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　 ６ 月 １６ 日現在

機関番号：１３９０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ１１６７５

研究課題名（和文）共通鍵暗号技術の古典・量子安全性解析

研究課題名（英文）Classical/Quantum Security Analyses of Symmetric Key Cryptosystems

研究代表者
岩田　哲（Iwata, Tetsu）

名古屋大学・工学研究科・教授

研究者番号：９０３４４８３７

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究は量子コンピュータ時代にも適した共通鍵暗号技術の開発に向け、主要な共通鍵暗号技術を取り上げ、これらの安全性解析を古典的攻撃と、量子攻撃の両方の観点から行うものである。主な成果として、tweakableブロック暗号を構成要素として用いた一般化Feistel暗号の古典的攻撃に対する安全性を解析した。繰り返し回数と安全性との関連を明らかにするとともに、秘密鍵の鍵長と安全性のトレードオフを明らかにした。また、Sum of Even-Mansour擬似ランダム関数、ディスクセクタ暗号Adiantum等の方式に対し、量子攻撃に対する安全性を明らかにした。

研究成果の学術的意義や社会的意義
古典的攻撃に対し高い安全性と計算効率を兼ね備えた共通鍵暗号技術の設計は重要な研究課題であり、本研究のブロック暗号の構成に関する成果は、この課題に対する一定の解を与えている。また、量子コンピュータが実現された際の共通鍵暗号技術の安全性への影響は解明しきれていない、という課題があった。本研究の量子安全性、量子攻撃に関する成果は、この課題に対する一定の解を与えている。

研究成果の概要（英文）：This research aims to develop symmetric key cryptosystems suitable for use in the quantum era. Towards this goal, we study the security of main techniques of symmetric-key cryptosystems in terms of both classical and quantum attacks. As our main results, we analyzed the security of generalized Feistel ciphers, where a tweakable block cipher is used as a component, in a classical setting. We clarified the relationship between the number of rounds and the security, and we also clarified the trade-off between the length of the secret key and the security. In the quantum setting, we analyzed the security of the Sum of Even-Mansour pseudorandom function and the disk sector encryption called Adiantum.

研究分野：情報学基礎論関連

キーワード：共通鍵暗号　安全性解析　古典的攻撃　量子攻撃

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

共通鍵暗号技術はデータの暗号化及び認証に幅広く用いられる基盤技術である。その応用範囲は広がり続けており、様々な環境に応じて、優れた安全性、計算効率、実装性能を兼ね備えた方式の設計・開発が望まれている。
量子コンピュータの実現に向けた取り組みが進められている中で、これが実現した際、共通鍵暗号技術の安全性に与える影響は限定的であると考えられてきた。しかし、桑門と森井により、古典的に安全性が証明可能なブロック暗号であっても、量子攻撃により効率的に解読が可能である場合があることが示された。これを契機として、ブロック暗号やメッセージ認証コード、認証暗号化方式など様々な共通鍵暗号技術の量子攻撃に対する安全性解析が進められてきた。これまでに古典的な攻撃に比べて著しく安全性が低下する方式と、量子攻撃に対しても安全性の低下が限定的である方式があることが明らかとなってきたが、その影響が未解決である多くの方式が存在する。

２．研究の目的

上記の背景のもと､本研究では｢ポスト量子コンピュータ時代にも適した共通鍵暗号技術の開発｣に向け、これに対する一歩として主要な共通鍵暗号技術を取り上げ、それらの安全性を古典的攻撃と、量子攻撃の両方の観点から解析する。解析対象として暗号学的置換、Feistel 暗号などのブロック暗号、ディスクセクタ暗号や擬似ランダム関数等の利用モードを取り上げる。安全性解析は、攻撃手法の開発と、安全性証明の両方を考える。

３．研究の方法

古典的な安全性証明は Patarin による Coefficient-H 手法による。攻撃手法の開発はバースデーパラドクスに基づく識別攻撃を考えるとともに、平文回復攻撃、偽造攻撃等のより深刻な攻撃の可能性を考える。量子攻撃の開発は汎用的な量子アルゴリズムである Simon の周期発見アルゴリズム、Grover のデータベース探索アルゴリズム等を用いて行う。

４．研究成果

本研究では、主に下記の研究成果を得た。

1) 鍵長の長い Ideal Cipher（理想ブロック暗号）を用いた繰り返し構造を有する暗号学的置換に対し、繰り返し回数と古典的安全性のトレードオフを明らかにした。より詳細には、ブロック長が n ビットである Ideal Cipher を用い、強識別不可能性という安全性定義を考え、入力長が dn ビットである暗号学的置換を構成する。このとき、繰り返し回数（ラウンド数）が 2d+1 で従来技術よりも高い安全性を達成することを示した。また、ラウンド数を 2 回増やすにしたがって、安全性が指数関数的に改善することを示した。

2) 量子攻撃に対して証明可能安全性を有する tweakable ブロック暗号の構成法を明らかにした。量子攻撃に対して安全なブロック暗号の存在を仮定し､これを 3 回呼び出すことで tweakable ブロック暗号を構成し、量子選択平文-tweak 攻撃に対する安全性を証明した。より詳細には、ブロック暗号のブロック長が n ビットの場合、構成した tweakable ブロック暗号は、O(2^n/6)回の任意の平文-tweak の量子重ね合わせクエリを行う敵に対して安全であることを証明した。

3) Even-Mansour ブロック暗号の排他的論理和により構成される擬似ランダム関数である Sum of Even-Mansour 構成法の量子攻撃に対する安全性を評価した。暗号学的置換の数、用いる鍵長により、量子多項式時間で鍵回復攻撃ができる場合があることを示した。また一般の場合でも、古典攻撃に比べて指数関数的に攻撃効率が改善することを示した。

4) ブロック暗号の構成について、一般化 Feistel 暗号の拡散層の構成法の検討を行った。方式内部で構成要素を並列計算可能な方式に着目し、DRmax という安全性指標について、特定の入力サイズに対して理論限界を達成するような構成法の例を示した。また、データを細分して処理することにより、DRmax の指標の観点からは改良ができることを示した。

5) ハッシュ関数から擬似ランダム関数、あるいはメッセージ認証コードを構成する手法である HMAC と NMAC について、これらの量子攻撃に対する安全性を解析した。従来示されていたよりも高い安全性を有することを証明した。得られた安全性限界式は、それに対応する攻撃が存在し、

この意味で厳密である。また、SKINNY-HASH というハッシュ関数の内部関数の古典攻撃に対する安全性について、indifferentiability という安全性を有することを証明した。

6) ブロック暗号の構成について、一般化 Feistel 暗号の構成要素として、tweak 長とブロック長が等しい tweakable ブロック暗号を用いた方式の安全性解析を行い、ラウンド数と古典的安全性のトレードオフを明らかにした。より詳細には、tweak 長とブロック長が n ビットである tweakable ブロック暗号を用いる type-1、type-2、type-3 一般化 Feistel 暗号を考える。全体の入出力長が dn ビットであるブロック暗号を構成し、type-1 の場合、選択平文攻撃に対しては 2d-2 ラウンドで安全性証明ができ、3d-2 ラウンドでは指数関数的に安全性が向上することを示した。同様に、type-1、type-2、type-3 の選択暗号文攻撃に対する安全性が証明できるラウンド数と、指数関数的に安全性が向上するラウンド数を明らかにした。

7) Google が開発したディスクセクタ暗号である Adiantum について、Shor のアルゴリズムを用いた量子線形化攻撃に対する安全性解析を行った。また、McGrew と Fluhrer によって提案された tweakable enciphering 方式である XCBv2 の量子攻撃に対する安全性について、部分鍵回復攻撃が知られていたのに対し、偽造攻撃と平文回復攻撃の検討を行った。

8) ブロック暗号の構成について、秘密鍵の鍵長と安全性のトレードオフを解析した。通常の Feistel 暗号を含む一般化 Feistel 暗号である Contracting Feistel 暗号を解析対象とし、構成要素として、tweakable ブロック暗号を用いた方式を扱った。これらの鍵がすべて同じ場合の構成について、ラウンド数と古典的安全性のトレードオフを明らかにした。また、ラウンド定数を導入した構成の安全性を解析した。

9) IEEE 標準のディスクセクタ暗号化方式である EME2 の基となった方式である EME について、量子クリエが可能であるという状況での平文回復攻撃、偽造攻撃に関する安全性解析を行った。また、ディスクセクタ暗号化方式に関する一連の研究の最初期に提案された CMC について、同様の設定で平文回復攻撃、偽造攻撃に関する安全性解析を行った。

５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　7件／うち国際共著　0件／うちオープンアクセス　7件）

１．著者名 Kento Tsuji and Tetsu Iwata	４．巻 E107.A
２．論文標題 Feistel Ciphers Based on A Single Primitive	５．発行年 2024年
３．雑誌名 IEICE Trans. Fundamentals	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2024EAP1006	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 Kazuki Nakaya and Tetsu Iwata	４．巻 2022(4)
２．論文標題 Generalized Feistel Structures Based on Tweakable Block Ciphers	５．発行年 2022年
３．雑誌名 IACR Transactions on Symmetric Cryptology	６．最初と最後の頁 24-91
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tosc.v2022.i4.24-91	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 Akinori Hosoyamada and Tetsu Iwata	４．巻 E104.A
２．論文標題 Indifferentiability of SKINNY-HASH Internal Functions	５．発行年 2021年
３．雑誌名 IEICE Trans. Fundamentals	６．最初と最後の頁 1156～1162
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020DMP0005	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 Kazuo Shinagawa and Tetsu Iwata	４．巻 173
２．論文標題 Quantum attacks on Sum of Even-Mansour pseudorandom functions	５．発行年 2022年
３．雑誌名 Information Processing Letters	６．最初と最後の頁 106172～106172
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ipl.2021.106172	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 Kyoji Shibutania and Tetsu Iwata	4．巻 174
2．論文標題 On the (im)possibility of improving the round diffusion of generalized Feistel structures	5．発行年 2022年
3．雑誌名 Information Processing Letters	6．最初と最後の頁 106197～106197
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ipl.2021.106197	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 Ryota Nakamichi and Tetsu Iwata	4．巻 2020(2)
2．論文標題 Beyond-Birthday-Bound Secure Cryptographic Permutations from Ideal Ciphers with Long Keys	5．発行年 2020年
3．雑誌名 IACR Transactions on Symmetric Cryptology	6．最初と最後の頁 68-92
掲載論文のDOI（デジタルオブジェクト識別子） 10.13154/tosc.v2020.i2.68-92	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 Akinori Hosoyamada and Tetsu Iwata	4．巻 2021(1)
2．論文標題 Provably Quantum-Secure Tweakable Block Ciphers	5．発行年 2021年
3．雑誌名 IACR Transactions on Symmetric Cryptology	6．最初と最後の頁 337-377
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tosc.v2021.i1.337-377	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 －

〔学会発表〕　計23件（うち招待講演　1件／うち国際学会　3件）

1．発表者名 辻健斗，岩田哲
2．発表標題 Tweakableブロック暗号を用いたType-1，Type-2一般化Feistel構造に対する識別攻撃
3．学会等名 電気・電子・情報関係学会東海支部連合大会
4．発表年 2023年

１．発表者名
栗原昂汰，岩田哲

２．発表標題
CMCに対する量子偽造・平文回復攻撃

３．学会等名
電気・電子・情報関係学会東海支部連合大会

４．発表年
2023年

１．発表者名
Kento Tsuji and Tetsu Iwata

２．発表標題
Feistel Ciphers Based on a Single Primitive

３．学会等名
IMACC 2023（国際学会）

４．発表年
2023年

１．発表者名
辻健斗，岩田哲

２．発表標題
Tweakableブロック暗号を用いたType-2一般化Feistel暗号の安全性の再検討

３．学会等名
2024年暗号と情報セキュリティシンポジウム，SCIS 2024

４．発表年
2024年

１．発表者名
栗原昂汰，岩田哲

２．発表標題
EMEに対する古典偽造・平文回復攻撃と量子攻撃への応用

３．学会等名
2024年暗号と情報セキュリティシンポジウム，SCIS 2024

４．発表年
2024年

１．発表者名
中家一輝，岩田哲

２．発表標題
Tweakableブロック暗号を用いた6ブロックのType-2 Feistel暗号の改良

３．学会等名
電気・電子・情報関係学会東海支部連合大会

４．発表年
2022年

１．発表者名
辻健斗，岩田哲

２．発表標題
カウンタと単一鍵のtweakableブロック暗号を用いたブロック暗号の安全性

３．学会等名
電気・電子・情報関係学会東海支部連合大会

４．発表年
2022年

１．発表者名
栗原昂汰，岩田哲

２．発表標題
Google Adiantumに対するShorのアルゴリズムを用いた量子線形化攻撃

３．学会等名
電気・電子・情報関係学会東海支部連合大会

４．発表年
2022年

１．発表者名
岡﨑雅哉，岩田哲

２．発表標題
複数SP層からなるF関数を用いたType-2一般化Feistel構造のMILPによるActive S-box数解析

３．学会等名
電子情報通信学会ISEC研究会

４．発表年
2022年

１．発表者名
辻健斗，岩田哲

２．発表標題
単一のIdeal Cipherを用いた暗号学的置換の安全性

３．学会等名
2023年暗号と情報セキュリティシンポジウム，SCIS 2023

４．発表年
2023年

１．発表者名
栗原昂汰，岩田哲

２．発表標題
XCBv2の部分鍵を利用した量子偽造・平文回復攻撃

３．学会等名
2023年暗号と情報セキュリティシンポジウム，SCIS 2023

４．発表年
2023年

１．発表者名
中家一輝，岩田哲

２．発表標題
Tweakableブロック暗号を用いたType-2 Feistel暗号の改良

３．学会等名
2023年暗号と情報セキュリティシンポジウム，SCIS 2023

４．発表年
2023年

１．発表者名
岡﨑雅哉，岩田哲

２．発表標題
Sub-Block Dividingを用いたType-2一般化Feistel構造に対するMILPによるActive S-box数解析

３．学会等名
電子情報通信学会ISEC研究会

４．発表年
2023年

１．発表者名
Akinori Hosoyamada and Tetsu Iwata

２．発表標題
On Tight Quantum Security of HMAC and NMAC in the Quantum Random Oracle Model

３．学会等名
CRYPTO 2021（国際学会）

４．発表年
2021年

１．発表者名
岡崎 雅哉, 佐々木 悠, 岩田 哲

２．発表標題
ForkSkinnyに対するMILPを用いた差分パス探索

３．学会等名
電子情報通信学会ISEC研究会

４．発表年
2021年

１．発表者名
栗原 昂汰, 岩田 哲

２．発表標題
Google Adiantumに対する量子攻撃

３．学会等名
2022年暗号と情報セキュリティシンポジウム, SCIS 2022

４．発表年
2022年

１．発表者名
辻 健斗, 岩田 哲

２．発表標題
単一鍵のTweakableブロック暗号を用いたブロック暗号の安全性

３．学会等名
2022年暗号と情報セキュリティシンポジウム, SCIS 2022

４．発表年
2022年

１．発表者名
笠原 颯登，岩田 哲

２．発表標題
PMACrx：ベクトル入力をサポートする高安全なメッセージ認証コード

３．学会等名
2022年暗号と情報セキュリティシンポジウム，SCIS 2022

４．発表年
2022年

１．発表者名
Tetsu Iwata

２．発表標題
Quantum Security of Feistel Ciphers

３．学会等名
ProvSec 2020（招待講演）（国際学会）

４．発表年
2020年

１．発表者名
土生亮，岩田哲

２．発表標題
Google Adiantumに対する識別，偽造，平文回復攻撃

３．学会等名
電子情報通信学会ISEC研究会

４．発表年
2020年

１．発表者名
品川和生，岩田哲

２．発表標題
Sum of Even-Mansour擬似ランダム関数に対する量子攻撃

３．学会等名
電子情報通信学会ISEC研究会

４．発表年
2020年

１．発表者名 品川和生，岩田哲
２．発表標題 Sum of Even-Mansour擬似ランダム関数の一般化と量子攻撃耐性評価
３．学会等名 電気・電子・情報関係学会東海支部連合大会
４．発表年 2020年

１．発表者名 中家一輝，岩田哲
２．発表標題 Tweakableブロック暗号を用いた4ブロックのType-2 Feistel暗号
３．学会等名 電子情報通信学会ISEC研究会
４．発表年 2021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

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