる検討は、セキュリティホールを残す可能性がある。特に、電子署名で用いられるRSA公開鍵暗号系に対する詳細な実験的検討は殆どなされていなかった。しかし、RSA暗号は、電子マネーや個人認証を支える重要なものであり、電子商取引の普及とともに、今後重要性を増すと考えられるものである。本研究では、このRSA暗号に対して、実装面からの安全性評価実験を行うことにより、実用上十分な安全性を確保するための実装コストを明らかにするものであり、実際にICカードシステムを構成する際に、重要な情報を与えると考えられる。

[研究内容]

本研究では、RSA暗号処理に関して、(1)中国人剰余定理を用いた高速実装、(2)中国人剰余定理を用いない実装、の二通りの場合について、電流解析攻撃、誤動作攻撃対策技術の提案、ICカードへの実装、セキュリティ評価を行った。(1), (2)は、セキュリティ上防衛すべきポイントが異なるが、両者の消費電力攻撃対策方法の骨子は、指数のランダム分割及び実行順序のランダム化、剰余乗算コプロセッサにおける処理データのランダム化である。(2)に対しては、秘密指数のプロテクト領域の局所化についても数学的な検討を行った。誤動作解析攻撃対策は、(1)につ

いては、モジュラスの冗長表現を利用し、(2)に対しては、指数のランダム化による再現性回避により行った。

セキュリティ評価には、(株) ルネサステクノロジ社製 IC カード用マイクロコントローラ AE45C を用いた。評価内容は、オシロスコープによる消費電力測定実験、任意波形生成装置による強制誤動作注入実験である。

[研究結果]

RSA 暗号の実装において、代表的な高速化手法として、中国人剰余定理を用いるものがある。この方式は高速であるが、素朴な実装方法に対して消費電力解析、誤動作解析の手法を用いた強力な攻撃方法が知られている。これに対する耐タンパー実装方式を研究発表論文[1]で検討した。結果、現在知られている主要な攻撃に対し安全性が確認された。全ての攻撃に対する対策コストは、従来見積もられていたものよりも大きく、外部クロック 3.57MHz 時に、約 2.4 倍の処理時間(173[ms])が必要なことが明らかになった。現在投稿中の[2]においては、中国人剰余定理を用いない実装に対し、[1]とは異なる対策技術（特許[1]）を実装し、その安全性を確認した。この際、プロテクト領域の局所化について、公開鍵指数が小さい場合は、秘密指数の上位ビットが数学的に計算可能であること、また、公開鍵指数の大きさと無関係に、下位ビットの特定領域の情報から多項式時間で秘密指数を復元できることを考慮し、防衛すべきプロテクト領域を明らかにした。また、従来知られていた入力のランダム化手法であるブラインド署名方式を改良し、ランダム化コストを従来の 1/10 以下に抑えることに成功した。又、外部クロック 3.57MHz 時の処理時間が、プロテクト領域のビット長 u に対し、2.4u+700[ms]であることを明らかにした。

[研究発表論文]

[1] 渡邊高志，神永正博，遠藤隆「中国人剰余定理を用いた耐タンパーRSA 暗号処理方式」，電子情報通信学会和文論文誌 Vol.J87-A, No.4 April 2004, pp 545

[2] 神永正博、渡邊高志、遠藤隆、大河内俊夫「RSA 暗号の電力解析法による攻撃とその対策」，電子情報通信学会和文論文誌に投稿中

[特許]

[1] Masahiro Kaminaga, Takashi Endo, Takashi Watanabe, Masaru Ohki, "Information processing device, information processing method and smartcard", United States Patent 6,666,381, December 23, 2003(Application Number 809214, March 16, 2001(Assignee: HITACHI Ltd.))

[参考文献]

[1] P.Kocher, J.Jaffe, and B.Jun, "Differential Power Analysis," Proc. of CRYPTO'99, LNCS1666, Springer-Verlag, pp.388-397, 1999.

[2]R Anderson, M.Kuhn, "Low cost Attacks on tamper resistant devices," Security Protocols, 5th International Workshop, LNCS1361, pp.125-136, Springer-Verlag, 1997.