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　５ 年　 ６ 月 ２０ 日現在

機関番号：３０１０８
研究種目：研究活動スタート支援
研究期間：2021～2022
課題番号：２１Ｋ２１２９２

研究課題名（和文）共通鍵暗号ＫＡＳＵＭＩの安全性評価に関する研究

研究課題名（英文）Security evaluation of the symmetric-key block cipher KASUMI

研究代表者
杉尾　信行（Sugio, Nobuyuki）

北海道科学大学・工学部・准教授

研究者番号：４０９０７８４６

交付決定額（研究期間全体）：（直接経費）　　1,200,000円

研究成果の概要（和文）：　本研究は，移動体通信サービスの標準暗号ＫＡＳＵＭＩに対し，積分攻撃への安全性を明らかにする事を目的とする．
　本研究は，Ｓ－ｂｏｘのビット単位分割属性の伝搬特性を解析すると共に，混合整数線形計画法を用いて従来型ビット単位分割属性による積分特性探索を行う手法を新たに開発した．続いて，Ｓ７－ｂｏｘのＭＩＬＰモデルと前述の手法を組合せ，4.5段の積分特性が存在する事を明らかにした．また，得られた積分特性を用いて7段縮小版のＫＡＳＵＭＩが秘密鍵の総当たり攻撃よりも効率的に解読出来る事を示した．ＫＡＳＵＭＩの標準仕様は８段である為，ＫＡＳＵＭＩは積分攻撃に対して安全性を有す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
　暗号の安全性が低下すると，通話や通信内容の盗聴や改竄の脅威が現実的となり，日本国民が移動体通信サービスを安全に利用することが困難になる．
　本研究成果によって，7段縮小版のＫＡＳＵＭＩが秘密鍵の総当たり攻撃よりも効率的に解読可能であることを示した．ＫＡＳＵＭＩの標準仕様段数は８段である為，ＫＡＳＵＭＩは積分攻撃に対して安全性を有している事が明らかとなり，日本国民が移動体通信サービスを安心して使うことが可能である．また，移動体通信サービスは日本だけでなく，世界中で利用されている為，移動体通信サービスで使用される暗号アルゴリズムの安全性を評価した本研究成果は社会的に大変意義があるものである．

研究成果の概要（英文）：The purpose of this study is to clarify the security against integral attack on KASUMI used in the mobile communication networks. We analyzed the propagation characteristics of S-boxes by the bit-based division property. We also developed a new method to search integral properties by the conventional bit-based division property using mixed integer linear programming (MILP). We have discovered that 4.5-round integral characteristics by using S7-box’s MILP model combined with the aforementioned method. We showed that 7-round KASUMI is attackable faster than the brute-force search method. Because the recommended number of rounds is 8, we found that KASUMI is secure against integral attack.

研究分野：情報科学、情報工学およびその関連分野

キーワード：積分攻撃　ＫＡＳＵＭＩ　暗号解読　混合整数線形計画法

機関番号：３０１０８
研究種目：研究活動スタート支援
研究期間：令和３年度～ 令和４年度
課題番号：21K21292
研究課題名：共通鍵暗号ＫＡＳＵＭＩの安全性評価に関する研究
研究代表者：
杉尾　信行（SUGIO Nobuyuki）
北海道科学大学・工学部情報工学科・准教授
研究者番号：40907846
交付決定額（研究期間全体）：（直接経費）１，２００，０００円

研究成果の概要

現在，携帯端末を用いた移動体通信サービスは世界中に普及している．携帯端末と無線基地局間の無線通信は，第三者による盗聴や改竄を防ぐ目的で暗号技術が採用されている．本研究では，移動体通信網の世界標準暗号である共通鍵暗号ＫＡＳＵＭＩに対し，積分攻撃に対する安全性を明らかにする事を目的とする．

既存研究では，杉尾らが分割属性による積分特性探索を行っている．然しながら，既存研究では積分特性探索において，入出力サイズに合わせて７ビット又は９ビット単位での分割属性による解析しか実施しておらず，混合整数線形計画法（ＭＩＬＰ）を応用した１ビット単位での積分特性探索は行なわれていない．そこで本研究では，共通鍵暗号ＫＡＳＵＭＩに対し，ＭＩＬＰを応用した１ビット単位での詳細な積分特性探索を行い，得られた積分特性から積分攻撃に対する安全性を明らかにする．

２０２１年度の研究では，上記の既存研究を改良し，ＭＩＬＰを用いて従来型ビット単位分割属性による１ビット単位の積分特性探索を行う手法を開発した．続いて，ＫＡＳＵＭＩの最小構成要素であるＳ－ｂｏｘに限定し，１ビット単位分割属性の伝搬特性を解析した。解析の結果，１ビット単位分割属性はＳ－ｂｏｘの代数展開式を考慮した評価が可能であることを明らかにした．

２０２２年度の研究では，導出したＳ７－ｂｏｘのＭＩＬＰモデルと２０２１年度に開発した従来型ビット単位分割属性によるＳ９－ｂｏｘのＭＩＬＰモデルを組み合わせる手法を新たに開発した．その結果，4.5 段の積分特性が存在する事を明らかにした．また，得られた積分特性を用いて 7 段縮小版のＫＡＳＵＭＩが秘密鍵の総当たり攻撃よりも効率的に解読可能であることを示した．

研究成果の学術的意義や社会的意義

暗号の安全性が低下すると，通話や通信内容の盗聴や改竄の脅威が現実的となり，日本国民が移動体通信サービスを安全に利用することが困難になる．

本研究成果によって，7 段縮小版のＫＡＳＵＭＩが秘密鍵の総当たり攻撃よりも効率的に解読可能であることを示した．ＫＡＳＵＭＩの標準仕様段数は８段である為，ＫＡＳＵＭＩは積分攻撃に対して安全性を有している事が明らかとなり，日本国民が移動体通信サービスを安心して使うことが可能である．また，移動体通信サービスは日本だけでなく，世界中で利用されている為，移動体通信サービスで使用される暗号アルゴリズムの安全性を評価した本研究成果は社会的に大変意義があるものである．

Outline of Research Achievements

The purpose of this study is to clarify the security against integral attack on KASUMI used in the mobile communication networks. We analyzed the propagation characteristics of S-boxes by the bit-based division property. We also developed a new method to search integral properties by the conventional bit-based division property using mixed integer linear programming (MILP). We have discovered that 4.5-round integral characteristics by using S7-box's MILP model combined with the aforementioned method. We showed that 7-round KASUMI is attackable faster than the brute-force search method. Because the recommended number of rounds is 8, we found that KASUMI is secure against integral attack.

研究分野：

情報科学、情報工学およびその関連分野

キーワード：

積分攻撃，ＫＡＳＵＭＩ，暗号解読，混合整数線形計画法

１．研究開始当初の背景

現在，携帯端末を用いた移動体通信サービスは国内，及び海外で普及している．総務省が公表した「電気通信サービスの契約数及びシェアに関する四半期データの公表」（令和２年度第２四半期（９月末））によると，２０２０年９月時点の携帯電話契約数が１億８，９１７万であり，契約数の内訳はそれぞれ３Ｇ（第三世代）２，９３４万，ＬＴＥ（第四世代）１５，９１５万，５Ｇ（第五世代）７９万となっている．　共通鍵暗号ＫＡＳＵＭＩは３Ｇ（第三世代）移動体通信の世界標準暗号として２０００年に採用され，今日も世界中で利用されている代表的な暗号アルゴリズムである．ＫＡＳＵＭＩの内部構造を図１に示す．

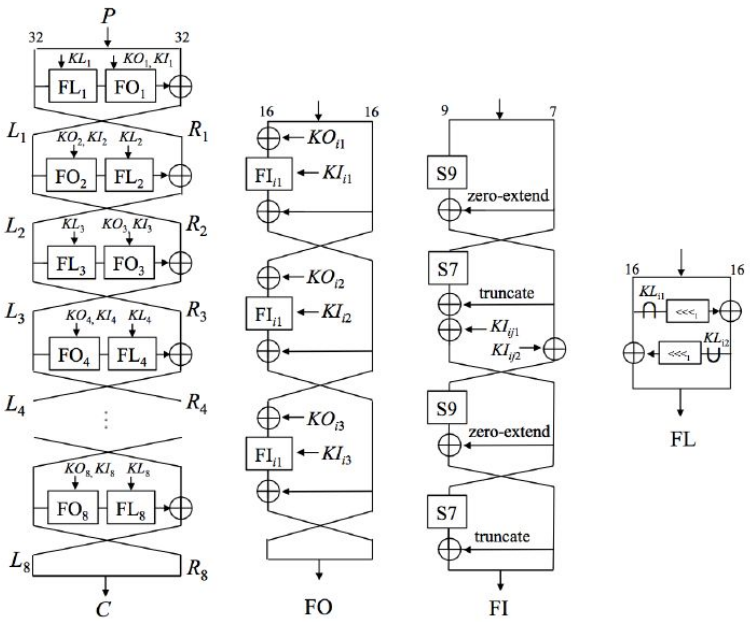

図１．KASUMI の構造

ＫＡＳＵＭＩは携帯電話と無線基地局間の無線通信におけるデータの秘匿と完全性保証に利用されており，ＫＡＳＵＭＩの安全性を明らかにする事は携帯電話サービスの通信の安全性を担保する上で大変重要である．

ＫＡＳＵＭＩの安全性評価に関する既存研究では，杉尾らが分割属性による積分特性探索を行い，得られた積分特性を用いて積分攻撃に対する安全性を評価している．**然しながら，既存研究ではＳ－ｂｏｘと呼ばれるＫＡＳＵＭＩを構成する最小単位の非線形関数の入出力サイズに合わせて７ビット又は９ビット単位での分割属性による解析しか実施しておらず，１ビット単位での探索結果は未だ解明されていない**．従って，**現状ではＫＡＳＵＭＩの積分攻撃に対する安全性評価が十分であるとは言い難く，更なる詳細評価が必要である**．

２．研究の目的

本研究の目的は，入出力サイズが６４ビットのＫＡＳＵＭＩに対し，混合整数線形計画法（M

ＩＬＰ）を応用した１ビット単位での分割属性による積分特性探索を行い，どの様な特性が存在するのか解明することである．

本研究の独自性は，図１に示す通り，多段の入れ子型構造を有する暗号アルゴリズムに対し，Ｓ－ｂｏｘの入出力サイズに合わせたブロック単位の積分特性探索と１ビット単位での積分特性探索結果を比較し，**ビット単位による探索の優位性の有無を明らかにする点**である．また，上記の優位性の有無に基づき，暗号設計の観点から１ビット単位の暗号処理を構成することで積分攻撃への安全性が向上するのか明らかにする点である．

３．研究の方法

本研究では，**ＫＡＳＵＭＩに対して混合整数線形計画法（ＭＩＬＰ）を応用した１ビット単位での分割属性による積分特性探索を行い，どの様な特性が存在するのか解明する**．また，明らかにした積分特性を用いて鍵回復に必要な平文・暗号文組数と計算量の見積りを行い，ＫＡＳＵＭＩがどの程度安全に利用可能であるか評価を行う．

４．研究成果

２０２１年度の研究では，以下２つの観点で研究を進めた．

1. **最小構成要素（Ｓ－ｂｏｘ）に対する１ビット単位分割属性の伝搬特性解析**

   ＫＡＳＵＭＩの最小構成要素であるＳ－ｂｏｘに対し，１ビット単位分割属性の伝搬特性を解析した．解析の結果，１ビット単位分割属性はＳ－ｂｏｘの代数展開式を考慮した評価が可能であることを明らかにした．

2. **混合整数線形計画法（ＭＩＬＰ）の適用に向けた既存研究の改良**

   Ｓ－ｂｏｘの入出力単位（７ビット，又は９ビット）で解析した既存研究を改良し，混合整数線形計画法（ＭＩＬＰ）を用いて従来型ビット単位分割属性による１ビット単位の積分特性探索を行う手法を開発した．その結果，4.5 段の積分特性が存在する事を明らかにし，その得られた積分特性を用いて 7 段縮小版のＫＡＳＵＭＩが解読可能であることを示した．

２０２２年度の研究では，以下２つの観点で研究を進めた．

1. **最小構成要素（Ｓ－ｂｏｘ）伝搬特性のＭＩＬＰモデル策定**

   混合整数線形計画法（ＭＩＬＰ）を用いて積分特性探索を行う為，伝搬特性に関するＭＩＬＰモデルを策定する必要がある．Ｓ７－ｂｏｘのＭＩＬＰモデルは作成する事が出来たが，Ｓ９－ｂｏｘのＭＩＬＰモデルは２０２１年に解析した伝搬特性結果から導出する事が出来なかった．原因は変数が多い事に起因した計算量の問題であった．

2. **混合整数線形計画法（ＭＩＬＰ）の適用**

   導出したＳ７－ｂｏｘのＭＩＬＰモデルと２０２１年度に開発した従来型ビット単位分割属性（Ｃｏｎｖｅｎｔｉｏｎａｌ－BDP）によるＳ９－ｂｏｘのＭＩＬＰモデルを組み合わせる手法を新たに開発し，前述の課題に対処した．その結果，4.5 段の積分特性が存

在する事を明らかにした.

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Nobuyuki SUGIO, Yasutaka IGARASHI, Sadayuki HONGO	４．巻 －
２．論文標題 Integral Cryptanalysis on Reduced-round KASUMI	５．発行年 2022年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics,Communications snd Computer Sciences(EA)	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） なし	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 －

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 杉尾 信行，本郷 節之，五十嵐 保隆
２．発表標題 ブロック暗号KASUMIに対するBit-Based Division Propertyの適用に向けた解析
３．学会等名 令和3年電気・情報関係学会　北海道支部連合大会
４．発表年 2021年

１．発表者名 杉尾 信行，五十嵐 保隆，本郷 節之
２．発表標題 ブロック暗号KASUMIに対するBit-based Division Propertyの適用に向けた解析(II)
３．学会等名 情報処理学会第84回全国大会
４．発表年 2022年

１．発表者名 杉尾 信行，五十嵐 保隆，本郷 節之
２．発表標題 ブロック暗号KASUMIに対するBit-based Division Propertyの適用に向けた解析(III)
３．学会等名 令和4年度 電気・情報関係学会　北海道支部連合大会
４．発表年 2022年

１．発表者名 杉尾 信行，五十嵐 保隆，本郷 節之
２．発表標題 ブロック暗号MISTY2に対するBit-Based Division Propertyを用いた積分特性探索
３．学会等名 令和4年度 電気・情報関係学会　北海道支部連合大会
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

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