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　 ５ 月 ２８ 日現在

機関番号：１３４０１
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ１１８８５

研究課題名（和文）応用の広がりを考慮した暗号方式の設計と評価

研究課題名（英文）Design and Evaluation of Cryptographic Schemes Considering Extension of Applications

研究代表者
廣瀬　勝一（Hirose, Shoichi）

福井大学・学術研究院工学系部門・教授

研究者番号：２０２２８８３６

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：本研究では計算資源の乏しい環境での使用に耐える軽量暗号方式および応用が要求する機能を提供する暗号方式の設計と評価という課題に取り組んだ。これらの暗号方式について，従来方式と同等の安全性を有し，かつ，より処理効率の高い方式を提案した。提案方式の安全性については，それらの数学的な定義に基づき，構成要素の安全性により保証されること，すなわち，構成要素が安全であれば提案方式の安全性が達成されることを証明により明らかにした。

研究成果の学術的意義や社会的意義
暗号技術は情報通信の安全性を保証する基盤技術であり，その応用範囲はますます広がっている。暗号技術の研究開発に関する重要な点は，安全性はもとより，処理性能の向上と機能の充実である。暗号は，計算資源の潤沢な環境から乏しい環境に至るまで，多様な環境で使用される。さらに，暗号の利用が浸透するにつれて多様な応用により新たな機能が要求される。このような観点から本研究成果の学術的意義や社会的意義が認められる。

研究成果の概要（英文）：In this study, we addressed the design and evaluation of lightweight cryptographic schemes that are useful in environments with limited computational resources and cryptographic schemes that provide functions required by applications. For these cryptographic schemes, we proposed schemes that are as secure as conventional schemes and have higher efficiency. We proved that the security of the proposed schemes is guaranteed by the security of their components based on their mathematical definitions, i.e., the security of the proposed schemes is achieved if the components are secure.

研究分野：暗号学

キーワード：暗号　帰着可能性　軽量暗号　暗号応用

様　式　C－１９、F－１９－１（共通）

１．研究開始当初の背景

暗号は安全・安心な情報通信環境の構築に不可欠な情報セキュリティの基盤技術であり，今後も期待される IoT (Internet of Things) 技術の発展と普及により，暗号技術が我々の生活にますます浸透することが予想される。暗号技術の研究開発に関する重要な点は，安全性はもとより，処理性能の向上と機能の充実である。暗号は，計算資源の潤沢な環境から乏しい環境に至るまで，多様な環境で使用される。このため，近年では，計算資源の乏しい環境での使用に適した軽量暗号の研究開発が大きな関心を集めている。さらに，暗号の利用が浸透するにつれて，従来の暗号が提供する基本的な機能のみでなく，多様な応用が新たな機能を要求することが予想される。

２．研究の目的

本研究は「各々の暗号方式がどのような暗号要素のどのような安全性要件に基づいて構成されるか」を明らかにすることを目的とする。これは暗号における帰着可能性の問題であり，帰着可能性は理論計算機科学の最も重要な基礎概念の一つである。この問題について，本研究では特に，計算資源が乏しい環境での使用に適した暗号（軽量暗号）と，応用の広がりによる新たな機能の要求という二つの点に着目し，「軽量暗号方式を，より少ないあるいはより簡素な暗号要素を用いてより効率よく構成できるか」と「応用が要求する新たな機能の実現のために，新たな暗号要素や安全性要件が必要となるか」という問題に取り組む。

３．研究の方法

(1)軽量暗号方式の設計と評価

衝突計算困難かつ擬似ランダムハッシュ関数は暗号の重要な構成要素である。このようなハッシュ関数として，国際標準の HMAC が広く用いられている。HMAC は国際標準ハッシュ関数 SHA-2，SHA-3 をそのまま用いて構成できることが利点であるが，軽量暗号という観点からは，特に短い入力に対する処理効率に問題がある。本研究では，SHA-2 に代表される Merkle-Damgård ハッシュ関数に基づく衝突計算困難かつ擬似ランダムハッシュ関数の設計と評価を行った。

Merkle-Damgård ハッシュ関数は固定長入出力の圧縮関数$F\colon\{0,1\}^n\times\{0,1\}^w\to\{0,1\}^n$とそれを利用して任意長入力を処理する方法（定義域拡大）とからなる（図 1）。IVは固定の初期値である。入力メッセージ$M=(M_1,\dots,M_{m-1},M_m)$には，長さが圧縮関数で処理されるメッセージブロック長wの倍数となるよう系列padが付加される。本研究では，padが必要最小限かつ衝突計算困難性と疑似ランダム性が同時に満たされるような定義域拡大を開発し，圧縮関数の計算回数を最小化することを目標とした。さらに，軽量暗号としての利用を考慮して，圧縮関数を tweakable ブロック暗号を用いて構成する方式を検討した。

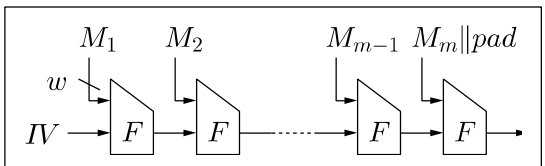


図 1　Merkle-Damgård ハッシュ関数

(2)応用が要求する機能を有する暗号方式の設計と評価

認証暗号（AEAD）は秘匿性と偽造不能性を同時に提供する共通鍵暗号であり，現在も盛んに研究が行われている。AEAD の応用の広がりに伴い，近年，message franking 機能の実現に有用なコンパクトなコミット機能を有する認証暗号（ccAEAD）が提案された。Message franking 機能は，エンドツーエンドの暗号通信において不適切なメッセージの受信の通報を可能とする技術であり，Facebook などの SNS で用いられている。Dodis ら[1]は，encryptment と呼ばれる ccAEAD の構成要素を定式化し，encryptment と通常の AEAD を用いて ccAEAD が実現できることを示した(図 2)。ECenc と ECdec はそれぞれ encryptment の暗号化と復号である。ECkg は encryptment の鍵生成である。AEenc と AEdec はそれぞれ AEAD の暗号化と復号である。Kは送信者と受信者が共有する秘密鍵，A,Mはそれぞれ関連データとメッセージであり，Lは encryptment の秘密鍵である。C_0,C_1はそれぞれM,Lの暗号文であり，BはA,M,Lに対する認証子であり，TはB,Lに対する認証子である。

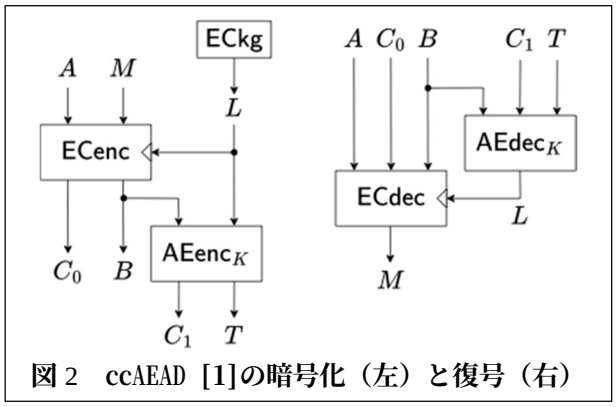


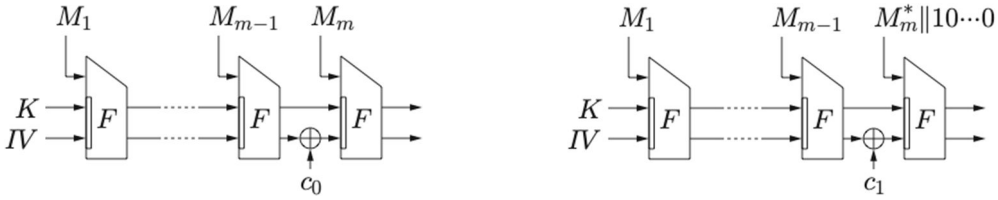
図 2　ccAEAD [1]の暗号化（左）と復号（右）

本研究では，encryptment を用いて，Dodis らの ccAEAD よりも効率の良い方式が実現可能であるかを検討した。特に，暗号化の出力にB,T二つの認証子が含まれることから，Tを削減することを検討した。

４．研究成果

(1)軽量暗号方式の設計と評価

①本研究で提案した衝突計算困難かつ擬似ランダムハッシュ関数KMDP⁺を図 3 に示す。この関数は，Merkle-Damgård ハッシュ関数に基づく鍵付きハッシュ関数であり，[2]で提案された Keyed-MDP の改良版である。図 3 で，$F:\{0,1\}^n \times \{0,1\}^w \to \{0,1\}^n$ は圧縮関数，$M = (M_1, \ldots, M_{m-1}, M_m)$は入力メッセージ，$K \in \{0,1\}^{n/2}$は秘密鍵，$IV \in \{0,1\}^{n/2}$は固定の初期値，$c_0, c_1 \in \{0,1\}^{n/2}$は相異なる非零の定数であり，$\oplus$はビットごとの排他的論理和である。図 3 に示されているとおり，Mの長さがwの正の整数倍でないときのみ，Mの末尾に1に続き 0 個以上の最小個数の0が付加される。したがって，圧縮関数の計算回数最小化を達成している。



(a) Mの長さがwの正の倍数のとき　　(b) 左記(a)以外のとき

図 3　衝突計算困難かつ擬似ランダムハッシュ関数の提案方式

本研究では，ランダムオラクルモデル（Fが一様分布に基づいて選択されるランダム関数であるという仮定のもと）でKMDP⁺が衝突計算困難性を満たすことを示した。さらに，Fが以下のような関連鍵攻撃のもとで安全な擬似ランダム関数であるとき，KMDP⁺が擬似ランダム関数であることを示した。

1. 鍵Kが$\{0,1\}^{n/2} \times \{IV\}$から無作為に選択されるとき，$F(K||IV,\cdot), F(K||(IV \oplus c_0),\cdot), F(K||(IV \oplus c_1),\cdot)$が３つの独立なランダム関数と識別不能である。
2. 鍵$\tilde{K}$が$\{0,1\}^n$から無作為に選択されるとき，$F(\tilde{K},\cdot), F(\tilde{K} \oplus (0^{n/2}||c_0),\cdot), F(\tilde{K} \oplus (0^{n/2}||c_1),\cdot)$が３つの独立なランダム関数と識別不能である。

ここで||は系列の連接を表す。なお，関連鍵攻撃は攻撃者に有利な強力な攻撃手法と考えられているが，IV, c_0, c_1は設計時に定められる定数であり，攻撃者は選択できない。

②本研究ではさらに，tweakable ブロック暗号を用いてKMDP⁺を実現する方式（以下ではKMDP⁺wTBCと呼ぶ）を提案した。KMDP⁺wTBCでは，圧縮関数が tweakable ブロック暗号 $E:\{0,1\}^\kappa \times \{0,1\}^\nu \to \{0,1\}^\nu$（$\kappa \geq 2\nu$）を用いて構成される。この方式を図 4 に示す。$\delta \in \{0,1\}^\nu$は最下位ビットが1の定数である。さらに，KMDP⁺wTBCは厳密にはKMDP⁺とは異なり，圧縮関数の最終呼出しの入力について４つの非零の定数$c_{00}, c_{01}, c_{10}, c_{11} \in \{0,1\}^\nu$を用いる。入力メッセージの長さが$(\nu - n)$の正の倍数のとき$c_{0b}$を用い，それ以外のとき$c_{1b}$を用いる。ここで，$b$は最終メッセージブロックの最下位ビットである。

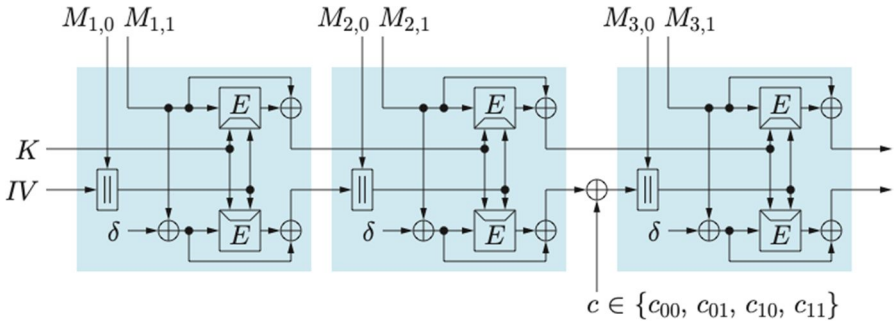


図 4　Tweakable ブロック暗号を用いた衝突計算困難かつ擬似ランダムハッシュ関数

本研究では，理想暗号モデル（Eが一様分布に基づいて選択されるランダム tweakable ブロック暗号であるという仮定のもと）でKMDP⁺wTBCが衝突計算困難性を満たすことを示した。さらに，Eが以下の条件を満たすならば，KMDP⁺wTBCが擬似ランダム関数であることを示した。

1. $\{0,1\}^\kappa = \{0,1\}^\nu \times \{0,1\}^{\kappa-\nu}$について，$\{0,1\}^\nu$が鍵集合，$\{0,1\}^{\kappa-\nu}$が tweak 集合である tweakable 擬似ランダム置換である。
2. $\{0,1\}^\kappa = \{0,1\}^{2\nu} \times \{0,1\}^{\kappa-2\nu}$について，$\{0,1\}^{2\nu}$が鍵集合，$\{0,1\}^{\kappa-2\nu}$が tweak 集合である tweakable 擬似ランダム置換であり，$K = (K_0, K_1) \in \{0,1\}^\nu \times \{0,1\}^\nu$が無作為に選択されるとき，$(K_0, K_1), (K_1, K_0), (K_0, K_1 \oplus c), (K_1 \oplus c, K_0)$（$c \in \{c_{00}, c_{01}, c_{10}, c_{11}\}$）を鍵とする 10 個の$E$が 10 個の独立な tweakable ランダム置換と識別不能である。

(2)応用が要求する機能を有する暗号方式の設計と評価

本研究で提案した ccAEAD 方式ECTの暗号化と復号を図 5 に示す。E, Dはそれぞれ tweakable ブ

ロック暗号の暗号化と復号である。

ECTと Dodis ら[1]の方式との相違点は，認証暗号の暗号化と復号の代わりに tweakable ブロック暗号の暗号化と復号を用いる点である。認証暗号の暗号化では，Lの暗号文に加えてB, Lに対する認証子も生成されるため，ECTの出力長は Dodis らの方式の出力長より小さい。

本研究では，以下のとおり，ECTの安全性が構成要素である encryptment と tweakable ブロック暗号の安全性に帰着できることを示した。

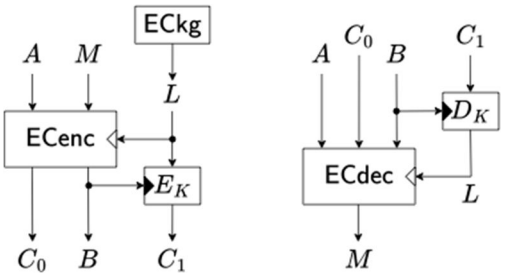


図 5　ECTの暗号化（左）と復号（右）

1. encryptment が秘匿性を満たし，tweakable ブロック暗号が tweakable 擬似ランダム置換ならば，ECTは秘匿性を満たす。
2. encryptment が偽造不能性を満たし，tweakable ブロック暗号が tweakable 強擬似ランダム置換ならば，ECTは偽造不能性を満たす。
3. encryptment が拘束性を満たすならば，ECTは拘束性を満たす。

〈引用文献〉

[1] Y. Dodis, P. Grubbs, T. Ristenpart, and J. Woodage: Fast Message Franking: From Invisible Salamanders to Encryptment. CRYPTO 2018. Lecture Notes in Computer Science, vol. 10991, pp. 155-186, 2018.

[2] S. Hirose, J.H. Park, and A. Yun: A Simple Variant of the Merkle-Damgård Scheme with a Permutation. ASIACRYPT 2007. Lecture Notes in Computer Science, vol. 4833, pp. 113–129, 2007.

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　1件／うちオープンアクセス　1件）

１．著者名 Hirose Shoichi	４．巻 13218
２．論文標題 Collision-Resistant and Pseudorandom Function Based on Merkle-Damgaard Hash Function	５．発行年 2022年
３．雑誌名 Lecture Notes in Computer Science (Proc. ICISC 2021)	６．最初と最後の頁 325～338
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-08896-4_17	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 Hirose Shoichi	４．巻 13720
２．論文標題 Collision-Resistant and Pseudorandom Hash Function Using Tweakable Block Cipher	５．発行年 2023年
３．雑誌名 Lecture Notes in Computer Science (Proc. WISA 2022)	６．最初と最後の頁 3～15
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-25659-2_1	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 Hirose Shoichi, Minematsu Kazuhiko	４．巻 14201
２．論文標題 Compactly Committing Authenticated Encryption Using Encryptment and Tweakable Block Cipher	５．発行年 2024年
３．雑誌名 Lecture Notes in Computer Science (Proc. SAC 2023)	６．最初と最後の頁 233～252
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-53368-6_12	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 Zheng Mingmei, Liu Zi-Yuan, Mambo Masahiro	４．巻 11
２．論文標題 A Provably Secure Lattice-Based Fuzzy Signature Scheme Using Linear Sketch	５．発行年 2023年
３．雑誌名 IEEE Access	６．最初と最後の頁 62510～62521
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2023.3287777	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 Zi-Yuan, Mambo Masahiro, Tso Raylin, Tseng Yi-Fan	4．巻 89
2．論文標題 Anonymous hierarchical identity-based encryption with delegated traceability for cloud-based data sharing systems	5．発行年 2024年
3．雑誌名 Computer Standards & Interfaces	6．最初と最後の頁 103817～103817
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.csi.2023.103817	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

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 李奕慷，桑門秀典
2．発表標題 同種写像鍵共有法SIDHのCGBNを用いたGPU上の実装
3．学会等名 2022年電子情報通信学会ソサイエティ大会
4．発表年 2022年

1．発表者名 李奕慷，桑門秀典
2．発表標題 同種写像鍵共有法CSIDHのCUDA用多倍長演算ライブラリCGBNを用いた実装
3．学会等名 第45回情報理論とその応用シンポジウム
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	桑門　秀典 (Kuwakado Hidenori) (30283914)	関西大学・総合情報学部・教授 (34416)	

６．研究組織（つづき）

	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	満保　雅浩 (Mambo Masahiro) (60251972)	金沢大学・電子情報通信学系・教授 (13301)	

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