様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月　 ３ 日現在

機関番号：１３４０１
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５３３０１５０

研究課題名（和文）証明可能安全性を有する応用指向セキュリティプロトコルの開発

研究課題名（英文）Design and Analysis of Application-Oriented Security Protocols with Provable Security

研究代表者

廣瀬　勝一（Hirose, Shoichi）

福井大学・工学（系）研究科（研究院）・教授

研究者番号：２０２２８８３６

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：セキュリティプロトコルは，情報通信の安全性を保証する基盤技術であり，様々な応用に対して多数の提案がなされているが，その中には安全性が十分に検討されていないものが多く存在する．本研究では，それらのうち，共通鍵暗号に基づく逐次型メッセージ認証方式やロギング方式について，それらの安全性を定義し，定義された安全性を満たすことが数学的に証明される新たな方式を提案した，さらに，これらの構成要素として利用できるハッシュ関数について新たな構成法を提案するとともに，攻撃，証明の両方の観点から安全性を評価した．

研究成果の概要（英文）：There are many security protocols proposed so far for various kinds of applications. Unfortunately, there also exist many protocols with few formal security analysis among them. In this project, we mainly focused on sequential message authentication and logging using symmetric key cryptographic primitives. We formalized their security requirements and proposed new schemes provably secure based on their formalized security requirements. We also evaluated security of cryptographic hash functions designed by ourselves in terms of cryptanalysis and provable security. These hash functions can be used for various kinds of security protocols including our proposed protocols for sequential message authentication and logging.

研究分野：暗号学

キーワード：セキュリティ　証明可能安全性　認証

１．研究開始当初の背景

セキュリティプロトコルは，情報通信ネットワークの安全性を保証する基盤であるが，その中には安全性が十分に検討されていないものが多数存在し，これまでに，そのようなセキュリティプロトコルが実際に利用され，深刻な問題の生じた例が報告されている．また，学術分野においても，国内外の幾つかの学術誌で，安全性を十分検討することなく提案されたセキュリティプロトコルに対するほぼ自明な脆弱性を指摘する論文が多数投稿されることが問題となっている．これらの問題は，セキュリティプロトコルの安全性解析が非常に解決困難な課題であり，さらに広くかつ深い研究を必要としていることを示している．

セキュリティプロトコルの研究開発においては，新しく提案されたプロトコルに対する攻撃（脆弱性の指摘）とそれを防ぐ修正の反復が不可欠である．一方，汎用性の高いセキュリティプロトコルやその構成要素である暗号アルゴリズムの研究開発では，「攻撃・修正」のアプローチに加えて，証明可能安全性，すなわち，要求される安全性を数学的に定義し，それが満たされることを証明することにより安全性を保証するという「定義・証明」アプローチが用いられている．これら二つのアプローチは，一方が他方より優れているというものではなく，相補的なものである．すなわち，定義・証明のアプローチによる安全性の定義でカバーされていない部分を，攻撃・修正アプローチで明らかにする．さらに，安全性を数学的に定義することにより，考慮すべき攻撃を限定することが可能となる．したがって，新たに開発したセキュリティプロトコルに関しては，これら二つのアプローチを用いて安全性の評価を行うことが不可欠である．

２．研究の目的

情報通信ネットワークは，社会生活のインフラの一つとなり，この安全性が損なわれると，重大な損害の生じるおそれがある．セキュリティプロトコルは，情報通信ネットワークの安全性を保証する基盤技術であり，多岐にわたる応用に対して様々な提案がなされているが，その中には，安全性が十分に検討されていないものが多数存在する．この主な原因は，安全性評価の際に，証明可能安全性のアプローチが利用されていないことである．本研究では，実用上重要な応用指向セキュリティプロトコルに対して安全性の数学的な定義を与えるとともに，その安全性を満たすことが証明可能なセキュリティプロトコルを開発することを目的とする．

３．研究の方法

本研究の課題は以下のとおりである．

(1) 応用を指向したセキュリティプロトコルに関する既存研究の調査
(2) セキュリティプロトコルに要求される安全性の数学的な定義
(3) 証明可能安全性を有するセキュリティプロトコルの開発

ただし，安全なセキュリティプロトコルの開発には，必然的に，新たな脆弱性の発見とそれに対する修正が伴うため，上記の(3)は，実際には，(2)，(3)のプロセスの繰り返し，すなわち，定義の修正，拡張とそれに即した安全性証明の付与の繰り返しとなる．

４．研究成果

(1) 逐次型集約可能メッセージ認証方式

① 背景

メッセージ認証は最も基本的かつ重要な暗号の機能であり，HMAC や CMAC のようなメッセージ認証関数が様々な応用で広く用いられている．

一方，幾つかの応用では，基本的なメッセージ認証に付加的な性質が要求される．例えば，ロギングシステムについては，個々のイベントの記録の改ざん検知のみでは不十分であり，個々の記録の順序の入替えや一部の消去なども検知可能であることが要求される．また，メッセージ認証では改ざん検知のために用いられるタグと呼ばれる固定長の系列が計算されるが，ロギングシステムでは，記憶領域の節約のために，個々の記録に対するタグが集約できることが望ましい．さらに，フォワード安全と呼ばれる安全性が満たされることも重要である．この安全性は一般に，秘密鍵の更新により実現されるが，これにより，システムへの侵入などにより現在使用されている秘密鍵が漏洩しても過去の記録の改ざんを抑止することができる．以上に述べたような性質は，センサーネットワークにおけるメッセージ認証などにおいても有用である．

フォワード安全な逐次型集約可能メッセージ認証の概念とそれを実現する方式は，Ma と Tsudik により 2007 年に提案されている[1]．しかし，これまでその概念は十分に定式化されておらず，提案方式の安全性も詳細には議論されていなかった．

上述の Ma と Tsudik の方式は，メッセージ認証関数（MAC 関数）とハッシュ関数を用いて構成されているが，ハッシュ関数には衝突計算困難性が要求される．衝突計算困難性と一方向性の間には大きなギャップのあることが知られており，衝突計算困難性を仮定することなく安全性が保証される方式が構成できれば望ましい．

② 成果の概要

本研究では最初に，フォワード安全な逐次型集約可能メッセージ認証方式とその安全性を定式化した．なお，この定式化では，秘密鍵は時間に応じて更新され，一般に，同一の鍵を用いて複数のメッセージに対応するタグが計算されることを仮定した．

次に，MAC 関数と擬似ランダムビット列生

成器を用いて構成される方式を提案した．提案方式では，新たに出現したメッセージとそれまでの一連のメッセージに対応するタグとに対して新たなタグを計算する．これにより，メッセージの順序の入替えや一部の消去を検出することを可能とした．また，提案方式のフォワード安全性を実現するために，フォワード安全な擬似ランダムビット列生成器が用いられている．

最後に，提案方式の構成要素である MAC 関数と擬似ランダムビット列生成器の安全性を仮定して，提案方式が安全であることを証明した．

③ 成果

フォワード安全な逐次型集約可能メッセージ認証方式は，鍵生成，鍵更新，タグ計算，検証，タグ集約の 5 個のアルゴリズムから構成される．鍵生成アルゴリズムの入力は鍵長であり，出力は与えられた鍵長を有する秘密鍵である．鍵更新アルゴリズムは，現在の秘密鍵を入力として，新しい秘密鍵を出力するアルゴリズムである．タグ計算アルゴリズムは現在の秘密鍵，新たに出現したメッセージ，それまでの一連のメッセージに対応するタグを入力として新しいタグを計算するアルゴリズムである．検証アルゴリズムは，一連のメッセージ，一連のメッセージの最初のメッセージ以前のすべてのメッセージに対応するタグ，一連のメッセージの最後のメッセージに対応するタグ，一連のメッセージのタグの計算に使用されたすべての秘密鍵を入力として，一連のメッセージとタグの組が正しい組であるかどうか，すなわち，改ざんがなされていないかどうかを検証するアルゴリズムである．タグ集約アルゴリズムは一連のメッセージの個々のメッセージに対応するタグを集約するアルゴリズムであるが，本定式化では，単に一連のメッセージの最後のメッセージに対応するタグ以外を消去するアルゴリズムである．

フォワード安全な逐次型集約可能メッセージ認証方式の安全性は偽造不能性に基づいて定義される．安全性の定義では，攻撃者はまず，攻撃者の選択した任意のメッセージに対してそれに対応するタグを得ることができると仮定する．さらに，攻撃者の選択した任意の時点で使用されている秘密鍵を得ることができると仮定する．これらの仮定のもとで，攻撃者が得た秘密鍵以前に使用されていた秘密鍵に対して正しいと判定される一連のメッセージとタグの組を攻撃者が生成できないとき，フォワード安全な逐次型集約可能メッセージ認証方式は安全であると定義される．

フォワード安全な逐次型集約可能メッセージ認証の提案方式を図 1 に示す．この図で F は MAC 関数，K_i は stage i で用いられる秘密鍵，$M_{i,j}$ は stage i で j 番目に出現したメッセージである．$\tau_{i,j}$ は，$M_{i,j}$ に対応するタグである．$M_{i,j}$ の先頭に 0 が付加された系列に対してタグが計算される．1 に対するタグは各ステージの終了を明示するために必要である．鍵 K_i は図 2 の鍵更新アルゴリズムにより計算される．G は擬似ランダムビット列生成器である．S_1 は鍵生成アルゴリズムにより生成される．

提案方式では衝突計算困難性が要求されるハッシュ関数は用いられていない．

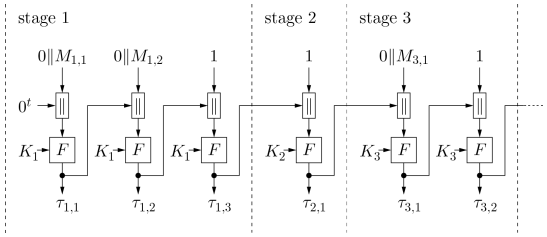

図 1 提案方式

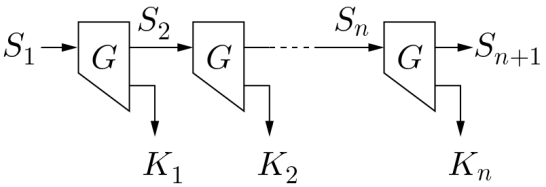

図 2 鍵更新アルゴリズム

提案方式は，MAC 関数 F と擬似ランダムビット列生成器 G が安全であるとき安全であることが証明される．ここで，F に要求される安全性は偽造不能性であり，G に要求される安全性は識別不能性である．なお，本研究では，F が偽造不能性を満たす関数よりも強い擬似ランダム関数である場合についても，提案方式の安全性を証明した．

(2) 秘匿と認証の機能をもつロギング方式

① 背景

ロギングは安全なシステムの運用のために不可欠な技術である．安全なロギングは，前項(1)の背景で述べたようなメッセージ認証機能に加えて，記録されるイベントの機密情報を保護するための秘匿機能を有することが望ましい．さらに，鍵の漏洩により過去の記録の安全性が損なわれることを抑止するためのフォワード安全性も不可欠である．

秘匿と認証の機能をもつロギング方式は 1998 年に Schneier と Kelsey により提案されている [2]．Schneier らはログファイルを生成する信頼できないシステムとログファイルを保存する信頼できるシステムとの間の通信プロトコルまで考慮しているが，本研究ではログファイルの生成にのみ着目する．なお，ログファイルの生成のみに関しても，その定式化はなされておらず，安全性も詳細には議論されていない．

② 成果

本研究では最初に，フォワード安全な秘匿と認証の機能をもつロギング方式とその安全性を定式化した．フォワード安全な秘匿と認証の機能をもつロギング方式は，鍵生成，

鍵更新，暗号化，復号の 4 個のアルゴリズムから構成される．また，本方式の安全性として，フォワード秘匿性とフォワード認証性を定義した．前者は，暗号化アルゴリズムの出力と乱数列との識別不能性，後者は復号アルゴリズムにより正当と判断される暗号文の偽造不能性に基づいて定義される．なお，フォワード安全性に関して，攻撃者は自身の選択した任意の時点で使用されている秘密鍵を得ることができると仮定する．

本研究では，秘密鍵が時間に応じて更新される場合と，秘密鍵がイベント毎に更新される場合のそれぞれについて，秘匿と認証の機能をもつロギング方式を提案した．秘密鍵が時間に応じて更新される場合に対する提案方式の暗号化アルゴリズムを図 3 に，秘密鍵がイベント毎に更新される場合に対する提案方式の暗号化アルゴリズムを図 4 に示す．なお，鍵更新アルゴリズムとしては図 2 のアルゴリズムが用いられる．図 4 の提案方式では，K_i と L_i の組が図 2 の K_i に相当する．

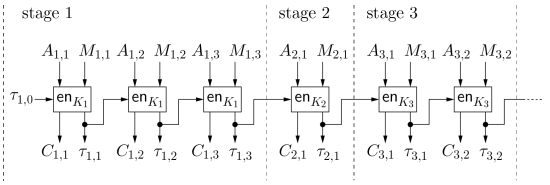

図 3 秘密鍵が時間に応じて更新される場合に対する提案方式

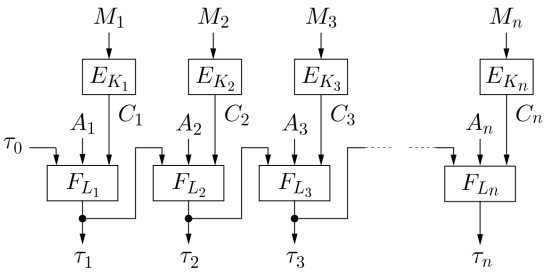

図 4 秘密鍵がイベント毎に更新される場合に対する提案方式

秘密鍵が時間に応じて更新される場合に対する提案方式は，認証暗号を用いて構成される．認証暗号方式は秘匿と認証の機能を同時に提供する共通鍵暗号方式である．図 3 で en は認証暗号の暗号化アルゴリズムである．en_{Ki} はナンス，メッセージ $M_{i,j}$，付随データ $A_{i,j}$ に対して秘密鍵 K_i を用いて計算された暗号文 $C_{i,j}$ とタグ $\tau_{i,j}$ を出力する．ここで，タグはメッセージと付随データ両方の改ざん検知のために生成される系列である．一方，暗号文はメッセージのみに対応しており，付随データは秘匿性保証の対象とならないデータである．ナンスは en の呼び出しごとに異なる値であることが要求される入力であり，提案方式では直前のイベントに対するタグ $\tau_{i,j-1}$ がナンスとして利用されている．タグはメッセージと付随データの改ざん検知のために生成される系列であり，安全な認証暗号では，相異なるメッセージと付随データの組に対して同一のタグが生成される確率は無視できる程度に小さくなる．このため，タグをナンスとして適切に利用できる．また，このような構成とすることにより，メッセージと付随データの組の順序の入替えや削除といった改ざんを検知することが可能となる．なお，前項(1)の方式と同様，本提案方式においても各 stage の終了を明示する処理が必要となるが，本方式では付随データを用いてそのような処理を行うこととしている．

本提案方式は，認証暗号と鍵更新アルゴリズムの擬似ランダムビット列生成器が安全であるとき，安全であることが証明される．

秘密鍵がイベント毎に更新される場合に対する提案方式は，暗号化方式と MAC 関数を用いて構成される．図 4 で，E は暗号化方式，F は MAC 関数である．E_{Ki} は i 番目のメッセージ M_i に対して秘密鍵 K_i を用いて計算された暗号文 C_i を出力する．MAC 関数はメッセージ M_i に対する暗号文 C_i，付随データ A_i，直前のイベントに対するタグ τ_{i-1} に対して秘密鍵 L_i を用いて計算されたタグ τ_i を出力する．本提案方式では，イベント毎に秘密鍵が更新されるため，秘密鍵が時間毎に更新される場合に対するような，各秘密鍵の使用の終了を明示するための処理は不要である．また，ナンスも不要であるため，特に，暗号化方式 E については，処理が簡潔で済み，教科書に掲載されているカウンタモードなどのブロック暗号の暗号利用モードをそのまま利用することが可能である．

本提案方式は，構成要素である暗号化関数，MAC 関数および擬似ランダムビット列生成器が安全性であるとき，安全であることが証明される．

本研究では，秘密鍵の更新頻度に関して，ある時間毎の更新と発生するイベント毎の更新を想定し，それぞれに対して秘匿と認証の機能を提供するロギング方式を提案した．イベント毎に鍵更新を行う方がシステムに対する負荷は大きくなるため，処理効率の観点からはある時間毎に鍵を更新することが望ましい．一方，システムに対する攻撃者の侵入がイベントとして検知された場合，イベント毎に鍵更新が行われる場合は，侵入に対応するイベントのログファイルへの登録直後に鍵が更新されるため，攻撃者が痕跡を残すことなくログファイルを改ざんすることは困難となる．ある時間毎に鍵更新が行われる場合は，一般に，侵入に対応するイベント登録後も同じ秘密鍵が使用されるため，痕跡を残すことなくログファイルを改ざんすることが可能となる．このように安全性の観点からは，イベント毎に鍵を更新することが望ましい．さらに，既に上記で述べたとおり，イベント毎に鍵を更新する方がより簡素な暗号方式を利用することが可能である．

〈参考文献〉

① D.Ma and G.Tsudik, Extended abstract: Forward-secure sequential aggregate authentication, IEEE Symposium on Security and Privacy, 2007, pp. 86-91.

② B. Schneier and J. Kelsey, Secure audit logs to support computer forensics, ACM Transactions on Information and System Security 2(2), 1999, pp. 159-176.

５．主な発表論文等

〔雑誌論文〕（計 4 件）

① S. Hirose, Generic Construction of Audit Logging Schemes with Forward Privacy and Authenticity, ICICS 2015, Lecture Notes in Computer Science vol. 9543, 2016, pp. 125-140, **査読有**, DOI: 10.1007/978-3-319-29814-6_11.

② J. Chen, S. Hirose, H. Kuwakado and A. Miyaji, A Collision Attack on a Double-Block-Length Compression Function Instantiated with 8-/9-Round AES-256, IEICE Trans. Fundamentals, vol. E99-A, no. 1, 2016, pp. 14-21, **査読有**, DOI: 10.1587/transfun.E99.A.14.

③ S. Hirose and H. Kuwakado, Forward-Secure Sequential Aggregate Message Authentication Revisited, ProvSec 2014, Lecture Notes in Computer Science, vol. 8782, pp. 87-102, **査読有**. DOI: 10.1007/978-3-319-12475-9_7.

④ H. Kuwakado and S. Hirose, Hashing Mode Using a Lightweight Blockcipher, IMACC 2013, Lecture Notes in Computer Science, vol. 8308, pp. 213-231, **査読有**. DOI: 10.1007/978-3-642-45239-0_13.

〔学会発表〕（計 5 件）

① S. Hirose, Application-Specific Cryptographic Schemes Based on Symmetric-Key Primitives, ASK 2014, Chennai, 2014 **年** 12 **月** 22 **日**.

② A. Akhimullah, **廣瀬勝一**, A TESLA-Based Authentication Protocol for Multiple Senders, 2014 **年暗号と情報セキュリティシンポジウム**, **鹿児島市**, 2014 **年** 1 **月** 23 **日**.

③ S. Hirose and H. Kuwakado, Redactable Signature Scheme for Tree-Structured Data Based on Merkle Tree, SECRYPT 2013, Reykjavík, 2013 **年** 7 **月** 31 **日**.

〔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〕
該当なし

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
桑門　秀典（KUWAKADO, Hidenori）
関西大学・総合情報学部・教授
研究者番号：３０２８３９１４