Analysis and Design of Symmetric Cryptographic Algorithms

Isobe, Takanori

(Degree)
博士（工学）

(Date of Degree)
2013-09-25

(Date of Publication)
2014-09-01

(Resource Type)
doctoral thesis

(Report Number)
甲第5940号

(URL)
https://hdl.handle.net/20.500.14094/D1005940

(別紙様式3)

論文内容の要旨

氏　名　五十部　孝典

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。）

Analysis and Design of Symmetric Cryptographic Algorithms
（共通鍵暗号アルゴリズムの解析と設計）

指導教員　森井　昌克

暗号は情報セキュリティの基盤を担うコア技術である．数多くの製品，システム，サービスでは，暗号の安全性を根拠にして，その安全性を担保している．中でもブロック暗号，ストリーム暗号，ハッシュ関数に代表される共通鍵暗号技術は，秘匿，認証等のさまざまな機能を，効率的に実装することができる技術である．世の中の暗号化データの99%は共通鍵暗号技術が用いられており，安心安全な情報化社会の根幹を支える技術である．そのため，共通鍵暗号技術の安全性評価と設計は，安全なシステムを構築する上で必要不可欠である．本研究では，共通鍵暗号技術のブロック暗号，ストリーム暗号，ハッシュ関数の安全性評価を行い，安全な構成方法について明らかにする．

1. ブロック暗号の安全性評価

ブロック暗号は固定長の入力(平文)を固定長の出力(暗号文)に鍵に依存して変換する関数である．鍵を秘密にしておくことにより，その安全性を保障する．そのため，秘密鍵の導出困難性がブロック暗号の安全性を評価する上での一つの重要な基準になる．

本稿では，ブロック暗号技術の強力攻撃な鍵回復手法である中間値一致攻撃(Meet-in-the-Middle Attack)についての改良，拡張，一般化を行い，より厳密な安全性手法を確立した．

まず，中間値一致攻撃の解析能力を高めることを目的に技術の改良を行った．具体的には，不動点と等価鍵の技術を用いることにより，新しい解析手法である Refection Meet-in-the-Middle Attack を考案した．この解析手法を用いることにより，ロシア政府標準ブロック暗号 GOST の鍵回復攻撃に世界で初めて成功した．

次に，中間値一致攻撃の拡張を行い，ハードウェアで小型に実装できる有力なブロック暗号 Piccolo, LED, XTEA に適用した．ブロック暗号の構造における鍵の情報の拡散性能に focus して，評価することにより，これまでの鍵回復攻撃成功段数を上回ることに成功した．これはこの解析手法がより，正確で厳密な安全性評価であることを意味する．

次に，中間値一致攻撃の一般化を行い，汎用的な解析ツールとした．これまでの解析手法では，鍵スケジュールアルゴリズムが暗号毎ことなるため，統一的な評価は非常に困難であった．そこで，鍵スケジュールが理想的なものと仮定しても評価することができる新しい評価技術である All Subkey Recovery Approach を考案した．それをさまざまな異なる種類の構成方法のブロック暗号 SHACAL-2, CAST, KATAN, Blowfish, FOX に適用し，これまでの攻撃段数を更新し，攻撃の効果を示した．

また，統計的な偏りを利用した関連鍵ブーメラン攻撃の拡張も行い，ブロック暗号 KATAN に適用し，これまでの評価を上回ることができた．

2. ストリーム暗号の安全性評価

ストリーム暗号は秘密鍵と公開値である Initial Vector(IV)からキーストリームと呼ばれる擬似乱数を生成し，平文と XOR することにより暗号文を生成する関数である．ブロック鍵と同様に鍵を秘密にすることでその安全性を保障するため，秘密鍵の導出困難性がストリーム暗号の安全性を評価する上での一つの重要な基準になる．

本稿では，ストリーム暗号,Py, RAKAPOSHI, RC4 に対しての新しい解析技術を導入することにより，新しい構造上の脆弱性を見つけることに成功した．

Py はヨーロッパを中心とした次世代のストリーム暗号を選定するプロジェクトに応募されたストリーム暗号技術である．この暗号に対しては異なる IV に対して同じキーストリームを生成する入力ペアの脆弱性を利用し，効率的に鍵の情報を求めることを示した．具体的には推測決定攻撃を用いることにより，秘密鍵を用いる計算量を現実的なオーダーに落とすことに成功し，大きな脆弱性があることを示した．

RAKAPOSHI は KDDI が開発したハードウェア用の超軽量ストリーム暗号である．この暗号に対して理想的なストリーム暗号では発生する確率が非常に小さいスライド特性が非常に高確率で観測できることを見つけた．ここでスライド特性とは，鍵と IV が異なる入力に対して，そのキーストリームペアが数ビットシフトしているのみであることを意味する．このスライド特性を用いることにより，関連鍵攻撃において，鍵を効率的に求めることができることも示した．

RC4 は SSL/TLS や WEP/WPA 等様々な規格等で用いられている世界で最も使われている暗号方式のひとつである．本稿では，RC4 の初期キーストリームが真性乱数と比較し，大きな偏りを持つことを示した．また各出力 byte において，最も強い偏りについては，その偏りが発生する理由についても理論的に示した．この初期キーストリームの偏りを利用することにより，Broadcast setting(同じ平文をユーザ毎の鍵で暗号文を生成する)で RC4 を用いた場合には，2^32 の暗号文を集めることにより，平文の初めの 257 bytes を高確率で求めることができることを示した．また 2^34 の暗号文があれば，理論的には 1000TB の平文がほとんど確率 1 で導出することが可能である．さらに，この攻撃は SSL/TLS への multi session(毎 session 同じ場所に同じデータが含まれている)攻撃へも応用可能である．さらに，鍵回復攻撃や識別攻撃への応用も可能である．

3. ハッシュ関数の安全性評価

ハッシュ関数は任意長の入力を固定長の出力に変換する関数であり，暗号学的ハッシュ関数には衝突困難性，原像復元困難性が求められる．ブロック暗号やストリーム暗号とは異なり，秘密のパラメータである鍵は持たない．

本稿では，まず初めに，アメリカ標準ハッシュ関数 SHA-2 と Tiger ハッシュ関数の原像復元困難について評価を行った．中間値一致攻撃フレームワークでのハッシュ関数の原像復元攻撃において，Independent transform と呼ぶ新しい技術を用いることにより，SHA-2, Tiger ともに既存の結果よりも上回る段数の現像復元攻撃に成功した．

次に中間値一致原像復元攻撃を擬似衝突攻撃へ変換する方法を与えた．これまで，原像復元攻撃と衝突攻撃については，独立な安全性評価技術が用いられていたが，中間値一致攻撃の一致ポイントをうまくコントロールすることにより，擬似衝突攻撃においても効率的に実行できる．この技術により，SHA-2 と SHA-3 の最終候補であった Skein の擬似衝突攻撃を大幅に改良することに成功した．また，汎用的な変換ツールとしても有用である．

4. ブロック暗号の設計

安全な設計のための設計方針をブロック暗号，ストリーム暗号，ハッシュ関数において示す．そのあと，それらを踏まえた安全な暗号の例としてブロック暗号 Piccolo を紹介する．Piccolo はセンサーノードや RFID 等のハードウェアリソースの制限された環境でも用いることが可能である超軽量ブロック暗号 Piccolo である．Piccolo はブロック長 64 ビット,鍵長 80, 128 ビットに対応している． Piccolo は全体構造として改良型 4-line type-II generalized Feistel network を,鍵スケジューリング部として置換型鍵生成関数を採用している．安全性としては，最新のもっとも強力な攻撃手法である関連鍵差分攻撃，および中間一致攻撃に対しても十分耐性をもっており，かつ既知の攻撃法に対して十分な安全性を有することを示す．

(別紙１)　　論文審査の結果の要旨

氏名	五十部　孝典		
論文題目	**Analysis and Design of Symmetric Cryptographic Algorithms** 共通鍵暗号アルゴリズムの解析と設計		
審査委員	区　分	職　名	氏　　名
	主　査	教授	森井　昌克
	副　査	教授	増田　澄男
	副　査	教授	八坂　保能
	副　査		
	副　査		印

要　　旨

概要
本論文では，情報セキュリティの基盤を担うコア技術である共通鍵暗号技術(ブロック暗号，ストリーム暗号，ハッシュ関数)の安全性評価を行っている．また，それらをもとに安全な暗号設計のための方針を示している．
第一章は introduction である．

第二章は **Symmetric Cryptographic Algorithms** でブロック暗号，ストリーム暗号，ハッシュ関数の構成とその安全性を説明している．

第三章から第六章はブロック暗号の安全性評価を行っている．
第三章ではブロック暗号の強力な解析手法である中間値一致攻撃の能力を高めることを目的に技術の改良を行っている．具体的には，不動点と等価鍵の技術を用いることにより，新しい解析手法である Refection Meet-in-the-Middle Attack を考案した．この解析手法を用いることにより，ロシア政府標準ブロック暗号 GOST の鍵回復攻撃に世界で初めて成功した．第四章では中間値一致攻撃の拡張を行い，ハードウェアで小型に実装できる有力なブロック暗号 Piccolo, LED, XTEA に適用した．ブロック暗号の構造における鍵の情報の拡散性能に focus して，評価することにより，これまでの鍵回復攻撃成功段数を上回ることに成功した．第五章では，中間値一致攻撃の一般化を行い，汎用的な解析ツールとした．これまでの解析手法では，鍵スケジュールアルゴリズムが暗号毎ことなるため，統一的な評価は非常に困難であった．そこで，鍵スケジュールが理想的なものと仮定しても評価することができる新しい評価技術である All Subkey Recovery Approach を考案している．それをさまざまな異なる種類の構成方法のブロック暗号 SHACAL-2, CAST, KATAN, Blowfish，FOX に適用し，これまでの攻撃段数を更新し，攻撃の効果を示した．第六章では統計的な偏りを利用した関連鍵ブーメラン攻撃の拡張も行い，ブロック暗号 KATAN に適用し，これまでの評価を上回った．

第七章から九章はストリーム暗号の安全性評価を行っている．
第七章では，Py の評価を行っている．Py はヨーロッパを中心とした次世代のストリーム暗号を選定するプロジェクトに応募されたストリーム暗号技術である．この暗号に対しては異なる IV に対して同じキーストリームを生成する入力ペアの脆弱性を利用し，効率的に鍵の情報を求めることを示した．具体的には推測決定攻撃を用いることにより，秘密鍵を用いる計算量を現実的なオーダーに落とすことに成功し，大きな脆弱性があることを示した．第八章では RAKAPOSHI の評価を行っている．RAKAPOSHI は KDDI が開発したハードウェア用の超軽量ストリーム暗号である．この暗号に対して理想的なストリーム暗号では発生する確率が非常に小さいスライド特性が非常に高確率で観測できることを見つけた．ここでスライド特性とは，鍵と IV が異なる入力に対して，そのキーストリームペアが数ビットシフトしているのみであることを意味する．このスライド特性を用いることにより，関連鍵攻撃において，鍵を効率的に求めることができることも示した．

氏名	五十部　孝典

第九章では RC4 の評価を行っている．RC4 は SSL/TLS や WEP/WPA 等様々な規格等で用いられている世界で最も使われている暗号方式のひとつである．本稿では，RC4 の初期キーストリームが真性乱数と比較し，大きな偏りを持つことを示した．また各出力 byte において，最も強い偏りについては，その偏りが発生する理由についても理論的に示した．この初期キーストリームの偏りを利用することにより，Broadcast setting(同じ平文をユーザ毎の鍵で暗号文を生成する)で RC4 を用いた場合には，2^32 の暗号文を集めることにより，平文の初めの 257 bytes を高確率で求めることができることを示した．また 2^34 の暗号文があれば，理論的には 1000TB の平文がほとんど確率 1 で導出することが可能である．さらに，この攻撃は SSL/TLS への multi session(毎 session 同じ場所に同じデータが含まれている)攻撃へも応用可能である．さらに，鍵回復攻撃や識別攻撃への応用も可能である．

第十章から十一章はハッシュ関数の安全性評価を行っている．
第十章では，アメリカ標準ハッシュ関数 SHA-2 と Tiger ハッシュ関数の原像復元困難について評価を行っている．中間値一致攻撃フレームワークでのハッシュ関数の原像復元攻撃において，Independent transform と呼ぶ新しい技術を用いることにより，SHA-2, Tiger ともに既存の結果よりも上回る段数の現像復元攻撃に成功した．第十一章では，次に中間値一致原像復元攻撃を擬似衝突攻撃へ変換する方法を与えている．これまで，原像復元攻撃と衝突攻撃については，独立な安全性評価技術が用いられていたが，中間値一致攻撃の一致ポイントをうまくコントロールすることにより，擬似衝突攻撃においても効率的に実行できる．この技術により，SHA-2 と SHA-3 の最終候補であった Skein の擬似衝突攻撃を大幅に改良することに成功した．また，汎用的な変換ツールとしても有用である．

第十二章では安全な設計のための設計方針をブロック暗号，ストリーム暗号，ハッシュ関数において示している．そのあと，それらを踏まえた安全な暗号の例としてブロック暗号 Piccolo を示している．安全性としては，最新のもっとも強力な攻撃手法である関連鍵差分攻撃，および中間一致攻撃に対しても十分耐性をもっており，かつ既知の攻撃法に対して十分な安全性を有することを示した．

第十三章は Conclusion である．

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，ストリーム暗号，ハッシュ関数等様々なプリミティブに対しての解析結果が示されており，かつ既存の結果を十分上回る結果となっている．またそれらをもとに有益な新しい設計方針も示している．よって，五十部 孝典は，博士（工学）の学位を得る資格があると認める．