様式 C-7-2

自己評価報告書

平成２３年４月２５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．研究計画の概要

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．

２．研究の進捗状況

(1)「機密性保証に適したストリーム暗号の安全性解析」に関しては，無線 LAN の WPA 等で広く利用されているストリーム暗号 RC4 について，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を提示した．さらに提案アルゴリズムを一般化し，衝突鍵の一般的な構成を実現した．

(2)「完全性保証に適したハッシュ関数の安全性解析」に関しては，SHA-2 の構成法を含む，ブロック暗号に基づく様々な構成法について，ハッシュ関数の衝突計算困難性を，理想暗号モデルやより弱いモデルを仮定して解析した．また，ハッシュ関数のアプリケーションとして，MAC(メッセージ認証コード)関数の構成に関する研究を行い，証明可能安全性の観点から，MAC 関数の安全性が構成要素であるブロック暗号の安全性に帰着可能であるかどうかを網羅的に検討した．その結果，SHA-2 の構成法は，他の多くの構成法と同様に必ずしも MAC 関数の構成に関して適切ではないことを確認するとともに，最適な構成法を特定した．

(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」に関しては，P2P（peer-to-peer）システムを仮定し，分散セグメント木と呼ばれるデータ構造を利用して，負荷分散を考慮した，範囲質問を処理できる認証付データ構造を設計した．また，P2P システムにおいて，分散ハッシュ表の代表的な実現である Chord システムを対象とし，そのオーバーレイネットワークとして，効率的な認証・秘匿機能付データ構造を設計した．さらに，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，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の構成と応用等について研究した．

３．現在までの達成度

② おおむね順調に進展している．

（理由）研究開始時の予想を上回る成果を得られているとまでは言い難いが，各研究分担者のそれまでの研究成果を基礎として，おおむね当初計画に沿って，研究成果が得られている．

４．今後の研究の推進方策

平成 23 年度は本研究の最終年度であり，以下の研究を実施する計画である．

(1)「機密性保証に適したストリーム暗号の安全性解析」に関しては，ストリーム暗号 RC4 について，引き続き，相関関係をもつ鍵(衝突鍵)の存在に関する研究を行う．これまで RC4 の最も短い衝突鍵は松井によって生成された 24bytes である．本研究ではこの結果を更新し，最少の衝突鍵を構成する．本研究により，RC4 の衝突鍵を用いた攻撃に対する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する．

(2)「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」に関しては，分散ハッシュ表の代表的な実現である Chord を対象として，効率的な認証・秘匿機能付データ構造についてさらに検討を推し進め，性能やセキュリティについてより詳細に検討する．また，昨年度には負荷分散を考慮した，範囲質問を処理できる認証付データ構造を設計したが，今年度はさらに，負荷分散を考慮した，より高度な質問を処理できる認証付データ構造を設計する．

５． 代表的な研究成果
（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 6 件）

① J. Chen and A. Miyaji, Generalized RC4 Key Collisions and Hash Collisions, The 7th Conference on Security and Cryptography for Networks (SCN 2010), Lecture Notes in Computer Science vol. 6280, pp. 73-87, 2010, 査読有.
② J. Chen and A. Miyaji, A New Class ofRC4 Colliding Key Pairs With Greater Hamming Distance, The 6th Information Security Practice and Experience Conference (ISPEC 2010), Lecture Notes in Computer Science vol. 6047, pp. 30-44, 2010, 査読有.
③ A. Miyaji and M. Sukegawa, New Analysis Based on Correlations of RC4 PRGA with Nonzero-Bit Differences, IEICE Trans. Fundamentals, vol. E93-A, pp. 1066-1077, 2010, 査読有.
④ 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 vol. 6513, pp. 160-174, 2010, 査読有.
⑤ S. Hirose and H. Kuwakado, Efficient Pseudorandom-Function Modes of a Block-Cipher-Based Hash Function, IEICE Transactions on Fundamentals, vol. E92-A, pp. 2447-2453, 2009, 査読有.

〔学会発表〕（計 19 件）

① 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，電子情報通信学会情報通信システムセキュリティ研究会，2010 年 11 月 5 日，広島市立大学.
② 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.
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 廣瀬勝一，桑門秀典，Constructing a Hash Function from a Weak Block Cipher in an Ideal Model，電子情報通信学会情報セキュリティ研究会，2009 年 9 月 18 日，機会振興会館（東京）.
⑤ 廣瀬勝一，ハッシュ関数の安全性に関する考察，電子情報通信学会情報通信基礎サブソサイェティ合同研究会，2009 年 3 月 10 日，公立はこだて未来大学.

〔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〕