論文審査の結果の要旨

氏名　　高安　敦

本博士論文は全七章からなる．第一章は序章で，第二章では必要な諸定義がなされている．第七章では，論文の総括と，いくつかの未解決問題の提起がなされている．現代の情報化社会を支える暗号技術が有用であるために，その暗号技術が実用的に安全であることは必要条件である．また，暗号技術の強度を確認することも理論的に意義深い．これらの二点を適切に確認するためには，最適な攻撃アルゴリズムを構成しなければならない．本博論では，代表的な公開鍵暗号方式である RSA 暗号を対象に，攻撃者が公開情報のみならず秘密鍵の部分情報を得られた際の攻撃アルゴリズムを構成している．いずれの結果も，多項式時間で攻撃する際には従来考えられていたより少ない部分情報で十分であることを示している．よって，従来知られていたよりも RSA 暗号の安全性が低いことを示す結果である．

各章の詳細の前に，全ての結果に共通する改良の指針を記す．攻撃アルゴリズムの構成に，本論文では，格子簡約アルゴリズムを用いた法付き方程式・整数方程式の小さな解を多項式時間で求める手法を用いている．簡単に言えば，攻撃状況を方程式で表現し，その方程式の代数構造を表現する格子を構成する．その格子基底に格子簡約アルゴリズムを適用することで得られるベクトルのノルムが十分小さければ，このベクトルの情報から元の方程式を解くことに繋がる．この手法によってどれだけ大きな解を求めることができるかは, RSA 暗号を攻撃する際にどれだけの部分情報を必要とするに対応する．適切にその安全性を見積もるために本論文で取られているアプローチは，法付き方程式を解く際の適切な格子の設計と，適切な場面での整数方程式を解く手法の活用である．

以下，各章の内容の詳細について説明する．

第三章では，small inverse 計算問題と呼ばれる RSA 暗号の安全性と関連する法付き方程式を扱う．この問題に対し，これまで様々な先行結果があったが，それらの概要をまとめ，いくつかの既存結果はその論文で言及されている条件では動かないことを示している．さらに，既存の正当な結果において構成されている格子の特性を相補的に利用することで, small inverse 計算問題を解くアルゴリズムを一部改良している．この改良によって，多素数 RSA 方式に対する攻撃を改良している．

第四章では，CRT-RSA の秘密鍵の部分情報が得られたときの攻撃を改良している．従来の結果では，秘密鍵の上位ビットが与えられたときは，下位ビットが与えられたときと比べて暗号化指数が小さなときにしか攻撃できないとされていた．この章では，まず，従来のアプローチとは異なり，整数方程式を解く手法を用いることで，上位ビットが得られたときにも同程度の大きさの暗号化指数まで攻撃可能であることを示した．さらに，下位ビットが得られたときには，法付き方程式を解く際の格子をより適切に設計することで，同じ大きさの暗号化指数に対して常により少ない部分情報で攻撃可能であることを示した．

第五章では，RSA 暗号や多素数 RSA 変形方式に対して，復号指数や素因数の部分情報が得られたときの統一的な攻撃を提案している．この文脈では様々な論文で多くの結果が提案されてき

たが，本論文ではこれらが本質的には同じ問題を取り組んでいるにすぎないことを示した．そして，多くの既存研究を包含する一般的な定式化を行い，その攻撃状況における攻撃を提案した．本章で提案されている攻撃は，現在知られている最高の攻撃を全て特殊な場合として包含するものであり，いくつかの文脈では既存の攻撃を改良している．

第六章では，$N=p^rq$ 型合成数を持つ二つの RSA 変形方式に対して，復号指数が小さい場合と復号指数の部分情報が得られる場合の二つの攻撃状況での改良攻撃を提案している．これらの変形方式は，鍵生成方程式の形が複雑になるため，既存攻撃の構成はいずれも難解で理解しにくく，さらに，$r = 1$ で通常の RSA 暗号に対する最高の攻撃と一致しないなどの問題点があった．本論文では，RSA 暗号を攻撃する際に用いる格子を，変形方式を攻撃する際の格子に変換する統一的な手法を提案しており，これにより簡潔な構成のもとで既存の結果を改良している．

本論文の内容は國廣昇との共同研究であるが，論文提出者が主体となり貢献を行っている．そのため，論文提出者の寄与が十分であり，博士（科学）の学位を授与できると認める．

以１８４２字