様式 C-19

科学研究費補助金研究成果報告書

平成２１年　４月３０日現　在

研究種目：若手研究(A)
研究期間：2006～2008
課題番号：18680001
研究課題名（和文）　ブロック暗号利用モードの証明可能安全性と標準化に関する研究
研究課題名（英文）　Study on the provable security and standardization of blockcipher mode of operation

研究代表者
岩田　哲(IWATA TETSU)
名古屋大学・大学院工学研究科・准教授
研究者番号：90344837

研究成果の概要：

本研究では、主に以下の研究成果を得た。
(1) 暗号化モード CENC の詳細な安全性の検討を行った。鍵系列と乱数を識別する敵の存在を示し、その成功確率を導いた。
(2) 次に、認証暗号化モード CHM の認証子の計算過程に改良を加え、安全性を向上させた方式を設計した。
(3) 最後に、メッセージ認証方式 CMAC 及び EMAC について、鍵チェック値との併用時に起こる安全性の問題点を指摘した。また、これらの脆弱性を回避する方法を提案した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	3,400,000	1,020,000	4,420,000
２００７年度	3,600,000	1,080,000	4,680,000
２００８年度	3,100,000	930,000	4,030,000
総　計	10,100,000	3,030,000	13,130,000

研究分野：情報セキュリティ
科研費の分科・細目：情報学・情報学基礎
キーワード：暗号理論、共通鍵暗号系、ブロック暗号、利用モード、暗号化モード、メッセージ認証コード、認証暗号化、証明可能安全性

１．研究開始当初の背景

ブロック暗号は 64 ビットや 128 ビットなど、ある固定された長さの平文を同じ長さの暗号文に暗号化する。2001 年、NIST はブロック暗号 AES を米国標準に制定した。AES は様々な暗号学的解析に十分耐えうるよう設計されている。

一方、平文と暗号文の長さが固定されているため、ブロック暗号自体は通常このまま使用されることは少なく、様々な暗号学的機能を実現するための構成要素として用いられる。ブロック暗号利用モードとは、ブロック暗号を構成要素として用い、

(1) ブロック長より長い、あるいは短い平文の暗号化（暗号化モード)、
(2) メッセージ認証コード、
(3) 認証暗号化モード、
の各機能を実現する。

暗号化モードは通信路上のデータの暗号化や、ファイルの暗号化をはじめ、あらゆるデータの暗号化に用いられる。

また、メッセージ認証コードは、メッセージの改ざんや、第三者による成りすましを検出するために用いられる。メッセージ認証コード自体にはメッセージを暗号化する機能はないため、通信内容は第三者に漏れる。

これらに対し、認証暗号化モードは、暗号化、及びメッセージ認証の二つの機能を同時に実現するものである。現実にブロック暗号が用いられる多くの場合において、暗号化、及びメッセージ認証の双方が必要な場合は、暗号化とメッセージ認証を別々に行うよりも認証暗号化モードを用いるほうが効率よく、また、実装の面からも有利である。

AES の制定に伴い、NIST は 2000 年よりブロック暗号利用モードの推奨方式を策定するプロジェクトを行っている。暗号化モードでは､1970 年代から NIST の標準であった ECB, CBC, OFB, CFB と、新たに CTR を加えた 5 方式を推奨方式に選定した。また、2005 年にはメッセージ認証コード CMAC を選定した｡CMAC は岩田と茨城大学黒澤馨が開発した方式である OMAC と同一のメッセージ認証コードである。そして、2004 年には認証暗号化モード CCM が選定され、2007 年にはさらに GCM が追加された。

NIST に推奨方式として選定された 5 つの暗号化モードのうち、ECB は安全ではないことが知られており、特殊な環境以外では使用できない。また、CBC、OFB、CFB、CTR にはバースデイパラドクスに基づく攻撃が存在する。すなわち、AES を用いた場合、2^{64} ブロック以上のデータを処理した時点で安全性は失われる。とくに、トリプル DES を用いた場合、これらのモードは 2^{32} ブロックのデータを処理した時点で安全性が失われ、その時点で秘密鍵を更新する必要があり、十分な安全性を有しているとは言えない。メッセージ認証コード CMAC､認証暗号化モード CCM と GCM にも同様の攻撃が存在する。

ECB 以外には安全性の証明がされており、この攻撃法よりも効率的な攻撃が存在しないことが理論的に示されている。これに対し、バースデイパラドクスに基づく攻撃を含め、より強力な攻撃が適用できないような、従来方式よりも安全なブロック暗号利用モードの開発が望まれる。

２．研究の目的

上記の背景を踏まえ、本研究では、新しいブロック暗号利用モードを開発することを目的とする。

とくに、上記のようなバースデイパラドクスに基づく攻撃を含め、従来考えられているよりも強力な攻撃が適用できないような、高い安全性を有するブロック暗号利用モードに関する研究を行う。

また、既存方式の安全性を見直し、様々な攻撃に対する耐性を評価し、ブロック暗号利用モードに関する知見を広げるとともに、NIST を始めとする標準化団体での採用も視野に入れ、実際に世の中で使用されるような方式を提案することを目的とする。

３．研究の方法

一般に、バースデイパラドクスに基づく攻撃を考えた場合、ブロック暗号利用モードの安全性を高めるには３つの方法がある。

① ブロック暗号に対する安全性の仮定を強める。
② 秘密鍵のサイズを増やす。
③ ブロック暗号の呼び出し回数を増やす。

メッセージ認証コード RMAC はフランスから NIST へ提案された。RMAC は①、②、③のすべてを用いており､OMAC よりも高い安全性を有する。NIST は、いったんはその高い安全性から RMAC を採択したが、後にその決定を覆し OMAC を採択した。RMAC が採択されなかった最も大きな要因は①と②であった。

本研究で提案する方式の設計にあたっては、③の方法のみを用いて安全性の改善を図る。

安全性解析について、ある方式の安全性を数学的に証明する場合は、その目的に応じた安全性定義について、敵の攻撃成功確率の上界を導出する。これには game-playing 技法や、数え上げにより成功確率を導出する手法を用いる。

また、安全性限界式の最適性を検証する場合には、具体的に敵を構成し、その敵の攻撃成功確率を計算する。これと安全性限界式が一致すれば、構成した敵は最適な攻撃者であり、また、安全性限界式はそれ以上改善できないことが示される。これらに差が有る場合には、安全性限界式が改善できるか、あるいは攻撃手法が最適でないことを示唆している。

４．研究成果

本研究では、主に以下の成果を得た。

(1) CENC の安全性について

暗号化モード CENC の安全性について詳細な検討を行った。CENC の鍵系列を乱数と識別する敵の存在を示し、その成功確率を導いた。

この攻撃成功確率は、国際会議 FSE 2006 にて示されている安全性限界式と、あるパラメータの範囲では一致する。これは、提案攻撃法が最良の攻撃法であること、及び FSE 2006 において示されている安全性限界式がこれ以上改善できないことを示している。

以上の結果を「Tightness of the Security Bound of CENC」と題して Dagstuhl Seminar, Symmetric Cryptography において発表した。

一方、パラメータの範囲外では、限界式が示す安全性と、提案攻撃の成功確率は一致していない。当初目的としていた標準化団体への提案には至っておらず、今後、安全性限界式を改善することによりこの差を埋め、提案を行いたいと考えている。

(2) CHM の改良について

認証暗号化モード CHM はバースデイパラドクスに基づく攻撃に対する証明可能安全性を有している。この認証子の計算過程に改良を加え、さらに安全性を向上させた方式を設計した。CHM は認証子のビット長 t をユーザがパラメータとして選択可能である。短い認証子は安全性が低下する一方、通信のオーバーヘッド、及び記憶領域の点で利点がある。CHM においては、t ビットの認証子を用いた場合、敵の偽造成功確率はおおむね (入手したデータブロック長)／2^t 以下となる。これは、認証子が t=32 や 64 と短い場合、現実的な量のデータを敵が入手することで、安全性限界式が意味のないものになる可能性を示唆している。

これに対し、提案方式では安全性限界式が (入手したデータブロック長)／2^n + 1／2^t となっている。ここで、n はブロック暗号のブロック長であり、n=128 が一般的である。これは、認証子が短い場合においても、提案方式が十分な安全性を有していることを示している。

一方、提案方式の安全性限界式、及び効率は、最適なものではない。これは暗号化部分に CENC を用いているためであり、今後、より安全で、より効率的な認証暗号化モードの設計が望まれる。

以上の結果を Echternach Symmetric Crypto Seminar、および AFRICACRYPT 2009 において発表した。

(3) メッセージ認証方式の安全性について

ISO/IEC 9797-1 にて規定されているメッセージ認証方式について、ANSI X9.24, Annex C, ″Retail Financial Services, Symmetric Key Management″ において定められている key check value との併用時に起こる安全性の問題点を指摘した。これは、ゼロビットからなる平文を暗号化し、その暗号文の一部のビット列を共通鍵の完全性のチェック用の値として用いるものである。

key check value として t ビットの値を用いた場合、これらのメッセージ認証方式の安全性が t/2 ビット分低下することを示した。さらに、NIST 推奨メッセージ認証方式 CMAC に特化した脆弱性の回避方法、及び一般的なブロック暗号利用モードに対し利用可能な方法を提案した。これらの方法を用いることにより、key check value との併用時における安全性が向上することを証明した。

以上の成果を Dagstuhl Seminar, Symmetric Cryptography において発表した。

当該発表ではメッセージ認証コードのみを扱ったが、暗号化モード、認証暗号化モード、また、PMAC などの ISO/IEC 9797-1 に規定されている以外のメッセージ認証コードについても同様の安全性解析が必要であると考えられる。

(4) その他、ブロック暗号利用モード、及びその構成要素となるブロック暗号に関連して、以下の成果を得た。

① メッセージ認証コードのサイドチャネル攻撃に対する安全性を解析し、EMAC や OMAC について、ブロック暗号が安全であったとしても、メッセージ認証コード全体としては安全とは限らないことを示した。これは、サイドチャネル攻撃を考える際は、ブロック暗号のみならず、モード全体に対する安全性を考慮する必要があることを示している。

② 擬似ランダム性と呼ばれる安全性を満たすブロック暗号の構成方法について、Feistel 構造に基づく鍵効率のよい方式を提案した。また、5 ラウンド KASUMI 型置換の擬似ランダム性を解析し、その安全性を数学的に示した。

③ ブロック暗号の利用形態の一つである Tweakable ブロック暗号の新たな設計方法を提案した。この設計は一般化 Feistel 構造に基づいており、また、内部のデータラインと Tweak の排他的論理和を直接とることで、Tweak 更新の効率を高めている。提案方式の安全性について、その擬似ランダム性を証明した。

④ ブロック暗号などの鍵の生成に必要な乱数の生成方式について解析した。乱数の性質を向上させるための後処理関数について、その性質の向上度合いの理論的限界値を導出した。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 3 件）

① Tetsu Iwata, Tohru Yagi, Kaoru Kurosawa, Security of the five-round KASUMI type permutation, IEICE Trans. Fundamentals, Vol. E91-A, No. 1, 2008, 30-38. （査読有）

② Tetsu Iwata and Kaoru Kurosawa, How to construct super-pseudorandom permutations with short keys, IEICE Trans. Fundamentals, Vol.E90-A, No. 1, 2007, pp. 2-13. （査読有）

③ Katsuyuki Okeya and Tetsu Iwata, Side channel attacks on message authentication codes, IPSJ Journal, Vol. 47, No. 8, 2006, pp. 2571-2581. （査読有）

〔学会発表〕（計 6 件）

① Tetsu Iwata, On the impact of key check value on CBC MACs and others, Dagstuhl Seminar, Symmetric Cryptography, Jan. 11-16, 2009, Dagstuhl, Germany. （査読無、2009 年 1 月 13 日発表、発表者 Tetsu Iwata）

② Atsushi Mitsuda and Tetsu Iwata, Tweakable pseudorandom permutation from generalized Feistel structure, Second International Conference, ProvSec 2008, LNCS 5342, Springer, Oct. 30-Nov. 1, 2008, Shanghai, China. （査読有、2008 年 10 月 30 日発表、発表者 Atsushi Mitsuda）

③ Kyohei Suzuki and Tetsu Iwata, Bounds on fixed input/output length post-processing functions for biased physical random number generators, Selected Areas in Cryptography, SAC 2008, Aug. 14-15, 2008, Moncton, Canada. （査読有、2008 年 8 月 15 日発表、発表者 Kyohei Suzuki）

④ Tetsu Iwata, Authenticated encryption mode for beyond the birthday bound security, Progress in Cryptology, AFRICACRYPT 2008, LNCS 5023, Springer, Jun. 11-14, 2008, Casablanca, Morocco. （査読有、2008 年 6 月 11 日発表、発表者 Tetsu Iwata）

⑤ Tetsu Iwata, Authenticated encryption mode for beyond the birthday bound security, ESC, Echternach Symmetric Crypto Seminar, Jan. 7-11, 2008, Echternach, Luxembourg. （査読無、2008 年 1 月 11 日発表、発表者 Tetsu Iwata）

⑥ Tetsu Iwata, Tightness of the security bound of CENC, Dagstuhl Seminar Proceedings, 07021, Symmetric Cryptography, Jan. 7-12, 2007, Dagstuhl, Germany. （査読無、2007 年 1 月 11 日発表、発表者 Tetsu Iwata, http://drops.dagstuhl.de/opus/volltexte/2007/1016/）

６．研究組織
(1)研究代表者
岩田 哲（IWATA TETSU）
名古屋大学・大学院工学研究科・准教授
研究者番号：90344837