論文の内容の要旨

論文題目　Finding a Very Short Lattice Vector in the Extended Search Space (拡張型探索空間において非常に短い格子ベクトルを求める手法)

氏名　深瀬　道晴

整数格子 Lは、線形独立なベクトルの組 b1,...,bn ∈ Z^mに関する整数係数線形結合の全ての集合である。nを Lの次元といい、(b1,...,bn)を Lの基底という。また、 Lに属する要素を格子ベクトルという。以下では、格子によって整数格子を意味するものとする。n≤ 2のとき、同一の格子を生成する基底は無数に多く存在する。

原点を除く最も短い格子ベクトルを、最短ベクトルという。与えられた基底に対して、その基底が生成する格子における最短ベクトルを求める問題を最短ベクトル問題 (SVP)という。 SVPを解く多項式時間アルゴリズムは知られていない。一方、 SVPを解く多項式時間アルゴリズムの代替として、SVPの近似版である近似最短ベクトル問題 (近似 SVP)を解く多項式時間アルゴリズムがいくつか提案されている。近似 SVPとは、与えられた基底と定数 γ ∈ Rに対して、その基底が生成する格子における最短ベクトルのノルムのγ倍以内のノルムを持つ格子ベクトルを求める問題である。近似SVPの解を、近似最短ベクトルという。γが小さいとき、高次元の格子に関する近似SVPを解くことは困難である。

格子暗号として知られるGGH暗号システム(Goldreich, 1997)、Micciancio’s GGH暗号システム(Micciancio, 2001)、NTRU暗号システム (Hoffstein, 1998)の秘密鍵は、格子ベクトル、または格子ベクトルの組から成っている。これらの暗号システムに関連付けられる格子をそれぞれ、GGH格子、Micciancio’s GGH格子、 NTRU格子という。これらの格子において秘密鍵の格子ベクトルを求める問題は、近似SVPに相当する。本論文では、秘密鍵の格子ベクトルをVSV(very short vector)と呼ぶことにする。 VSVは、小さな近似係数 (*apfa*)の近似最短ベクトルである。ここで、格子ベクトル vの apfaとは、vと最短ベクトルとのノルムの比である。また、NTRU格子において、VSVは最短ベクトルに一致することが知られている。従って、このような場合は、 VSVを求める問題は SVPに相当すると考えられる。

基底簡約は、VSVを求めるための手段の一つである。基底簡約とは、与えられた任意の基底に対して、短い格子ベクトルから成る基底を求めることである。代表的な基底簡約アルゴリズムとして、 LLLアルゴリズム (Lenstra, 1982)、BKZアルゴリズム (Schnorr, 1994)、RSRアルゴリズム (Schnorr, 2003)が知られている。 BKZアルゴリズムと RSRアルゴリズムは、100以上の次元において、 VSVを求めることができる。しかし、これらのアルゴリズムは、 200前後の高次元において、また、それ以上の高次元において、 VSVを求めることができなくなる。これらのアルゴリズムにおいて、基底の格子ベクトルの *apfa*を縮小するために全探索手法が用いられているが、 *apfa* は一度の全探索において$\sqrt{0.99}$ のような小さい比率でしか縮小されない。高次元において VSVを求めるためには、全探索の効率を上げる必要がある。効率を上げる方法として、一度の全探索において VSVを求めることが考えられる。しかし、既存の全探索手法の中で最も効率の良い Enumeration(Schnorr, 1994)は、低次元においてしか VSVを求めることができない。

本研究の目的は、高次元において高確率で VSVを求める全探索手法を構築することである。このため、本研究では、 RSRアルゴリズムにおいて用いられる探索空間である SA空間を改良することにより、探索空間が VSVを包含する確率を高くする。本研究における結果を、以下に示す。

1. VSV の係数の分布が増加幾何数列に関連することを示した。特に、 VSV の係数の分布は、GSA(Geometric Series Assumption)に直接的に関連していることを実験的に示した。また、GSA と VSV の係数に関する仮定とに基づいて VSV の係数の上限値を導くことによって、VSV の係数と増加幾何数列との関係を理論的に示した。

2. VSV の係数の分布に基づいて、拡張型探索空間 (ESS)を定義した。また、 ESS が VSV を高い確率で包含することを示した。例えば、 200 次元の GGH 格子において、ESS は SA 空間に対して 25 倍の頻度で VSV を包含することを実験的に示した。

3. ESS における VSV 包含確率の計算法を示し、 VSV 包含確率を最大にする ESS の適切なパラメータを決定するスキーム PR(Parameter Refi nement for ESS)を提案した。VSV 包含確率の計算のためには、VSV の係数の期待値からのずれに関する分布を導入した。また、この分布を得るために、VSV 既知の基底のセットであるサンプル基底を導入した。格子暗号においては、鍵生成アルゴリズムが知られているため、サンプル基底を得ることが可能である。PR によって決定したパラメータを用いた場合、 ESS は、既知の VSV から計算したパラメータを用いた場合と同程度の確率で VSV を包含することを実験的に示した。ランダムな格子に近い Micciancio's GGH 格子においては、 VSV の係数の期待値からのずれに関する分布を利用することができないために、PR を用いることができない。このような場合にも、実験的に適切なパラメータを決定することが可能であることを示した。

4. ESS における全探索が効果的であることを実験的に示した。特に、 ESS における探索の分散計算の効果を示した。8 個の CPU を用いた実験によって、 CPU の台数から予想されるよりも高い効率で高速化が達成され得ることを示した。この実験結果から、十分に多くの CPU が得られる場合、ESS における全探索は BKZ アルゴリズムよりも効率が良いと推定される。

以上の結果に基づいて、高次元において高確率で VSVを求める全探索手法が構築されたと結論する。本研究の応用としては、全探索のみで VSVを求める手法として用いることが考えられる。また、基底簡約アルゴリズムのサブルーチンとして用いるという応用が考えられる。本研究の手法を適用する格子に関して、本研究の手法はランダムに近い Micciancio'ｓGGH格子にも適用できたことから、ランダムな格子に一般的に適用しうると考えられる。