Integral Cryptanalysis against Symmetric-Key Cryptosystems

Todo, Yosuke

(Degree)
博士（工学）

(Date of Degree)
2017-03-25

(Date of Publication)
2019-03-25

(Resource Type)
doctoral thesis

(Report Number)
甲第6925号

(URL)
https://hdl.handle.net/20.500.14094/D1006925

(別紙様式3)

論文内容の要旨

氏　名　藤堂　洋介

専　攻　電気電子工学専攻

論文題目（外国語の場合は，その和訳を併記すること。）

Integral Cryptanalysis against Symmetric-Key Cryptosystems

共通鍵暗号に対するインテグラル攻撃

指導教員　森井　昌克

（注）2，000字～4，000字でまとめること。

情報システムやコンピュータネットワークが社会の重要なインフラとなり，個人情報を始め多くの秘匿すべき情報を管理・活用しなければならない時代が到来している．これらの情報を安全に利活用するためにセキュリティは必須であり，中でも暗号はセキュリティを支える最も重要な基盤技術として，公共・商業サービスは言うまでもなく個人によるネットショッピングなどでも広く利用されている．これらの多くのサービスのセキュリティ維持，より強固な暗号の設計，セキュリティリスクを低減できる新たな暗号利活用の模索などを題材とした研究分野として暗号理論がある．

暗号理論は学問の世界では比較的若い研究分野である．これは第二次世界大戦以前，暗号は防衛的観点より各国の最重要機密として管理されていたためである．現代の暗号学者は第二次世界大戦以前の暗号を現代暗号と区別して古典暗号と呼ぶ．現代暗号と古典暗号の決定的な違いは暗号化および復号の計算法(暗号アルゴリズム)を公開しても良いか否かである．古典暗号は暗号アルゴリズムを隠すことで安全性を確保しており，暗号アルゴリズムが仮に情報漏えいすると，それは暗号としての機能を果たせなくなる．したがって，この方式は暗号アルゴリズムそのものを厳格に管理する必要があり，インターネット上のサービスを始めとした現代のサービスでは利用不可能な方式である．現代暗号は暗号アルゴリズムに入力される鍵のみを秘匿し暗号アルゴリズムそのものは公開される．この方式では利用者は鍵のみを管理する．暗号アルゴリズムが公開可能になったことにより，その暗号の安全性を学問の場で広く議論可能になり，現在の暗号理論という研究分野が発展した．

暗号には大きく分けて公開鍵暗号と共通鍵暗号がある．公開鍵暗号は公開鍵を用いて暗号化し，秘密鍵を用いて復号する．これにより事前の鍵共有無しに暗号化・復号が可能となるが，一方で低速なため大量の情報の処理には不向きである．共通鍵暗号は暗号化と復号に共通の鍵を利用する方式である．そのため事前の鍵共有は必要となるが，高速なため大量の情報の処理に有効である．

暗号解析は暗号理論の中でも最も重要な研究分野の一つである．多くの暗号学者が暗号解析を試み，その安全性を示すことで初めて，その暗号は広く利用可能なものとして認められる．また，暗号解析によって得られた新たな知見は，新たな暗号の設計にも寄与する．そのため，暗号研究は暗号設計と暗号解析を繰り返すことで発展・進歩してきた．本研究では共通鍵暗号に対する最も強力な暗号解読法の一つとして知られるIntegral攻撃に注目し，この解読技術を大幅に発展させる様々な新技術を考案した．

1．Integral 攻撃のための改良技術の提案

● Integral 攻撃の発想を応用した Feistel 構造に対する汎用解析

Integral 攻撃は広義には特定の平分集合に対応する暗号文集合を解析して秘密鍵を解読する攻撃法である．通常，Integral 攻撃は暗号文集合に属する全ての暗号文の和の振舞いを利用するのに対し，この研究では暗号文集合の要素の和以外の特徴に注目する．応用として，共通鍵暗号を設計する際に頻用される Feistel 構造に対する汎用解析を改良する．この研究では汎用構造に対して自然な仮定を加えることで，初めて 6 段 Feistel 構造に対する汎用解析手法を示す．

● 高速フーリエ変換の計算技術を応用した Integral 攻撃の高速化

Integral 攻撃は通常『Integral 特性探索』と『鍵回復』の２段階で構成される．初めに攻撃者は Integral 特性を発見し，その後，Integral 特性の非理想的振舞を利用して秘密鍵を解読する．この研究では，高速フーリエ変換(FFT)の計算技術を応用することで Integral 攻撃の鍵回復に要する計算量を削減する．通常，鍵回復には非常に複雑な手順を要するが，FFT の計算手法を用いることで非常に単純に鍵回復に要する計算量を見積もることが可能になる．また，FFT 鍵回復を実在する暗号に対する Integral 攻撃へ応用することで認証暗号 Prøst・ブロック暗号 AES・PRESENT・CLEFIA に対する Integral 攻撃の鍵回復手順を改良できることを示す．

2．Integral 特性を探索する新汎用解析手法 Division Property

Integral 攻撃において最も重要な要素は，如何にして強力な Integral 特性を得るかにある．Integral 特性を探索する２つの著名な手法が知られており，一つは『Integral Property の伝搬』，もう１つは『代数次数の上界見積り』である．前者は 2002 年に提案され，Integral 特性を探索するツールとして最も利用されている．後者は 1994 年に導入された高階差分攻撃に端を発する．両者が発見する非理想的振舞は共に Integral 特性であるにも関わらず，それぞれ異なる数学的特徴を利用する．この研究では，両者の長所を融合させ，Integral 特性を探索する新しいツール『Division Property』を提案する．このツールを用いることで従来手法よりも正確な Integral 特性を効率的に発見可能になる．

ツールの優位性を示すため，非線形関数の代数次数を指定した Feistel 構造，SPN 構造，および AES 型暗号に対する汎用解析を試みる．汎用解析とは基本構造そのものが有する脆弱性を評価する解析であり，その知見は次世代共通鍵暗号設計時に役立つ．結果として，全ての構造に対して汎用解析を改良できることを示す．

● MISTY1 への適用

MISTY1 は CRYPTREC(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)の電子政府推奨候補暗号であり，また ISO/IEC でも標準化されている．MISTY1 の最大の特徴は共通鍵暗号の 2 大解読法として知られる差分解読法と線形解読法に対して安全性証明を持っていることである．ここでは，Division Property を用いて MISTY1 の Integral 特性を探索する．このとき MISTY1 の構成関数の一つである S-box の性質に注目することで Division Property の伝搬の最適化が可能なことを示すとともに，MISTY1 の S-box が最適に選択されていなかったことを示す．この MISTY1 の S-box の性質を利用することで MISTY1 が 128 ビット安全を有していないことを世界で初めて示す．

● Lilliput への適用

将来の IoT 社会を見据え，軽量デバイスで最適化された軽量暗号の研究が盛んに行われている．一般化 Feistel 構造は軽量暗号に適した暗号構造として注目されているが，撹拌性能が小さいという弱点を持つ．この弱点を補う構造として拡張一般化 Feistel 構造が提案されており，Lilliput はこの構造を採用した軽量ブロック暗号である．拡張一般化 Feistel 構造では従来の一般化 Feistel 構造よりも多くの線形変換を暗号内部に有しており，これが安全性向上に寄与すると期待されている．事実，設計者の自己解析では Integral 攻撃に対する安全性が大幅に向上することが報告されている．しかしながら，Division Property の観点から解析した結果，線形変換による Integral 攻撃に対する安全性向上の寄与は設計者が期待しているものより遥かに小さいことを示す．結果，Lilliput に対する最良解析手法を示す．

● **Bit-Based Division Property と Simon への適用**

Division Property は S-box と呼ばれる非線形演算に基づく共通鍵暗号に対して強力な解析ツールである．一方で S-box に基づかない暗号に対しては Division Property は大きな効果を期待できない．この研究では Division Property を拡張した『Bit-Based Division Property』を提案する．

Bit-Based Division Property の効果を示すために， NSA が提案した軽量ブロック暗号 Simon32 へ適用する．Simon32 に関しては以前から 15 段 Integral 特性が実験的に導出されていたが，その特性が全ての秘密鍵に対して成立するか否かの証明は未解決問題だった．初めに Bit-Based Division Property を用いて 14 段 Integral 特性を理論的に証明する．その後，更なる拡張である『Bit-Based Division Property using Three Subsets』を用いて 15 段 Integral 特性を理論的に証明する．

● **PRESENT への適用**

PRESENT は ISO/IEC で標準化されている軽量暗号の一つである．PRESENT は S-box を用いた暗号ではあるが，各 S-box の出力を bit 志向に組み替えるため，Division Property の直接的な適用は効果を期待できない．そこで S-box に対して Bit-Based Division Property を適用して解析する．このとき，Bit-Based Division Property の評価に膨大な計算量が必要となるが，新たに導入する『Compact Representation for Division Property』を用いることで計算量を大幅に削減可能なことを示す．結果，PRESENT に対する新しい Integral 特性を示し，従来の Integral 攻撃を 2 段改良できることを示す．

* 作成上の注意

1. A4 版とし，横書きすること。
2. 右上に氏名及びページ数を記入すること。
3. “要旨”及びその草稿を作成する時には，以上の注意事項を記載する必要はない。

(別紙１)　　論文審査の結果の要旨

氏名	藤堂　洋介		
論文題目	Integral Cryptanalysis against Symmetric-Key Cryptosystems (共通鍵暗号に対するインテグラル攻撃)		
審査委員	区　分	職　名	氏　　名
	主　査	教授	森井　昌克
	副　査	教授	竹野　裕正
	副　査	教授	太田　能
	副　査	准教授	白石　善明
	副　査		印

要　　旨

概要

暗号解析は暗号理論の中でも最も重要な研究分野の一つである．多くの暗号学者が暗号解析を試み，その安全性を示すことで初めて，その暗号は広く利用可能なものとして認められる．また，暗号解析によって得られた新たな知見は，新たな暗号の設計にも寄与する．そのため，暗号研究は暗号設計と暗号解析を繰り返すことで発展・進歩してきた．本論文では共通鍵暗号暗号に対する最も強力な暗号解読法の一つとして知られる Integral 攻撃に注目し，この解読技術を大幅に発展させる様々な新技術を考案した．

第一章は緒論である．

第二章は準備として共通鍵暗号と Integral 攻撃に関して解説している．

第一部では Integral 攻撃の鍵回復部分に注目した新しい解析手法および改良手法を提案している．

第三章では Integral 攻撃の発想を応用した Feistel 構造に対する汎用解析を示している．Integral 攻撃は広義には特定の平文集合に対応する暗号文集合を解析して秘密鍵を解読する攻撃法である．通常，Integral 攻撃は暗号文集合に属する全ての暗号文の和の振舞いを利用するのに対し，この研究では暗号文集合の要素の和以外の特徴に注目する．応用として，共通鍵暗号を設計する際に頻用される Feistel 構造に対する汎用解析を改良する．この研究では汎用構造に対して自然な仮定を加えることで，初めて 6 段 Feistel 構造に対する汎用解析手法を与えている．

第四章では高速フーリエ変換の計算技術を応用した Integral 攻撃の高速化を示している．Integral 攻撃は通常『Integral 特性探索』と『鍵回復』の 2 段階で構成される．初めに攻撃者は Integral 特性を発見し，その後，Integral 特性の非理想的振舞を利用して秘密鍵を解読する．この研究では，高速フーリエ変換 (FFT)の計算技術を応用することで Integral 攻撃の鍵回復に要する計算量を削減する．通常，鍵回復には非常に複雑な手順を要するが，FFT の計算手法を用いることで非常に単純に鍵回復に要する計算量を見積もることが可能になる．また，FFT 鍵回復を実在する暗号に対する Integral 攻撃へ応用することで認証暗号 Prøst・ブロック暗号 AES・PRESENT・CLEFIA に対する Integral 攻撃の鍵回復手順を改良できることを示している．

第五章では初めに Division Property を提案している．Integral 攻撃において最も重要な要素は，如何にして強力な Integral 特性を得るかにある．従来，Integral 特性を探索する手法として 2 つの著名な手法が知られており，一つは『Integral Property の伝搬』，もう 1 つは『代数次数の上界見積り』である．前者は Knudsen と Wagner によって 2002 年に提案され，Integral 特性を探索するツールとして最も利用されてきた．後者は 1994 年に Lai および Knudsen によって導入された高階差分攻撃に端を発する．両者が発見する非理想的振舞は共に Integral 特性であるにも関わらず，それぞれ異なる原理により Integral 特性を発見してきた．ここでは，両者の長所を融合させ，Integral 特性を探索する新しいツール『Division Property』を提案している．Division Property は従来の 2 つの手法よりも正確な Integral 特性を効率的に発見することができる．Division Property の効果を示すために共通鍵暗号を設計する際に頻用される二大構造である Feistel 構造と SPN 構造に対する汎用解析へ，また NIST が標準化している AES およびその類似型暗号への応用を示している．結果として全ての応用先において新しい Integral 特性を発見している．

氏名	藤堂　洋介

第六章では Division Property を用いた解析を MISTY1 へ適用している．MISTY1 は CRYPTREC(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)の電子政府推奨候補暗号であり，また ISO/IEC でも標準化されている．MISTY1 の最大の特徴は共通鍵暗号の 2 大解読法として知られる差分解読法と線形解読法に対して安全性証明を持っていることである．ここでは，Division Property を用いて MISTY1 の Integral 特性を探索する．このとき MISTY1 の構成関数の一つである S-box の性質に注目することで Division Property の伝搬の最適化が可能なことを示すとともに，MISTY1 の S-box が最適に選択されていなかったことを示している．この MISTY1 の S-box の性質を利用することで MISTY1 が 128 ビット安全を有していないことを世界で初めて明らかにしている．

第七章では Division Property を用いた解析を Lilliput への適用している．将来の IoT 社会を見据え，軽量デバイスで最適化された軽量暗号の研究が盛んに行われている．軽量暗号に適した共通鍵暗号のための基本構造として一般化 Feistel 構造がある．一方で，一般化 Feistel 構造はデータの撹拌性能が低い弱点を持つ．この弱点を補うためにブロックシャッフル型一般化 Feistel 構造や拡張型一般化 Feistel 構造が提案されている．Lilliput は拡張一般化 Feistel 構造を採用した軽量ブロック暗号である．拡張一般化 Feistel 構造では従来の一般化 Feistel 構造よりも多くの線形変換を暗号内部に有しており，この線形変換は暗号解析手法に対する安全性向上に寄与すると期待される．事実，設計者の自己解析では Integral 攻撃に対する安全性が大幅に向上することが報告されている．しかしながら，Division Property の観点から解析した結果，線形変換による Integral 攻撃に対する安全性向上の寄与は設計者が期待しているものより遥かに小さいことを示している．結果，従来より大幅に改良された Integral 特性を発見し，この Integral 特性を用いることで Lilliput に対する最良解析手法を与えている．

第八章では Division Property をビット型に改良した Bit-Based Division Property を提案するとともに NSA 提案の軽量暗号 Simon へ適用している．Division Property は S-box と呼ばれる非線形演算に基づく共通鍵暗号に対して強力な解析ツールである．一方で S-box に基づかない暗号に対しては Division Property は大きな効果を期待できない．この研究では Division Property を拡張した『Bit-Based Division Property』を提案する．Bit-Based Division Property を用いることで，S-box に基づかない暗号に対しても強力な Integral 特性を発見可能になる．さらに，Bit-Based Division Property を拡張させた『Bit-Based Division Property using Three Subsets』では通常の Bit-Based Division Property では発見不可能な Integral 特性を新たに発見できる．

Simon は NSA が提案した軽量ブロック暗号であり，その内部に S-box を有さない．そのため自然に Division Property を適用すると効果的な Integral 特性を発見できない．したがって Bit-Based Division Property を用いて Integral 特性を探索する．このとき 複数バージョンある Simon の中で最も軽量な Simon32 に対して Bit-Based Division Property を適用する．Simon32 に関しては以前から 15 段 Integral 特性が実験的に導出されていたが，その特性が全ての秘密鍵に対して成立するか否かの証明は未解決問題だった．初めに Bit-Based Division Property が 14 段 Integral 特性をもつことを理論的に示すとともに，Bit-Based Division Property using Three Subsets を用いることで 15 段 Integral 特性が全ての秘密鍵で成立することを示している．

第九章では Bit-Based Division Property を用いた解析を軽量暗号 PRESENT へ応用している．PRESENT は ISO/IEC で標準化されているは軽量暗号の一つである．PRESENT は S-box を用いた暗号ではあるが，各 S-box の出力を bit 志向に組み替えるため，Division Property の直接的な適用は効果を期待できない．そこで S-box に対して Bit-Based Division Property を適用して解析する．このとき，Bit-Based Division Property の評価に膨大な計算量が必要となるが，新たに導入する Compact Representation for Division Property を用いることで計算量を大幅に削減可能なことを示している．結果，PRESENT に対する新しい Integral 特性を示し，従来の Integral 攻撃を 2 段改良できることを示している．

Division Property は Eurocrypt2015 で発表した技術である．既に多くの後続研究が第三者により行われている．第十章ではこれらの後続研究を整理している．

以上のように，本論文では情報セキュリティの基盤技術である共通鍵暗号に対する新しい安全性評価手法の提案を行っている．本論文では，ブロック暗号に対しての Integral 攻撃の改良が示されており，かつ既存の結果を十分上回る結果となっている．提出された論文は工学研究科学位論文評価基準を満たしており，学位申請者の藤堂洋介は，博士(工学)の学位を得る資格があると認める．