論 文 の 内 容 の 要 旨

論文題目　RSA Cryptanalyses with the LLL Reduction
（LLL格子簡約を用いたRSA暗号の攻撃）

氏　名　高安　敦

RSA暗号は，初めて提案された公開鍵暗号方式であり，現在も広く実用化され，安全な情報化社会の確立に大きく貢献している．この安全性を適切に見積もるためには，様々な状況における最適な攻撃を構成する必要があり，また，その有用さゆえにRSA暗号には多くの変形方式が存在するため，RSA暗号の安全性解析は暗号理論において長く研究される重要なテーマの一つである．その安全性解析のツールとして，Coppersmithが提案した，LLL格子簡約アルゴリズムを用いて法付き方程式や整数方程式の小さな解を多項式時間で解く手法は代表的であり，これまでRSA暗号の安全性に関して多くの知見を与えてきた．本稿では，この手法を用いたRSA暗号の改良攻撃を提案する．

これらの改良を得るために，二つのアプローチを取る．まず一つは，法付き方程式を解く際に，より適切な格子の設計を行うものである．適切な設計を行うことができれば，より大きな解を持つ方程式を解くことが可能になるため，より広い範囲に攻撃を適用することが可能になる． もう一つのアプローチは，これまであまり用いられなかった整数方程式を解く手法を積極的に利用することで攻撃を構成することである．一般に，整数方程式を解くアプローチでは扱う変数の数が増えるため解析が複雑になるが，これを適切に利用することで改良攻撃を提案する．

最初の結果は，small inverse problem（以下，SIP）と呼ばれる法付き方程式を解くアルゴリズムを改良する．SIPはRSA暗号の安全性に関連する問題であり，これまで多くの論文で研究されてきた．本稿では，法付き方程式を解くための格子をより適切に設計することで，SIPを解くアルゴリズムを改良した．この改良アルゴリズムによって，素因数の大きさが近いRSA暗号の多素数変形方式に対する改良攻撃を得た．

二つ目の結果は，中国人の剰余定理を用いることで復号を高速化したCRT-RSAの秘密鍵が漏洩したときの攻撃の改良である．この攻撃状況において，法付き方程式を解くための

格子を適切に設計・整数方程式を解く手法を利用することで，従来より少ない漏洩情報・大きな暗号化指数のもとで動く改良攻撃を提案した．より具体的には，これまで暗号化指数が$e < N^{3/8}$を満たすほど小さければ攻撃できなかったが，秘密鍵d_pとd_qの上位/下位ビットの漏洩情報を用いて$e < N$のときに攻撃可能であることを示した．さらに，秘密鍵d_pまたはd_qの上位ビットの漏洩情報を用いてこれまで$e < N^{1/4}$を満たすほど小さければ攻撃できなかったが，$e < N^{3/8}$のときに攻撃できることを示し，これらの下位ビットの漏洩情報が得られるときには，従来より少ない情報で攻撃可能であることを示した．

三つ目の結果は，RSA暗号やその多素数変形方式において復号指数や素因数の部分情報が得られたときの攻撃の改良である．この問題はRSA暗号の安全性解析における代表的なものとして法付き方程式を解く手法と整数方程式を解く手法を用いてこれまで多くの論文で議論されてきたが，その多くはより包括的に定式化された問題の部分問題でしかないことを示した．さらに，その定式化のもとでの攻撃を提案した．この提案攻撃は，それぞれの部分問題において全ての既知の最高の攻撃を含んでいるという点で最適であると考えられ，また，この攻撃を用いることで，いくつかの特殊な場合における改良攻撃を提案している．

最後の結果は，$N = p^r q$という特殊な法を持つ変形方式に対する攻撃の改良である．その法の特殊さゆえに，通常のRSA暗号と比べて解析が複雑になるとされていたが，通常のRSA暗号に対する攻撃の際に設計する格子を変形方式への格子に変える統一的な変換法を提案した．この変換法を用いることで，変形方式に対する攻撃の改良を提案した．