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：

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)
論文調査委員	主査　東京大学　教授　高木 剛 副査　九州大学　教授　溝口 佳寛 副査　九州大学　准教授　安田 雅哉 副査　東芝 研究開発センター 研究主幹　秋山 浩一郎

論 文 審 査 の 結 果 の 要 旨

本博士論文では，最短ベクトル問題(SVP)の困難性に基づく格子暗号の安全性を考察している．Regev は国際会議 STOC2005 において，安全性が Learning with Errors (LWE)問題の困難性に帰着される格子暗号を発表した．格子暗号は，現在普及している RSA 暗号とは異なり，量子計算機を用いた攻撃に耐性があると期待されている安全性が高い次世代暗号である．

n 次元実ベクトル空間の 1 次独立な基底 B で生成される格子を L(B)とする．このとき，与えられた基底 B に対して，格子 L(B)に含まれる非零な最短ベクトルを求める問題を，最短ベクトル問題(SVP)と呼ぶ．ここで，SVP に対する解法アルゴリズムの研究は，格子暗号の安全なパラメータを正確に評価するために重要な問題となる．SVP を厳密に解くアルゴリズムとして Enumeration 法(ENUM)があり，SVP の近似解を求めるアルゴリズムとして Lenstra-Lenstra-Lovász (LLL)アルゴリズムがある．現在までに，SVP の近似解を求める最も高速な手法として，LLL をブロック化して部分格子に ENUM を利用する Block Korkin-Zolotarev (BKZ)アルゴリズムが知られている．一方，格子暗号を構成するために，Learning with Errors (LWE)問題が用いられる．n, m, q を正の整数とするとき，行列 A を Z/qZ 成分の m×n 行列，s を$(Z/qZ)^n$のベクトルとして，b = As+e mod q と定義する．ここで，e は各成分が平均 0 標準偏差 σ の離散ガウス分布から生成した整数値のエラーベクトルとする．LWE 問題は，与えられた(A, b = As+e mod q)に対して，ベクトル s を求める問題である．

本博士論文では，Progressive BKZ と言われる格子基底簡約アルゴリズムの高速化を行い，その改良アルゴリズムによる大規模解読実験を実施した．従来の BKZ アルゴリズムでは，固定したブロックサイズβを用いて ENUM のサブルーティンを計算していた．一方，提案手法ではブロックサイズβを可変として，ENUM の枝狩り半径αおよび成功確率 p, 更には BKZ の終端分布を示すパラメータ r の合計 4 変数(β, α, p, r)の関係に注目している．実際，Geometric Series Assumption を用いた終端分布 r に対して，与えられた枝狩り半径αと成功確率 p を持つ ENUM の計算量を最小化するブロックサイズβの決定方法を提案した．これにより，BKZ アゴリズム全体に対する計算量を削減できるブロックサイズβの導出が可能となった．更に，提案した Progressive BKZ の大規模実装を実施し，ダルムシュタット工科大が主催する SVP チャレンジ問題において世界記録となる 625 次元を，288 シングルスレッド日(CPU E5-2697)により解読することに成功している．

一方，LWE 問題(A, b = As+e mod q)において，エラーベクトル e の各成分は平均 0 標準偏差 σ の離散ガウス分布から生成した整数である．そのため，b は A の列ベクトルで張られる格子の元 w=As に近い点となり，LWE 問題は Bounded Distance Decoding (BDD)とみなすことができ，Babai による最近平面アルゴリズムにより求めることができる．現在のところ，LWE 問題に対して最も高速な計算法として，BDD を Kannan's Embedding 法により高い次元の格子の unique-SVP に帰着する方法が知られている．本博士論文では，LWE 問題を unique-SVP に帰着した問題に対して，Progressive BKZ を用いた解読計算量の評価を与えている．特に，LWE 問題の入力となるサンプル数 m の最適な選択方法を，次元 n に対する標準偏差 σ と法 q の依存関係式から考察している．これにより，Kannan's Embedding 法が高速となる，埋め込み係数の大きさ，LWE 問題のサンプル数の大きさ，BKZ アルゴリズムのブロックサイズを導出した．また，提案した改良アルゴリズムにより，ダルムシュタット工科大が主催する LWE チャレンジ問題において，70 次元の LWE 問題を 32.73 シングルコア時間(CPU E5-2697)で解読する世界記録を達成している．

本博士論文の結果は，国際会議 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2016) および The 19th International Conference on Information and Communications Security (ICICS 2017) において発表している．また，平成 28 年 10 月には，Forum Math-for-Industry 2017 におけるポスター発表 ″Breaking Lattice Challenges by Progressive BKZ Algorithm″ に対して Best Poster Award を受賞している．

以上の結果は，格子基底簡約アルゴリズムにより格子暗号の安全性評価法を考察したものであり，暗号理論の分野において学術的に高く評価できる研究業績である．

よって，本研究者は博士（機能数理学）の学位を受ける資格があるものと認める．