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　　元 年　　５ 月 ３０ 日現在

機関番号：１７４０１
研究種目：基盤研究(C)（一般）
研究期間：2015～2018
課題番号：１５Ｋ０４９７８

研究課題名（和文）P-進解析による耐量子計算機暗号系の構築

研究課題名（英文）Construction of post quantum cryptography systems by p-adic analysis

研究代表者
内藤　幸一郎（Naito, Koichiro）

熊本大学・大学院先端科学研究部（工）・名誉教授

研究者番号：１０１６４１０４

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：本研究では記号力学系理論を利用したp-進カオス解析を行い、生成されたp-進擬似乱数列のランダム性の理論証明と実験検証を行い、さらにその擬似乱数生成列を含むナップザック型行列を利用し、同行列で表されるp-進近似格子を利用した格子暗号系の提案及び、同行列のランダム性を利用して構成される非正則なRamanujanグラフの生成方法の提案を行なった。以上の研究結果及び関連研究結果は学術誌論文18編、学会講演発表論文20編の研究業績成果を得ている。

研究成果の学術的意義や社会的意義
量子計算機の実現が予想される事例が頻繁に報告されている現在、特にランダム性を取り入れ安全性をより高めた暗号研究が早急に必要であるため、本研究で解析されたp-進擬似乱数生成器とそれを利用した格子型暗号系の提案は今後の耐量子計算機暗号研究における重要な基礎研究成果である。さらにまた、極めて高性能な情報拡散伝達性をもつ Ramanujan expanderグラフは情報関連分野における最重要研究課題の一つであるため，本研究で解析されたより一般的な非正則Ramanujanに関わる研究結果も重要な基礎研究成果である。

研究成果の概要（英文）：Using the theory of symbol dynamics and p-adic analysis, we construct pseudorandom generators and we theoretically and numerically estimate their randomness. Constructing the knapsack type matrices which contain these pseudorandom sequences and using the p-adic approximation lattices given by these pseudorandom matrices, we propose some lattice cryptosystems and, furthermore, we propose an construction method of non-regular Ramanujan graphs, the adjacency matrices of which are these pseudorandom matrices. Our total research achievements are 18 papers and 20 lecture papers.

研究分野：基礎解析

キーワード：p-進数論　格子暗号理論　　耐量子計算機暗号　記号力学系理論　expander グラフ　Ramanujanグラフ　擬似乱数生成器

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

p-進解析と実解析との間の最も顕著な相違点はp-進ノルムもしくはp-進絶対値では強三角不等式が成立し、二等辺三角形法則や非アルキメデス的性質が現れることである。この非アルキメデス性質はプランクスケール以下の超微小な物理モデルでも現れることが知られており、理論物理の分野では盛んに p-進解析による研究が展開している。数学的な基礎に相関のあることから､これらの研究がポスト量子コンピュータ暗号の進展に今後深く影響することも考えられる。代表者のこれまでの研究では、この強三角不等式から導かれる解析的性質を利用した多次元 p-進近似格子の構成を行い、NP 問題である多重ディオファンタス近似問題と整数格子における最小ベクトル値問題を結合することにより、暗号系の構築を行った。その暗号化、復号化の過程でナップザック暗号由来の方式を取り入れている。通常のナップザック暗号では、超増大数列を秘密鍵として利用し、その暗号化、復号化の処理を行なっているが、この暗号に対する決定的な攻撃法が Shamir(1984) 等によって発見されて以来、種々の攻撃回避法が提案されてはいるものの汎用暗号系としての実用化には至っていない。p-進暗号系では、暗号化、復号化過程で p-進絶対値の増大性を持つ p-進数列を利用する。p-進数由来の二等辺三角形法則をその過程で適用することにより、通信文を含む項が完全に秘密鍵と公開鍵から構成される項に吸収される暗号文を構成することができ、Shamir 攻撃を回避でき、その安全性は秘密鍵の計算における NP 困難性で保証されている。オープンソース数式処理ソフト Sage 上にこの暗号系を実装し、暗号化, 復号化, 鍵生成などの処理機能についての計算機実験を行った。

近年の格子暗号系の最先端の研究では、Learning with errors problem や Short integer solution problem などのランダム性に関わる計算困難性を安全性の基礎とする研究が急速に展開している。暗号系の安全性を保証するために導入されるランダム摂動を、記号力学系理論によるカオス的摂動や擬似ランダム摂動に置き換えることにより、安全性が保証され、暗号鍵などのサイズが縮小された極めて斬新な暗号システムの構成が期待できる。代表者の構成したこれまでの格子暗号系では、安全性を飛躍的に高めるランダム性を取り入れた研究にまでは至っていなかったため、暗号的擬似乱数の生成を始めとするランダム性の導入研究が重要な最優先研究課題になっている。

２．研究の目的

代表者のこれまでの研究を基礎として、本研究では処理速度や LLL 攻撃などに対する安全性の理論的, 実験的な研究を進め、実用化を目指す研究を展開することを初年度からの第一の主目的とする。NTRU 暗号はこれまでに実用化された唯一の格子暗号系であり、本研究の p-進解析を利用した格子暗号は全く斬新なアイデアに基づいており、安全性も極めて高いことが予想されるため、実用的汎用性をもつ格子暗号系が構築できることが期待される。記号力学系理論を活用した p-進カオス解析のこれまでの研究成果を利用し、擬似ランダム性を取り入れたより強固な安全性が保証される新方式の p-進型ナップザック暗号を構築することが本研究の目的である。量子計算機の出現が現実となっている現状では、耐量子計算機暗号系の構築が必須となっている現在、本研究は極めて重要な研究課題を含んでいる。

３．研究の方法

格子暗号攻撃に最もよく利用される LLL アルゴリズムは現在も様々な改良が試みられており、これらの改良による格子最小ベクトル問題解法の次元世界記録への挑戦が Web 上で続いている。このため最速、最良のアルゴリズムの情報が常に必要であり、これらに対抗できる暗号系の開発、改良を重ねていかなければならない状況である。このため、国際会議などでの参加、発表、情報収集交流を常時行なった。さらに、擬似ランダム列を含む p-進型ナップザック型行列の理論及び数値実験的解析が本研究の最重要課題であるため、関連する国内外の研究集会へ積極的に参加し、乱数研究の理論及び数値解析研究に関わる最新情報収集を行なった。

LLL 攻撃や乱数度検証テストではオープンソース Sage を利用して行列の固有値計算等の数値実験を行っていたが、次元数が 500 を超える高次元では Sage 上 による単純数値計算の限界に達しているため、Numpy 等の数値計算パッケージを活用するなど、最新のソフトウエアの導入、更新を常時行なっている。

４．研究成果（[ⓝ] は雑誌論文リスト、(ⓝ)は学会発表リストより引用）

H27 年度には代表者は p-進 Liouville 数を振動数としてもつ準周期離散力学系の再帰性について解析し、再帰性を表す指標である再帰的次元の GAP 値が正の値をとることを示し、軌道の予測不能性の評価を行った。これらの研究結果については学術論文誌に発表した[⑮]。また、代表者が指導する博士後期課程学生がこの結果に関連する共同研究により九州若手数学賞を受賞した（⑱）。p-進解析の暗号理論への応用として、Shamir 型攻撃に耐性のある p-進ナップザック暗号方式を提案し､その研究結果について国際研究集会で講演発表を行った(⑳)。さらに、より強い安全性をもつ commitment scheme 付の p-進ナップザック暗号方式を構成、提案した。これらの研究結果については、国内研究集会（⑯）、国内学会（⑰）で講演発表を行った。関連する研究発表により､代表者が指導する博士前期課程学生が九州若手数学者発表賞を受賞した。分担者城本氏は暗号理論に深く関連する符号理論分野における Kung の定理の一般化について研究を行い、この研究結果を学術論文誌に発表し[⑭]、関連する符号理論についての多数の研

究結果を国内外の学会で発表した（⑮,⑲）。

H28 年度に代表者は記号力学系理論と p-進数論における非アルキメデス的性質等の共通性を利用した複雑性解析研究解析を行い、フィボナッチ記号列から記号力学的に定義される p-進 extremal number と呼ばれる p-進数と、そのべき乗を振動数として持つ準周期的力学系の再帰的挙動解析を行い、再帰性を表す指標である再帰的次元の GAP 値が正の値をとることを示すことにより、軌道の予測不能性が生じる十分条件を導いた。これらの研究結果については学術論文誌に発表、掲載された[⑥]。p-進解析の暗号理論への応用としては、27 年度に提案された Shamir 型攻撃に耐性のある p-進ナップザック暗号方式よりさらに強い安全性をもつ commitment scheme 付の p-進ナップザック暗号方式を構成提案した。これらの成果について国際学会で講演発表を行い（⑭）、学術論文誌に発表、掲載された[⑪]。さらに、これらの p-進ナップザック暗号系における通信符号の安全性を高める研究や暗号鍵のコンパクト化を進める研究に取り組み、これらの成果については国際学会で招待講演を含む講演発表行い（⑫,⑬）、同国際会議論文誌に掲載され[⑬,⑭]、さらに国際研究集会（⑪）、国内研究集会（⑨）でそれぞれ講演発表を行った。分担者は暗号理論に関連する符号理論分野における研究を進め、研究成果は学術論文誌[⑭]、国際会議論文誌[⑬]に発表、掲載された。さらに多数の研究結果を組み合わせ論関連の国内外の学会で発表した（⑧,⑩）。

H29 年度の代表者の研究では、p-進多重近似格子に現れる最短ベクトル問題の計算困難性を利用した格子暗号系の提案と LLL アルゴリズムを用いたその安全性に関わる数値実験結果を学術論文誌に発表した[⑦,⑧,⑨]。さらに、p-進馬蹄写像で定義される記号力学系のカオス性を証明し、この応用として擬似乱数生成器を提案し、生成された p-進擬似乱数列の乱数度をランダム行列理論検定により評価した。この研究成果については国際学会で基調講演発表を行い（⑥）、同国際会議論文誌に掲載予定である[②]。分担者は暗号理論に関連する符号理論分野における研究成果を、国際学術論文誌に発表し[⑩]、国際学会で招待講演発表を行った（⑧）。さらに、国内外の研究集会で最新の研究成果の講演発表を行っている（④,⑤）。

H30 年度の新たな研究は、p-進ロジスティック写像や p-進スメール馬蹄型写像による離散力学系のランダム・カオス性を利用して作成された擬似乱数生成器を用いてランダムグラフ隣接行列を構成し、最も優れた情報伝達性能をもつ expander グラフである Ramanujan グラフの生成を行なうことを主目的としている。極小のシードである一つの p-進数から p-進カオス写像を利用して擬似乱数列を生成し、この列を含むナップザック型ランダム行列を作成し、さらに LLL アルゴリズムにより簡約基底を持つ擬似ランダム行列を作成した。作成した擬似ランダム行列の各列を連結することにより擬似乱数列を構成し、RMT テストを用いてその乱数度の検証を行なった。さらに、生成された擬似ランダム行列を元にグラフ隣接行列を構成し、その固有値分布を測定することにより、Ramanujan グラフの隣接行列特有の固有値分布との比較検証実験を行なった。本研究で構成される非正則 Ramanujan グラフには mild, naive Ramanujan 等がこれまで定義されているが、各非正則グラフの固有値分布を極めて高い確率で満たしていることが検証された。これらの研究結果は、国際学会における基調講演で発表され（①）、学術雑誌に掲載予定である[①]。分担者は暗号理論に関連する符号理論分野における研究をさらに進め、研究成果は学術論文誌[⑤]に発表、掲載された。さらに多数の研究結果を組み合わせ論関連の国内外の学会で発表した（②,③）。

５．主な発表論文等

〔雑誌論文〕（計 18 件）

① Koichiro Naito, Pseudorandom number generator by p-adic chaos and Ramanujan expander graphs, Linear and Nonlinear Analysis, to appear in 2019, 査読有.

② Koichiro Naito, Randomness of p-adic discrete dynamical systems and its applications to cryptosystems, Proc. 10th International Conference on Nonlinear Anal. Convex Anal. 2017, to appear in 2019, 査読有.

③ Shoichi Kamada and Koichiro Naito, Shortest vector problems of p-adic random lattices and their application to a p-adic knapsack type cryptosystem, Journal of Nonlinear and Convex Analysis 19, 2018, 1587-1597, 査読有.

④ Shoichi Kamada and Koichiro Naito, Simultaneous approximation problems and knapsack cryptosystems with commitment schemes in p-adic numberlands, Journal of Nonlinear and Convex Analysis 19, 2018, 1599-1608, 査読有.

⑤ Yoshitaka Koga, Tatsuya Maruta and Keisuke Shiromoto, On critical exponents of Dowling matroids, Designs, Codes and Cryptography 86, 2018, 1947-1962, 査読有. DOI: 10.1007/s10623-017-0431-8

⑥ Shoichi Kamada and Koichiro Naito, Unpredictability of quasi-periodic dynamical systems with multiple frequencies of a p-adic extremal number and its square, Journal of Nonlinear and Convex Analysis 18, 2018, 1349-1359, 査読有.

⑦ Hirohito Inoue and Koichiro Naito, The shortest vector problems in p-adic lattices and simultaneous approximation problems of padic numbers, Linear and Nonlinear Analysis 3, 2017, 213-224, 査読有.

⑧ Hirohito Inoue, Shoichi Kamada and Koichiro Naito, Simultaneous approximations of

p-adic numbers and their applications to cryptography, Linear and Nonlinear Analysis 3, 2017, 225-238. 査読有.

⑨ Hirohito Inoue, Shoichi Kamada and Koichiro Naito, Transference principle on simultaneous approximation problems of p-adic numbers and multidimensional p-adic approximation lattices, Linear and Nonlinear Analysis 3, 2017, 239-249, 査読有.

⑩ Y. Koga, T. Maruta and K. Shiromoto, On critical exponents of Dowling matroids, Designs, Codes and Cryptography, 2017, 1-16, 査読有.

⑪ Hirohito Inoue, Shoichi Kamada and Koichiro Naito, Simultaneous Approximation Problems of p-Adic Numbers and p-Adic Knapsack Cryptosystems - Alice in p-Adic Numberland -, P-Adic Numbers, Ultrametric Analysis, and Applications 8, 2016, 312-324, 査読有. DOI:10.1134/S207004661604004X

⑫ Hirohito Inoue, Shoichi Kamada and Koichiro Naito, Transference principle on simultaneous approximation problems of p-adic numbers and construction of lattice based cryptosystems, 京都大学数理解析研究所講究録 2011, 2016, 57-63, 査読無.

⑬ Thomas Britz and Keisuke Shiromoto, On the Covering Dimension of a Linear Code, IEEE Trans. Information Theory 62, 2016, 2694-2701, 査読有.

⑭ Trygve Johnsen, Keisuke Shiromoto and Hugues Verdure, A generalization of Kung's theorem, Des. Codes Cryptography 81, 2016, 169-178, 査読有.
DOI: 10.1007/s10623-015-0139-6

⑮ Hirohito Inoue and Koichiro Naito, Entropy and recurrent dimensions of discrete dynamical systems given by p-adic expansions, P-Adic Numbers, Ultrametric Analysis, and Applications 7, 2015, 157-167, 査読有.DOI: 10.1134/S2070046615020077

⑯ Hirohito Inoue and Koichiro Naito, Simultaneous rational approximations of a p-adic number and its powers by p-adic approximation lattices, Proc. of the 8th International Conf. on Nonlinear Anal. and Convex Anal., 2015, 155-166, 査読有.

⑰ Hirohito Inoue, Koichiro Naito, Yuma Yamada, Lattice reduction algorithms and their cryptographic applications, Proc. of the 8th International Conf. on Nonlinear Anal. and Convex Anal., 2015, 167-176, 査読有.

⑱ Hirohito Inoue and Koichiro Naito, The shortest vector problems in p-adic approximation lattices and their applications to cryptography, 京都大学数理解析研究所講究録 1963 「非線形解析学と凸解析学の研究」, 2015, 16-23, 査読無.

〔学会発表〕(計 20 件)

① Koichiro Naito, Pseudorandom number generator by p-adic chaos and Ramanujan expander graphs, The 6th Asian Conference on Nonlinear Analysis and Optimization 2018 (基調講演).

② Keisuke Shiromoto, Critical Problem for Binary Matroids, The 17th Japan-Korea Workshop on Algebra and Combinatorics, The 17th Japan-Korea Workshop on Algebra and Combinatorics, 2018 (招待講演).

③ Keisuke Shiromoto, Critical Problem for Binary Matroids, Monash Univ. Discrete Maths Research Group Meeting, 2018 (招待講演).

④ Keisuke Shiromoto, Codes with Rank Metric and Matroids, The Japanese Conference on Combinatorics and its Applications, 2018.

⑤ Keisuke Shiromoto, Critical Problem for matroids and Code, Discrete Structures and Algorithms Seminar in University of Melbourne 2018 (招待講演)

⑥ Koichiro Naito, Unpredictability and randomness of p-adic symbolic dynamical systems, The 10th Anniversary Conference on Nonlinear Analysis and Convex Analysis 2017 (基調講演).

⑦ Koichiro Naito, Randomness of p-adic discrete dynamical systems and its applications to cryptosystem, The 10th Anniversary Conference on Nonlinear Analysis and Convex Analysis 2017.

⑧ Keisuke Shiromoto, Matroids and Codes with Rank Metric, 5th International Combinatorics Conference (5ICC) 2017 (招待講演).

⑨ Shoichi Kamada and Koichiro Naito, Compact knapsack problems and p-adic lattices, Workshop「数論とエルゴード理論 2017」.

⑩ Keisuke Shiromoto, Critical problem for matroids and codes, Discrete Mathematics Research Group meeting 2017.

⑪ Shoichi Kamada and Koichiro Naito, Construction of lattice based cryptosystems by simultaneous approximation problems in p-adic numberlands, RIMS International

Workshop on Nonlinear Analysis and Convex Analysis 2016（招待講演）.

⑫ Shoichi Kamada and Koichiro Naito, Shortest vector problems on the random p-adic lattices given by powers of a p-adic number and their applications to p-adic knapsack type cryptosystem, The 6th Asian Conf. on Nonlinear Analysis and Optimization 2016（招待講演）.

⑬ Shoichi Kamada and Koichiro Naito, Simultaneous approximation problems and knapsack cryptosystems with commitment schemes in p-adic numberlands, The 6th Asian Conf. on Nonlinear Analysis and Optimization 2016.

⑭ Hirohito Inoue, Shoichi Kamada, Koichiro Naito and Keisuke Shiromoto, Simultaneous approximation problems and knapsack cryptosystems in p-adic numberlands, Numeration 2016.

⑮ Keisuke Shiromoto, On the covering number of matroids, The 40th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing 2016.

⑯ Shoichi Kamada, Hirohito Inoue, Koichiro Naito, Multi-dimensional p-adic approximation lattices and their applications to knapsack cryptosystems, Workshop「数論とエルゴード理論 2016」.

⑰ Shoichi Kamada, Hirohito Inoue, Koichiro Naito, Simultaneous approximation problems of p-adic numbers and their application to lattice based Cryptosystems, 日本数学会九州支部会 2016.

⑱ Hirohito Inoue, Koichiro Naito, Complexity and recurrency of p-adic dynamical systems and its application, 日本数学会九州支部会 2016 （招待講演）.

⑲ Keisuke Shiromoto, Critical problem in coding theory, The 4th Japan-Taiwan Conference on Combinatorics and its Applications 2016.

⑳ Shoichi Kamada, Hirohito Inoue, Koichiro Naito, Transference principle on simultaneous approximation problems of p-adic numbers and construction of lattice based cryptosystems, RIMS International Workshop on Nonlinear Analysis and Convex Analysis 2015 （招待講演）.

〔図書〕（計　　件）

〔産業財産権〕
○出願状況（計　　件）

名称：
発明者：
権利者：
種類：
番号：
出願年：
国内外の別：

○取得状況（計　　件）

名称：
発明者：
権利者：
種類：
番号：
取得年：
国内外の別：

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者

研究分担者氏名：城本　啓介

ローマ字氏名：(SHIROMOTO, keisuke)

所属研究機関名：熊本大学
部局名：大学院先端科学研究部（工）
職名：教授
研究者番号（8桁）：00343666

(2)研究協力者
研究協力者氏名：
ローマ字氏名：