様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　２２　日現在

機関番号：　８２６３６
研究種目：　若手研究(B)
研究期間：　2014～2015
課題番号：　２６７３００６９

研究課題名（和文）格子暗号実用化のための安全性評価手法の進展

研究課題名（英文）Progress of the lattice cryptanalysis

研究代表者
青野　良範（Aono, Yoshinori）

国立研究開発法人情報通信研究機構・ネットワークセキュリティ研究所　セキュリティ基盤研究室・研究員

研究者番号：５０６１１１２５

交付決定額（研究期間全体）：（直接経費）　　1,300,000円

研究成果の概要（和文）：格子暗号を社会展開するための具体的なパラメータの選定を行うため、既存アルゴリズムの改良と正確なシミュレータの作成を行い、国際会議Eurocrypt2016において発表を行った。
このアルゴリズムを基礎として、格子暗号の安全性評価における時間-空間トレードオフの新たな議論が可能となり、また応用としてLWE問題等の評価が可能となると期待されるため、実用化に向けて一歩前進した。

研究成果の概要（英文）：We developed the improved lattice basis reduction algorithm and its precise simulator, which allows us to simulate the security (and concrete parameters) of seceral lattice based cryptographies. We have presented it in Eurocrypt 2016.
We expect that we can discuss the time-space trade-off relation in lattice based cryptography and will have applications for the concrete analyses of sieve-type algorithms and LWE problems.

研究分野：　格子暗号の安全性評価

キーワード：　格子暗号　安全性評価　基底簡約　BKZアルゴリズム

１．研究開始当初の背景

研究開始時の平成 26 年 4 月において、格子暗号の具体的なパラメータを決定するためには、(1)既存の攻撃モデルからパラメータと計算量の関係式を導出、(2)小規模実験により式の係数を決定し、(3)それを用いたシミュレーションにより暗号方式のパラメータを決定するというフレームワークは固定されていた。

しかしながら、(1)の攻撃アルゴリズムの発展が格子基底簡約アルゴリズムをはじめとする多項式空間アルゴリズムに限られており、また実用的な格子暗号解読アルゴリズムも格子分野から発生したものに限られていた。このことは、学術的には格子暗号の安全性評価に関して改良の余地が大いにあることを表していた。反面、暗号の安全性を議論する立場からは将来予測が困難であり、長期間にわたり安全なパラメータを提案する土壌を作り上げることが急務であった。

２．研究の目的

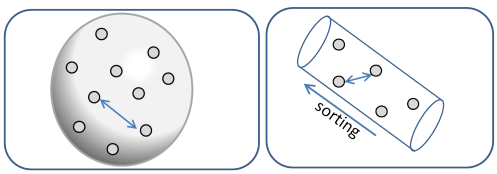
以上の背景のもと、実用的な格子暗号解読アルゴリズムを徹底的に研究し、改良の余地を潰しきることができれば、格子暗号のパラメータをコンピュータ性能の将来予測（例：ムーアの法則）のみから決定することが可能となる。

本課題の目的は、(1)多項式空間アルゴリズムのみが実用的とされていたが、時間-空間トレードオフを用いてよりメモリを多く使うアルゴリズムについて研究を行うこと、(2)格子分野以外のアルゴリズムで、格子暗号解読に適用可能なアルゴリズムについて研究し、その適用可能性について議論を行うことであった。

３．研究の方法

目的(1)に対して、時間-空間トレードオフの議論を行うため、既存の Sieve アルゴリズムの改良を目的とした。この種のアルゴリズムの性能は計算時間 T と使用メモリ空間 S の積 T・S により評価されるため、計算時間を下げることで改良を行う。

具体的には図１のように、N個の点をサンプリングした後に、既存の Sieve アルゴリズムでは球状領域における点のマッチングを行うため、$T=O(N^2)$であったが、右図のように細長い円筒状の領域からのサンプリングを考えると、その軸方向でソートすることで$T=O(N\log N)$まで下げることが可能と考えられる．



既存のアルゴリズム：
球状の領域から格子点をサンプリングするため、マッチングのコストが$O(N^2)$で非効率

提案アルゴリズム：
細長い円柱内の格子点をサンプリングし、円柱の軸方向でソートすることにより、マッチングが$O(N\log N)$で行えるため効率的

図１：アルゴリズム改良の概要

次に目的(2)の手法について述べる．
主に格子暗号の解読に用いられるアルゴリズムは、格子分野で活発に研究されている格子基底簡約アルゴリズム、格子点探索アルゴリズム、そして前述の Sieve アルゴリズムなどが主である。しかし、格子暗号理論以外の分野に目を向ければ無線通信分野における MIMO 通信の信号復元問題と暗号分野の LWE 問題には類似性があり、かつ互いの分野で解析アルゴリズムが独自に発展を遂げていることから、信号復元用アルゴリズムを LWE 問題にあてはめて解析を行うことで新たな知見が得られることが期待される．

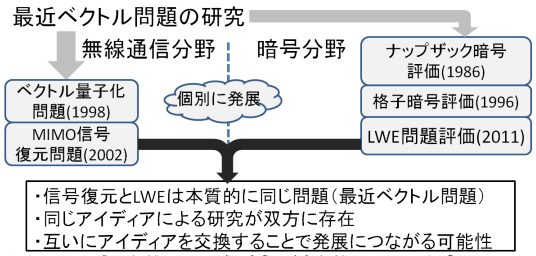


図２：暗号分野と無線通信分野の関連

４．研究成果

課題(1)に関して、格子点列挙アルゴリズムを改良し、円柱内の格子点を列挙するアルゴリズムを作成し、予備実験を行ったところ、Gram-Schmidt 係数の計算時に精度落ちする問題が判明した。これは、大体 100 次元以上の格子基底において 64 ビット浮動小数点実数(C 言語における double 型)を用いた時に発生するが、GPGPU 実装を行う場合に障害となる。そのため、実装を中心とした研究を一旦回避し、理論を中心とした研究を行った。提案アルゴリズムの性能を議論するためには、格子基底を格子基底簡約アルゴリズムによって前処理した後の、基底の Gram-Schmidt 基底の形($|\mathbf{b}^*_1|,\cdots,|\mathbf{b}^*_n|$)について議論する必要がある。

この議論のため、既存の格子基底簡約アルゴリズムの改良と正確な Gram-Schmidt 基底シミュレータの作成を行い、国際会議 Eurocrypt2016 において発表を行った（学会発表①および⑥）。

提案するアルゴリズムの完成系までは至らなかったが、上記基底簡約アルゴリズムを基礎として、格子暗号の安全性評価における時間-空間トレードオフの新たな議論が可能となり、また応用として LWE 問題等の評価が可能となると期待されるため、実用化に向けて一歩前進したと考えられる。

課題(2)に関して、MIMO 通信における信号復元問題を整数上の最適化問題とみて、整数計画法ソルバーを用いる解析に着目し、この手法を LWE 問題の亜種である binary-LWE 問題に対して適用することで、新たな結果を得た。（学会発表⑤）binary LWE 問題は固定された秘密ベクトル $\mathbf{s}\in\{0,1\}^n$ から以下のサンプル $(\mathbf{a}_i, b_i)$ $(i=1,2,\cdots,$ ただし $b_i=\langle\mathbf{a}_i,\mathbf{s}\rangle+e_i$, e_i はエラーで、離散ガウス分布から取られる）が与えられた時に、$\mathbf{s}$ を復元する問題であり、解が一意に定まるためにはある程度のサンプル数を与える必要がある。この結果の特徴として、binary-LWE 問題を必要最低限のサンプル数で解くことが可能であることが実験的に示されており、これは与えられた情報から貪欲に信号を復元する通信理論との対応が見て取れる。今後も、信号復元に用いられる類似手法である Semi-definite relaxation 等との組み合わせで発展する可能性がある。

以上の結果(1)(2)の他に、格子暗号の安全性の根拠となっている LWE 問題の現実的な評価を行い、実際のプロトコルのパラメータ設定を行った。（学会発表②、③、④）

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　１件）

① 清藤　武暢, 青野　良範, 四方　順司, ”量子コンピュータの解読に耐えうる暗号アルゴリズム”, 日本銀行金融研究所機関誌『金融研究』, 査読有, 第３４巻第４号, 2015 年 10 月, pp. 135-170.
http://www.imes.boj.or.jp/research/abstracts/japanese/15-J-09.html

〔学会発表〕（計　6 件）

① Yoshinori Aono, Yuntao Wang, Takuya Hayashi, Tsuyoshi Takagi " Improved Progressive BKZ Algorithms and their Precise Cost Estimation by Sharp Simulator ", Eurocrypt 2016, 査読有, 2016 年 5 月 12 日,「ウイーン市, オーストリア」.

② Yoshinori Aono, Takuya Hayashi, Le Trieu Phong and Lihua Wang, ”Scalable and Secure Logistic Regression via Homomorphic Encryption”, ACM CODASPY 2016, 査読有, 2016 年 3 月 9 日,「ニューオーリンズ, アメリカ」.

③ 青野 良範, 林 卓也, レ チュウ フォン, 王 立華, “大規模かつプライバシー保護を可能とするロジスティック解析手法の提案”, 暗号と情報セキュリティシンポジウム 2016, 査読無, 2016 年 1 月 19 日, 「ANA クラウンプラザホテル熊本ニュースカイ（熊本県熊本市）」.

④ 青野 良範, 林 卓也, レ チュウ フォン, 王 立華 ” セキュリティアップデータブル準同型暗号を用いた秘匿データの線形回帰計算”, 暗号と情報セキュリティシンポジウム 2015, 査読無, 2015 年 1 月 21 日, 「リーガロイヤルホテル小倉（福岡県北九州市）」.

⑤ 町野 義貴, 青野 良範, 高安 敦, 國廣 昇 ”整数計画問題による binary-LWE 問題の求解アルゴリズム”, 暗号と情報セキュリティシンポジウム 2015, 査読無, 2015 年 1 月 22 日, 「リーガロイヤルホテル小倉（福岡県北九州市）」.

⑥ Yuntao Wang, Yoshinori Aono, Takuya Hayashi, Tsuyoshi Takagi " A New Progressive BKZ Algorithm",暗号と情報セキュリティシンポジウム 2015, 査読無, 2015 年 1 月 22 日, 「リーガロイヤルホテル小倉（福岡県北九州市）」.

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　2　件）

① 名称：サーバ、サービス方法
発明者：王 立華、青野 良範、林 卓也、レ チュウ フォン
権利者： 同上
種類： 特許
番号： 特願 2015-227711
出願年月日： 2015 年 11 月 20 日
国内外の別： 国内

② 名称：サーバ、サービス方法
発明者：レ チュウ フォン, 青野 良範, 林 卓也, 王 立華
権利者： 同上
種類： 特許

番号： 特願 2015-004024
出願年月日： 2015 年 1 月 13 日
国内外の別： 国内

○取得状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

Progressive BKZ C++ library
（2016 年 5 月 7 日公開）
http://www2.nict.go.jp/security/pbkzcode/index.html.

６．研究組織

(1)研究代表者
青野　良範（AONO, Yoshinori）
国立研究開発法人　情報通信研究機構　ネットワークセキュリティ研究所　セキュリティ基盤研究室　研究員
　研究者番号：　50611125