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　５ 年　 ５ 月 １０ 日現在

機関番号：２４５０６
研究種目：基盤研究(B)（一般）
研究期間：2019～2022
課題番号：１９Ｈ０２１４１

研究課題名（和文）軽量共通鍵暗号の解析と安全な構成方法とそのIoTへの応用に関する研究

研究課題名（英文）Cryptanalysis and Design of Lightweight Symmetric-key Cryptography and Its Application to IoT

研究代表者

五十部　孝典（Takanori, Isobe）

兵庫県立大学・情報科学研究科・教授

研究者番号：３０７８５４６５

交付決定額（研究期間全体）：（直接経費）　　10,400,000円

研究成果の概要（和文）：本研究では、低回路規模ブロック暗号WARP、低遅延暗号Orthrom、低消費電力暗号Atom、高速暗号Rocca，低遅延ハッシュ関数Areionを開発した。それぞれの実装性能で世界一を達成しているアルゴリズムであり、成果は暗号分野のトップ会議CHES，FSE，SACに採録されるなど学術的にも高い評価を得た。また、軽量暗号への解析技術として、代数攻撃をベースとしたさまざまな解析技術を開発し、Rasta，LowMC，Friet，Lesamntaなどの既存の暗号の解析記録を更新した。この技術もCRYPTO，ASIACRYPTなどのトップ会議に採録されている。

研究成果の学術的意義や社会的意義
本研究では安全なSociety 5.0のため、軽量共通鍵暗号の厳密な安全性評価手法の開発、高い安全性と実装性能を有する軽量共通鍵暗号の構成方法の開発，、軽量共通鍵暗号をベースとした軽量暗号ソリューションの開発を実施した。解析技術としては、NISTの標準候補暗号に対して安全性の解析を行うことで世界的な標準化プロセスに貢献し、軽量共通鍵暗号に対する新しい解析手法を考案した。軽量暗号に対する安全性評価技術をベースに新しい軽量共通鍵暗号の開発を行った。本研究では、128 bit 安全性を有した上で、理論限界に近いハードウェア性能を持つ軽量暗号技術構造を明らかにした。

研究成果の概要（英文）：We developed the low-area scale block cipher WARP, the low-latency cipher Orthrom, the low-power consumption cipher Atom, the high-speed cipher Rocca, and the low-latency hash function Areion. Each of these is an algorithm that has achieved world-leading performance in its respective implementation. Our results have been highly acclaimed academically, having been accepted at top cryptography conferences such as CHES, FSE, and SAC. Furthermore, we developed various analytical techniques based on algebraic attacks as a method for analyzing lightweight ciphers, and we have broken the analysis records for existing ciphers such as Rasta, LowMC, Friet, and Lesamnta. This technology has also been accepted at top conferences such as CRYPTO and ASIACRYPT.

研究分野：暗号

キーワード：軽量暗号　ブロック暗号　ストレージ暗号　ハッシュ関数　代数攻撃　差分攻撃

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景
自動運転，知能ロボット，スマート工場などに代表される超スマート社会（Society5.0）では，大量のセンサーから情報を取得・解析し，クラウド側での他の蓄積データとの比較・分析などを行い，システム全体としての適切な情報処理技術を高効率に行うことが求められる．一般的にデータ収集に用いられるセンシング用のエッジデバイスは十分なハードウェアリソースを持っておらず，軽い演算で実装可能な軽量暗号技術が求められる．

２．研究の目的
本研究では安全な Society 5.0 のため，①軽量共通鍵暗号の厳密な安全性評価手法の開発，②高い安全性と実装性能を有する軽量共通鍵暗号の構成方法の開発，③軽量共通鍵暗号をベースとした軽量暗号ソリューションの開発を行う．①に関しては，2019 年から NIST(アメリカ国立標準技術研究所)により，軽量共通鍵暗号の標準を決めるプロジェクトが実施される．本研究では，候補暗号に対して安全性の解析を行うことで世界的な標準化プロセスに貢献するとともに，軽量共通鍵暗号に対する新しい解析手法を考案し，汎用的な安全性評価手法の開発を行う．②では，①で得た軽量暗号に対する安全性評価技術をベースに新しい軽量共通鍵暗号の開発を行う．これまで提案された多くの軽量共通鍵暗号は，軽量化を図るために安全性を 64 bit に削減したもの(ブロックサイズが 64 bit)が主流である．しかしながら，実際の IoT での利用を考えると 128 bit 安全性は必要不可欠である．本研究では，128 bit 安全性を有した上で，理論限界に近いハードウェア性能を持つ軽量暗号技術構造を明らかにする．次に③において，実際に IoT 等で暗号通信を行う場合は，共通鍵暗号単独では実現不可能である．本研究では，適切な暗号化モードの選択や軽量公開鍵暗号を適切に組み合わせることにより，IoT 用途の軽量暗号技術のトータルソリューションを提供する．

３．研究の方法
＜①軽量共通鍵暗号に対する厳密な安全性評価手法の開発＞
Tweak 入力を攻撃者が自由にコントロールできる場合(関連 Tweak 仮定)での安全性を定量的に見積もる方法を開発する．既存研究では，関連 Tweak 仮定では，差分・線形攻撃の評価しかできておらず，不能差分攻撃，Integral 攻撃，中間一致攻撃，Slide 攻撃などの安全性評価手法は不明である．本研究では，まず攻撃ベースにこれらの攻撃が Tweak によってどのような拡張，発展があるか明らかにする．そして，解析技術をもとに，各種攻撃技術に対して関連 Tweak 仮定での汎用的な安全性評価方法を与え，既存の暗号に適応し安全性を厳密に見積もる．

＜②高い安全性と実装性能を有する軽量共通鍵暗号の構成方法の開発＞
128 bit 安全を保持したままで，上記の関連 Tweak 仮定での安全性を強く保障した共通鍵ブロック暗号技術の開発を行う．現在想定している具体的な構成方法としては，ブロック長 64 bit で，128 bit key と 64 bit tweak を入力にとる Tweakble ブロック暗号である．ハードウェア実装の数値上の目標は，ゲートサイズ 1000 GE 以下，消費電力は 1 pJ/bit，Critical path 2ns 以下である．これらの数値は AES と比較して 2-10 倍の性能であり，既存の有力な 64bit 安全性の軽量暗号 PRESENT，Piccolo，Midori と比較しても優れており，これが達成できれば軽量暗号の実装の限界を達成したといえる．

＜③軽量共通鍵暗号をベースとした軽量暗号ソリューションの開発＞
②で作成した軽量 Tweakable ブロック暗号をベースにして，実際の IoT 向けのプロトコルを構成する．具体的には，乱数生成，認証暗号，ハッシュ関数を暗号化モードにより構成する．また，共通鍵暗号のみでは実現不可能な鍵交換等は公開鍵暗号を用いて実現する．これら全体を IoT 向けの軽量暗号のトータルソリューションとして提案し，すべてを含んだコストの評価を様々な実装環境で評価し，暗号通信を IoT 向けで利用する場合の最軽量な暗号方式として与える．

４．研究成果
令和元年は当初の計画通り，NIST(アメリカ国立標準技術研究所)による軽量共通鍵暗号の標準を決めるプロジェクトに応募された軽量暗号アルゴリズムの解析を実施した．目的は，世界的な標準化プロセスに貢献することと，新しい解析や安全性手法の考案である．代表的な成果としては，Subterranean と Gimli の二つの有力アルゴリ ズムに対して解析を行い，これまで見つかっていない特性を導出することに成功した．Subterranean に関しては，代数的な構造の特性を用いることで，Nonce- misuse setting の仮定の下で，Practical な計算量で，秘密鍵と等価な秘密の内部状態を復元することが可能であることを示した．この結果は設計者の claim を破 るものであり，その結果は共通鍵暗号の top journal の ToSC に採録された．また，Gimli に関して，混合整数計画法の modeling をうまく用いることで，差分攻撃や 衝突攻撃の探索に成功した．この技術は汎用性が非常に高く，Gimli type の暗号には適応可能であり，結果は暗号のトップカ

ンファレンス CRYPTO に採録され高い 評価を得た.これらの成果のほかにも，TRIFLE と呼ばれる軽量暗号，ディスク暗号モード XTS モード，Troika ハッシュ関数，EM 暗号などの新しい解析結果を得て， それぞれメジャーな国際学会，国際 journal に採録され，発表を行った.また，来年度に実施予定の新しい軽量暗号設計に向けた研究も前倒しして進めた.具体的 には，軽量 Matrix の探索を Shortest Linear Programs を用いて実施し，既存の研究を大きく上回る結果を示すことができた.また，既存の軽量暗号を Tweak を加 えるアプローチの研究も行い，Tweak を加えてた場合のオーバーヘッドが小さい構成を示した.それぞれ国際会議で発表を行った.

令和２年度は、軽量暗号の安全性解析も継続しつつ，高い安全性と実装性能を有する軽量共通鍵暗号の構成方法の開発に行った。 解析研究の代表的な成果としては、Gimli と呼ばれる軽量認証暗号の新しい解析手法を考案した。具体的には、内部の代数構造を使う解析手法で、暗号分野の トップ会議 CRYPTO と FSE に採録された。他には、CBC モードの安全性解析も実施し、未知の脆弱性を発見し、国際会議 ACNS に採録された。この結果は、社会的影響 を考慮し JPCERT と協力し、事前にベンダーに情報の開示を行った。その他、ストリーム暗号 SNOW や Kcipher-2 の安全性評価を実施し、結果は国際ジャーナル IEICE に採録された。 設計に関しては、軽量暗号 WARP の開発を実施した。軽量な部品から安全性を高める置換処理を適切に設計することで、WARP は回路規模で世界最小を達成し、結 果は国際会議 SAC に採録された。また、暗号処理の遅延が小さい低遅延暗号 Orthros の設計も行った。低遅延の非線形関数と線形関数を設計し、うまく組み合わせ ることで、世界標準の AES と比較して、暗号化処理の遅延を 1/10 に大幅に削減することに成功した。また、軽量ストリーム暗号 Atom の開発も行った。Double key filter と呼ぶ新しい設計理論をベースにすることで、ストリーム暗号としては最軽量の実装結果を達成した。低遅延暗号 Orthros と軽量ストリーム暗号 Atom は共通 鍵暗号のトップ会議 FSE に採録された。また、軽量線形層の設計方法に関する論文が国際ジャーナル IEICE に採録された。

令和 3 年度は、前年度設計した基本構造をベースにして，軽量暗号技術の設計を実施した。具体的には，ソフトウェアとハードウェアで軽量な暗号方式の設計を実施した。ソフトウェアで軽量な暗号としては Rocca と呼ばれる認証暗号の設計を実施した。Rocca ではソフトウェアでのパフォーマンスを最大化させるため、AES-NI と 呼ばれるハードウェア命令をベースとした構成を設計した。速度としては、世界最高である 140Gbps 以上を汎用の CPU で達成した。結果は、共通鍵暗号のトップ会 議 FSE に採録された。ハードウェアでの軽量暗号としては、消費電力が最小となる設計理論の構築をおこなった。アプローチとしては、ストリーム暗号でリーク電 流を最小化する技術で、この技術を既存の Trivium や Triad 等のアルゴリズムに適用した新しい暗号アルゴリズムを提案した。結果は論文としてまとめ、FSE に採録 された。また、同時に軽量暗号の評価技術の開発も進めた。代表的な成果としては、ソフトウェアで高速な暗号 AEGIS への解析結果である。既存の解析手法では発 見困難であった性質を特定の鍵のクラスに限定することで発見することに成功し、これまでの解析結果の記録と更新した。この結果は、FSE に採録されるとと も に、Best Paper Award を受賞した。また、軽量暗号に対して最も強力な攻撃手法である代数攻撃に対しても新しい技術を解析しより厳密な評価を可能にした。結 果は、暗号分野のトップ会議 CRYPTO， ASIACRYPT に採録されるなど学術的に高い評価を得た。それ以外の結果としては、MILP を用いた Friet や Lesamnta への新しい 解析技術を示し、結果は国際論文誌に採録された。

最終年度は、モバイルデバイス等で高速に処理可能な共通鍵暗号の設計を実施した。具体的にはソフトウェアで高速に処理可能な SIMD（Single Instruction/Multiple Data）命令で実行可能な構成について検討した。特に、暗号演算に特化している AES-NI と呼ばれる演算と XOR のみからなる究極に高速化可能な構成について検討した。具体的な成果としては、Areion と呼ばれる暗号学的置換を設計した。Areion は前述の通り、AES-NI と XOR 命令のみから構成されており、安全性と実装性能の観点で最適な構造や組み合わせをとっている。最適な組み合わせの探索は、数理ソルバーを用いた自動安全性評価ツールを作成し、数百万の候補の中から最適なものを選択した。この暗号学的置換からハッシュ関数や認証暗号へ拡張可能であり、いずれもモバイルやラップトップ環境では世界最速を達成する性能を持っている。これらをまとめた結果は、暗号実装のトップ会議 CHES に採録されている。また設計と同時に、暗号の解析技術の開発も実施した。代表的な成果としては、5G 標準のストリーム暗号 ZUC に対する差分攻撃、プライバシー保護技術フレンドリ暗号 Rasta や LowMC への代数攻撃、Rocca や AEGIS 等の認証暗号に対する安全性評価が挙げられる。これらの結果は、暗号分野のトップ会議 ASIACRYPT，FSE に採録されるなど学術的に高い評価を得た。

雑誌論文

1. Takanori Isobe and Kyoji Shibutani, "Key-Recovery Security of Single-Key Even-Mansour Cipher", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, Vol.E103-A, No.07, pp893-905,2020.
2. Kosei Sakamoto, Kazuhiko Minematsu, Nao Shibata, Maki Shigeri, Hiroyasu Kubo, Yuki Funabiki, Andrey Bogdanov, Sumio Morioka and Takanori Isobe, "Tweakable TWINE: Building a Tweakable Block Cipher on Generalized Feistel Structure", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, No.: Vol.E103-A, no.12, pp.1629-1639, 2020.

3. Fukang Liu, Takanori Isobe and Willi Meier, "Cube-based Cryptanalysis of Subterranean-SAE", IACR Trans. Symmetric Cryptol (ToSC/FSE), issue 4, pp.192-222, 2019.
4. Takanori Isobe and Kazuhiko Minematsu, "Security Analysis and Countermeasures of an End-to-End Encryption Scheme of LINE", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, vol.E103-A, no.9, pp. 313-324 , 2020.
5. Fukang Liu, Christoph Dobraunig, Florian Mendel, Takanori Isobe , Gaoli Wang and Zhenfu Cao, "New Semi-Free-Start Collision Attack Framework for Reduced RIPEMD-160 ", IACR Trans. Symmetric Cryptol (ToSC/FSE), issue 3, pp.169-192, 2019.
6. Subhadeep Banik, Khashayar Barooti and Takanori Isobe, "Cryptanalysis of Plantlet ", IACR Trans. Symmetric Cryptol (ToSC/FSE), issue 3, pp.103-120, 2019.
7. Kosei Sakamoto, Kazuhiko Minematsu, Nao Shibata, Maki Shigeri, Hiroyasu Kubo, Yuki Funabiki, a and Takanori Isobe, "Security of Related-Key Differential Attacks on TWINE, Revisited", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, vol.E103-A, no.9, pp. 212-214 , 2020.
8. Fukang Liu, Christoph Dobraunig, Florian Mendel, Takanori Isobe, Gaoli Wang and Zhenfu Cao, "Efficient Collision Attack Frameworks for RIPEMD-160", Advances in Cryptology (CRYPTO) 2019, Lecture Note in Computer Science, Part 2, vol. 10992, pp. 117-149, Springer, 2019.
9. Subhadeep Banik, Yuki Funabiki and Takanori Isobe, "More results on Shortest Linear Programs", (IWSEC) 2019, Lecture Note in Computer Science, vol. 11689, pp. 109-128. Springer, 2019.
10. Fukang Liu and Takanori Isobe, "Preimage Attacks on Reduced Troika with Divide-and-Conquer Methods", International Workshop on Security, (IWSEC) 2019, Lecture Note in Computer Science, vol. 11689, pp. 306-326. Springer, 2019
11. Kosei Sakamoto, Kazuhiko Minematsu, Nao Shibata, Maki Shigeri, Hiroyasu Kubo, Yuki Funabiki, Andrey Bogdanov, Sumio Morioka and Takanori Isobe, "Tweakable TWINE: Building a Tweakable Block Cipher on Generalized Feistel Structure", International Workshop on Security, (IWSEC) 2019, Lecture Note in Computer Science, vol. 11689, pp. 129-145. Springer, 2019.
12. Fukang Liu and Takanori Isobe, "Iterative Differential Characteristic of TRIFLE-BC", Conference on Selected Areas in Cryptography (SAC) 2019, Lecture Note in Computer Science, vol. 11959, pp. 85-100. Springer, 2019
13. Takanori Isobe and Kazuhiko Minematsu, "Plaintext Recovery Attacks against XTS Beyond Collisions", Conference on Selected Areas in Cryptography (SAC) 2019, Lecture Note in Computer Science, vol. 11959, pp. 103-123. Springer, 2019
14. Jin Hoki ,Kosei Sakamoto ,Kazuhiko Minematsu and Takanori Isobe, "Practical Integral Distinguishers on SNOW 3G and KCipher-2", IEICE Vol.E104-A,no.11,pp.1603-1611, 2021.
15. Subhadeep Banik, Takanori Isobe, Fukang Liu, Kazuhiko Minematsu and Kosei Sakamoto, "Orthros: A Low-Latency PRF", IACR Trans. Symmetric Cryptol (ToSC/FSE), 2021, issue 1, pp.37-77, 2021.
16. Subhadeep Banik, Yuki Funabiki and Takanori Isobe, "Further Results on Efficient Implementations of Block Cipher Linear Layers", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, Vol.E104-A, no.01, pp. 213-225, 2021.
17. Subhadeep Banik, Andrea Caforio, Takanori Isobe, Fukang Liu, Willi Meier, Kosei Sakamoto and Santanu Sarkar, "Atom: A Stream Cipher with Double Key Filter", IACR Trans. Symmetric Cryptol (ToSC/FSE), issue 1, pp.5-36, 2021.
18. Rintaro Fujita, Takanori Isobe and Kazuhiko Minematsu, "ACE in Chains : How Risky is CBC Encryption of Binary Executable Files ?" 18th International Conference on Applied Cryptography and Network Security (ACNS 2020), Lecture Note in Computer Science, Part 1, vol. 12146, pp. 187-207, Springer, 2020.
19. Fukang Liu, Takanori Isobe and Willi Meier, "Automatic Verification of Differential Characteristics:Application to Reduced Gimli", Advances in Cryptology (CRYPTO) 2020, Lecture Note in Computer Science, Part 3, vol. 12172, pp. 219-248, Springer, 2020.
20. Subhadeep Banik and Zhenzhen Bao and Takanori Isobe and Hiroyasu Kubo and Kazuhiko Minematsu and Fukang Liu and Kosei Sakamoto and Nao Shibata and Maki Shigeri, "WARP : Revisiting GFN for Lightweight 128-bit Block Cipher", Conference on Selected Areas in Cryptography (SAC) 2020, Lecture Note in

Computer Science, vol. 12804, pp. 535--564. Springer, 2020
21. Fukang Liu, Takanori Isobe and Willi Meier, "Exploiting Weak Diffusion of Gimli: Improved Distinguishers and Preimage Attacks", IACR Trans. Symmetric Cryptol (ToSC/FSE), issue 1, pp.185-216, 2021.
22. Ryoma Ito, Rentaro Shiba, Kosei Sakamoto, Fukang Liu and Takanori Isobe, "Bit-wise Cryptanalysis on AND-RX Permutation Friet-PC", Journal of Information Security and Applications, vol. 59, no. 102860 , 2021.
23. Kosei Sakamoto, Fukang Liu, Yuto Nakano, Shinsaku Kiyomoto and Takanori Isobe, "Rocca: An Efficient AES-based Encryption Scheme for Beyond 5G", IACR Trans. Symmetric Cryptol (ToSC/FSE), 2021, issue 2, pp.1-30, 2021.
24. Andrea Caforio, Subhadeep Banik, Yosuke Todo, Willi Meier, Takanori Isobe, Fukang Liu and Bin Zhang, "Perfect Trees: Designing Energy-Optimal Symmetric Encryption Primitives", IACR Trans. Symmetric Cryptol (ToSC/FSE), 2021, issue 4, pp. 36-73, 2021.
25. Fukang Liu, Takanori Isobe, Willi Meier and Kosei Sakamoto, "Weak Keys in Reduced AEGIS and Tiaoxin", IACR Trans. Symmetric Cryptol (ToSC/FSE),no.2, pp.104-139, 2021
26. Rentaro Shiba, Kosei Sakamoto, Fukang Liu, Kazuhiko Minematsu, Takanori Isobe, "Integral and Impossible-Differential Attacks on the Reduced-Round Lesamnta-LW-BC", IET Information Security, vol. 16, no.2, pp. 75-85, 2022.
27. Fukang Liu, Santanu Sarkar, Willi Meier and Takanori Isobe, "Algebraic Attacks on Rasta and Dasta Using Low-Degree Equations", Advanced in Cryptology (ASIACRYPT) 2021, Lecture Note in Computer Science, Part 1, vol. 13090, pp. 214-240, Springer, 2021.
28. Fukang Liu, Takanori Isobe, Willi Meier, "Cryptanalysis of Full LowMC and LowMC-M with Algebraic Techniques" Advances in Cryptology (CRYPTO) 2021, Lecture Note in Computer Science, Part 3, vol. 12827, pp. 368-401, Springer
29. Takeuchi Nobuyuki, Kosei Sakamoto and Takanori Isobe, On Optimality of the Round Function of Rocca", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, Vol.E106-A,no.1,pp. 45-53, 2023.
30. Takeuchi Nobuyuki, Kosei Sakamoto and Takanori Isobe, "Security Evaluation of Initialization Phases and Round Functions of Rocca and AEGIS", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, 2023.
31. Takanori Isobe, Ryoma Ito, Fukang Liu, Kazuhiko Minematsu, Motoki Nakahashi, Kosei Sakamoto, and Rentaro Shiba, " Areion: Highly-Efficient Permutations and Its Applications to Hash Functions for Short Input", TCHES 2023.
32. Rentaro Shiba, Kosei Sakamoto and Takanori Isobe, "Efficient constructions for large-state block ciphers based on AES-NI" , IET Information Security, vol. 16, No.3, pages 145-160, 2022.
33. Fukang Liu, Santanu Sarkar, Willi Meier and Takanori Isobe, "The Inverse of χ and Its Applications to Rasta-like Ciphers", Journal of Cryptology, vo.35, no.4, pp. 28-47, 2022.
34. Fukang Liu, Willi Meier, Santanu Sarkar, Gaoli Wang, Ryoma Ito, Takanori Isobe, "New Cryptanalysis of ZUC-256 Initialization Using Modular Differences" ,IACR Trans. Symmetric Cryptol (ToSC/FSE), 2022, issue 3, pp. 152-190, 2022.
35. Fukang Liu, Santanu Sarkar, Willi Meier and Takanori Isobe, "New Low-Memory Algebraic Attacks on LowMC in the Picnic Setting", IACR Trans. Symmetric Cryptol (ToSC/FSE), 2022, issue 3, pp. 102-122, 2022.
36. Fukang Liu, Santanu Sarkar, Gaoli Wang, Willi Meier and Takanori Isobe, “Algebraic Meet-in-the-Middle Attack on LowMC ”, ASIACRYPT 2022

５．主な発表論文等

〔雑誌論文〕　計27件（うち査読付論文　27件／うち国際共著　17件／うちオープンアクセス　8件）

１．著者名 Ito Ryoma、Shiba Rentaro、Sakamoto Kosei、Liu Fukang、Isobe Takanori	４．巻 59
２．論文標題 Bit-wise cryptanalysis on AND-RX permutation Friet-PC	５．発行年 2021年
３．雑誌名 Journal of Information Security and Applications	６．最初と最後の頁 102860～102860
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jisa.2021.102860	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 Sakamoto Kosei、Liu Fukang、Nakano Yuto、Kiyomoto Shinsaku、Isobe Takanori	４．巻 2
２．論文標題 Rocca: An Efficient AES-based Encryption Scheme for Beyond 5G	５．発行年 2021年
３．雑誌名 IACR Transactions on Symmetric Cryptology	６．最初と最後の頁 1～30
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tosc.v2021.i2.1-30	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 Caforio Andrea、Banik Subhadeep、Todo Yosuke、Meier Willi、Isobe Takanori、Liu Fukang、Zhang Bin	４．巻 3
２．論文標題 Perfect Trees: Designing Energy-Optimal Symmetric Encryption Primitives	５．発行年 2021年
３．雑誌名 IACR Transactions on Symmetric Cryptology	６．最初と最後の頁 36～73
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tosc.v2021.i4.36-73	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 該当する

１．著者名 Liu Fukang、Isobe Takanori、Meier Willi、Sakamoto Kosei	４．巻 2
２．論文標題 Weak Keys in Reduced AEGIS and Tiaoxin	５．発行年 2021年
３．雑誌名 IACR Transactions on Symmetric Cryptology	６．最初と最後の頁 104～139
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tosc.v2021.i2.104-139	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 該当する

1．著者名 Shiba Rentaro、Sakamoto Kosei、Liu Fukang、Minematsu Kazuhiko、Isobe Takanori	4．巻 16
2．論文標題 Integral and impossible‐differential attacks on the reduced‐round Lesamnta‐LW‐BC	5．発行年 2021年
3．雑誌名 IET Information Security	6．最初と最後の頁 75～85
掲載論文のDOI（デジタルオブジェクト識別子） 10.1049/ise2.12044	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 Liu Fukang、 Santanu Sarkar、Meier Willi、Takanori Isobe	4．巻 13090}
2．論文標題 Algebraic Attacks on Rasta and Dasta Using Low-Degree Equations	5．発行年 2021年
3．雑誌名 Advances in Cryptology - ASIACRYPT 2021	6．最初と最後の頁 214～240
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-92062-3_8	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 該当する

1．著者名 Liu Fukang、 Takanori Isobe、 Meier Willi	4．巻 12827
2．論文標題 Cryptanalysis of Full LowMC and LowMC-M with Algebraic Techniques	5．発行年 2021年
3．雑誌名 Advances in Cryptology - CRYPTO 2021	6．最初と最後の頁 368～401
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-84252-9_13	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 該当する

1．著者名 HOKI Jin、SAKAMOTO Kosei、LIU Fukang、MINEMATSU Kazuhiko、ISOBE Takanori	4．巻 E104.A
2．論文標題 MILP-Aided Security Evaluation of Differential Attacks on KCipher-2	5．発行年 2021年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 203～212
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020CIP0018	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 BANIK Subhadeep、FUNABIKI Yuki、ISOBE Takanori	4．巻 E104.A
2．論文標題 Further Results on Efficient Implementations of Block Cipher Linear Layers	5．発行年 2021年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 213～225
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020CIP0013	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 該当する

1．著者名 Banik Subhadeep、Caforio Andrea、Isobe Takanori、Liu Fukang、Meier Willi、Sakamoto Kosei、Sarkar Santanu	4．巻 issue 1
2．論文標題 Atom: A Stream Cipher with Double Key Filter	5．発行年 2021年
3．雑誌名 IACR Transactions on Symmetric Cryptology	6．最初と最後の頁 5～36
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tosc.v2021.i1.5-36	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 該当する

1．著者名 Banik Subhadeep、Isobe Takanori、Liu Fukang、Minematsu Kazuhiko、Sakamoto Kosei	4．巻 issue 1
2．論文標題 Orthros: A Low-Latency PRF	5．発行年 2021年
3．雑誌名 IACR Transactions on Symmetric Cryptology	6．最初と最後の頁 37～77
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tosc.v2021.i1.37-77	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 該当する

1．著者名 Liu Fukang、Isobe Takanori、Meier Willi	4．巻 issue 1
2．論文標題 Exploiting Weak Diffusion of Gimli: Improved Distinguishers and Preimage Attacks	5．発行年 2021年
3．雑誌名 IACR Transactions on Symmetric Cryptology	6．最初と最後の頁 185～216
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tosc.v2021.i1.185-216	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 該当する

1．著者名 Fujita Rintaro、Isobe Takanori、Minematsu Kazuhiko	4．巻 issue 1
2．論文標題 ACE in Chains: How Risky Is CBC Encryption of Binary Executable Files?	5．発行年 2020年
3．雑誌名 International Conference on Applied Cryptography and Network Security	6．最初と最後の頁 187～207
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-57808-4_10	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 Liu Fukang、Isobe Takanori、Meier Willi	4．巻 issue 1
2．論文標題 Automatic Verification of Differential Characteristics: Application to Reduced Gimli	5．発行年 2020年
3．雑誌名 Advances in Cryptology- CRYPTO 2020	6．最初と最後の頁 219～248
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-56877-1_8	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 該当する

1．著者名 Takanori Isobe and Kyoji Shibutani	4．巻 TBA
2．論文標題 Key-Recovery Security of Single-Key Even-Mansour Cipher	5．発行年 2020年
3．雑誌名 IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences	6．最初と最後の頁 TBA
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Kosei Sakamoto, Kazuhiko Minematsu, Nao Shibata, Maki Shigeri, Hiroyasu Kubo, Yuki Funabiki, Andrey Bogdanov, Sumio Morioka and Takanori Isobe,	4．巻 TBA
2．論文標題 Tweakable TWINE: Building a Tweakable Block Cipher on Generalized Feistel Structure	5．発行年 2020年
3．雑誌名 IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences	6．最初と最後の頁 TBA
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 該当する

1．著者名 Fukang Liu, Takanori Isobe and Willi Meier	4．巻 4
2．論文標題 "Cube-based Cryptanalysis of Subterranean-SAE	5．発行年 2019年
3．雑誌名 IACR Transactions on Symmetric Cryptology	6．最初と最後の頁 192-222
掲載論文のDOI（デジタルオブジェクト識別子） 10.13154/tosc.v2019.i4.192-222	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 該当する

1．著者名 Takanori Isobe and Kazuhiko Minematsu	4．巻 E103-A
2．論文標題 Security Analysis and Countermeasures of an End-to-End Encryption Scheme of LINE	5．発行年 2020年
3．雑誌名 IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences	6．最初と最後の頁 313-324
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2019EAP1041	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 Fukang Liu, Christoph Dobraunig, Florian Mendel, Takanori Isobe , Gaoli Wang and Zhenfu Cao	4．巻 3
2．論文標題 New Semi-Free-Start Collision Attack Framework for Reduced RIPEMD-160	5．発行年 2019年
3．雑誌名 IACR Transactions on Symmetric Cryptology	6．最初と最後の頁 169-192
掲載論文のDOI（デジタルオブジェクト識別子） 10.13154/tosc.v2019.i3.169-192	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 該当する

1．著者名 Subhadeep Banik, Khashayar Barooti and Takanori Isobe,	4．巻 3
2．論文標題 Cryptanalysis of Plantlet	5．発行年 2019年
3．雑誌名 IACR Transactions on Symmetric Cryptology	6．最初と最後の頁 103-120
掲載論文のDOI（デジタルオブジェクト識別子） 10.13154/tosc.v2019.i3.103-120	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 該当する

1．著者名 Kosei Sakamoto, Kazuhiko Minematsu, Nao Shibata, Maki Shigeri, Hiroyasu Kubo, Yuki Funabiki, and Takanori Isobe	4．巻 E103-A
2．論文標題 Security of Related-Key Differential Attacks on TWINE, Revisited	5．発行年 2020年
3．雑誌名 IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences	6．最初と最後の頁 212-214
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2019CIL0004	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 該当する

1．著者名 Fukang Liu, Christoph Dobraunig, Florian Mendel, Takanori Isobe, Gaoli Wang and Zhenfu Cao	4．巻 10992
2．論文標題 Efficient Collision Attack Frameworks for RIPEMD-160	5．発行年 2019年
3．雑誌名 Advances in Cryptology (CRYPTO) 2019, Lecture Note in Computer Science	6．最初と最後の頁 117-149
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-26951-7_5	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 該当する

1．著者名 Subhadeep Banik, Yuki Funabiki and Takanori Isobe	4．巻 11689
2．論文標題 More results on Shortest Linear Programs	5．発行年 2019年
3．雑誌名 , International Workshop on Security, (IWSEC) 2019, Lecture Note in Computer Science	6．最初と最後の頁 109-128
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-26834-3_7	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 該当する

1．著者名 Fukang Liu and Takanori Isobe	4．巻 11689
2．論文標題 Preimage Attacks on Reduced Troika with Divide-and-Conquer Methods	5．発行年 2019年
3．雑誌名 International Workshop on Security, (IWSEC) 2019, Lecture Note in Computer Science	6．最初と最後の頁 109-128
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-26834-3_18	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 Kosei Sakamoto, Kazuhiko Minematsu, Nao Shibata, Maki Shigeri, Hiroyasu Kubo, Yuki Funabiki, Andrey Bogdanov, Sumio Morioka and Takanori Isobe	４．巻 11689
２．論文標題 weakable TWINE: Building a Tweakable Block Cipher on Generalized Feistel Structure	５．発行年 2019年
３．雑誌名 International Workshop on Security, (IWSEC) 2019, Lecture Note in Computer Science	６．最初と最後の頁 129-145
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-26834-3_8	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 該当する

１．著者名 Fukang Liu and Takanori Isobe	４．巻 11959
２．論文標題 Iterative Differential Characteristic of TRIFLE-BC"	５．発行年 2019年
３．雑誌名 Conference on Selected Areas in Cryptography (SAC) 2019, Lecture Note in Computer Science	６．最初と最後の頁 85-100.
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-38471-5_4	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 Plaintext Recovery Attacks Against XTS Beyond Collisions	４．巻 11959
２．論文標題 Takanori Isobe and Kazuhiko Minematsu	５．発行年 2019年
３．雑誌名 Conference on Selected Areas in Cryptography (SAC) 2019, Lecture Note in Computer Science	６．最初と最後の頁 103-123
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-38471-5_5	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 －

〔学会発表〕　計13件（うち招待講演　1件／うち国際学会　1件）

１．発表者名 Subhadeep Banik and Zhenzhen Bao and Takanori Isobe and Hiroyasu Kubo and Kazuhiko Minematsu and Fukang Liu and Kosei Sakamoto and Nao Shibata and Maki Shigeri
２．発表標題 WARP : Revisiting GFN for Lightweight 128-bit Block Cipher
３．学会等名 Selected Areas in Cryptography (SAC) 2020（国際学会）
４．発表年 2020年

１．発表者名
芝 廉太朗，阪本 光星，Fukang Liu，峯松　一彦，五十部 孝典

２．発表標題
"Integral and Impossible Differential Attacks on the Reduced-Round Lesamnta-LW-BC

３．学会等名
2021年 暗号と情報セキュリティシンポジウム(SCIS 2021)

４．発表年
2021年

１．発表者名
寶木 仁，阪本 光星，五十部　孝典

２．発表標題
KCipher-2に対する差分攻撃の耐性評価

３．学会等名
2021年 暗号と情報セキュリティシンポジウム(SCIS 2021)

４．発表年
2021年

１．発表者名
阪本 光星，Fukang Liu，仲野 有登，清本 晋作，五十部　孝典

２．発表標題
AES-NIを用いた効率的なスポンジ構造のラウンド関数の設計

３．学会等名
2021年 暗号と情報セキュリティシンポジウム(SCIS 2021)

４．発表年
2021年

１．発表者名
芝 廉太朗，阪本 光星，五十部 孝典

２．発表標題
AES-NIを用いたラージブロック暗号の効率的な構成

３．学会等名
コンピュータセキュリティシンポジウム（CSS） 2020

４．発表年
2020年

１．発表者名
五十部 孝典

２．発表標題
軽量暗号の研究・標準化動向

３．学会等名
ハードウェアセキュリティフォーラム 2019（招待講演）

４．発表年
2019年

１．発表者名
寶木 仁，阪本 光星，峯松 一彦，五十部 孝典

２．発表標題
KCipher-2に対する差分攻撃への耐性評価

３．学会等名
ISEC研究会

４．発表年
2020年

１．発表者名
寶木 仁，阪本 光星，峯松 一彦，五十部 孝典

２．発表標題
KCipher-2とSNOW 3Gに対するIntegral攻撃への耐性評価

３．学会等名
2020年 暗号と情報セキュリティシンポジウム(SCIS 2020)

４．発表年
2020年

１．発表者名
小池 祐二，林 卓也，五十部 孝典

２．発表標題
スペースハード暗号を用いたデータ流出耐性のあるシステムの提案

３．学会等名
2020年 暗号と情報セキュリティシンポジウム(SCIS 2020)

４．発表年
2020年

１．発表者名
阪本 光星，峯松 一彦，五十部 孝典

２．発表標題
複数線形層を用いた低遅延ブロック暗号の構成方法

３．学会等名
2020年 暗号と情報セキュリティシンポジウム(SCIS 2020)

４．発表年
2020年

１．発表者名
Fukang Liu，五十部 孝典，Willi Meier，Zhonghao Yang

２．発表標題
Algebraic Attacks on Reduced Keccak

３．学会等名
2020年 暗号と情報セキュリティシンポジウム(SCIS 2020)

４．発表年
2020年

１．発表者名
阪本 光星，峯松 一彦，五十部 孝典

２．発表標題
Low-latency ブロック暗号に適した線形層の設計

３．学会等名
コンピュータセキュリティシンポジウム（CSS 2019）

４．発表年
2019年

１．発表者名
Fukang Liu，五十部 孝典

２．発表標題
Cryptanalysis of Subterranean-SAE

３．学会等名
コンピュータセキュリティシンポジウム（CSS 2019）

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
研究分担者	林　卓也 (Hayashi Takaya) (70739995)	国立研究開発法人情報通信研究機構・サイバーセキュリティ研究所セキュリティ基盤研究室・研究員 (82636)	

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1件

国際研究集会	開催年
The 9th Asian-workshop on Symmetric Key Cryptography (ASK 2019)	2019年～2019年

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