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

平成　３０　年　　６　月　２０　日現在

機関番号：　１３９０１
研究種目：　基盤研究(B)（一般）
研究期間：　2014～2017
課題番号：　２６２８００４５

研究課題名（和文）認証暗号化方式の構成と安全性解析に関する研究

研究課題名（英文）Constructions and Security Analyses of Authenticated Encryption Schemes

研究代表者
岩田　哲（Iwata, Tetsu）

名古屋大学・工学研究科・准教授

研究者番号：９０３４４８３７

交付決定額（研究期間全体）：（直接経費）　　13,000,000円

研究成果の概要（和文）：本研究では、暗号化とデータ認証を同時に行うための認証暗号化方式を中心に研究を進めた。主な結果として、GCM、CLOC、SILCといった認証暗号化方式の安全性を詳細に解析した。また、ブロック暗号SIMONの安全性解析を行った。さらに、Tweakableブロック暗号を構成要素として用いるメッセージ認証方式を設計した。CAESARの運営に参画し、国際会議DIAC 2016とASK 2016を開催した。CAESARへ提案したCLOCとSILCは最終ラウンド候補方式としては選定されなかった。

研究成果の概要（英文）：We studied authenticated encryption, a symmetric key primitive for privacy and authenticity. As our main results, we analyzed the security of various authenticated encryption schemes including GCM, CLOC, and SILC. We also studied the security of a block cipher called SIMON. We designed a message authentication scheme based on a tweakable block cipher. Finally, we contributed to the international competition called CAESAER, and organized international conferences DIAC 2016 and ASK 2016. Our proposal to CAESAR, CLOC and SILC, were not selected as the final round candidates.

研究分野：　暗号理論

キーワード：　暗号・認証等　共通鍵暗号技術　認証暗号化方式

１．研究開始当初の背景

暗号技術はネットワークやコンピュータの安全性を支える基盤技術であり、優れた安全性、計算効率、実装性能を有する共通鍵暗号技術の設計は、重要な課題として広く研究されてきた。またその応用範囲は広く、実装上の様々な要求を満たす方式の設計が必要とされている。

本研究では共通鍵暗号技術のうち、暗号化とデータ認証を同時に行うための「認証暗号化方式」を中心に研究を進める。2001 年に IAPM とよばれる優れた方式が提案され、これを契機としてこの分野の研究は世界的に進められてきた。標準化プロジェクトも進められ、とくに 2004 年には CCM が、2007 年には GCM とよばれる認証暗号化方式が NIST（米国商務省標準技術局）の推奨方式として採用され、その後 GCM は IEEE（米国電気電子学会)、ISO/IEC（国際標準化機構/国際電気標準会議)、NSA（米国国防総省国家安全保障局）などにおいて標準化され、幅広く利用されている。

一方で、これらの方式には安全性、計算効率、実装性能についての欠点が存在する。CCM は処理するデータ量を事前に知る必要があるため、ストリーミングデータの保護に用いることはできない。GCM の証明可能安全性の解析には不備があることが知られている。また、CCM/GCM では安全性を保証するために、繰り返すことのないナンスとよばれるデータを用いる。暗号デバイスに対するリセットや物理的な攻撃が行われたとしてもこのデータは繰り返してはならず、ナンスの実装が現実的には困難であることがたびたび指摘されている。

以上のように、標準化されている認証暗号化方式には克服すべき課題が存在する。共通鍵暗号研究者の間ではこのことは広く共有されつつあり、2012 年の Dagstuhl セミナーにおいて認証暗号化方式に関する公募の実施が検討され、CAESAR プロジェクト（http://competitions.cr.yp.to/caesar.html）として公募を実施することが決定された。

２．研究の目的

本研究では、安全性、計算効率、実装性能のすべての面で優れた認証暗号化方式を設計することを目標とする。このために必要となる要素技術の設計の検討、安全性解析、効率解析を行う。設計した方式が CAESAR プロジェクトにおいてポートフォリオとして選定されることを目指す。また、本プロジェクトへ提案された方式やその周辺技術の安全性解析を行う。CAESAR プロジェクトと密接に関連しながら認証暗号化方式に関する研究を推し進め、共通鍵暗号技術に関する学術研究を発展させることを目的とする。

３．研究の方法

本研究では下記 4 項目の研究を進める。

(1) 既存技術の安全性解析

GCM をはじめとする既存技術の安全性解析を行う。

(2) 認証暗号化方式の構成要素とその周辺技術の安全性解析

様々な認証暗号化方式の構成法があり、その中でもブロック暗号に基づく構成は、証明可能安全性を達成できるというメリットがある。ブロック暗号や、これの拡張である Tweakable ブロック暗号の構成法の検討や安全性解析を行う。

(3) 新規方式の設計、その安全性解析、効率解析

新しい認証暗号化方式を設計し、その安全性解析、効率解析を行う。

(4) 標準化プロジェクトへの参画、運営への貢献

共通鍵暗号分野では、たびたび公募を行うことで当該分野の発展に貢献してきた。これまでにブロック暗号、ストリーム暗号、ハッシュ関数の公募が行われ、次に共通鍵暗号分野がターゲットにする分野として、CAESAR プロジェクトが 2012 年より開始された。本プロジェクトは、認証暗号化方式に関する学術界主導の国際的な公募であり、これの運営に参画する。

４．研究成果

(1) 既存技術の安全性解析

まず GCM の証明可能安全性について詳細な解析を行った。その結果、従来の安全性証明手法に従う限り、GCM の安全性限界式に現れる 2^22 という定数が、2^19.74 を下回ることはないことを示した。さらに、安全性証明において sum bound を回避するという証明手法を考案し、従来知られている安全性限界式よりも、実際には GCM が 2^17 倍程度高い安全性を有していることを数学的に証明することに成功した。本研究成果により、国際会議 FSE 2015 において Best Paper Award を受賞した。さらに GCM の証明可能安全性についての解析を進め、安全性限界式の定数 32 を半減できることを示した。

また、その他の関連する認証暗号方式としてChaCha20 と Poly1305 を組わせた方式の安全性解析を進めた。確定的認証暗号化方式である GCM-SIV について、その安全性を向上させ、漸近的に最適にできるような手法を提案した。また、ストリーム暗号とユニバーサルハッシュ関数を構成要素として用いて汎用的に認証暗号化方式を構成する手法が提案されており、これらの安全性を解析した。とくに認証に関する安全性に着目し、従来安全であると考えられてきた方式に欠陥があることを明らかにした。また、CENC とよばれる暗号化方式の安全性を解析し、IACR ePrint 2016/1087 として成果を公表した。既存のメッセージ認証方式 PMACx と PMAC2x、確定的認証暗号化方式 SIVx の安全性を解析し、これらの方式が期待される安全性を有していないことを明らかにした。さらに、認証暗号化方式 AES-GCM-SIV の安全性を解析した。既存の解析手法の問題点を指摘するとともに、新しい安全性証明を与えた。

(2) 認証暗号化方式の構成要素とその周辺技術の安全性解析

ブロック暗号と Tweakable ブロック暗号は認証暗号方式をはじめとする様々な技術への応用があり、Tweakable ブロック暗号の構成法について、汎用的に Tweak 長を拡張できる方式を設計した。設計した方式は、安全性の面で従来方式より優れていることを示した。

また、軽量ブロック暗号 Simon に関する安全性解析を進めた。ゼロ相関攻撃、Integral 攻撃、不能差分攻撃、関連鍵差分攻撃に対する安全性解析を行った。さらに、Tweakable ブロック暗号によるブロック暗号の構成法を検討した。また、4 ラウンド Feistel 暗号の量子選択暗号文攻撃に対する安全性を解析した。

(3) 新規方式の設計、その安全性解析、効率解析

CAESAR コンペティションへ応募した認証暗号化方式 CLOC について、Tweak 関数の設計の最適性という観点から解析を行った。その結果、安全性証明に用いられている 55 通りの条件はすべて必要であることを明らかにした。同じく CAESAR コンペティションへ応募した SILC について、安全性限界式を導出し、ソフトウェアとハードウェア実装評価を行った。

新しい方式の検討として、Tweakable ブロック暗号を構成要素として用いた認証方式 ZMAC を設計し、その安全性を解析した。さらに、これを確定的認証暗号化方式 ZAE の設計に応用した。これらは高い安全性と計算効率を同時に有する方式である。また、ストリーム暗号とユニバーサルハッシュ関数を用いた認証暗号化方式の構成法を検討した。

(4) 標準化プロジェクトへの参画、運営への貢献

CAESAR プロジェクトへ提案した CLOC および SILC は 2015 年に第二ラウンド候補として選出された。第二ラウンド候補には仕様のアップデートが許されており、CLOC と SILC の同じ鍵での共用を考慮し、ナンスのフォーマットを変更した。また、これらの方式のハードウェア実装評価を行い、CLOC の設計の最適性の解析を行った。CAESAR プロジェクトの運営面について、第二ラウンド候補の選定作業に参画した。2016 年には CLOC および SILC が第三ラウンド候補として選出された。第三ラウンド候補選出に際し仕様の変更は行わなかったが、パラメータの微調整を行った。また、CAESAR からの指示に従い応募ドキュメントを大幅に改定した。SILC の認証に関する安全性について、INT-RUP とよばれる安全性を有していることを証明した。また、CLOC のソフトウェア実装性能評価を進めた。運営面について、選定委員として第三ラウンド候補の選定作業に参画した。また、国際会議 DIAC 2016（Directions in Authenticated Ciphers 2016）および ASK 2016（6th Asian Workshop on Symmetric Key Cryptography）を開催した。2017 年には CAESAR の最終候補方式の選定作業に選定委員として参画した。2018 年 3 月に最終候補方式がアナウンスされ、第三ラウンド候補であった提案中の CLOC および SILC は最終候補方式としては選出されなかった。今後引き続き、最終ポートフォリオ方式の選定作業に参画する。

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 6 件）


① Kota Kondo, Yu Sasaki, Yosuke Todo, and Tetsu Iwata. On the Design Rationale of Simon Block Cipher: Integral Attacks and Impossible Differential Attacks against Simon Variants. IEICE Trans. Fundamentals, E101-A(1), 88-98 (2018). 10.1587/transfun.E101.A.88（査読有）
② Tetsu Iwata and Yannick Seurin. Reconsidering the Security Bound of AES-GCM-SIV. IACR ToSC, FSE 2018, Vol. 2017, Issue 4, pp. 240-267, 2017. 10.13154/tosc.v2017.i4.240-267（査読有）
③ Kazuya Imamura, Kazuhiko Minematsu, and Tetsu Iwata. Integrity Analysis of

Authenticated Encryption Based on Stream Ciphers. International Journal of Information Security, IJIS, 2017. 10.1007/s10207-017-0378-9（査読有）

④ Kazuhiko Minematsu and Tetsu Iwata. Cryptanalysis of PMACx, PMAC2x, and SIVx. IACR ToSC, FSE 2018, Vol. 2017, Issue 2, pp. 162-176, 2017. 10.13154/tosc.v2017.i2.162-176（査読有）

⑤ Tetsu Iwata and Kazuhiko Minematsu. Stronger Security Variants of GCM-SIV. IACR ToSC, FSE 2017, Vol. 2016, Issue 1, pp. 134-157, 2016. 10.13154/tosc.v2016.i1.134-157（査読有）

⑥ Hayato Kobayashi, Kazuhiko Minematsu, and Tetsu Iwata. Optimality of Tweak Functions in CLOC. IEICE Trans. Fundamentals, E98-A(10), 2152-2164 (2015). 10.1587/transfun.E98.A.2152（査読有）

〔学会発表〕（計 28 件）

① 伊藤 玄武, 岩田 哲, 松本 隆太郎. 4 ラウンド Feistel 暗号に対する量子選択暗号文攻撃. SCIS 2018, 2C2-3, 2018.

② 中道 良太, 岩田 哲. Tweakable ブロック暗号から構成されたブロック暗号の選択暗号文攻撃に対する安全性証明. SCIS 2018, 2C2-2, 2018.

③ Tetsu Iwata. ZMAC: Specification Review, Security Proof, and Instantiation Updates. 7th Asian Workshop on Symmetric Key Cryptography, ASK 2017, 2017.

④ Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, and Mridul Nandi. Blockcipher-based Authenticated Encryption: How Small Can We Go? CHES 2017, LNCS 10529, pp. 277-298, Springer, 2017.

⑤ Kazuya Imamura and Tetsu Iwata. How to Improve AEAD-{2a, 4a} and DAEAD-2a. IWSEC 2017, poster session, 2017.

⑥ Kota Kondo, Yu Sasaki, Yosuke Todo, and Tetsu Iwata. Analyzing Key Schedule of Simon: Iterative Key Differences and Application to Related-Key Impossible Differentials. IWSEC 2017, LNCS 10418, pp. 141-158, Springer, 2017.

⑦ Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. CRYPTO 2017, LNCS 10403, pp. 34-65, Springer, 2017.

⑧ 大山 武浩, 近藤 倖大, 岩田 哲. Simon32 とパラメータを変更した Simon32 のゼロ相関攻撃, Integral 攻撃, 不能差分攻撃に対する安全性比較. SCIS 2017, 2B1-3, 2017.

⑨ 近藤 倖大, 佐々木 悠, 藤堂 洋介, 岩田 哲. MILP ソルバによる Related-key モデルにおける Simon32 の差分解読法に対する安全性解析. SCIS 2017, 2B1-2, 2017.

⑩ Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, and Eita Kobayashi. SILC Is INT-RUP Secure. Early Symmetric Crypto (ESC) seminar, 2017.

⑪ Tetsu Iwata. Breaking and Repairing Security Proofs of Authenticated Encryption Schemes. Indocrypt 2016, invited talk, 2016.

⑫ Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, and Eita Kobayashi. Updates on CLOC and SILC Version 3. Directions in Authenticated Ciphers, DIAC 2016, 2016.

⑬ 今村 和弥, 岩田 哲. ChaCha20-Poly1305 の Nonce-Misuse と Decryption-Misuse 耐性. SCIS 2016, 3D1-2, 2016.

⑭ Kazuhiko Minematsu and Tetsu Iwata. Tweak-Length Extension for Tweakable Blockciphers. IMACC 2015, LNCS 9496, pp. 77-93, Springer, 2015.

⑮ Shohei Ando, Kazuhiko Minematsu, and Tetsu Iwata. Provable Security Bounds of GCM. 5th Asian Workshop on Symmetric Key Cryptography, ASK 2015, 2015.

⑯ Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, and Eita Kobayashi. Updates on CLOC and SILC. Directions in Authenticated Ciphers, DIAC 2015, 2015.

⑰ Yuichi Niwa, Keisuke Ohashi, Kazuhiko Minematsu, and Tetsu Iwata. GCM Security Bounds Reconsidered. FSE 2015, LNCS 9054, pp. 385-407, Springer, 2015.

⑱ Kazuhiko Minematsu and Tetsu Iwata. More on Generic Composition. Early Symmetric Crypto (ESC) seminar, 2015.

⑲ Tetsu Iwata. Security of the Galois/Counter Mode of Operation. Technical Committee on Cryptologic Mathematics, Chinese Association for Cryptologic Research, TCCM-CACR, 2014.

⑳ Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, and Eita Kobayashi. SILC: SImple Lightweight CFB. Directions in Authenticated Ciphers, DIAC 2014, 2014.

６．研究組織

(1)研究代表者

岩田　哲（IWATA, Tetsu）
名古屋大学・工学研究科・准教授
研究者番号：90344837