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　 ２ 日現在

機関番号：１３４０１
研究種目：基盤研究(B)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０２８２８

研究課題名（和文）標準暗号とその利用法の安全性評価に関する研究

研究課題名（英文）Security Analyses of Standardized Cryptographic Schemes and Their 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）　　13,000,000円

研究成果の概要（和文）：本研究で得られた主な成果は，共通鍵暗号に関して，標準暗号の構成要素を利用して，標準暗号と同等の安全性を保証しつつ，もとの標準暗号よりも効率の良い構成法を提案したことである。これらの提案法の安全性については，それを数学的な証明によって明らかにした。また，公開鍵暗号については，将来の標準暗号の有力な候補と考えられる誤り訂正符号に基づく暗号化方式について，それに対する攻撃アルゴリズムを一般化し，その性能を評価した。

研究成果の学術的意義や社会的意義
本研究の主な成果は，標準暗号の構成要素を用いて，安全性を犠牲にすることなく，より効率の良い方式を提案したことである。安全性を犠牲にすることなく効率の向上を実現することは，暗号に関する研究の重要な課題の一つであり，本研究の学術的意義はこれが達成できる例を示したことである。さらに，近年，モノのインターネット（IoT）に対する関心が高まっており，計算資源に制約のある機器での利用に適した暗号技術を開発したことが，本研究の社会的意義として挙げられる。

研究成果の概要（英文）：Our major contribution is to use primitives of standardized cryptographic schemes and design new schemes as secure as and more efficient than the standardized schemes for symmetric-key cryptography. The security of the proposed schemes are confirmed by mathematical proofs. For public-key cryptography, we extend a cryptanalytic algorithm for encryption schemes based on error-correcting codes and evaluate its performance.

研究分野：暗号学

キーワード：暗号・認証等　標準暗号

１．研究開始当初の背景

情報通信ネットワークは我々の生活を支えるインフラの一つであり，今や情報通信環境と呼ばれるほどに遍在している。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，特に，標準に規定された暗号技術が実用に供されることが多い。ところが，標準であることは必ずしも安全性が保証されていることを意味しておらず，標準暗号の脆弱性が明らかとなり重大な問題の発生した例が後を絶たない。したがって，現在広く利用されている，あるいは，利用機会の高い標準暗号の安全性評価を継続することは非常に重要な研究課題である。

さらに，今後ますます暗号の適用範囲が広がり，利用環境の制約に応じて標準暗号をカスタマイズして利用する機会の増えることが予想される。このようなカスタマイズに関して，もとの標準暗号の安全性評価結果を利用することによりカスタマイズされた方式の安全性評価の支援や容易化が可能となれば，処理性能等の面でより効果的な暗号の利用が促進される。

また，今後の有力な標準暗号候補の安全性評価を行い，新たな標準暗号の規定に寄与することは，既存の標準暗号の安全性評価に勝るとも劣らない重要な研究課題である。公開鍵暗号に関しては，符号や格子に基づく暗号が，量子計算による攻撃への耐性を有すると期待されており，将来の有力な標準暗号候補と考えられるが，その安全性評価については今後の研究課題が多く残されている。一方，共通鍵暗号に関しては，暗号化と改竄検知の両方の機能を有する認証暗号について，CAESAR と称される国際暗号評価コンテストが NIST の支援の下で実施されており，本コンテストの応募アルゴリズムの安全性評価も重要な課題である。

２．研究の目的

本研究では，現在の標準暗号や今後の標準暗号の有力な候補と考えられる種々の暗号方式の安全性評価を進めるとともに，標準暗号をカスタマイズした方式の安全性評価を支援する手法を確立することを目的とする。

３．研究の方法

(1) 圧縮関数による反復型ハッシュ関数と擬似乱関数の効率改善

標準ハッシュ関数である SHA-2 は，図 1 のような圧縮関数を構成要素とする反復型構造を有している。この構造では，任意長の入力メッセージ$M = (M_1, M_2, \ldots, M_m)$を処理するために，系列$pad$を付加して，入力系列の長さを$F$のメッセージブロック入力の長さ$w$の倍数とする処理が必要である。本研究では，IoT への応用を想定した軽量暗号実現を目標として，ハッシュ関数の処理性能を改善するため，付加される系列padの長さが最小となるような構成を提案し，その安全性を検討した。本提案手法の安全性については，証明可能安全性の観点から，衝突計算困難性，強識別困難性（indifferentiability）について検討した。さらに，初期値IVを秘密鍵に置き換えて得られる擬似乱関数について，同じく証明可能安全性の観点から安全性を検討した。

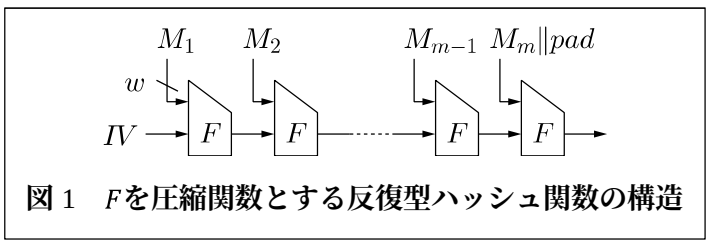


図 1　Fを圧縮関数とする反復型ハッシュ関数の構造

(2) Lesamnta-LW とそれに基づく擬似乱関数のカスタマイズ

本研究代表者らが過去に開発した軽量ハッシュ関数 Lesamnta-LW が 2016 年に国際標準 ISO/IEC 29192-5:2016 に規格化されたことを受けて，Lesamnta-LW を用いたあるいはそれに基づく暗号方式の開発とその安全性評価を行った。Lesamnta-LW を図 2 に示す。ここで，Eはブロック長 256 ビット，鍵長 128 ビットの専用ブロック暗号である。Lesamnta-LW はブロック暗号Eを圧縮関数とする反復型ハッシュ関数である。本研究では，Lesamnta-LW のさらなる軽量化を目標として，上記の(1)と同様の手法を Lesamnta-LW に適用し，その効果を確認した。

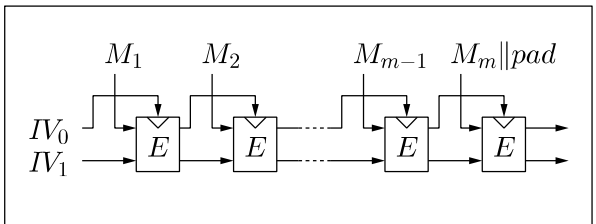


図 2　ハッシュ関数 Lesamnta-LW

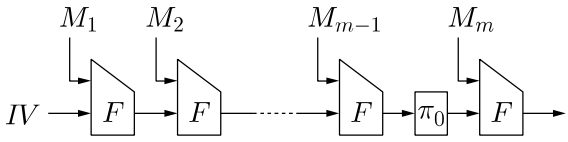
(3) 誤り訂正符号に基づく公開鍵暗号に対する攻撃アルゴリズムの一般化

量子コンピュータを用いた攻撃（量子攻撃）への耐性を有すると期待されている誤り訂正符号に基づく公開鍵暗号方式については，Information Set Decoding（ISD）と呼ばれる手法を用いた攻撃法が知られており，古くから研究が行われている。本研究では，近年提案された ISD の改良法を任意の有限体上の符号に拡張してその計算量を評価した。

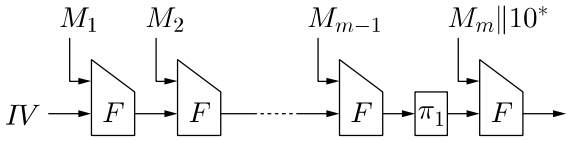
４．研究成果

(1) 圧縮関数による反復型ハッシュ関数と擬似乱関数の効率改善

本研究で提案した反復型ハッシュ関数を図 3 に示す。ここで，圧縮関数を $F:\{0,1\}^n \times \{0,1\}^w \to \{0,1\}^n$ とする。提案方式では Merkle Damgård with a Permutation (MDP) [1] と呼ばれる定義域拡大法を利用しており，メッセージの最終ブロックの処理の前にメッセージ長に応じた置換が挿入されている。MDP と異なる点は，MDP では単一の置換の挿入のみが考慮されていることである。提案方式では，入力 M の長さに応じて π_0 または π_1 を用いることにより，M の長さがメッセージブロック長 w の正の倍数のときには，パディングが不要となっている。なお，π_0, π_1 には暗号学的な安全性は要求されず，例えば，定数との排他的論理和などの演算を用いることが想定されている。提案方式で，標準ハッシュ関数 SHA-256 の圧縮関数（$F:\{0,1\}^n \times \{0,1\}^w \to \{0,1\}^n$ で，$n = 256$，$w = 512$）を利用するとき，入力メッセージの長さを ℓ とすると，圧縮関数の計算回数は $\lceil \ell/512 \rceil$ である。一方，SHA-256 では，圧縮関数の計算回数は $\lceil (\ell - 447)/512 \rceil + 1$ となる。ここで，$\lceil x \rceil$ は x 以上の最小の整数を表す。



(a) $|M|$がメッセージブロック長の正の倍数のとき



(b) 上記(a)以外のとき

図 3　提案方式，$|M|$は入力Mの長さを表す

本研究では，この提案方式について，ハッシュ関数の主要な安全性要件である衝突計算困難性と強識別困難性を証明可能安全性の観点から評価した。衝突計算困難性は，出力が一致する相異なる入力の組を計算することが困難であるという性質であり，圧縮関数 F が以下の性質を有するとき，提案方式が衝突計算困難性を有することを明らかにした。

- F が衝突計算困難性を有する。
- $\pi_0(F(v,X)) = \pi_1(F(v',X'))$ を満たす相異なる (v,X) と (v',X') の組の計算が困難である。
- 与えられた $Y \in \{0,1\}^n$ について，$Y = F(X)$ を満たす X の計算が困難である。

一方，強識別困難性は，圧縮関数 F が乱関数であるという理想的な仮定のもとで定式化される安全性要件であり，乱関数との識別困難性を意味する。強識別困難性に関する識別攻撃の計算量は，攻撃における圧縮関数 F の計算回数で評価される。本研究では，任意の識別攻撃に必要な F の計算回数が $2^{n/2}$ に比例する回数以上であることを明らかにした。この結果は，強識別困難性に関して，提案方式が，それと同様の反復型構造を有する他のハッシュ関数と同等以上の安全性を満たしていることを示している。なお，標準ハッシュ関数 SHA-256 は，同一の仮定のもとでも強識別困難性を満たさないことが知られている。

本研究ではさらに，提案方式の初期値 IV を秘密鍵に置き換えることにより得られる MAC 関数の効率と安全性についても検討した。この方式で SHA-256 の圧縮関数を利用するとき，入力メッセージの長さを ℓ とすると，圧縮関数の計算回数は $\lceil \ell/512 \rceil$ である。一方，SHA-256 を用いて構成された標準 MAC 関数 HMAC では，圧縮関数の計算回数は $\lceil (\ell - 447)/512 \rceil + 4$ となる。このことから，提案方式は短いメッセージに対して特に有効であることが分かる。また，圧縮関数 F が π_0, π_1 に関する関連鍵攻撃のもとで擬似乱関数であれば，提案した MAC 関数も擬似乱関数となることを明らかにした。関連鍵攻撃は一般に非常に強力な攻撃であると考えられているが，提案方式では，攻撃者に有利とならないように設計者が π_0, π_1 を決定できる。

(2) Lesamnta-LW とそれに基づく擬似乱関数のカスタマイズ

本研究では上記の (1) と同様に，Lesamnta-LW に MDP 定義域拡大を適用して構成されるハッシュ関数 (図 4) の特徴と安全性について検討した。

本研究では，まず，このハッシュ関数の衝突計算困難性について検討し，出力長を n とするとき，E の内部構造を利用しない任意の衝突攻撃の時間計算量が $2^{n/2}(\log n)/n$ に比例する時間以上であることを明らかにした。この結果は，図 4 のハッシュ関数が Lesamnta-LW と同等の衝突計算困難性を有していることを示している。

次に，図 4 のハッシュ関数の初期値 $IV = (IV_0, IV_1)$ を秘密鍵で置き換えて得られる MAC 関数について，E が擬似乱関数であれば，この MAC 関数も擬似乱関数となることを明らかにした。この MAC 関数は二つの特

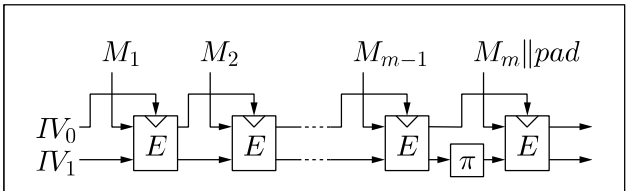


図 4　Lesamnta-LW に基づくハッシュ関数

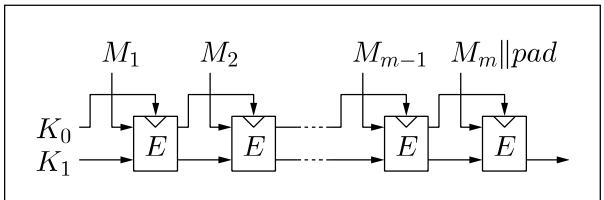


図 5　Lesamnta-LW を用いた MAC 関数

徴を持つ。一つは，上記(1)の研究で提案された MAC 関数と異なり，Eの関連鍵攻撃のもとでの安全性が要求されないことである。もう一つは，Lesamnta-LW の初期値を秘密鍵に置き換えた MAC 関数（図 5）と比較して，出力長が 2 倍であることである。これは例えば，擬似乱数列生成への応用において有利である。MAC 関数についてはさらに，上記(1)の研究と同様に，二つの置換π_0, π_1を用いてパディングが最小となる構成についても検討した。この構成についても，Eが擬似乱関数であれば，この MAC 関数が擬似乱関数となることを明らかにした。

(3) 誤り訂正符号に基づく公開鍵暗号に対する攻撃アルゴリズムの一般化

誤り訂正符号に基づく公開鍵暗号の安全性は，ランダム線形符号の復号問題の計算困難性に基づく。ランダム線形符号の復号問題を解く効果的な手法として知られる ISD は，転置と探索の二つのステップから成るが，アルゴリズムの計算量削減を目的として，探索ステップに関して多くの提案がなされている。本研究では，当時最も有効な手法であった May と Ozerov の２元体上の最近傍問題を解くアルゴリズムを任意の有限体上へ一般化し，それを用いた ISD の効果を評価した。なお，誤り訂正符号に基づく公開鍵暗号に関しては，鍵長の削減を目的として，２元体以外の有限体上での構成が検討されている。

本研究では，任意の有限体上の最近傍問題を解くアルゴリズムを用いた ISD の時間計算量を評価した。表 1 に各アルゴリズムによる限界距離復号の時間計算量を示す。表 1 で，qは有限体の元の個数，Stern-MO，BJMM-MO はそれぞれ，任意の有限体上の最近傍問題を解くアルゴリズムを用いた Stern による ISD アルゴリズム，Becker，Joux，May，Meurer による ISD アルゴリズムを示す。さらに，比較のために，もとの Stern による ISD アルゴリズムの時間計算量も示している。なお，表の各項は，時間計算量を$\tilde{O}(2^{\alpha n})$と表したときの，αの値を示している。ここで，nは符号長であり，$\tilde{O}(2^{\alpha n})$は，ある多項式$p(n)$について，時間計算量が$p(n)2^{\alpha n}$以下であることを示している。

表 1　限界距離復号の時間計算量

q	Stern	Stern-MO	BJMM-MO
2	.05563	.05498	.04730
3	.05217	.05242	.04427
4	.04987	.05032	.04194
5	.04815	.04864	.03955
7	.04571	.04614	.03706
8	.04478	.04519	.03593
11	.04266	.04299	.03335

表 1 から，Stern の ISD アルゴリズムについては，2 元体上の誤り訂正符号以外に対して，最近傍問題を解くアルゴリズムを利用すると，時間計算量が増大していることが分かる。ただし，本研究の最近傍問題を解くアルゴリズムの一般化は，自然な拡張であるものの，アルゴリズムのパラメータの選択が最適であるかどうかについては，さらなる検討が必要であると考えられる。

〈参考文献〉

[1] S. Hirose, J. H. Park and A. Yun, A Simple Variant of the Merkle-Damgård Scheme with a Permutation, Journal of Cryptology, vol. 25, no. 2, 2012, pp. 271-309.

[2] A. May and I. Ozerov, On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes, EUROCRYPT (1), Lecture Notes in Computer Science, vol. 9056, 2015, pp. 203-228.

５．主な発表論文等

〔雑誌論文〕（計８件）

① Shoichi Hirose, The PRF Security of Compression-Function-Based MAC Functions in the Multi-user Setting, IEICE Transactions on Fundamentals, vol. E102-A, 2019, pp. 270-277, 査読有. DOI: 10.1587/transfun.E102.A.270

② Shoichi Hirose, Sequential Hashing with Minimum Padding, Cryptography, vol. 2, 2018, 23 pages, 査読有. DOI: 10.3390/cryptography2020011

③ Shoichi Hirose, Hidenori Kuwakado and Hirotaka Yoshida, A Pseudorandom-Function Mode Based on Lesamnta-LW and the MDP Domain Extension and Its Applications, IEICE Transactions on Fundamentals, vol. E101-A, no. 1, 2018, pp. 110-118, 査読有. doi: 10.1587/transfun.E101.A.110

④ Shoichi Hirose, Yu Sasaki and Kan Yasuda, Rate-One AE with Security Under RUP, ISC 2017, Lecture Notes in Computer Science vol. 10599, 2017, pp. 3-20, 査読有. doi: 10.1007/978-3-319-69659-1_1

⑤ Praveen Gauravaram, Shoichi Hirose and Douglas Stebila, Security Analysis of a Design Variant of Randomized Hashing, ATIS 2017, Communications in Computer and Information Science (CCIS) vol. 719, 2017, pp. 14-22, 査読有. doi: 10.1007/978-981-10-5421-1_2

⑥ Cheikh Thiécoumba Gueye, Jean Belo Klamti and Shoichi Hirose, Generalization of BJMM-ISD Using May-Ozerov Nearest Neighbor Algorithm over an Arbitrary Finite Field Fq, C2SI2017, Lecture Notes in Computer Science, vol. 10194, 2017, pp. 96–109, 査読有. doi: 10.1007/978-3-319-55589-8_7

⑦ Shoichi Hirose, May-Ozerov Algorithm for Nearest-Neighbor Problem over Fq and Its Application to Information Set Decoding, SECITC 2016, Lecture Notes in Computer Science, vol. 10006, 2016, pp. 115-126, 査読有. doi: 10.1007/978-3-319-47238-6_8
⑧ Shoichi Hirose and Atsushi Yabumoto, A Tweak for a PRF Mode of a Compression Function and Its Applications, SECITC 2016, Lecture Notes in Computer Science, vol. 10006, 2016, pp. 103-114, 査読有. doi: 10.1007/978-3-319-47238-6_7

〔学会発表〕（計８件）
① 広瀬僚太，西永俊文，満保雅浩，IoT 向け暗号における効率的な剰余計算方法の検討，2019 年暗号と情報セキュリティシンポジウム，2019.
② Hidenori Kuwakado, Shoichi Hirose and Masahiro Mambo, Parallelizable Message Preprocessing for Merkle-Damgaard Hash Functions, 2018 International Symposium on Information Theory and Its Applications, 2018.
③ Shoichi Hirose, Compression-Function Modes of Operations for Symmetric Cryptography, The 2017 International Symposium for Advanced Computing and Information Technology (ISACIT 2017), 2017.
④ 森田保成，西本賢大，廣瀬勝一,小規模マイクロコントローラ上での標準ハッシュ関数およびそれらに基づくメッセージ認証関数の実装について，電子情報通信学会基礎・境界ソサイエティ大会，A-7-3，2017.
⑤ Asraf Akhimullah and Shoichi Hirose, Lightweight Hashing Using Lesamnta-LW Compression Function Mode and MDP Domain Extension, The 3rd International Workshop on Information and Communication Security (WICS '16), 2016. doi: 10.1109/CANDAR.2016.0107
⑥ Shoichi Hirose, Sequential Hashing with Minimum Padding, The Sixth Asian Workshop on Symmetric Key Cryptography (ASK 2016), 2016.

６．研究組織

(1)研究分担者

研究分担者氏名：桑門 秀典

ローマ字氏名：KUWAKADO, Hidenori

所属研究機関名：関西大学

部局名：総合情報学部

職名：教授

研究者番号（8 桁）：30283914

研究分担者氏名：満保 雅浩

ローマ字氏名：MAMBO, Masahiro

所属研究機関名：金沢大学

部局名：電子情報通信学系

職名：教授

研究者番号（8 桁）：60251972