Efficient Lattice Reduction Algorithms and their Applications to Lattice-Based Cryptography

王, 贇弢

出版情報：Kyushu University, 2018, 博士（機能数理学）, 課程博士
バージョン：
権利関係：

（様式３）

氏　　名　：王　贇弢

論 文 名　：Efficient Lattice Reduction Algorithms and their Applications to Lattice-Based Cryptography
(効率的な格子基底簡約アルゴリズムと格子暗号への応用に関する研究)

区　　分　：甲

論　文　内　容　の　要　旨

現代の情報通信では、暗号通信技術を利用することで、悪意ある第三者による改ざんや盗聴などができない安全な通信経路を確立し、情報の安全性を高めている。現在、これらの暗号通信技術は、電子商取引や電子投票などで広く利用されている。特に、暗号理論は情報セキュリティの基盤であり、安全な情報社会を実現する上で必要不可欠である。

現在、情報通信の多くで公開鍵暗号方式が用いられており、特に素因数分解に基づくRSA暗号や楕円曲線暗号が幅広く利用されている。しかし、量子計算機により、上記の暗号方式は多項式時間で解読できることが数学的に証明されている。量子計算機は2029年前後に開発されると期待されているため、アメリカ国立標準技術研究所(NIST)は耐量子暗号(PQC、次世代暗号とも呼ばれる)の標準化に向け活動を開始した。具体的には，2016年秋から2017年冬までの期間で耐量子暗号の候補方式を募集し、その後5年程をかけて安全性を解析し、標準化方式を決定すると公表した。そのため、量子計算機による解読に対して安全である次世代暗号の研究は喫緊の課題になっている。現在、数学の研究対象である格子理論を利用した格子暗号が注目され、格子暗号は次世代暗号の有力な候補になると期待されている。実際、NIST PQC標準化では暗号方式と署名を含めて合計69件の提案があり、そのうち26件は格子ベースであった。

格子は$\mathbb{R}$上n次元のベクトル空間の離散部分加群であり、図形的に記述できる幾何的な対象である。格子理論の中で暗号に利用される最短ベクトル問題(SVP問題)はNP困難問題があり、数学において古くからの研究対象である。高い次元のSVP問題は量子計算モデルにおいても効率的な解読が不可能と予想されているため、格子暗号の安全性の根拠として利用されている。しかし、格子暗号は比較的新しく提案された暗号技術であるため、安全性解析が不十分であり、安全なパラメータが決定おらず実用化には至っていない。格子暗号の安全性を評価するためには、SVPなどの格子問題を解く最適な格子アルゴリズムの開発とその計算量評価が必要である。SVP問題を解析するための重要なツールとして格子簡約アルゴリズムがあり、世界中で活発に研究されている。

本研究では、(１) BKZと呼ばれる格子簡約アルゴリズムの改良を行い、格子暗号の安全性根拠となるSVP問題の計算量を正確に解析する；(２) (１) の成果を利用して、耐量子暗号として最適な格子暗号のパラメータ(LWEベース格子暗号のパラメータ法q、次元n、分散α)を提案する；(３) さらに、(１) で改良したBKZアルゴリズムとそのシミュレーターを用いて格子鍵交換方式「Ding Key Exchange」の安全かつ最適なパラメータの評価を行う。

（１） 格子簡約アルゴリズムの改良及び世界記録達成

格子簡約アルゴリズムとは、与えられた格子基底からより短い、より直交した基底を出力するア

ルゴリズムである。1982年に提案されたLLL簡約アルゴリズムは、多項式時間$O(n^6)$（nは格子の次元）でSVP問題を高確率に解けるが、次元が高くなるにつれSVPを解く確率が低くなることが知られている[Lenstra et al, Math. Ann. 1982]。その欠点を補うため、LLLアルゴリズムを前処理とし、計算量$O(2^n)$である格子点列挙法と組み合わせたBKZ簡約アルゴリズムが提案された[Schnorr-Euchner, Math. Program. 1994]。[Gama et al., EUROCRYPT2010]では枝切り手法を利用し、格子点列挙法における探索ノードを$O(1.414^n)$倍に削減した高速化手法を提案した。さらに、[Chen-Nguyen, Asiacrypt2011]は上記の改良した列挙法を用いて、実用的な簡約アルゴリズムBKZ2.0を提案された。2011年ChenとNguyenは枝刈りや前処理など様々な技術を用い、実用的なBKZ2.0アルゴリズムを提案した[Chen-Nguyen, Asiacrypt2011]。一方、BKZアルゴリズムの簡約状況によりブロックサイズを段階的に上げることで、ブロックサイズを固定したBKZアルゴリズムよりも計算時間を短縮することが出来る手法がいくつか知られている。本研究ではこのブロックサイズを段階的に上げる新しい方法を提案した。具体的には、BKZ2.0アルゴリズムのシミュレータなどを利用して、格子の簡約状況を表すGeometric Series Assumption (GSA)[Schnorr, STACS2003]の値を定期的に監視し、ブロックサイズの上昇条件に関係するパラメータを導入した新たな逐次BKZアルゴリズムを提案した。本研究は国立研究開発法人情報通信研究機構と共同で行った。提案した逐次BKZアルゴリズムを用いて、最短ベクトルの解読チャレンジ“Ideal Lattice Challenge”（652次元）と“SVP Challenge”（123次元）などの世界記録を達成した。本研究の成果をまとめた論文が、暗号分野の査読付き国際会議EUROCRYPT 2016に採録され，2016年5月に発表した。

（２）LWE問題の計算困難性の評価及び世界記録達成

2005 年に Oded Regev 氏は格子理論における「Learning With Errors」(LWE)問題を提出し、LWE に基づく暗号方式も提案された[O. Regev, J.ACM 56(6), 2009]。LWE 問題とは、人工知能の機械学習から派生したもので、乱数eでランダム化した線形方程式から、秘密ベクトルsを求める問題となる。LWE 問題の平均困難性は SVP 問題の困難性と一致するため、SVP 問題を解くアルゴリズムを用いて、LWE 問題に基づく格子暗号の安全性解析が行われている。格子問題の困難性評価を目的とした、ドイツのダルムシュタット工科大学が主催する格子暗号解読コンテスト LWE Challenge がある。我々は（１）で提案した逐次 BKZ アルゴリズムと Kannan 埋込法[R. Kannan, Math. Oper. Res. 12(3), 1987]を用いて LWE 問題の困難性を評価し、最適なパラメータ設定を見積もった。さらに、LWE 解読コンテスト“LWE Challenge”（70 次元）などの世界記録を達成した。本研究成果をまとめた論文が、査読付き国際会議 ICICS2018 に採録された。

（３）NISTに鍵交換方式を提案、特に安全性評価

LWEの変種として、Ring-LWEやModule-LWEなども提案されている。我々はアメリカシンシナティ大学のJintai Ding教授と中国交通大学のXinwei Gao氏と共同でRing-LWEベースの鍵交換方式「Ding Key Exchange」をNIST PQC標準化へ提案した。その際に、（１）で行った逐次BKZシミュレーターを用いてAES-128/196/256ビット安全性をもつパラメータを見積もった。本研究成果をまとめた論文を、査読付き国際会議Asiacrypt 2018に投稿した。

本研究では効率的な格子基底簡約アルゴリズムと格子暗号への応用による安全性解析を中心に、格子簡約アルゴリズムの改良と格子ベース暗号方式の構成と安全性評価を行ってきた。格子暗号の実用化、いわゆる次世代暗号の標準化には欠かせない重要な研究である。