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２４年５月１８日現在

機関番号：１３４０１
研究種目：基盤研究（Ｂ）
研究期間：2008～2011
課題番号：２０３００００３
研究課題名（和文）大量の情報の機密性・完全性を保証する情報セキュリティ技術の研究

研究課題名（英文）Study on techniques to keep confidentiality and integrity of a large amount of information

研究代表者
廣瀬　勝一（HIROSE SHOICHI）
福井大学・大学院工学研究科・教授
研究者番号：２０２２８８３６

研究成果の概要（和文）：本研究では，機密性保証のためのストリーム暗号と完全性保証のためのハッシュ関数という二つの効率の良い暗号構成要素の安全性解析を行うとともに，それらを用いて構成できる認証・秘匿機能付データ構造の設計と評価を行った．本研究成果は，大量の情報に関する問合せに対して過不足のない正しさの保証された応答を効率良く行うことに寄与するものであり，近年注目を浴びているクラウドを利用したデータベースサービスのアウトソーシング等への応用が期待できる．

研究成果の概要（英文）：We made security analyses of two efficient cryptographic primitives: stream ciphers to keep confidentiality and hash functions to keep integrity. We also designed authenticated data structures with confidentiality, which can be constructed using these cryptographic primitives, and confirmed their efficiency and security. The results are useful to make secure and reliable responses efficiently to queries on a large amount of information. An example of applications is outsourcing of database services using clouds.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	5,000,000	1,500,000	6,500,000
２００９年度	3,400,000	1,020,000	4,420,000
２０１０年度	3,400,000	1,020,000	4,420,000
２０１１年度	2,700,000	810,000	3,510,000
総　計	14,500,000	4,350,000	18,850,000

研究分野：暗号学，情報セキュリティ工学
科研費の分科・細目：情報学・情報学基礎
キーワード：暗号・認証等，情報基礎，セキュア・ネットワーク

１．研究開始当初の背景

情報の機密性と完全性を保証するためには，情報セキュリティ技術が必要不可欠である．特に，処理効率を損なうことなく非常に大量な情報の機密性および完全性を保証するためには，機密性を保証するストリーム暗号，完全性を保証するハッシュ関数が有効である．しかし，ストリーム暗号とハッシュ関数は，これまで情報セキュリティ研究の非主流分野であり，それらの構成法については未解決問題が数多く残されている．

さらに現実のシステムにおける重要な課題として，ストリーム暗号やハッシュ関数などのセキュリティ機能をシステムに組み込

む際に生じる脆弱性への対策が挙げられる．現在のウェブなどのシステムにおいて，機密性や完全性を保証するセキュリティ機能は必須であるが，提供するサービスの主目的ではないため，システム全体の中でセキュリティ機能に利用できるメモリやCPUなどの資源が制限される場合が多い．こうして，セキュリティ機能組み込みシステムでは，ストリーム暗号やハッシュ関数などの初期状態がメモリ量，実行時間などの要求に応じて設定されることが多い．このため，セキュリティ機能単体では安全であっても，組み込みシステム条件が脆弱性に繋がることが多い．

ストリーム暗号は，ブロック暗号と比較して，速度及びハード・ソフトウエア規模等を圧倒的に高性能に実現できる可能性を有しており，大量の情報の秘匿に不可欠である．しかし，ブロック暗号については，安全性の理論的解析手法が確立され，国際標準暗号が規格化されたのに対し，ストリーム暗号は次々に攻撃が指摘され，安全性の保証が確立されていない．このため，安全かつ高性能なストリーム暗号の選定に向けた国際プロジェクトが正に進行中である．

一方，ハッシュ関数は大量情報の完全性保証に適した認証付データ構造のみならず，ほとんどすべてのセキュリティシステムに利用される必須技術である．しかしながら，現在広く利用されているデファクトスタンダードのハッシュ関数 SHA-1 に対する強力な攻撃法が 2005 年に提案されたことから，米国標準技術局（NIST）は数年にわたる標準ハッシュ関数の公募選定プロジェクトを 2007 年中に開始する予定である．

安全性解析の研究は情報セキュリティの基盤研究に相当する．本研究は，ストリーム暗号とハッシュ関数の安全性解析に関する未解決問題を解決するとともに，これらの技術を利用して，効率を損なうことなく，様々な構造をもつデータとして蓄積される情報から必要かつアクセスの許可された情報のみを抽出し，改ざんのないことを保証して提供する技術の確立を目的とする．

２．研究の目的

本研究開発は以下の三つの研究を行うことを目的とする．

(1) 機密性保証に適したストリーム暗号の安全性解析
(2) 完全性保証に適したハッシュ関数の安全性解析
(3) 大量の情報を扱うための効率的な認証・秘匿機能付データ構造の設計と評価

上記(1)では，現在進行中のストリーム暗号の選定プロジェクトやRC4などの普及型ストリーム暗号を対象とし，安全・安心なストリーム暗号の構築を研究する．(2)では，標準ブロック暗号 AES を利用したハッシュ関数や，現在 NIST が利用を推奨している SHA-2 族のハッシュ関数を対象として，それらの構成法の妥当性および安全性を研究する．(3)では大量の情報を扱うための効率的な認証・秘匿機能付データ構造を設計し，(1)及び(2)で行った成果を要素技術として利用し，安全性と効率の観点から性能を評価する．

３．研究の方法

(1) 機密性保証に適したストリーム暗号の安全性解析

本研究項目では，暗号組み込み時に設定されるパラメータである鍵に着目し，鍵の相関性が出力に及ぼす影響を実験的に検出し，その実験結果を用いて，鍵の相関性を利用した安全性解析を行った．これまでに得られている RC4 の最も短い衝突鍵は，松井によって示された 24 バイトの衝突鍵であった．本研究ではこの結果を更新し，構成アルゴリズムに最新のハッシュ関数の衝突攻撃で利用されていた方法を一般化して応用することで，最短の衝突鍵を構成した．図 1 は衝突鍵が起こる原理を表す．

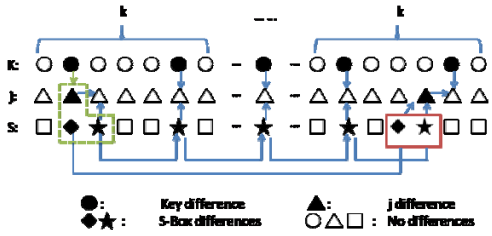

図 1 衝突鍵が起こる原理

さらに，暗号の脆弱性のレベルを鍵の相関性毎に理論的に求め，脆弱性につながる鍵の条件を明らかにした．これにより，安全性の観点から望まれるシステム組み込み時の設計条件を明らかにした．

一方，衝突鍵が見つかることの具体的な脅威を示すために，RC4 を用いたハッシュ関数の脆弱性を RC4 の衝突鍵を求めるアルゴリズムを用いて示した．さらに衝突鍵を得るアルゴリズムを一般化することで，この方法を RC4 の解読に適用することを検討した．

(2) 完全性保証に適したハッシュ関数の安全性解析

現在広く用いられている SHA-2 などのハッシュ関数は反復型ハッシュ関数と呼ばれ，図 2 に示すような構造を有している．ここで，F は圧縮関数と呼ばれる固定長入出力関数である．

圧縮関数の構成法は，ハッシュ関数専用の構成法と既存のブロック暗号を利用する方法に分類される．SHA-2 は前者に相当するが，

SHA-2 専用に構成されたブロック暗号を利用した構成法とみなすこともできる．このような構成法のモデルを図 3 に示す．この図で，Eはブロック暗号であり，x，kはそれぞれ平文，秘密鍵に相当する．x，k，zはそれぞれ，M_i，H_{i-1}，M_i+H_{i-1}(+は 2 を法とする加算)，定数のいずれかである．SHA-2 は，$k=M_i$，$x=z=H_{i-1}$とした構成に基づいており，この構造は Davies-Meyer (DM) モードと呼ばれている．

ハッシュ関数は様々なアプリケーションで利用されており，アプリケーションがハッシュ関数に対して要求する安全性基準として，衝突計算困難性，ランダム関数の代替，メッセージ認証コード（偽造困難性），擬似ランダム性が挙げられる．本研究項目では，これらの安全性の観点から，図 3 のモデルに属する圧縮関数の望ましい構成法に関する研究を行った．

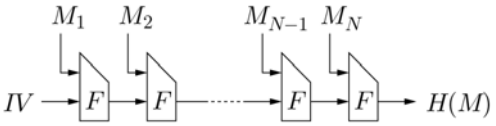

図 2　反復型ハッシュ関数

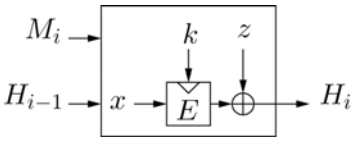

図 3　圧縮関数 F のモデル

(3) 大量の情報を扱うための効率的な認証・秘匿機能付データ構造の設計と評価

これまでの認証付データ構造に関する研究のほとんどは，クライアント・サーバモデルを仮定していた．一方，それらの研究と異なり，Tamassia と Triandopoulos は，P2P (peer-to-peer) システムを仮定して，情報の更新が可能な認証付辞書を分散ハッシュ表で実現している．本研究では，グラフのデータ構造や，辞書よりも複雑な質問処理の可能なデータ構造について，それらの認証付データ構造を P2P システムで実現する方式を設計し，その効率を評価した．

本研究項目では，さらに，ストリーム暗号を利用してデータ構造の秘匿機能を実現する方法を検討した．具体的には，構造を有するデータの検索や更新などの利用効率を損なわない暗号化方式，ストリーム暗号のシステム組込み時の制約により生じる脆弱性等を検討した．

４．研究成果

(1) 機密性保証に適したストリーム暗号の安全性解析

本研究項目では，暗号組み込み時に設定されるパラメータである鍵に着目し，相関性をもつ鍵(衝突鍵)を人為的に構成できる新たなアルゴリズム提案した．さらに，そのアルゴリズムを一般化し，与えられた相関性に対して，その相関性を満足する衝突鍵の構成を実現した．また衝突鍵を求めるアルゴリズムを改良し，既存研究よりも小さい計算量で衝突鍵が求められるようになった．図 4 では，衝突鍵のサイズと計算量について，本研究と既存研究を比較する．

また，RC4 を用いたハッシュ関数の衝突攻撃に RC4 の衝突鍵を求めるアルゴリズムを適用することで，RC4 を用いたハッシュ関数の新たな衝突を示した．本研究ではさらに，衝突鍵を生成するアルゴリズムを暗号解読に適用する方法を構築し，この方法を用いて，RC4 が解読できることを具体的に示した．表 1 では，提案した解読と既存解読において，鍵サイズ毎の計算量と復元確率について比較する．

本研究成果により，衝突鍵を生じるストリーム暗号の特徴，さらにその脅威が明らかになり，ストリーム暗号設計時の脆弱性解析に大きな成果をもたらした．

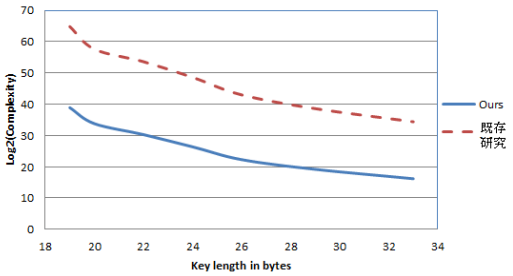

図 4 衝突鍵のサイズと計算量

表 1　鍵復元の確率と計算量

Models	Key Length	Complexity	Probability
RKA	$k = 13$	2^{20}	1
KFISA	$k = 5$	2^{20}	0.86
	$k = 16$	2^{64}	0.005
	$k \gg 16$	Not given	Not given
KFISA	$k = 5$	2^{24}	0.998
	$k = 16$	2^{35}	0.075
	$k \gg 16$	Not given	Not given
Modified RKA (ours)	$k < 256$	$> 2^{23}$	1
	$k > 40$	$< 2^{48}$	1
	$k < 16$	-	-
Related-Key KFISA (ours)	$k > 16$	$< 2^{25}$	1

(2) 完全性保証に適したハッシュ関数の安全性解析

3 節(2)に示したブロック暗号に基づく反

復型ハッシュ関数の安全性解析は，通常，安全なブロック暗号が利用されることを仮定して行われる．一方で，ブロック暗号に要求される安全性が必ずしも反復型ハッシュ関数の安全性に寄与するとは限らず，さらに，ブロック暗号としての安全性を満たさない構成要素を用いて安全な反復型ハッシュ関数が構成できる可能性もある．この点を明らかにするために，本研究項目では，ブロック暗号としての安全性を満たさない構成要素を用いて安全な反復型ハッシュ関数が構成できるかどうかを検討した．なお，このような検討は，反復型ハッシュ関数で利用されているブロック暗号に脆弱性が見出された際の安全性評価にも有益であると考えられる．

本研究項目では，与えられた平文と暗号文に対して，その暗号化に利用される鍵が容易に計算できるようなブロック暗号を仮定し，このブロック暗号により構成される図 2 の圧縮関数を用いて，衝突計算困難性を有する反復型ハッシュ関数が構成できるかどうかを検討した．なお，ここで仮定するブロック暗号は明らかに暗号化関数としての安全性を満たさない．

ブロック暗号に基づく反復型ハッシュ関数の衝突計算困難性は，通常，ブロック暗号 E がすべてのブロック暗号の集合から無作為に選択されるという理想暗号モデルと呼ばれる仮定の下で論じられる．これに対して本検討では，与えられた平文と暗号文に対応する鍵が一意に定まるような（安全でない）すべてのブロック暗号の集合から無作為に選択されることを仮定した．

本検討は，図 2 のモデルに属する圧縮関数の内，理想暗号モデルの下で衝突計算困難性を有する反復型ハッシュ関数を与える 20 個すべての圧縮関数について行った．この結果，20 個中 17 個の圧縮関数については，いずれを用いても衝突困難性を有する反復型ハッシュ関数が構成できることが明らかとなった．なお，SHA-2 の構成の基礎である DM モードはこれらの 17 個には含まれなかった．一方，DM モードとともに図 2 のモデルに属する主要な圧縮関数の一つである Matyas-Meyer-Oseas (MMO)モードは，この 17 個に含まれる．MMO モードは $k=H_{i-1}$，$x=z=M_i$ により定義される．さらに，このモードは，研究代表者らにより擬似ランダム性を有する反復型ハッシュ関数の構成にも適していることが明らかにされている．これらの結果から，安全性の観点からは，DM モードよりも MMO モードが優れていることが明らかとなった．

(3) 大量の情報を扱うための効率的な認証・秘匿機能付データ構造の設計と評価

本研究項目に関しては以下の成果を得た．

① 認証・秘匿機能付データ構造に適した分散ハッシュ表の構成と応用

分散ハッシュ表は P2P システムの最も重要な応用の一つであり，これまでに様々な実現法が提案されている．本研究では，個々の分散ハッシュ表の特徴を利用して，より効率的な認証・秘匿機能付データ構造を設計するために，分散ハッシュ表への応用が可能な，ネットワーク環境におけるハッシュ連鎖とその応用法について検討した．本研究で提案したハッシュ連鎖法では，複数のハッシュ連鎖を用意し，同じインデックスであっても，異なるハッシュ連鎖値を持つことが可能である．このようなハッシュ連鎖法を利用することにより，大規模ネットワークにおける効率的な認証が可能になるだけでなく，状況に応じた柔軟なリボケーションが可能になる．さらに，分散ハッシュ表の代表的な実現である Chord 上でハッシュ木を実現し，大量の情報の完全性を保証する方法を研究開発した．具体的には，Chan らが考案した固定トポロジにおけるブロードキャスト認証法を応用した．また，NS2 によるネットワークシミュレーションを実施して実験的な評価を行った．

② P2P システム上での実現に適した範囲質問処理可能な認証・秘匿機能付データ構造

本研究では，範囲質問に対して答とともにその正当性を保証するデータを提供することを可能とする認証付分散セグメント木を提案した．このデータ構造は，これまでに提案されていた分散セグメント木と分散 Merkle 木を統合することにより構成することができ，P2P システム上での実現に適している．なお，P2P システムにおいては負荷分散が重要な課題であるため，認証付分散セグメント木に対して，超高効率検証法と呼ばれる既存手法を適用することにより，データ構造それ自体に負荷分散を実現する機能を付加できることを示した．さらに，質問に対する答の正当性を保証するデータから質問範囲外のデータに関する情報の漏洩を防ぐ秘匿機能も実現した．

③ 認証・秘匿機能付データ構造のためのハッシュ関数を用いたデジタル署名

本研究では，木構造データに対する編集可能署名法を提案した．この署名法では，署名者の秘密鍵を用いることなく，木構造データとその署名から，もとの木構造データの任意の部分木の署名を作成することが可能であり，さらに，部分木以外の情報に関する秘匿機能も有している．従来方式では，木構造データの全枝数よりも大きな回数だけ通常のデジタル署名を計算する必要があったため，処理効率に問題があった．一方，提案方式では Merkle 木に基づいて鍵付ハッシュ関数を用いて木構造データのダイジェストを計算することにより，通常のデジタル署名を根に

対応するダイジェストに対して１回だけ計算するのみで良く，高速処理が可能である．図５に提案方式で構成されるMerkle木の例を示す．この図で，r_iは鍵付ハッシュ関数で用いられる秘密鍵を表すが，これらは単一のマスタ秘密鍵を用いて計算することが可能である．また，破線の節点と枝は，秘匿機能を実現するために署名の際に付加されるダミーである．さらに，提案方式で利用される署名法と鍵付ハッシュ関数の安全性に関する妥当な仮定の下で，提案方式が従来方式と同等の安全性を有することを証明した．さらに，本研究ではハッシュ関数のみを用いた認証法として，one time signature の効率的な構成法も提案している．

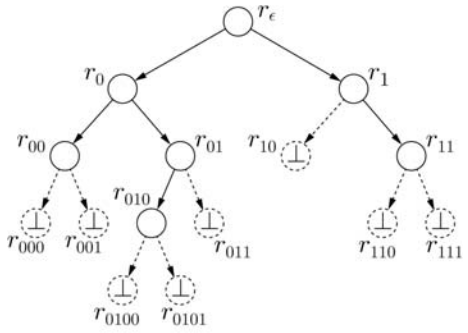

図５　木構造データに対応するMerkle木の例

④　ハッシュ関数を用いたストリーム型データ認証法の効率化

データ消失が起こるような通信路において効率よくストリーム型データの認証を行う方式として，Perrig らによる TESLA (Efficient Stream Loss-tolerant Authentication) と呼ばれる方式がある．この方式はハッシュ連鎖を用いるもので，ストリーム暗号化にも応用できる．しかしながらこの方式では，ハッシュ連鎖の最初の値を安全に送る必要があり，その際，デジタル署名などが必要になり，効率が悪い．そこで，複数のストリーム通信の初期値をさらに TESLA を用いることにより，その複数のストリーム認証をより効率よくできる方法を提案した．

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１８件）

① S. Hirose, Collision Resistance of Hash Functions in a Weak Ideal Cipher Model, IEICE Transactions on Fundamentals, 査読有, vol. E95-A, pp. 252-255, 2012.
② 双紙正和, 早稲田篤志, One time signature の効率的な構成の検討, 情報処理学会研究報告, 査読無, vol. 35, pp. 1-4, 2012.
③ J. Chen, A. Miyaji, How to Find Short RC4 Colliding Key Pairs, The 14th Information Security Conference, Lecture Notes in Computer Science, 査読有, vol. 7001, pp. 32-46, 2011.
④ 廣瀬勝一, Content Authentication for Range Queries in Peer-to-Peer Networks, 電子情報通信学会技術研究報告, 査読無, vol. 111, pp. 177-180, 2011.
⑤ A. Miyaji and M. Sukegawa, New Analysis Based on Correlations of RC4 PRGA with Nonzero-Bit Differences, IEICE Trans. Fundamentals, 査読有, vol. E93-A, pp. 1066-1077, 2010.
⑥ J. Chen and A. Miyaji, A New Class of RC4 Colliding Key Pairs With Greater Hamming Distance, The 6th Information Security Practice and Experience Conference (ISPEC 2010), Lecture Notes in Computer Science, 査読有, vol. 6047, pp. 30-44, 2010.
⑦ 双紙正和, 新しいハッシュ連鎖の構成による単純な認証方式とその応用, 電子情報通信学会技術研究報告, 査読無, vol. 110, pp.1-5, 2010.
⑧ A. Miyaji, M. Rahman, M. Soshi, Hidden credential retrieval without random oracles, The 11th International Workshop on Information Security Applications (WISA 2010), Lecture Notes in Computer Science, 査読有, vol. 6513, pp. 160-174, 2010.
⑨ A. Miyaji and M. Sukegawa, New Correlations of RC4 PRGA Using Nonzero-Bit Differences, ACISP 2009, Lecture Notes in Computer Science, 査読有, vol. 5594, pp. 134-152, 2009.
⑩ 廣瀬勝一, ハッシュ関数の安全性に関する考察, 電子情報通信学会技術研究報告, 査読無, vol. 108, pp. 267-271, 2009.

〔学会発表〕（計２１件）

① 廣瀬勝一, 桑門秀典, 木構造データに対する Merkle 木に基づく編集可能署名, 2012 年暗号と情報セキュリティシンポジウム, 2012 年 2 月 2 日, 金沢エクセルホテル東急.
② 市丸祐, 宮地充子, 初期差分を用いた RC4 PRGA の解析, 2012 年暗号と情報セキュリティシンポジウム, 2012 年 1 月 31 日, 金沢エクセルホテル東急.
③ 廣瀬勝一, 共通鍵認証暗号における再暗号化について, コンピュータセキュリティシンポジウム 2010, 2010 年 10 月 19 日, 岡山コンベンションセンター.
④ 柿脇一穂, 宮地充子, 差分情報を利用し

たRC4 PRGA内部状態復元アルゴリズムの提案，コンピュータセキュリティシンポジウム2010，2010年10月19日，岡山コンベンションセンター.
⑤ 双紙正和，ハッシュ連鎖による単純な認証法とセンサーネットワークへの応用，コンピュータセキュリティシンポジウム2010，2010年10月19日，岡山コンベンションセンター.

〔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〕
特記事項なし.

６．研究組織
(1)研究代表者
廣瀬　勝一（HIROSE SHOICHI）
福井大学・大学院工学研究科・教授
研究者番号：20228836
(2)研究分担者
宮地　充子（MIYAJI ATSUKO）
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：10313701
双紙　正和（SOSHI MASAKAZU）
広島市立大学・情報科学部・准教授
研究者番号：00293142
(3)連携研究者
田邉　英彦（TANABE HIDEHIKO）
福井大学・大学院工学研究科・助教
研究者番号：80236661