様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年　６月　５日現在

機関番号：１３９０１
研究種目：若手研究(A)
研究期間：2010　～　2012
課題番号：22680001
研究課題名（和文）
高安全、高効率な共通鍵暗号要素技術に関する研究
研究課題名（英文）
Study on Highly Secure and Efficient Symmetric Key Cryptosystems
研究代表者
岩田　哲（IWATA TETSU）
名古屋大学・工学研究科・准教授
研究者番号：90344837

研究成果の概要（和文）：
本研究では主に以下の成果を得た。
・n ビットの Tweakable ブロック暗号から 2n ビット以外の Tweakable ブロック暗号を構成する方法を提案した.
・Type 1 一般化 Feistel 構造において，データの拡散性の観点から優れた置換部分の構成法を提案した.
・EAX-prime の安全性解析を行い，効率的な攻撃が可能であることと，cleartext と呼ばれるデータのビット長が使用するブロック暗号のブロック長よりも常に長い場合は証明可能安全性を有することを示した.
・GCM の従来の安全性証明には誤りがあることを突き止めた．さらに，その証明の誤りを修正することに成功し，GCM が証明可能安全性を有することを明らかにした.

研究成果の概要（英文）：
We obtain the following main results.
・We propose a construction of a tweakable block cipher whose block length is shorter or longer than 2n bits, from an n-bit tweakable block cipher.
・We propose constructions of a permutation layer for Type-1 generalized Feistel structures so that they have a good diffusion property.
・We show that EAX-prime allows various efficient attacks. We also prove its security if the input data called a cleartext is always longer than the block length of the underlying block cipher.
・We show that the original security proof of GCM contains a flaw. We also show that the flaw can be fixed and therefore GCM maintains its provable security.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	3,500,000	1,050,000	4,550,000
2011 年度	2,500,000	750,000	3,250,000
2012 年度	3,000,000	900,000	3,900,000
総　計	9,000,000	2,700,000	11,700,000

研究分野：現代暗号理論
科研費の分科・細目：情報学・情報学基礎
キーワード：暗号系

１．研究開始当初の背景

ブロック暗号は暗号化方式，メッセージ認証コード，認証暗号化方式といった様々ブロック暗号利用モードの構成要素として用いられる．これに対し，Tweakable ブロック暗号は Tweak と呼ばれる入力をとり，Tweak を更新することであたかも秘密鍵を更新したかのように動作する．この性質を用いることで，高い効率性を有する暗号化方式，メッセージ認証コード，認証暗号化方式が構成可能となる．したがって，高い安全性と高い効率性を有する Tweakable ブロック暗号の設計が望まれている．

また，認証暗号化方式はメッセージの暗号化と認証を同時に実現する案技術であるが，ディスクセクタ暗号化や確定的認証暗号化モードといった新しい用途向けのブロック暗号利用モードが提案されており，高い安全性と高い効率性を有する様々なブロック暗号利用モードの構成法を確立することが望まれている．

２．研究の目的

本研究は、従来の共通鍵暗号要素技術の安全性、及び効率を格段に高度化した方式を開発することを目的とする。また、国際標準化を視野に入れ、開発した方式の提案を行うとともに、最終的に標準方式として採用されることを目的とする。

本研究で扱う共通鍵暗号要素技術は、(1)高安全、高効率な Tweakable ブロック暗号技術、(2)Tweakable ブロック暗号利用モード、及びブロック暗号利用モードである。

３．研究の方法

(1)に関しては，既存方式の検討から行い，ブロック暗号の構成に適した構造を見出すとともに，様々な攻撃に対する評価を行う．
(2)に関して，既存方式の安全性検証を行い，方式の設計を行うとともに，その安全性解析を数学的に行う．

４．研究成果

(1) に関連する主な研究成果：

【一般化 Feistel 構造】

FSE 2010 において洲崎・峯松は Type 2 一般化 Feistel 構造に対し，データの拡散性について最適な置換を用いることによって，様々な攻撃に対する安全性が向上することを示した．本研究では，データライン数が 8 以下の Type 1, Source-Heavy, Target-Heavy 一般化 Feistel 構造に対し，データの拡散性について最適な置換を計算機により導出した．そして，導出した置換を用いた構造の不可能差分攻撃，飽和攻撃，差分攻撃，線形攻撃に対する安全性を解析した．

さらに，データライン数が偶数の場合の Type 1 一般化 Feistel 構造に対し，データの拡散性について最適な置換の一般的な構成法を示した．また，Type 3 一般化 Feistel 構造に対し，各出力データラインがすべての入力データラインに依存するための，置換部分に関する必要十分条件を示した．

また，Type 1 一般化 Feistel 構造と Type 2 一般化 Feistel 構造を特殊な場合として包含する Type 1.x 一般化 Feistel 構造を提案し，その構造に適した置換部分の構成に関する検討を行った．

【ブロック暗号 HyRAL の安全性解析】

CRYPTREC 応募暗号である HyRAL の等価鍵に関する解析を行った．その結果，鍵長が 249 ビットの場合に等価鍵が 2^33.4 ペア存在することを示した．さらに，計算量 2^50.8 で等価鍵の例を導出するアルゴリズムを設計した．また，提案アルゴリズムをスーパーコンピュータを用いて実行した際にかかるコストの見積もりを示した．

【Tweakable ブロック暗号の構成】

Tweakable ブロック暗号の設計に関して，峯松による FSE 2009 の構成法を拡張し，n ビットの Tweakable ブロック暗号から 2n ビット以外の Tweakable ブロック暗号を構成する方法を提案した．さらに，提案構成法がバースデーバウンドを超える安全性を有することを数学的に証明した．

(2) に関連する主な研究成果：

【authenticated key wrap の構成】

ブロック暗号利用モードに関して，共通鍵暗号の秘密鍵など，それ自体が乱数性を有しているデータを暗号化，認証するための技術として，authenticated key wrap 方式が知られている．SAC 2009 において，Gennaro と Halevi は authenticated key wrap 方式として，ハッシュ関数と ECB モードを組み合わせた HtECB 方式，及び CBC モードと組み合わせた HtCBC 方式の安全性を解析した．ハッシュ関数として universal ハッシュ関数を用いた場合，HtECB 方式が一般には安全ではないことが示され，HtCBC 方式の安全性は未解決問題であった．これに対し本研究では，ハッシュ関数に関する新たな条件を提案し，提案する条件を満たす universal ハッシュ関数を用いた HtECB 方式と HtCBC 方式が安全な authenticated key wrap 方式であることを数学的に証明した．

次に，authenticated key wrap 方式において暗号文長を削減できれば，記憶領域や通信コストと安全性のトレードオフが可能とな

るが，HtECB 方式では暗号文長を削減すると復号を行うことができない．本研究では，HtECB 方式の復号方法を修正することにより，暗号文長を削減可能な方式を設計した．また，上記の universal ハッシュ関数を用いた場合，提案方式が安全な authenticated key wrap 方式であることを証明した．

さらに HtCBC 方式ついて，この方式が従来知られているよりも強い安全性である確定的認証暗号としての安全性を有することを数学的に証明した．

【EAX-prime の安全性解析】

ANSI C12.22-2008 で標準化されている EAX-prime の解析を行い，効率的な偽造攻撃，識別攻撃，平文回復攻撃が可能であることを示した．本研究成果を Dagstuhl セミナーにて発表し，IACR ePrint で結果を公開するとともに NIST へパブリックコメントを提出した．EAX-prime は NIST において推奨方式としての採用が計画されていたが，本研究成果により，推奨方式とはされないこととなった．

また，EAX-prime の証明可能安全性の観点からの解析を行った．その結果，EAX-prime に対しては，入力の一部である cleartext と呼ばれるデータのビット長が使用するブロック暗号のブロック長よりも常に長い場合，EAX-prime が証明可能安全性を有することを示した．さらに，EAX-prime を安全に使用するための方式を 3 通り開発した．

【GCM の安全性解析】

認証暗号化モード GCM (Galois Counter Mode) の詳細な安全性解析を行った．これは NIST の推奨方式であり，NSA Suite B に含まれているほか，SSH，TLS/SSL で用いられるなど，重要な暗号技術である．GCM の安全性は提案者らによって数学的に証明されているものの，その議論には誤りがあることを突き止めた．カウンタ衝突と呼ばれる事象が起こると GCM の安全性は崩れる．したがって GCM の安全性を証明する際には，この事象の生起確率が十分に小さいことを示す必要がある．しかし，提案者らが主張するよりも実際には高い確率でカウンタ衝突が起こることを，反例を挙げることにより示した．さらに，その数学的な証明の誤りを修正することに成功し，GCM が証明可能安全性を有することを明らかにした．

【確定的認証暗号化方式の設計】

ブロック暗号利用モードの開発に関して，AES-NI が使用できる環境に適した確定的認証暗号化方式のプロトタイプを設計した．ブロック暗号を基本要素として用い，認証部分を含めて並列計算が可能である．AES-NI が利用できる環境では GCM よりも高速に動作する．

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 Shingo Yanagihara and Tetsu Iwata. Improving the permutation layer of type 1, type 3, source-heavy, and target-heavy generalized Feistel structures. IEICE Trans. Fundamentals, Vol. E96-A, No. 1, pp. 2--14, January 2013. （査読有） DOI: 10.1587/transfun.E96.A.2

② Yasushi Osaki and Tetsu Iwata. Security of hash-then-CBC key wrapping revisited. IEICE Trans. Fundamentals, Vol. E96-A, No. 1, pp. 25--34, January 2013. （査読有） DOI: 10.1587/transfun.E96.A.25

③ Yasushi Osaki and Tetsu Iwata. Further more on key wrapping. IEICE Trans. Fundamentals, Vol. E95-A, No. 1, pp. 8--20, January 2012. （査読有） DOI: 10.1587/transfun.E95.A.8

〔学会発表〕（計 16 件）

① Shingo Yanagihara. Type 1.x generalized Feistel structures. Pre-proceedings of International Workshop on Coding and Cryptography, WCC 2013, April 15--19, 2013, Bergen, Norway.

② Kazuhiko Minematsu. Attacks and security proofs of EAX-prime. Fast Software Encryption, FSE 2013, LNCS, Springer-Verlag, March 11--13, 2013, Singapore.

③ 小林　隼人.「OKH 認証暗号化方式に対する攻撃」 2013 年暗号と情報セキュリティシンポジウム，SCIS 2013, 1B2-2, 2013 年 1 月 22--25 日，京都市.

④ 大橋　佳祐.「SGCM のカウンタ衝突確率」 2013 年暗号と情報セキュリティシンポジウム，SCIS 2013, 1B2-1, 2013 年 1 月 22--25 日，京都市.

⑤ Tetsu Iwata. Breaking and repairing GCM security proofs. Advances in Cryptology, CRYPTO 2012, LNCS 7417, pp. 31--49, Springer-Verlag, August 19--23, 2012, Santa Barbara, USA.

⑥ Kazumaro Aoki. How fast can a two-pass mode go? A parallel deterministic authenticated encryption mode for AES-NI (Extended abstract of work in progress). Workshop records of DIAC, Directions in Authenticated Ciphers,

July 5--6, 2012, Stockholm, Sweden.

⑦ Kazuhiko Minematsu. Cryptanalysis of EAX-prime. Workshop records of DIAC, Directions in Authenticated Ciphers, July 5--6, 2012, Stockholm, Sweden.

⑧ Yuki Asano. Cryptanalysis of 256-bit key HyRAL via equivalent keys. ACNS 2012, LNCS 7341, pp. 257--274, Springer-Verlag, June 26--29, 2012, Singapore.

⑨ 柳原　慎吾.「Type 1, Type 3 一般化 Feistel 構造の置換層の改良」 2012 年暗号と情報セキュリティシンポジウム, SCIS 2012, 2C1-2, 2012 年 1 月 30--2 月 2 日, 石川県金沢市.

⑩ Yasushi Osaki. Security of Hash-then-CBC key wrapping revisited. Cryptography and Coding, 13th IMA International Conference, IMACC 2011, LNCS 7089, pp. 413--430, Springer-Verlag, December 12--15, 2011, Oxford, UK.

⑪ Tetsu Iwata. Building blockcipher from tweakable blockcipher: Extending FSE 2009 proposal. Cryptography and Coding, 13th IMA International Conference, IMACC 2011, LNCS 7089, pp. 391--412, Springer-Verlag, December 12--15, 2011, Oxford, UK.

⑫ Shingo Yanagihara. On permutation layer of Type 1, Source-Heavy, Target-Heavy Generalized Feistel structures. The 10th International Conference on Cryptography and Network Security, CANS 2011, LNCS 7092, pp. 98--117, Springer-Verlag, December 10--12, 2011, Sanya, China.

⑬ 浅野　優貴.「249 ビット鍵 HyRAL の等価鍵」 コンピュータセキュリティシンポジウム 2011, CSS2011, 2C2-1, 2011 年 10 月 19--21 日, 新潟県新潟市.

⑭ 柳原　慎吾.「Type 1, Source-Heavy, Target-Heavy 一般化 Feistel 構造の改良」 2011 年暗号と情報セキュリティシンポジウム, SCIS 2011, 3B2-3, 2011 年 1 月 25--28 日, 福岡県北九州市.

⑮ 尾崎　泰司.「暗号文長を削減可能な HtECB 方式」 2011 年暗号と情報セキュリティシンポジウム, SCIS 2011, 3B2-4, 2011 年 1 月 25--28 日, 福岡県北九州市.

⑯ Yasushi Osaki. Further more on key wrapping. Conference record of Symmetric Key Encryption Workshop (SKEW) 2011, February 16--17, 2011, Lyngby, Denmark.

〔図書〕(計 0 件)

〔産業財産権〕
○出願状況 (計 0 件)

○取得状況 (計 0 件)

〔その他〕
ホームページ等

なし

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

(2)研究分担者　なし

(3)連携研究者　なし