平成30年度 情報工学コース卒業研究報告要旨

楫 研究室	氏　　名	平 田　智 紀
卒業研究題目	RSA 復号の実行時間から漏洩する鍵の情報量について	

暗号システムにおけるサイドチャネル攻撃とは, 暗号を処理する装置が発する電磁波や熱, 電力量や処理時間の違いなどを物理的手段で観察することで暗号解読の手がかりを得ようとする攻撃手法のことである. サイドチャネル攻撃のうち, 処理時間の違いをもとに秘密鍵の情報を取得しようとする攻撃手法のことをタイミング攻撃という. タイミング攻撃は比較的容易に実行可能であるため, どのシステムでもタイミング攻撃の対象となる可能性がある. 特に，定期券や電子マネーとしても使用される IC カード等のシンプルなシステムでは処理時間が外部から明確に観測される可能性も高く，タイミング攻撃の脅威が深刻となりうる．一方，未知・未発見のタイミング攻撃を具体的に想定し，安全性評価を行うことは非常に困難である．より包括的に，どれだけの秘密鍵情報が処理時間から漏洩しているかを定量的に見積もる，いわゆる情報理論的安全性の評価が重要となる．

本論文では, 主要な 3 種類の RSA 暗号復号アルゴリズムのうち 2 種類を対象とし，タイミング攻撃によって秘密鍵の情報がどれだけ漏洩するかを定量的に評価する．復号にかかる時間が RSA 復号アルゴリズムにおける乗算回数と剰余演算回数のみに依存して変化すると仮定し, 秘密鍵パラメータと乗算回数・剰余回数の確率分布の関係式を導出した上で，漏洩する鍵情報量を計算する．先行研究では, 実行時間に対して鍵が与える影響を全く無視し, 荒い粒度で議論を進めていたが, 本研究では鍵に関する具体的なパラメータの影響を考慮に入れて漏洩情報量を導出しているため, 先行研究より精密に秘密鍵の漏洩情報量を評価することが可能である．本研究によって, バイナリ法と ModBin 法として知られる 2 種類の RSA 復号アルゴリズムに対してタイミング攻撃を仕掛けた場合に, 漏洩する秘密鍵情報量をより精密な式として導出することができた．一方，より高い効率が求められる場面で使用される CRT-ModBin 法に対しては，提案手法を適用することができていない．CRT-ModBin 法では，鍵の素因数に大きく依存して実行時間が変化するため，系列としての鍵を特徴づける秘密鍵パラメータと実行時間の間に直接の相関を見出すことが難しいためである．この問題への対処が今後の課題と考えられる．