様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月 ２５ 日現在

機関番号：８２６２６
研究種目：若手研究
研究期間：2018～2019
課題番号：１８Ｋ１８０５４

研究課題名（和文）確率的性能評価に基づく超高速な格子基底簡約アルゴリズム設計法の構築

研究課題名（英文）Efficient Lattice Basis Reduction Algorithm Based on Probabilistic Analysis

研究代表者
照屋　唯紀（Teruya, Tadanori）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・研究員

研究者番号：２０６３６９７２

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：サンプリングアルゴリズムの動作がランダムネス仮定で説明できるか調査した．SVP Challengeなどの格子を使用して実験を行なった範囲では，説明できることがわかった．この得られた結果に基づき，効率的なアルゴリズムを構築するための道具として，ランダムネス仮定を利用してサンプリングアルゴリズムの性能を確率的に推定する方法を構築した．これは入力からGram-Charlier級数展開を利用して出力される格子ベクトルの長さの確率分布を推定できる．そしてこの方法の推定誤差を理論的に解析し，SVP Challenge格子を用いた数値実験により実際に精度良く推定できることを確認した．

研究成果の学術的意義や社会的意義
格子暗号は耐量子計算機暗号の有力候補である．その安全性は格子問題の困難性が根拠である．代表的な格子問題である最短ベクトル問題は，格子の次元数の増加に対して求解困難性が指数関数的に増大する．しかし，次元数を大きくし過ぎると実用性が喪失する．よって，可能な限り高速な求解法を構築し，その性能を精密に推定することで，安全性と効率性のバランスが取れた次元数を明らかにする必要がある．本研究では，高速な求解法を構築するための部品である格子のサンプリングアルゴリズムの性能を確率的に高精度および高効率に推定する新しい方法を構築した．これにより，安全かつ実用的な格子暗号の実現に一定の貢献ができたと考えられる．

研究成果の概要（英文）：We investigated whether the randomness assumption captures the sampling algorithm's behavior. The experimental results on SVP Challenge lattices show that this assumption well captured the behavior. Then we constructed a probabilistic evaluation method for sampling algorithms to design efficient algorithms. This method can estimate the probability distribution of the length of the lattice vector output from the input using the Gram-Charlier series expansion. We showed that an upper bound of the estimation error decreases monotonically when the order of expansion increases. We also showed numerical experiments using SVP Challenge lattices. Consequently, our method can estimate with reasonable accuracy.

研究分野：暗号技術

キーワード：格子暗号　格子基底簡約　統計　パラメトリック推定　Gram-Charlier A型級数展開

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

研究代表者の照屋は柏原賢二氏と共同で，代表的な格子問題である最短ベクトル問題(Shortest Vector Problem, SVP)の解読コンテスト SVP Challenge に取り組み，格子ベクトルのサンプリングアルゴリズムに対して行なった確率的解析により得られた知見を応用して，効率的な格子基底簡約アルゴリズムを開発した．この研究と実験により，格子ベクトルのサンプリングアルゴリズムと格子基底簡約アルゴリズムの性能などを Gram-Charlier A 型級数展開を用いて，高い精度かつ高い効率で確率的に推定できる可能性が有ることがわかった．

２．研究の目的

本研究では，Gram-Charlier A 型級数展開による確率的推定について詳細に調査し，具体的な推定方法の構築を試みる．さらに，構築した推定方法を応用し，高速な格子基底簡約アルゴリズムの新しい設計法の構築を試みる．そして，この新しい設計法を用いた高速な格子基底簡約アルゴリズムを使用し，その性質を詳細に解析および数値実験を行うことで，格子問題の求解困難性を評価する方法の構築を試みる．格子暗号は格子問題の求解困難性を安全性の根拠とする．本研究の大きな目的は，実社会利用に耐えうる安全性と効率性を持つ格子暗号の実現方法の構築に貢献することである．

３．研究の方法

格子ベクトルのサンプリングアルゴリズムの入力は格子の基底と探索範囲であり，出力は探索範囲に含まれる格子ベクトルの集合である．なお，具体的なアルゴリズムにはいくつかの変形・変種が存在する．例えば，探索範囲の部分集合をランダムに選択し，その選択された部分集合に含まれる格子ベクトルを出力する方法や，単純に与えられた探索範囲に含まれる格子ベクトルを全て出力する方法などがある．

本研究は，格子ベクトルのサンプリングアルゴリズムが出力する格子ベクトルの長さ(正しくはノルムの 2 乗．以降も単に長さと呼ぶ)の分布を，Gram-Charlier A 型級数展開を用いて，入力から確率的に推定可能であることに着想を得ている．しかし，確率的な推定を可能とするためには，何らかの適切なモデル化を行う必要がある．モデル化の方法はこれまでに複数提案されている．本研究では，Schnorr (STACS 2003)が提案した，独立連続一様分布という素朴な確率モデルを与える「ランダムネス仮定」と呼ばれるモデル化に注目した．この仮定は，アルゴリズムを実行することによって得られる値がどのように分布するのかを説明するものである．よって，このモデル化が現実のアルゴリズムの振る舞いに対して乖離している場合，Gram-Charlier A 型級数展開による推定は極めて困難になると予想される．

そこで，本研究は次のように段階を設けて実施する：

(1) サンプリングアルゴリズムの動作がランダムネス仮定によって適切にモデル化可能であるか，つまり，ランダムネス仮定の妥当性を調査する．

(2) ランダムネス仮定によって適切にモデル化可能であるとのデータが得られた場合には，ランダムネス仮定に基づいた Gram-Charlier A 型級数展開による確率的推定法の具体的な構築を行い，その性質を理論と実践の両面から評価する．

(3) 構築した確率的推定法を利用した高速な格子基底簡約アルゴリズムの構築を行う．

なお本研究は，確率論および統計学の観点からの詳細な解析については松田源立氏(研究協力者)，サンプリングアルゴリズムと格子基底簡約アルゴリズムについての助言は柏原賢二氏(研究協力者)，高性能計算分野の観点からの助言は池上努氏(研究協力者)より協力を得ながら行う計画である．

４．研究成果

(1) ランダムネス仮定の妥当性を調査するために，SVP Challenge で出題されている格子など，求解の研究で広く利用されている格子の基底を対象に，実際にアルゴリズムを実行して得られた数値の統計量と，ランダムネス仮定により得られる統計量を比較する実験を行なった．実験を行なった範囲ではランダムネス仮定の妥当性が確認できた．つまり，ランダムネス仮定はサンプリングアルゴリズムの動作を良く説明するモデルであると考えられる．この成果は査読付き国際会議である ISITA 2018 に採択された．

この研究成果の概要を解説する．実施した実験では，SVP Challenge で出題されている 150 次元シード 0 の格子の基底に対してブロックサイズ 20 の BKZ 格子基底簡約を実行し，出力された基底$B = (\mathrm{b}_1, \ldots, \mathrm{b}_{150})$を使用した．入力する探索範囲はインデックス 1 から 129 は$\{0\}$，インデックス 130 から 149 は$\{0,1\}$，そして最後のインデックス 150 は$\{1\}$の直積$\Upsilon = \{0\}^{129} \times \{0,1\}^{20} \times \{1\}$に対応する(原点を含まない)超直方体の和集合とした．これは，Schnorr (STACS 2003)のアルゴリズムのパラメータを$u = 20$とした時の探索範囲である．また，Υに 1 対 1 対応するように格子ベクトルが存在し，サンプリングアルゴリズムはこれを求める．

得られた格子ベクトルから射影座標系の係数値を求め，これらからさらにカイ 2 乗値(カイ 2 乗検定で用いられる統計量)と，インデックス間と出力された格子ベクトル間の 2 つのピアソンの積率相関係数(以降単に相関係数と呼ぶ)を求めた．なお，カイ 2 乗値の算出はインデックスごとに行い，求めた係数値の集合からヒストグラムを求めて算出した．カイ 2 乗値の算出に使用する期待値は，ランダムネス仮定により得られる値とした．その結果，カイ 2 乗値については次のような結果が得られた：インデックス 1 から 120 までのカイ 2 乗値はカイ 2 乗分布の期待値の周辺に分布し，それ以外のインデックスのカイ 2 乗値は期待値から大きく離れた値となった．インデックス間の相関係数は大きいインデックスの間で相関が見られ，他はほぼ 0 の値となった．格子ベクトル間の相関係数は全体的にやや相関有りの値となった．
これら結果から，小さいインデックスでは，ランダムネス仮定はサンプリングアルゴリズムの動作を説明できると考えられる．この予想を実験的に確認するために，121 から 150 までの係数値を無視して格子ベクトル間の相関係数を算出し直したところ，0 周辺に分布する相関係数値を得た．
これら実験結果により，大きなインデックス間では相関が見られる，つまり，ランダムネス仮定の妥当性を否定する結果が得られた．しかしその一方で，小さいインデックスでは妥当性を否定できる結果が得られなかった．よって，大きなインデックスではランダムネス仮定は妥当なモデルではないが，次元数に対して十分に小さいインデックスにおいてはアルゴリズムの動作をよく説明し，有用であると考えられる．サンプリングアルゴリズムが出力する格子ベクトルの長さに大きな影響を与えるのは，多くの場合においてインデックスが小さな係数値であると考えられる．よって，ランダムネス仮定は妥当で有用なモデル化であるという結論を得た．

(2) ランダムネス仮定の妥当性を示す一定のデータが得られたため，ランダムネス仮定に基づき，Gram-Charlier A 型級数展開による確率的推定法の構築を行った．この確率的推定法は，サンプリングアルゴリズムが出力する格子ベクトルの長さの分布を入力のみから推定できる．また，構築した推定方法は展開次数をパラメータとして持つ．この展開次数を増加させると，有限の展開次数による推定結果と，ランダムネス仮定により得られる真の分布との誤差の上界が単調減少することを理論的に示した．また，SVP Challenge で出題されている格子を使用し，実際に推定実験を行なった．実験を行なった範囲では，分布の裾となる短い格子ベクトルの分布に対しても，既存の方法よりも高速かつ精度良く推定できることがわかった．この成果は査読付き国際会議である APKC 2019 に採択された．
この研究成果の概要を解説する．Gram-Charlier A 型級数展開は，平均，分散，歪度，尖度などの統計量を一般化した高次キュムラントを使用して確率密度関数と累積分布関数の級数展開表示を与える．よって，サンプリングアルゴリズムの入力から Gram-Charlier A 型級数展開の入力となる高次キュムラントを算出する方法を具体的に与えれば，Gram-Charlier A 型級数展開による確率的推定法を構築できる．
本研究では，ランダムネス仮定を利用することで，サンプリングアルゴリズムの入力である基底と探索範囲から，出力される格子ベクトルの長さの分布の高次キュムラントを算出する方法を厳密に与えた．
出力される格子ベクトルの数は有限であり，よって長さの分布には最大値と最小値が存在する．すなわち分布の裾は有限である．この時，Gram-Charlier A 型級数展開は展開次数を無限大に近づけると，ランダムネス仮定の元で真の分布に収束する．しかし，実際に計算できるのは有限次数の級数展開である．そこで，展開次数が有限の場合，これを大きくすると真の分布に対する誤差がどのように変化するか解析した．その結果，展開次数の増加に対して，誤差の上界が単調に減少することを理論的に示した．
また，SVP Challenge で出題されている 100 次元，128 次元，150 次元のシードがそれぞれ 0 の格子を使用し，探索範囲はnを次元数として$\Upsilon_1 = \{0\}^{n-26} \times \{0,1\}^{25} \times \{1\}$と$\Upsilon_2 = \{0\}^{n-23} \times \{0,1\}^{17} \times \{0,1,2\}^5 \times \{1\}$の 2 種類，展開次数は 120 としてそれぞれについて推定を行なった．この実験により，本研究で構築した推定方法は既存の方法よりも高速であること，そして，実際にサンプリングアルゴリズムを実行して得た出力と比較したところ，精度良く推定できたことを確認した．

(3) 以上の研究により，サンプリングアルゴリズムの性能を，効率的かつ精度良く推定できるようになった．この方法を応用して 効率的な格子基底簡約アルゴリズムの構築を行うべく研究を行なった．現在，得られた知見の整理および論文化・投稿準備中である．
なお，他の研究チームにより高速な SVP 求解および格子基底簡約の新しいアルゴリズムの提案とその実装が示され，SVP Challenge の記録が大きく更新された．使用された主な方法は，射影格子ふるいと格子基底簡約である．
安全かつ実用的な格子暗号の実現には，高速な格子基底簡約アルゴリズムの設計法を構築することが極めて重要であり，これは本研究の目的の一つでもある．SVP Challenge の記録が大きく更新されたという事実から，今後は射影格子ふるいも含めた研究を行うべきであると考えられる．

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 Tadanori Teruya
２．発表標題 An Observation on the Randomness Assumption over Lattices
３．学会等名 The International Symposium on Information Theory and Its Applications (ISITA) 2018（国際学会）
４．発表年 2018年

１．発表者名 Yoshitatsu Matsuda, Tadanori Teruya, Kenji Kashiwabara
２．発表標題 Efficient Estimation of Number of Short Lattice Vectors in Search Space under Randomness Assumption
３．学会等名 The 6th ACM ASIA Public-Key Cryptography Workshop (APKC 2019)（国際学会）
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	松田　源立 (Matsuda Yoshitatsu)		
研究協力者	柏原　賢二 (Kashiwabara Kenji)		

6．研究組織（つづき）

	氏名 （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	池上　努 (Ikegami Tsutomu)		