別紙2

論文審査の結果の要旨

論文提出者氏名　深瀬道晴

離散格子の与えられた基底から、その格子に属する格子ベクトルのなかで最も短いベクトル(最短ベクトル)を求める問題はSVP(Shortest Vector Problem)と呼ばれているが、NP困難であることが知られている。応用においては十分短い格子ベクトルであれば有用であることがあり、最短ベクトルの定数倍の長さまでSVP問題の条件を緩和した“近似SVP問題”を解くアルゴリズムが研究されてきた。近似SVP問題を解くためには、格子の基底ベクトル全体を短くする基底簡約アルゴリズムが使われ、そのアルゴリズムはLLL(Lenstra, 1982)、BKZ(Schnorr, 1987)、RSR(Schnorr, 2003)と進歩してきた。しかし、これらの基底簡約アルゴリズムをもってしても、数百次元を超える格子における近似SVP問題は依然として難しい問題である。本論文は、近似SVP問題を解くために使える可能性のある新たな手法を提案したものである。本論文は6章からなる。

第1章は導入である。まず、近似SVP問題の背景と現状を説明した後で、現状の問題について述べ、本論文の目的を定めている。第2章では、本論文を理解するために必要となる基礎知識について説明している。そして、格子暗号で使われる、GGH格子、NTRU格子、Micciancio GGH格子において、秘密鍵を構成する短い格子ベクトルをVSV(Very Short Vector)と呼び、VSVを求めることで実験を評価したことが述べられている。格子暗号において秘密鍵を構成する格子ベクトルは十分短いと考えられており、意味のある評価であると審査委員会は判断した。

第3章と第4章が新たな手法を提案している部分である。第3章では、RSRにおけるVSVの探索手法を拡張し、VSVを探索する格子ベクトルの空間としてESS(Extended Search Space)を提案している。ESSの妥当性を検証するために、まず、その前提となるグラムシュミット基底ベクトルの分布に関するGSA仮説とVSVの係数ベクトルの分布の仮定が成り立つ事を実験により確認している。次に、最適なパラメータを用いた場合、同じ探索空間の大きさ(候補となる格子ベクトルの数)では、ESSを用いることで、RSRの探索よりも高確率でVSVを発見できることを実験的に示している。この実験では3種類の格子に対して有効性を確認しており、十分な一般性がある結果であると審査委員会は評価した。

第4章では、ESSのパラメータの決定方法が提案されている。VSVが未知の時に与えられた基底のみからESSのパラメータを決定するのは困難である。そこで、本論文では、対象となる基底と同様の方法で生成され、VSVが既知であるサンプル基底が多数利用できるという前提のもとで、サンプル基底の統計的性質を利用することで、より良いパラメータの推定が可能であることを実験的に示している。この方法は格子の生成アルゴリズムの“癖”を利用する方法として有効であると審査委員会は評価した。

第5章では、8 CPUで並列にESSを探索し台数分の高速化の効果が得られたことが示されている。小規模な実験であるが、本論文の成果の応用の可能性を実際に示したものとして意味があると審査委員会は判断した。

第6章は結論である。

以上のように本論文は、従来、基底簡約アルゴリズムの補助的役割しか与えられてこなかった探索の部分を研究の主な対象とし、高い確率でVSVを含む新しい探索空間を提案したものであり、近似SVP問題に関連する研究成果として高く評価することができる。したがって、本審査委員会は博士(学術)の学位を授与するにふさわしいものと認定する。