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 ２４ 日現在

機関番号：３２６６０
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１９３

研究課題名（和文）共通鍵暗号アルゴリズムの安全性評価の研究

研究課題名（英文）Cryptanalysis of symmetric key encryption algorithm

研究代表者
五十嵐　保隆（Igarashi, Yasutaka）

東京理科大学・理工学部電気電子情報工学科・講師

研究者番号：８０４３４０２５

交付決定額（研究期間全体）：（直接経費）　　1,100,000円

研究成果の概要（和文）：共通鍵ブロック暗号MISTY1に対する先行研究として積分特性の探索を効率的に行う手法であるDivision属性が新たに提案され，世界で初めてフルラウンドのMISTY1が全数探索法よりも効率的に解読可能である事が示されている背景がある．本研究では，この手法 をブロック暗号KASUMIに適用して積分特性探索を行い，5段特性を新たに発見した．また，この5段特性と確率2^ {-18} で発生する弱 鍵条件を組み合わせる事で，7段の KASUMIが2^ {63} 個の選択平文と2^ {63.3} 回の暗号化計算量で攻撃可能である事を明らかにした．

研究成果の学術的意義や社会的意義
本研究では1ビット単位の平文と暗号文の関連を精密に分析し、今までに知られていない暗号の弱点となる特性を計算機探索や理論解析により導出するという特色・独創性がある。その結果として安全性評価の信頼性が高まることとなる。それと同時に様々な暗号方式に対しても本研究の解析手法が適用できる可能性も広がり、暗号解読技術の発展にも寄与できることが期待される。このように本研究成果は独創性や革新性が認められると確信する。また本研究は高度情報化社会における安全に貢献するという意義をもち、安全性評価の研究分野の進展に対する貢献や学術的波及効果が十分に期待でき科学技術・産業など社会に与えるインパクト・貢献も期待できる。

研究成果の概要（英文）：Division property, which is a method to efficiently search integral characteristics as a prior study for common key block cipher MISTY1, is newly proposed, and it is the first in the world that full round MISTY1 can be deciphered more efficiently than the exhaustive search method. In this research, we apply this method to the block cipher KASUMI to search for integral characteristics and newly discover five-round characteristics. Also, by combining this 5-round property with the weak key condition generated with probability 2^ {-18} , the 7-round KASUMI has 2^ {63} chosen plaintexts and 22^ {63.3} encryption calculations, it revealed that it was possible to attack.

研究分野：暗号解析

キーワード：暗号解析　暗号解読　共通鍵暗号　ブロック暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

暗号方式は情報の秘密や正当性を担保する技術であり、人々が情報化社会の中で安心して生活するためには、その安全性評価は極めて重要な課題となっている。従って安全性評価の研究は国内外や政府、民間を問わず活発である。例えば、欧州では 2000 年から 2003 年まで NESSIE(New European Schemes for Signature, Integrity, and Encryption)プロジェクトを実施し、欧州連合の暗号規格を制定した。制定の過程において、多くの暗号アルゴリズムの安全性を多角的に評価し、十分な安全性が見込まれたアルゴリズムのみを暗号規格として採用した。また 2004 年から 2008 年にかけては eSTREAM プロジェクトを実施し、多くの安全性評価を経てストリーム暗号の推奨リストを制定した。米国では 2007 年から 2012 年まで SHA-3(Secure Hash Algorithm 3）選定プロジェクトを実施し、応募されたハッシュ関数の安全性を精力的に評価した。結果としてハッシュ関数 Keccak を米国標準ハッシュ関数 SHA-3 として制定した。一方、日本においても 2000 年から CRYPTREC プロジェクトが経産省と総務省主導のもとに進行中で、多くの暗号アルゴリズムが評価されており、2013 年には日本の電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）が策定された。

我々も 2006 年からこれまでに eSTREAM、SHA-3、CRYPTREC の候補暗号やその他様々な暗号方式の安全性評価に従事してきた。具体的にはブロック暗号である CLEFIA や MISTY, Camellia, HyRAL, LED の安全性評価、ストリーム暗号である MUGI や Enocoro、SNOW3G、Trivium, 混合乱数方式の安全性評価、公開鍵暗号である線形持駒方式の安全性評価、ハッシュ関数である Lesamnta や BLAKE, Hamsi の安全性評価に従事してきた。またこうした暗号方式全体の安全性評価だけではなく、暗号回路部品単位での安全性評価にも従事してきた。更に一連の研究の過程で、特殊な飽和特性の存在の証明や制御用変換、観測用変換といった新たな暗号解読技術も提案、確立し、暗号の安全性評価の発展にも貢献できた。

暗号方式は世の中の技術進歩や解読技法の進歩に伴い危殆化していくものであるので、ここで紹介したような推奨暗号選定プロジェクトは１回限りのものではなく、約 10 年に１回程度の割合で開催されていくものである。従って暗号の安全性評価技術も絶えず磨き続けていかなければならない重要な研究分野であり、私もこれまでの研究成果をさらに発展させ、更に優れた安全性評価技術の確立を目指す。具体的には、従来は暗号解読に要するデータ量や計算量の上界を示す程度に留まっていたが、今回は１ビット単位の平文と暗号文の関連を精密に分析し、暗号解読に要するデータ量や計算量の平均値や厳密値を導出することを目指す。また暗号解読可能な暗号回路の段数を増やしたり、解読手法を改良し解読に要する計算量やデータ量を削減し、従来の暗号解読の成果を上回る成果を上げることを目指す。このように本研究は学術的に見て、推進すべき重要な課題であり、応募額の規模に見合った研究上の意義が十分に認められる。

２．研究の目的

国内外で提案され、世の中でよく知られているブロック暗号、ストリーム暗号の安全性を詳細に評価し、それらの暗号回路部品の安全性も評価する。具体的に安全性評価対象と考えている暗号方式は CLEFIA や MISTY1、MISTY2、HyRAL、enocoro、Trivium、MUGI、SNOW3G、MULTI2 などである。この中で例えば MULTI2 は 1988 年に日立製作所が開発したブロック暗号方式であり、日本の衛星・地上ディジタル放送の標準暗号として採用されている。現在、衛星ディジタル放送、東経 110 度 CS ディジタル放送、地上ディジタルテレビジョン放送の放送波は全て MULTI2 で暗号化されており、受信器にて復号されている。MULTI2 は開発から既に 27 年が経過している。2009 年には 32 段中、16 段構成の MULTI2 は解読可能との研究成果が発表されている。

また 2012 年に 24 段の MULTI2 は線形攻撃により鍵復元が可能であると報告されている。これ以前については特筆すべき研究成果は発表されていない。一方、暗号解読の研究はここ 20 年で大きく進歩し、差分攻撃のみならず、線形攻撃、高階差分攻撃、不能差分攻撃、中間一致攻撃、補間攻撃などの多くの解読手法が開発されている。最近では有料衛星放送の暗号を解読したカード(B-CAS)のコピー品が世の中に不正に出回っており、問題となっている。

そこで本研究ではこれら様々な暗号方式の差分特性、高階差分特性、不能差分特性、線形特性、中間一致特性、補間特性を計算機探索や理論解析により徹底的に調査し、解読の糸口となる特性の有無を調べる。調べる際には我々が証明した特殊な飽和特性の有無も同時に調べ、解読の手掛かりとする。次に解読に一番有利な特性を用いて暗号方式の解読を試みる。解読を試みる際には、我々が開発した制御用変換、観測用変換技術、あるいは mod2 頻度分布、頻度分布の直接操作、S-box 特性定数、線形化法、特性拡張などの解読の効率化に結びつく様々な技術を併用し、従来よりも少ないデータ量または計算量、計算時間、メモリー量で暗号方式が解読できることを明らかにする。または従来は解読不可能であった段数の多い暗号方式が解読できることを明らかにする。その結果として、世の中の多くの暗号研究者によって客観的に危険と判断された暗号方式は自然と淘汰されてゆくこととなり、情報化社会の安全に資することができる。

安全性の評価は差分特性、高階差分特性、不能差分特性、線形特性、飽和特性を用いる攻撃に対する耐性評価といった既知の項目のみならず、未知の要素についてもその存在を含めて多角的に検討する。未知の要素の検討は独創性が要求され非常に困難な課題である。具体的には従来、世の中では計算機能力の制限から 1 ビット単位の精密な解析は困難であり、8 ビット単位や 32 ビット単位の大雑把な解析が主流であった。しかしながら計算機の進歩に伴い、最近は 1 ビット単位の精密な解析も可能となってきた。そこで本研究では 1 ビット単位の平文と暗号文の関連を精密に分析し、今までに知られていない差分特性、高階差分特性、不能差分特性、線形特性、飽和特性を計算機探索や理論解析により導出するという特色・独創性がある。これらの導出には多くの時間を要し、困難な課題であるが、その課題が達成された際には安全性の評価項目に新たな項目が加わることになり、結果として安全性評価の信頼性が高まることとなる。それと同時に本研究課題で取り上げていないその他様々な暗号方式に対しても、我々が開発する解析手法が適用できる可能性も広がり、暗号解読技術の発展にも寄与できるという結果が予想される。このように本研究手法及びそれによりもたらされる成果は独創性や革新性が認められると確信する。また本研究は高度情報化社会における安全に貢献するという意義をもち、安全性評価の研究分野の進展に対する大きな貢献や学術的波及効果が十分に期待でき、科学技術・産業など社会に与えるインパクト・貢献も期待できる。

３．研究の方法

暗号方式のうち、ブロック暗号 MULTI2、ストリーム暗号 Enocoro、ブロック暗号 HyRAL、ストリーム暗号 MUGI、ブロック暗号 CLEFIA 、MISTY、ストリーム暗号 SNOW3G、Trivium 等のブロック暗号、ストリーム暗号についてその安全性を評価する。さらにこれらの暗号方式の要素部品である線形関数及び非線形関数や換字表の安全性を評価する。具体的には差分攻撃、線形攻撃や代数攻撃に対する耐性を評価するために、1 ビット単位の平文と暗号文の関連を精密に分析し、差分特性、高階差分特性、不能差分特性、線形特性を計算機探索や理論解析により徹底的に調査し、解読の糸口となる特性を洗い出す。調査の際には我々が存在を証明した特殊な飽和特性の有無も同時に調べ、解読の手掛かりとする。次に解読に一番有利

な特性を用いて暗号方式の解読を試みる。解読を試みる際には、制御用変換、観測用変換、mod2頻度分布、頻度分布の直接操作、S-box特性定数、線形化法などの解読の効率化に結びつく様々な技術を併用し、従来よりも少ないデータ量または計算量で暗号方式が解読できることを明らかにする。または従来は解読不可能であった段数の多い暗号方式が解読できることを明らかにする。作業内容は文献調査、安全性評価項目の適用方法の検討、理論解析、計算機シミュレーションプログラム作成、解析プログラム作成、計算機探索、評価結果の取りまとめである。

４．研究成果

Midori64はBanikらが2015年に提案した秘密鍵長128ビットのSPN型64ビットブロック暗号アルゴリズムである．高階差分攻撃はLaiが提案した暗号攻撃手法である．暗号化関数のブール多項式の代数次数に着目した攻撃法であり,共通鍵暗号アルゴリズム全般に広く適用 できる攻撃法である．本研究では，高階差分攻撃で利用できる複数種類の特異な3 階差分特性を計算機解析により発見し､その特性の 存在をブール多項式の理論解析により明らかにした．また，共通鍵ブロック暗号 MISTY1 に対する先行研究として積分特性の探索を効率的に行う手法であるDivision属性が新たに提案され，世界で初めてフルラウンドのMISTY1が全数探索法よりも効率的に解読可能である事が示されている背景がある．本研究では，この手法 をブロック暗号KASUMIに適用して積分特性探索を行い，5段特性を新たに発見した．また，この5段特性と確率2^ {-18}で発生する弱 鍵条件を組み合わせる事で，7段の KASUMIが2^ {63}個の選択平文と2^ {63.3}回の暗号化計算量で攻撃可能である事を明らかにし た．次に，Piccoloは2011 年に提案された 64 ビットブロック暗号である．これまでに 8 ビット単位での飽和特性の調査によって，Piccolo には 5 ラウンド後の出力 16 ビットの高階差分値が 0 となる 16 階差分特性が示されている．本研究では，Piccolo の新しい高 階差分特性について明らかにした．具体的には計算機探索により,Piccolo の 5 ラウンド後の出力 8 ビットの高階差分値が 0 となる新しい 13 階差分特性を発見した．また，その特性が実在することをブール多項式の次数を解析することにより証明した．

更にブロック暗号Fewを解析した．FeWは2014年にKumarらによって提案された64ビットブロック暗号であり，鍵長は80ビット及び128ビットをサポートしている．これまでに，FeWには9ラウンドの高階差分特性が存在し，この特性を利用することによって，鍵長が80ビットのとき，12ラウンドのFeWに対して高階差分攻撃が可能であることが報告されている．なお，9ラウンドの高階差分特性の成立理由については示されていない．本研究では，FeWの新しい高階差分特性を発見した．具体的には,3ラウンド拡張が可能な新しい6ラウンドの21階差分特性を発見した．また，鍵スケジュール部を解析した13ラウンドのFeWに対する高階差分攻撃が可能であることを示した．更にブロック暗号QTL-64を解析した．QTL-64は2016年にLang Liらによって提案されたFeistel構造を持つブロック暗号である。QTL-64の仕様はブロック長64bit、段数16段、鍵長は64bitである。QTL-64の提案論文では線形解析､差分解析､代数攻撃に対する安全性評価は行われているが、不能差分攻撃に対しては評価が行われていない。不能差分攻撃とは、差分確率が0となる特定の入出力差分を用いて解読を行う方法である。出現確率が0である入出力差分(つまり、実際には出現し得ない入出力差分)と一致したときの鍵を偽鍵とし、偽鍵を捨て、鍵推定を行う。本研究ではQTL-64に対しS-boxの差分特性から4.5段の不能差分特性を発見し、このパスを用いて6.5段の鍵回復攻撃を行えることを新たに発見した。

５．主な発表論文等

〔雑誌論文〕（計１８件）

1. 近藤龍一，五十嵐保隆，金子敏信、ランダムパルス発生器 Atomic Pulse Generator の確率密度モデルと適合度検定、平成 30 年　電気関係学会関西連合大会、G10-10 号、317 - 318 頁、2018 年 12 月、査読無

2. 金子泰志、五十嵐保隆、金子敏信、超軽量ブロック暗号 QTL-64 の不能差分攻撃耐性評価、2019 年　暗号と情報セキュリティシンポジウム　予稿集、2B2-3 号、1 - 8 頁、2019 年 1 月、査読無

3. 芝山直喜、五十嵐保隆、金子敏信、鍵スケジュール部を解析したブロック暗号 FeW-80 に対する高階差分攻撃、2019 年　暗号と情報セキュリティシンポジウム 予稿集、2B2-2 号、1 - 8 頁、2019 年 1 月、査読無

4. Naoki Shibayama, Yasutaka Igarashi, Toshinobu Kaneko、A New Higher Order Differential of FeW、2018 Sixth International Symposium on Computing and Networking Workshops、466 - 471 頁、2018 年 11 月、査読有

5. Nobuyuki SUGIO, Yasutaka IGARASHI, Toshinobu KANEKO、Integral Cryptanalysis of Reduced-round KASUMI、Proceedings of 2018 International Symposium on Information Theory and Its Applications、447 - 451 頁、2018 年 10 月、査読有

6. 工藤昌士、五十嵐保隆、金子敏信、MILP によるブロック暗号 HIGHT の差分マルチパスの解析、2018 年 暗号と情報セキュリティシンポジウム予稿集、2C1-4 号、2018 年 1 月、査読無

7. 林浩成、五十嵐保隆、金子敏信、6.5 段の"超軽量"ブロック暗号 QTL-128 に対する零相関線形攻撃、2018 年 暗号と情報セキュリティシンポジウム予稿集、2C1-3 号、2018 年 1 月、査読無

8. 藤山雄輔、五十嵐保隆、金子敏信、ブロック暗号 SHipher の選択平文解読と既知平文解読、コンピュータセキュリティシンポジウム 2017 論文集、2E4-2 号、2017 年 10 月、査読無

9. Tadashi Sasaki, Yasutaka Igarashi, and Toshinobu Kaneko、MILP-Aided Bit-Based Division Property for M6 and M8、Advanced Science Letters、24 巻、3 号、1571 - 1574 頁、2018 年 3 月、査読有

10. 中澤 俊、五十嵐 保隆、金子 敏信、軽量型ブロック暗号 Halka の差分パス解析、コンピュータセキュリティシンポジウム 2017 論文集、2E4-1 号、2017 年 10 月、査読無

11. 芝山直喜・五十嵐保隆・金子敏信、ブロック暗号 Few の高階差分特性、信学技報、117 巻、39 号、37 - 42 頁、2017 年 5 月、査読無

12. Yusuke Takahashi; Yasutaka Igarashi; Toshinobu Kaneko、The 12th-Order Differential Attack on the 10-Round Variants of Midori64 Block Cipher、Proc. of 2017 IEEE 31st International Conference on Advanced Information Networking and Applications、925 - 930 頁、2017 年 3 月、査読有

13. 高橋勇介、五十嵐保隆、金子敏信、ブロック暗号 Midori64 の特異な 3 階差分特性(II)、コンピュータセキュリティシンポジウム 2016、3C4-2 号、2016 年 10 月、査読無

14. Yusuke Takahashi; Yasutaka Igarashi; Toshinobu Kaneko、The peculiar third-order differential characteristics of Midori64 block cipher(II)、2017 International Conference on Recent Advances in Signal Processing, Telecommunications & Computing、199 - 204 頁、2017 年 1 月、査読有

15. Nobuyuki SUGIO, Yasutaka IGARASHI, and Toshinobu KANEKO、Integral Characteristics of MISTY2 Derived by Division Property、2016 International Symposium on Information Theory and Its Applications、151 - 155 頁、2016 年 10 月、査読有

16. 芝山直喜、五十嵐保隆、金子敏信、ブロック暗号 Piccolo の高階差分特性、2017 年 暗号と情報セキュリティシンポジウム予稿集、2B2-1 号、2017 年 1 月、査読無

17. 杉尾信行, 五十嵐保隆, 金子敏信、共通鍵ブロック暗号アルゴリズム KASUMI の積分攻撃、2017 年 暗号と情報セキュリティシンポジウム予稿集、2B1-4 号、2017 年 1 月、査読無

18. Nobuyuki Sugio, Yasutaka Igarashi, Toshinobu Kaneko, Kenichi Higuchi、New Integral Characteristics of KASUMI Derived by Division Property、Lecture Notes in Computer Science、10144 巻、267 - 279 頁、2016 年 8 月、査読有

〔学会発表〕（計２２件）

1. 伊藤亮・五十嵐保隆、軽量ブロック暗号 GIFT に対する高階差分特性調査、電子情報通信学会東京支部学生会研究発表会、東京都港区、2019 年　3 月　2 日

2. 近藤龍一，五十嵐保隆，金子敏信、ランダムパルス発生器 Atomic Pulse Generator の確率密度モデルと適合度検定、平成 30 年　電気関係学会関西連合大会、大阪府大阪市、2018 年 12 月

3. 金子泰志、五十嵐保隆、金子敏信、超軽量ブロック暗号 QTL-64 の不能差分攻撃耐性評価、2019 年　暗号と情報セキュリティシンポジウム、滋賀県大津市、2019 年 1 月

4. 芝山直喜、五十嵐保隆、金子敏信、鍵スケジュール部を解析したブロック暗号 FeW-80 に対する高階差分攻撃、2019 年　暗号と情報セキュリティシンポジウム、滋賀県大津市、2019 年 1 月

5. Naoki Shibayama, Yasutaka Igarashi, Toshinobu Kaneko、A New Higher Order Differential of FeW、2018 Sixth International Symposium on Computing and Networking Workshops、Takayama, Japan、2018 年 11 月

6. Nobuyuki SUGIO, Yasutaka IGARASHI, Toshinobu KANEKO、Integral Cryptanalysis of Reduced-round KASUMI、Proceedings of 2018 International Symposium on Information Theory and Its Applications、Singapore、2018 年 10 月

7. 工藤昌士、五十嵐保隆、金子敏信、MILP によるブロック暗号 HIGHT の差分マルチパスの解析、

2018 年 暗号と情報セキュリティシンポジウム、新潟市、2018 年 1 月
8. 林浩成、五十嵐保隆、金子敏信、6.5 段の"超軽量"ブロック暗号 QTL-128 に対する零相関線形攻撃、2018 年 暗号と情報セキュリティシンポジウム、新潟市、2018 年 1 月
9. 芝山直喜、五十嵐保隆、金子敏信、ブロック暗号 Few の新しい高階差分特性、2018 年 暗号と情報セキュリティシンポジウム、新潟市、2018 年 1 月
10. 藤山雄輔、五十嵐保隆、金子敏信、ブロック暗号 SHipher の選択平文解読と既知平文解読、コンピュータセキュリティシンポジウム 2017、山形市、2017 年 10 月
11. 中澤 俊、五十嵐 保隆、金子 敏信、軽量型ブロック暗号 Halka の差分パス解析、コンピュータセキュリティシンポジウム 2017、山形市、2017 年 10 月
12. 芝山直喜・五十嵐保隆・金子敏信、ブロック暗号 Few の高階差分特性、電子情報通信学会・情報理論研究会、山形県米沢市、2017 年 5 月
13. 高橋勇介・五十嵐保隆・金子敏信、ブロック暗号 Midori64 の特異な 3 階差分特性、2016 年電子情報通信ソサイエティ大会、北海道 札幌市、2016 年 9 月
14. 佐々木理・高橋勇介・五十嵐保隆・金子敏信、ブロック暗号 QARMA64 の飽和特性、2016 年電子情報通信ソサイエティ大会、北海道 札幌市、2016 年 9 月
15. Yusuke Takahashi, Yasutaka Igarashi and Toshinobu Kaneko、The particular third-order differential characteristics of Midori64 block cipher、2016 International Symposium on Information Theory and Its Applications、Monterey, California, USA、2016 年 10 月
16. Yusuke Takahashi; Yasutaka Igarashi; Toshinobu Kaneko、The 12th-Order Differential Attack on the 10-Round Variants of Midori64 Block Cipher、2017 IEEE 31st International Conference on Advanced Information Networking and Applications、台湾 台北、2017 年 3 月
17. 高橋勇介、五十嵐保隆、金子敏信、ブロック暗号 Midori64 の特異な 3 階差分特性(II)、コンピュータセキュリティシンポジウム 2016、秋田県 秋田市、2016 年 10 月
18. Yusuke Takahashi; Yasutaka Igarashi; Toshinobu Kaneko、The peculiar third-order differential characteristics of Midori64 block cipher(II)、2017 International Conference on Recent Advances in Signal Processing, Telecommunications & Computing、ベトナム ダナン、2017 年 1 月
19．芝山直喜、五十嵐保隆、金子敏信、ブロック暗号 Piccolo の高階差分特性、2017 年 暗号と情報セキュリティシンポジウム、沖縄県 那覇市、2017 年 1 月
20．杉尾信行，五十嵐保隆，金子敏信､共通鍵ブロック暗号アルゴリズム KASUMI の積分攻撃、2017 年 暗号と情報セキュリティシンポジウム、沖縄県 那覇市、2017 年 1 月
21．Nobuyuki Sugio, Yasutaka Igarashi, Toshinobu Kaneko, Kenichi Higuchi、New Integral Characteristics of KASUMI Derived by Division Property、International Workshop on Information Security Applications、Jeju Island, South Korea、2016 年 8 月
22．Nobuyuki SUGIO, Yasutaka IGARASHI, and Toshinobu KANEKO、Integral Characteristics of MISTY2 Derived by Division Property、2016 International Symposium on Information Theory and Its Applications、Monterey, California, USA、2016 年 10 月

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計０件）
○取得状況（計０件）

〔その他〕
ホームページ等
五十嵐 保隆 ┆ 論文･著書･学会発表･特許 ┆ 東京理科大学
https://www.tus.ac.jp/fac_grad/p/achievement.php?4d2c

６．研究組織
(1)研究分担者
なし

(2)研究協力者
研究協力者氏名：金子敏信
ローマ字氏名：Toshinobu Kaneko