氏名（本籍）	杉尾信行（神奈川県）
学位の種類	博士（工学）
学位記番号	甲第939号
学位授与の日付	平成29年3月18日
学位授与の要件	学位規則第4条第1項該当
学位論文題目	**共通鍵ブロック暗号に対する攻撃手法の高速化とKASUMIの安全性評価への適用**
論文審査委員	（主査）教授　樋口　健一
	教授　前田　譲治　　教授　松田　一朗
	教授　明石　重男　　教授　伊丹　　誠

論文内容の要旨

第二世代(GSM方式)，及び第三世代(W-CDMA方式)移動体通信システムは世界中で利用されており，国内においても主要ネットワークオペレータによる第三世代移動体通信サービスが提供されている．電気通信事業者協会公表値に拠れば，国内の3G比率は84%(平成26年3月時点)まで普及している．携帯電話・スマートフォンと無線基地局間の無線通信において，第三者による通信データ(利用者の音声データや制御信号等)の盗聴・改竄を防止する為，共通鍵ブロック暗号KASUMIを用いた秘匿・完全性保証が実現されている．共通鍵ブロック暗号の安全性は攻撃手法を用いて，どの程度耐性を有しているかで評価を行う．共通鍵ブロック暗号に対する代表的な攻撃手法に差分攻撃，線形攻撃が知られている．近年の暗号はこれらの攻撃手法に配慮した設計がなされており，差分攻撃と線形攻撃に対する証明可能安全性を有する暗号として共通鍵ブロック暗号MISTYが提案された．共通鍵ブロック暗号KASUMIはこの共通鍵ブロック暗号MISTYを改良して開発されている為，差分攻撃と線形攻撃に対する耐性を有している．そこで本論文では，差分攻撃と線形攻撃以外の攻撃手法として強力，且つ汎用的に利用可能な高階差分攻撃と積分攻撃を取り扱い，攻撃手法の高速化を行って共通鍵ブロック暗号KASUMIの安全性評価を行う．また，高階差分攻撃と積分攻撃の関係性を明らかにする事を目的とする．

第2章では，共通鍵ブロック暗号アルゴリズムの構造と安全性評価の方法について纏める．共通鍵ブロック暗号の代表的なデータ攪拌部の構造として，Feistel構造，SPN(Substitution Permutation Network)構造が存在する．本論文では，安全性評価の対

象である共通鍵暗号アルゴリズムKASUMIとMISTYの内部構造に関する説明を行う．また，共通鍵ブロック暗号に対する計算量的安全性評価方法について説明を行う．

第3章では，共通鍵ブロック暗号に対する強力，且つ，汎用的な攻撃手法である高階差分攻撃に対し，特性探索法と鍵回復の両面で高速化が可能な技術の提案と，KASUMIの安全性評価への適用を示す．具体的には，田中らが示した32階差分の4段特性に対し，効果的な選択平文の探索を行う事で，16階差分の4段特性が存在する事を示す．この手法を用いる事により，1組の4段特性を構築する為に必要な選択平文数を最大2^{-16}に削減可能である．また，鍵回復を行う際には，全数探索法よりも効率的な線形化手法を採用し，更に線形化手法の高速化を行う事で，5段のKASUMIの鍵回復に必要な計算量を$2^{85.5}$倍高速化する事が可能である事を示す．線形化手法の高速化技術は，(1)事前に方程式を解析し，鍵(未知項)の係数導出を高速化する技法と，(2)事前に解析した係数が暗号文の低次項で表される未知項に着目し，鍵(未知項)の係数を0に制御し，導出する鍵(未知項)の数を削減する技法の２つから成る．この２つの高速化技術は，KASUMI以外の共通鍵暗号にも適用可能な汎用性を有する技術である．

第4章では，高階差分攻撃と同様に，強力，且つ汎用的な積分攻撃を用いたKASUMIの安全性評価について纏める．先行研究として，藤堂は積分特性の探索を高速化する新たな手法としてDivision属性を新たに提案し，新たに発見したMISTY1の6段特性を用いてフルラウンドのMISTY1が全数探索法よりも効率的に解読可能である事を示した．本論文では，この積分特性探索の高速化手法を用いてKASUMIの積分特性探索を行い，新たな4段，及び5段の積分特性が存在する事を示す．また，今回発見した積分特性を用いて7段のKASUMIが2^{63}の選択平文数と$2^{63.3}$の計算量で攻撃可能である事を示す．この結果は，従来知られていた7段KASUMIの攻撃の中で最良な結果となっている(2016年9月時点において)．

第5章では，高階差分攻撃と積分攻撃の関係性を明らかにする．具体的には，m bit入力のd次関数に対し，Division属性から導出される最良の積分攻撃は，高階差分攻撃の(d+1)階差分と等しく，2^{d+1}の選択平文数を必要とする事を示す．また，その種類数が積分攻撃と高階差分攻撃で一致する事を示す．

第6章では，3章と4章で示したKASUMIの鍵回復攻撃に必要な計算量に対し，現在，及び今後の計算機能力の向上を見込んだ実行可能性に基づく利用可能期間の評価を行う．具体的には，今後の計算機能力の向上について，スーパーコンピューターのベンチマーク結果の 1 位から 500 位を 1993 年から半年毎に集計している Web サイト TOP500.Org と CRYPTREC が公表している報告書を参考に評価を行う．
5段のKASUMIを攻撃する為に必要な計算量は$2^{31.5}$回の暗号化計算量であり，この計算量は汎用的なPCの計算機程度で実行可能である．また，7段のKASUMIを攻撃する為に必要な計算量は$2^{63.3}$回の暗号化計算量であり，この計算量は現在の世界Top500位のスーパーコンピューターが有する計算能力で実行可能な計算量である．従って，実際のシス

テムにおいて，7段以下のKASUMIを用いる事は，秘密鍵に対する鍵回復攻撃の影響を受ける可能性が無視できないものである．また，暗号解読技術は日々進化している為，今後も新たな攻撃手法に対する耐性を評価してく事が重要である．

第7章では，3章から6章までの結果に基づき，本論文の結論を纏める．

論文審査の結果の要旨

第二世代（GSM方式）、及び第三世代（W-CDMA方式）移動体通信システムは現在世界中で広く利用されている。これらの移動体通信システムでは、無線通信において第三者による通信データの盗聴・改竄を防止する為、共通鍵ブロック暗号KASUMIにより秘匿・完全性保証を実現している。一般に、暗号の安全性は攻撃手法に対してどの程度耐性を有しているかに基づいて評価され、暗号の安全性評価は通信の秘匿・完全性を保証するために非常に重要な研究分野である。共通鍵ブロック暗号に対する代表的な攻撃手法に差分攻撃と線形攻撃がある。差分攻撃と線形攻撃に対する証明可能安全性を有する暗号として共通鍵ブロック暗号MISTYが提案された。共通鍵ブロック暗号KASUMIはこの共通鍵ブロック暗号MISTYを改良して開発されており、差分攻撃と線形攻撃に対する耐性を有している。

そこで本論文では、差分攻撃と線形攻撃以外の攻撃手法として強力、且つ汎用的に利用可能な高階差分攻撃と積分攻撃を取り扱い、攻撃手法の高速化法を提案したうえで、共通鍵ブロック暗号KASUMIの安全性評価を行っている。また、これまで不明であった高階差分攻撃と積分攻撃の関係性を明らかにすることも目的としている。

第1章での序論を踏まえ、第2章では、共通鍵ブロック暗号アルゴリズムの構造と安全性評価の方法について述べている。特に本論文が主に対象とする共通鍵暗号アルゴリズムKASUMIとMISTYの内部構造を中心に説明し、共通鍵ブロック暗号に対する代表的な攻撃手法と計算量的安全性評価方法について説明している。

第3章では、高階差分攻撃を対象として、特性探索法と鍵回復の両面で高速化が可能な技術を提案し、さらにこの高速化された攻撃法をKASUMIの安全性評価へ適用している。具体的には、田中らが示した32階差分の4段特性に対し、効果的な選択平文の探索を行うことにより、16階差分の4段特性が存在することを示し、特性探索法の高速化により1組の4段特性を構築する為に必要な選択平文数を最大 2^{-16} に削減可能であることを示している。また、鍵回復において、効率的な線形化手法をさらに高速化する方法を提案し、5段のKASUMIの鍵回復に必要な計算量を $2^{85.5}$ 倍だけ高速化できることを示している。線形化手法の高速化は、(1)事前に方程式を解析し、鍵（未知項）の係数導出を高速化する技法と、(2)事前に解析した係数が暗号文の低次項で表される未知項に着目し、鍵の係数を0に制御し、導出する鍵の数を削減する技法の2つから成っている。提案したこれら2つの高速化技術は、KASUMI以外の共通鍵暗号にも適用可能な汎用性を有する。

第4章では、積分攻撃に着目したKASUMIの安全性評価について述べている。藤堂は積分特性の探索を高速化する手法としてDivision属性を提案し、新たに発見したMISTY1の6段特性を用いてフルラウンドのMISTY1が全数探索法よりも効率的に解読可能であることを示した。本論文では、この積分特性探索の高速化手法を用いてKASUMIの積分特性探索を行い、新たな4段、及び5段の積分特性が存在することを明らかにし、7段のKASUMIが 2^{63} の選択平文数

と $2^{63.3}$ の計算量で攻撃可能であることを示している。この結果は現時点で最良の結果となっている。

第5章では、高階差分攻撃と積分攻撃の関係性を明らかにしている。具体的には、m bit 入力の d 次関数に対し、Division 属性から導出される最良の積分攻撃は、高階差分攻撃の$(d+1)$階差分と等しく、2^{d+1} の選択平文数を必要とすることを示している。また、その種類数が積分攻撃と高階差分攻撃で一致することも明らかにしている。

第6章では、3章と4章で示した KASUMI の鍵回復攻撃に必要な計算量に対し、今後の計算機能力の向上を見込んだ実行可能性に基づく利用可能期間の評価を行っている。5 段の KASUMI を攻撃する為に必要な計算量は $2^{31.5}$ 回の暗号化計算量であり、この計算量は汎用的な PC の計算能力程度で実行可能であることが示されている。また、7 段の KASUMI を攻撃する為に必要な計算量は $2^{63.3}$ 回の暗号化計算量であり、この計算量は現在の世界上位 500 位のスーパーコンピューターが有する計算能力で実行可能な計算量であることが明らかにされている。このことは、実際のシステムにおいて 7 段以下の KASUMI を用いることは、秘密鍵に対する鍵回復攻撃の影響を受ける可能性が無視できないものであることを示している。

第7章では、3章から6章までの結果に基づき、本論文の結論を述べている。

以上を要するに、現在および将来の情報通信システムにおいて必須となる共通鍵ブロック暗号による秘匿・完全性保証に対して、攻撃者の立場から安全性評価をより精度よく実現する汎用的な手法を提案するとともに、現在広く用いられている KASUMI の安全性評価に適用した場合の結果を開示したという観点で工学上、また関連する学術分野において貢献するところが大きい。よって、我々は本論文が博士（工学）の学位論文として十分価値があるものと認める。