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　　６ 月 １２ 日現在

機関番号：２４５０６
研究種目：若手研究(B)
研究期間：2017～2018
課題番号：１７Ｋ１２６９８

研究課題名（和文）軽量ストリーム暗号の構成法に関する研究

研究課題名（英文）Research on Lightweight Stream cipher

研究代表者
五十部　孝典（Isobe, Takanori）

兵庫県立大学・応用情報科学研究科・准教授

研究者番号：３０７８５４６５

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：本研究では，軽量ストリーム暗号に対する安全性評価とその技術を用いた新しい軽量ストリーム暗号設計を行った．安全性評価に関しては，軽量ストリーム暗号の構造に特化した新しい解析技術をいくつも開発し，既存の軽量ストリーム暗号の厳密な安全性の見積もりに成功した．また軽量ストリーム暗号に適した構成方法や実装方法についても明らかにした．これらの解析，設計技術をもとに，実際に3つの軽量ストリーム暗号，LILLE，TRIVIUM　Triadを設計して提案した．それぞれ軽量実装，低消費電力，安全性に関して既存技術をはるかにしのぐ性能の達成に成功した．特にTriadは高い安全性と優れた性能を持っている．

研究成果の学術的意義や社会的意義
本研究では，未解決問題であった様々な新しい軽量ストリーム暗号の安全性評価手法を開発することに成功した．これにより，構造毎の正確な安全性評価ができ，安全でかつ効率的な構造の設計が可能になった．実際，新しい設計方法に基づく軽量ストリーム暗号アルゴリズムを複数開発した．これは，学術レベルでは軽量ストリーム暗号の理論の発展に寄与し，また産業レベルでは，今後世の中で求められる様々な実装や安全性要求に適応可能な軽量なストリーム暗号の効果的な開発につながる．具体的には，RFIDやセンサー等のリソースの乏しいデバイスに対しても実装可能なストリーム暗号の開発等につながり，その波及効果は非常に大きい．

研究成果の概要（英文）：In this research project, we proposed new security evaluation methods for lightweight stream ciphers. Specifically, we focused on some structural properties of lightweight stream ciphers, and then developed new attacks exploiting structures of stream ciphers such as impossible collision attacks, cube attacks based on non-blackbox analysis. These enable more accurate security evaluations of known stream ciphers, and finding some insights to design new primitives and components for lightweight stream ciphers. As a result, we succeeded in designing new three lightweight stream ciphers called LILLE, TRIVIUM and Triad. LILLE is based on an Even-Mansour structure, and achieves low area while keeping a strong security property. TRIVIUM is a variant of well-known stream cipher Trivium, and enables low energy implementation but requires more area than LILLE. Triad achieves lightweight implementation, low energy, and high security. These are expected to be used for IoT devices.

研究分野：暗号技術

キーワード：共通鍵暗号　ストリーム暗号　軽量暗号　暗号解析

１．研究開始当初の背景

ストリーム暗号は共通鍵暗号の一つであり，秘密鍵と初期化ベクトルからキーストリームと呼ばれる擬似乱数系列を作成し，平文との排他的論理和をとることで暗号文を生成する．代表的なストリーム暗号としてはSSL/TLS等で用いられているRC4や，ISO標準のMUGI, SNOW 2.0, KCipher-2 が挙げられる．これらは主にソフトウェアで高速に実装できるように開発されたものである．近年，モノのインターネット(IoT)を背景として，センサーノードやRFID 等のハードウェアリソースの制限された環境においても実装可能な回路規模の小さい軽量暗号が注目を浴びている．2013 年から米国国立標準技術研究所（NIST）も標準化に向けた活動をスタートさせるなど産業的にも注目されている.共通鍵暗号の一種であるブロック暗号に関しては，2011 年頃から活発に研究が行われており，多くの有力な暗号方式が提案されている．

ストリーム暗号に関しては，FSE 2015 において新しい軽量設計方法が示されたが，その後すぐに他の研究者により脆弱性が指摘された．軽量のストリーム暗号の安全な設計方法については学術レベルにおいても，未解決な問題となっている．軽量ブロック暗号は基本的にブロックサイズが小さいため(例えば 64 bits)，一つの鍵で暗号化できるデータサイズに制限があり，birthday bound と呼ばれる上限（数 Gytes)を超えた場合には，安全性に大きな問題があることが指摘されている．一方，ストリーム暗号は，特に暗号化可能なデータサイズの制限がないことや初期化フェーズが終われば，非常に高速に動作することなどから，多くのデータを一つの鍵で暗号化したい場合にはブロック暗号よりも優れている．IoT のユースケースでは鍵交換は頻繁に行われないことも十分考えられるため，一つの鍵で長いデータを高速に演算可能な，軽量なストリーム暗号の開発が求められている．

２．研究の目的

本研究では，軽量ストリーム暗号の安全な設計方法を確立することを目的とする．具体的には,既知の脆弱性に対して耐性のある安全な軽量ストリーム暗号の汎用的な構成方法を与える．また，構成方法の有用性を示すため，実装性能と安全性を両立した内部関数を考案し，実際の軽量ストリーム暗号アルゴリズムを開発する．この研究課題により，軽量ストリーム暗号の汎用的な設計方法を初めて与えることができ，さらにその設計方法に基づく具体的なストリーム暗号アルゴリズムを開発できる．これは，軽量ストリーム暗号の理論の発展に寄与し，今後世の中で求められる様々な要求に適応可能な軽量なストリーム暗号の効果的な開発につながると考える．具体的には，RFID やセンサー等のリソースの乏しいデバイスに対しても実装可能なストリーム暗号や，クラウド環境における重要なセキュリティ技術である準同型暗号，マルチパーティ計算において効率的に演算可能なストリーム暗号等の開発等につながり，その波及効果は産業的にも非常に大きい．

３．研究の方法

研究期間の前半(平成 29 年度)において，既存の方式の脆弱性について調査，検討し，これらに対して耐性のある構造を明らかにする．一般的に軽量ストリーム暗号は，レジスタのサイズを削減するために内部状態のサイズをできる限り小さくする必要がある．そのような構成方法の場合，安全性評価の手法が定かでない．そのため，新しい安全性性評価方法を考案するとともに，それに対して理論的に安全性を証明可能な構造を与える．

研究期間の後半(平成 30 年度)では，前半で考案した構成方法に対して，実装性能と安全性を両立した内部関数を開発し，実際の軽量ストリーム暗号アルゴリズムを設計する．さらに，さまざまな環境において実装評価を実施し，また既存のすべての攻撃に対しても安全性評価を行い，既存技術より優れている客観的な評価を与える．また，第三者が実際に利用できるようにインターネット上でソースコード等も公開する予定である．これらの結果は，段階ごとに国際会議，国際ジャーナルに投稿して公開していく．

以上のようにこの期間で，軽量ストリーム暗号への基礎的な構成方法の理論から，実際に世の中で使うことのできる安全性の高いかつ実装性能の高いストリーム暗号を成果として生み出す．

４．研究成果

平成 29 年度は，当初の計画通り以下の 2 点について研究を進めた．
(1)軽量ストリーム暗号に対する攻撃方法の整理
(2)既存の攻撃に対して耐性のある構成方法の考案

(1)に関しては，既存の軽量ストリーム暗号に対して有効な攻撃方法に対して検討した．具体的には，ストリーム暗号 LIZARD に対しては，内部状態の衝突を利用した不能衝突攻撃と呼ぶ新しい解析手法を開発した.これにより LIZARD の安全性のマージンを正確に見積もることに成功し，設計者の評価よりも安全性のマージンが少ないことを明らかにした．この成果は，国際会議 FSE2018 に採録され高い評価を得た[雑誌論文⑩]．さらに，Cube 攻撃と呼ばれる強力な攻撃方

法の一般化と改良を行い，より厳密な安全性評価を可能にした［学会発表⑱］．また別の構造の軽量ストリーム暗号である Plantlet に対しても，タイムメモリトレードオフ攻撃の一般化を行い，より現実的なパラメータでの評価を行った[学会発表⑫]．さらに，ストリーム暗号に有効な攻撃手法である高速相関攻撃に関しても，改良を行い，より厳密な安全性評価を行った[学会発表⑭]．

(2)に関しては，まず強い安全性を保障することが可能な Even-Mansour 構成方法に着目して研究を進めた．この構成方法では，いい置換さえ設計できれば，既存の攻撃方法に対しては安全性を保障できるため，安全な軽量ストリーム暗号の有力な構成方法である．具体的には，より強い安全性を保障できる 2-round Even-Mansour 構成方法の安全性の上界を更新して，安全性の限界を明らかにし，この構成が有力な候補であることを示した[学会発⑲]．また，もう一つの有力な構造である一般化 Feistel 構造についても評価を行い，新たな効率的な構造を考案した．[学会発表⑬]．具体的には少ない演算量で安全性を達成する構成を発見した．また，低消費実装技術についても，Inverse Gating 技術を開発し，実装時に工夫することで低消費電力化に成功した[学会発表⑦]

平成 30 年度は当初の計画通り以下の 2 点について研究を進めた．

(3)実装効率のよい内部関数の候補の開発
(4)実際の軽量ストリーム暗号の開発

(3)に関しては，効率の良い内部関数の安全性を評価する技術として，符号理論をベースにした高速相関攻撃の改良と代数構造を用いた評価方法の改良を行い，より厳密な安全性を評価する手法を開発した．これらの 2 つの研究成果は暗号系のトップカンファレンス CRYPTO 2018 に採録されるなど学術レベルで高い評価を得た[学会発表⑧⑨]．また，ハードウェアにおいて効率でかつ高い安全性を達成可能な線形関数を見つけることにも成功し，共通鍵暗号のトップジャーナル ToSC 2019 にも採録された[雑誌論文⑥]．さらに，ストリーム RC4 の構造の理論的解析[雑誌論文⑨]と，Kreyvium に対する解析結果[雑誌論文⑧]，代数構造を用いた評価方法[雑誌論文⑦]，MILP を用いた評価方法[雑誌論文③，学会発表⑪]，ストリーム暗号の乱数性[学会発表⑰⑱]，暗号プロトコル[学会発表⑩，⑮]など安全性評価技術も開発を行い，(4)の設計技術に生かした．

(4)に関しては，(1)-(3)の結果を用いて，3 つの実際のストリーム暗号の開発を行った．１つめはストリーム暗号 LILLE で，Even-Mansour 構造をベースにした構成方法であり，軽量用途の性能が優れている[雑誌論文④]．2 つ目は，低消費電力用途を目的としたもので，既存構成と比べて約 1/10 の低消費電力化に成功した[雑誌論文⑤]．この技術を基にした認証暗号とハッシュ関数を次世代の標準軽量暗号を選定することを目的とした NIST の軽量暗号プロジェクトに提案した．[学会発表⑥]

結果として，軽量ストリーム暗号に対しての多くの新しい解析を考案し，効率的でかつ安全な構成方法を複数提案した．これらの結果として，実際に 3 つの新しい軽量ストリーム暗号の開発に成功した．それぞれ，軽量，低消費電力，安全性の観点で既存のものよりはるかに優れており，今後の IoT の用途での利用が期待される技術であり，本研究の目的は十分に達成された．

学術的にも，査読付きの国際会議，ジャーナルに 17 件採録されており，その中には CRYPTO, ASIACRYPT, ToSC/FSE 等の国際会議暗号学会が主催する暗号のトップカンファレンスへの論文も多数含まれており，国際的にも非常に評価の高い成果を生み出した．また学会発表⑮は SCIS イノベーション論文賞，学会発表⑯⑰ISEC 情報セキュリティ研究奨励賞を受賞した．

５．主な発表論文等

〔雑誌論文〕（計　10 件 ）

① Takanori Isobe and Kyoji Shibutani, ″Meet-in-the-Middle Key Recovery Attacks on A Single-Key Two-Round Even-Mansour Cipher″, IEICE 2018, IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, vol.E102-A, no.11, pp.17-26, Nov. 2019. **［査読あり］**

② Yonglin Hao, Takanori Isobe, Lin Jiao, Chaoyun Li, Willi Meier, Yosuke Todo, and Qingju Wang,, ″Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly″, IEEE Trans. on Computers 2019.(accepted) **［査読あり］**

③ Yuki Funabiki, Yosuke Todo, Takanori Isobe and Masakatu Morii, ″Improved Integral

Attack on HIGHT", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, 2019. (accepted) **[査読あり]**

④ Subhadeep Banik, Takanori Isobe and Masakatu Morii, "On Design of Robust Lightweight Stream Cipher with Short Internal State", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, vol.E101-A, no.1, pp.99-109, 2018. **[査読あり]**

⑤ Subhapeep, Banik, Vasily Mikhalev, Frederik Armknecht, Takanori Isobe, Willi Meier, Andrey Bogdanov, Yuhei Watanabe, Francesco Regazzoni, "Toward Low Energy Stream Ciphers", IACR Trans. Symmetric Cryptol (ToSC/FSE), no.2, pp.20-47 2018. **[査読あり]**

⑥ Gianira N. Alfarano, Christof Beierle, Takanori Isobe, Stefan Kölbl, Gregor Leander, "ShiftRows Alternatives for AES-like Ciphers and Optimal Cell Permutations for Midori and Skinny", IACR Trans. Symmetric Cryptol (ToSC/FSE), no.2, pp.1-19 2018. **[査読あり]**

⑦ Yosuke Todo, Takanori Isobe, Yonglin Hao, and Willi Meier, "Cube Attacks on Non-Blackbox Polynomials Based on Division Property", IEEE Trans. on Computers, vol.67, issue.12, pp.1548-1556, 2018. **[査読あり]**

⑧ Yuhei Watanabe, Takanori Isobe, and Masakatu Morii, "Cryptanalysis of Reduced Kreyvium", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, vol.E101-A, no.9, pp.1548--1556, 2018. **[査読あり]**

⑨ Sonu Jha, Subhadeep Banik, Takanori Isobe, Toshihiro Ohigashi, Santanu Sarkar, "Theoretical Understanding of Some Conditional and Joint Biases in RC4 Stream Cipher", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, vol.E101-A, no.11, pp.1869-1879, Nov. 2018. **[査読あり]**

⑩ Subhadeep Banik, Takanori Isobe, Tingting Cui and Jian Guo, "Some cryptanalytic results on Lizard", IACR Trans. Symmetric Cryptol (ToSC/FSE), no.4, pp.82-98 2017. **[査読あり]**

〔学会発表〕(計 19 件 (うち 7 件査読あり))

① 窪田恵人, 小家武, 藤堂洋介, 五十部孝典, 森井昌克, " Wi-Fi 機器に対する中間者攻撃の実装と考察", 2019 年暗号と情報セキュリティシンポジウム(SCIS 2019), 2019 年 1 月

② 小家武, 五十部孝典, 藤堂洋介, 森井昌克, " Type-1.x 一般化 Feistel 構造におけるブロックシャッフルの評価", 2019 年暗号と情報セキュリティシンポジウム(SCIS 2019), 2019 年 1 月

③ 船引悠生, 藤堂洋介, 五十部孝典, 森井昌克, "Enocoro-128v2 の Cube 攻撃に対する安全性評価", 2019 年暗号と情報セキュリティシンポジウム(SCIS 2019), 2019 年 1 月

④ 正木史明, 渡辺優平, 五十部孝典, "軽量ストリーム暗号に対する衝突攻撃の一般化とその対策", 2019 年暗号と情報セキュリティシンポジウム(SCIS 2019), 2019 年 1 月

⑤ 阪本光星, 峯松一彦, 柴田直, 茂真紀, 久保博靖, 船引悠生, アンドレイボグダノフ, 五十部孝典, " TWINE を基にした Tweakable ブロック暗号の検討", 2019 年暗号と情報セキュリティシンポジウム(SCIS 2019), 2019 年 1 月

⑥ Subahdeep Banik, Takanori Isobe, Willi Meier, Yosuke Todo, Bin Zhang, "Triad", submission to NIST Lightweight cryptography, 2019

⑦ Subhadeep Banik, Andrey Bogdanov, Francesco Regazzoni, Takanori Isobe, Toru Akishita, Harunaga Hiwatari. Inverse Gating for Low Energy Block Ciphers. IEEE International Symposium on Hardware Oriented Security and Trust (IEEE HOST 2018), IEEE Computer Society, pp. 173--176, Springer, 2018. (acceptance rate : 0.26% = 22/84) **[査読あり]**

⑧ Qingju Wang, Yonglin Hao, Yosuke Todo, Chaoyun Li, Takanori Isobe, Willi Meier, ″Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly″, Advances in Cryptology (CRYPTO) 2018, Lecture Note in Computer Science, Part 1, vol. 10991, pp. 275--305, Springer, 2018. (acceptance rate : 0.22% = 79/351) **[査読あり]**

⑨ Yosuke Todo, Takanori Isobe, Willi Meier, Kazumaro Aoki, and Bin Zhang, ″Fast Correlation Attack Revisited --Cryptanalysis on Full Grain-128a, Grain-128, and Grain-v1″, Advances in Cryptology (CRYPTO) 2018, Lecture Note in Computer Science, Part 2, vol. 10992, pp. 129--159, Springer, 2018. (acceptance rate : 0.22 = 79/351) **[査読あり]**

⑩ Takanori Isobe and Kazuhiko Minematsu, ″Breaking the Message Integrity of End-to-End Encryption Schemes of LINE″, ESORICS 2018, part2, vol. 11099, pp. 249-268, Springer, 2018. (acceptance rate : 0.19% = 66/283) **[査読あり]**

⑪ Yuki Funabiki, Yosuke Todo, Takanori Isobe and Masakatu Morii, ″Several MILP-Aided Attacks against SNOW 2.0″, CANS 2018, vol. 11124, pp. 394--413, Springer, 2018. (acceptance rate : 0.33% = 26/79) **[査読あり]**

⑫ 正木 史明, 渡辺 優平,五十部 孝典, ″軽量ストリーム暗号に対するタイムメモリデータトレードオフ攻撃の改良″, 2018 年暗号と情報セキュリティシンポジウム(SCIS 2018), 2018 年 1 月

⑬ 小家 武, 五十部 孝典, 藤堂 洋介, 森井 昌克, ″一般化 Feistel 構造における最適なブロックシャッフルの評価″, 2018 年暗号と情報セキュリティシンポジウム(SCIS 2018), 2018 年 1 月.

⑭ 船引 悠生, 藤堂 洋介,五十部 孝典,森井 昌克, ″SNOW 2.0 に対する新たな線形近似探索手法と高速相関攻撃への応用″, 2018 年暗号と情報セキュリティシンポジウム(SCIS 2018), 2018 年 1 月.

⑮ 五十部 孝典, 峯松 一彦, ″LINE の End-to-End Encryption に対するなりすましと偽造攻撃″, 2018 年暗号と情報セキュリティシンポジウム(SCIS 2018), 2018 年 1 月.

⑯ 木村 隼人, 五十部 孝典, 大東 俊博, “ニューラルネットワークを用いた擬似乱数検証ツールに関する検討,” 電子情報通信学会技術研究報告, 情報セキュリティ(ISEC)研究会, ISEC2018, 2018 年 11 月.

⑰ 棚本 清也, 五十部 孝典, 大東 俊博, “ストリーム暗号のバイアス探索に関する統計的な評価手法,” 電子情報通信学会技術研究報告, 情報セキュリティ(ISEC)研究会, ISEC, 2018 年 11 月.

⑱ Yosuke Todo, Takanori Isobe, Yonglin Hao, and Willi Meier, ″Cube Attacks on Non-Blackbox Polynomials Based on Division Property″, Advances in Cryptology (CRYPTO) 2017, Lecture Note in Computer Science, Part 3, vol. 10403, pp. 250--279, Springer, 2017. (acceptance rate : 0.23% = 72/311) **[査読あり]**

⑲ Takanori Isobe and Kyoji Shibutani, ″New Key Recovery Attacks on Minimal Two-Round Even-Mansour Ciphers″, Advanced in Cryptology (ASIACRYPT) 2017, Lecture Note in Computer Science, Part 1, vol. 10624, pp. 244-263, Springer, 2017. (acceptance rate : 0.27% = 67/243) **[査読あり]**

〔図書〕(計　0 件)

〔産業財産権〕
○出願状況（計　0　件）

○取得状況（計　0　件）

〔その他〕
ホームページ等　なし

６．研究組織

(1)研究分担者　なし

(2)研究協力者　なし