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　６ 年　 ６ 月 １９ 日現在

機関番号：３１３０２
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ１１８１７

研究課題名（和文）耐タンパー性を持つ論理演算型軽量ブロック暗号の設計原理の研究

研究課題名（英文）A Study of Design Principles for Tamper-Resistant Logic-Based Lightweight Block Ciphers

研究代表者

神永　正博（KAMINAGA, Masahiro）

東北学院大学・工学部・教授

研究者番号：６０２６６８７２

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：耐タンパー性を持つ論理演算型軽量ブロック暗号の設計原理の研究のため、格子行列を用いたフェイステル型ブロック暗号（LBF）の提案やSVPの解法、乱数発生装置のモデリングに関する研究を進めた。LBFのF関数としてランダムGoldstein-Mayer格子を調査し、LBFの差分解読法に関する研究を深化させた。これらの研究は、量子計算機に耐性を持つ暗号システムの構築に貢献している。今後もランダム格子の暗号理論的性質の研究を進める予定である。現在、LBFに関する論文を投稿中（プレプリントは、Cryprology eprint archive 2024/763から取得可能）である。

研究成果の学術的意義や社会的意義
本研究は、暗号理論における格子理論の応用を深めるものであり、特に格子を用いたブロック暗号の構築と解析に焦点を当てている。具体的には、ランダム格子の数学的特性を明らかにし、それをフェイステル型ブロック暗号（LBF）に応用することで、耐量子計算機性を持つ安全な暗号システムを提案した。この研究は、SIS問題に基づく差分解読法に対する耐性を初めて体系的に検討した点で、理論的なブレークスルーとなる。理論的研究を推進し、耐量子計算機暗号の必要性が高まる中で、新しい暗号技術の確立に貢献した。この成果は、将来の情報セキュリティの基盤を強化し、量子計算時代における安心安全な社会の実現に寄与する。

研究成果の概要（英文）：Our research on the design principles of tamper-resistant logic-based lightweight block ciphers has not only proposed a Feistel-type block cipher using lattice matrices (LBF), but also explored solutions to the SVP and modeled random number generators. We have studied random Goldstein-Mayer lattices as the F function for LBF and deepened our research on differential cryptanalysis of LBF. These studies hold significant promise in the development of cryptographic systems resistant to quantum computing, a crucial area of concern in our field. Our future research will continue to focus on the cryptographic properties of random lattices. We are pleased to share that a paper on LBF is currently under review (a preprint is available at Cryptology ePrint Archive 2024/763).

研究分野：暗号理論

キーワード：格子理論　ランダム格子　ブロック暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

SIMON に代表される非線形変換部に論理演算を導入したブロック暗号が登場し、その差分電力解析、相関電力解析の研究が行われているが、成果に乏しく、なんらかの成果が出ている場合でも、ブロックサイズが 32 ビットであるなど非現実的な仮定を必要とした。その原因として考えられるのは、論理演算を導入したことでテーブルルックアップが不要となり、結果、巨大な S ボックスが存在するのと等価になったことが挙げられる。SIMON の S ボックスの設計原理は判然とせず、ad-hoc なものに見える。実際、非線形変換部の出力は一様ではなく、値域は入力よりもかなり小さくなる。結果ビット雪崩効果も十分ではないが、ラウンド数を増やすことで安全性を向上させていた。Ad-hoc な非線形変換部のままでは、この問題を解決できないことが問題と思われたため、なんらかの数学的な設計原理が必要であった。

一方、量子計算機の研究が急速に進展してきており、Shor のアルゴリズムによる RSA 暗号、楕円曲線暗号の解読がじわじわと現実になりつつあった。ブロック暗号も Grover のアルゴリズムにより影響を受けることがわかっていた。ブロック暗号においても、量子計算機の出現に耐えられるものが求められ、これらが数学的に保証されれば最善と考えられた。量子計算機でも解けない暗号（耐量子計算機暗号）の研究は、公開鍵暗号に集中していた。特に LWE(Learning with Errors)に基づくものが大部分を占め、SIS(Short Integer Solution)に基づく暗号はわずかで、しかも純粋理論的なものであった。

研究開始当初は、新型コロナウイルスの影響で大学構内に立ち入ることもままならず、オンライン講義の準備に追われ、実験的な研究が困難であったため、理論的な研究に集中した。

２．研究の目的

本研究は、ブロック暗号の構成において、特に差分および相関電力解析に強い大きな S ボックスを実現する論理演算型の非線形変換の設計を目指したものである。

３．研究の方法

F 関数における S ボックスとして採用可能な論理演算を種々検討する。SIMON、SPECK、SIMECK などが参考になるので、これらの論理演算に対し暗号理論的な考察、つまり、差分特性、線形特性を調べる。一方で、非線形変換部の演算として、特に、q-ary 格子行列を用いた Ajtai のハッシュ関数を採用した場合にブロック暗号としてよい性質を持つかを調べる。格子については、これまでに、ラビン暗号の最適なパディングサイズの決定問題を扱った論文 M. Kaminaga, T. Suzuki, and M.Fukase, Determining the Optimal Random-Padding Size for Rabin Cryptosystems, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 14, NO. 8, AUGUST 2019 を書いたのみでまだ十分に使いこなせているとは言えなかった。この論文で扱ったのは、特定の多項式の零点を計算するための deterministic な格子であり、ランダムではなかったからである。そこで、ランダム格子に習熟するため、ランダム格子の性質の数学的に厳密な定義、そのハール測度などを検討し、それらを利用して逐次最小のノルム分布や、遺伝的アルゴリズムなどによる格子簡約の研究を行うこととした。一つのゴールとして、Ajtai のハッシュ関数を F 関数としたフェイステル型ブロック暗号に差分解読法を適用し、安全なラウンド数を見積もる。

４．研究成果

当初は論理演算型ブロック暗号の種々の方式を考えており、耐タンパー技術で用いられる小型の dual oscillator を用いた乱数生成のモデル化など周辺の論文を書いた。その論理演算による非線形変換が、ad-hoc に設計されると安全性の証明ができない点が大きな問題であった。そこで、格子行列を用いた Ajtai のハッシュ関数を F 関数に持つフェイステル型ブロック暗号 LBF（Lattice based Feistel cipher）を設計することを思いついた。ランダム格子行列の扱いを習得するため、遺伝的アルゴリズムによる SVP の解法の論文と Goldstein-Mayer 格子のグラム行列の固有値と最短ベクトルの研究を行った。ランダム格子の数学的研究は、Siegel に始まるが、L 関数との関係や双曲幾何との関係など、数学的に興味深い性質を持つ。例えば 2 次元のランダム格子は Poincare 上半平面と対応する。Goldstein-Mayer 格子は、ランダム格子における代表元の集まりと考えることができるものである（ただし、少数ながらこのタイプとは異なる格子も存在する）。最終年度にようやく SIS(Short Integer Solution)問題に基礎を置く具体的な LBF に対する差分解読法を詳細に検討し、その統計的特性を導き、安全なラウンド数などを求めることに成功した。その手法は、折りたたまれた二次元正規分布と一般化極値分布を組み合わせた新しいものであり、今後、類似の研究をする際の基礎となるものと考えられる。この結果は、

論文 4 としてまとめられ、IEEE Transactions on Information Theory に投稿中である。以下の 4 つの論文を発表した（3 つは出版済、1 つは投稿中で preprint を公開）。なお、完成には至らなかったが、ランダム格子の逐次最小のノルム分布を格子のハール測度に基づいて計算中であり、今後論文として発表する予定である。

(1) Masahiro Kaminaga, Random Numbers Generated by the Oscillator Sampling Method as a Renewal Process, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences Vol.E105-A(No.2), pp. 118-121 2022 年 2 月

(2) Masaharu Fukase, Masahiro Kaminaga, Improving genetic algorithms for solving the SVP: focusing on low memory consumption and high reproducibility, Iran Journal of Computer Science 5(4), pp. 359-372 2022 年 12 月

(3) Masahiro Kaminaga, Upper bound for the coefficients of the shortest vector of random lattice, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science E106-A(12), pp. 1585-1588, 2023 年 12 月

(4) Yu Morishima, Masahiro Kaminaga, On SIS-problem-based random Feistel ciphers and its statistical evaluation of resistance against differential cryptanalysis（投稿中）preprint は、 Cryptology ePrint Archive 2024/763 から取得可能

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Fukase Masaharu, Kaminaga Masahiro	４．巻 5
２．論文標題 Improving genetic algorithms for solving the SVP: focusing on low memory consumption and high reproducibility	５．発行年 2022年
３．雑誌名 Iran Journal of Computer Science	６．最初と最後の頁 359～372
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s42044-022-00118-5	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Masahiro Kaminaga	４．巻 Vol.E105-A(No.2)
２．論文標題 Random Numbers Generated by the Oscillator Sampling Method as a Renewal Process	５．発行年 2022年
３．雑誌名 IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 118-121
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021EAL2023	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 KAMINAGA Masahiro	４．巻 E106.A
２．論文標題 Upper Bound for the Coefficients of the Shortest Vector of Random Lattice	５．発行年 2023年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1585～1588
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2023EAL2032	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 大宮悠暉
２．発表標題 格子行列に基づくブロック暗号の提案と解析
３．学会等名 電気関係学会東北支部連合大会
４．発表年 2022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
研究分担者	志子田　有光 (SHIKODA Arimitsu) (00215972)	東北学院大学・工学部・教授 (31302)	
研究分担者	鈴木　利則 (SUZUKI Toshinori) (20500432)	東北学院大学・工学部・教授 (31302)	
研究分担者	深瀬　道晴 (FUKASE Masaharu) (30626502)	東北学院大学・工学部・准教授 (31302)	
研究分担者	吉川　英機 (YOSHIKAWA Hideki) (60259885)	東北学院大学・工学部・教授 (31302)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関