様式 C-19

科学研究費補助金研究成果報告書

平成２１年　５月１５日現在

研究種目：若手研究（B）
研究期間：2006 年度～2008 年度
課題番号：18700009
研究課題名（和文）　汎用的結合可能な安全性をもつ長期署名の開発

研究課題名（英文）　Development of universally composable long term signatures

研究代表者
吉田　真紀（YOSHIDA MAKI）
大阪大学・大学院情報科学研究科・助教
研究者番号：50335387

研究成果の概要：電子文書の改ざんを防止し真正性を保つためのセキュリティ技術である長期署名について，まず既存方式とその要素技術が保証する安全性を評価し，問題点を指摘した．その上で，安全性を適切に定式化し，定式化した安全性を満たす方式を提案した．さらに，安全性の形式的検証法を提案し，その主要部分を実装し，実用性と有効性を評価した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	1,400,000	0	1,400,000
2007 年度	1,200,000	0	1,200,000
2008 年度	800,000	240,000	1,040,000
年度			
年度			
総　計	3,400,000	240,000	3,640,000

研究分野：総合領域
科研費の分科・細目：情報学・情報学基礎
キーワード：電子文書，真正性，長期署名，汎用的結合，セキュリティ

１．研究開始当初の背景

近年，電子政府の推進や民間での電子文書の利用に関する法律が整備され，紙文書から電子文書への移行が進みつつある．電子文書は紙文書と異なり，痕跡を残さず内容を改ざんすることが容易となる．よって，保存を義務付けられた期間中，電子文書の改ざんを防止し真正性を保つためのセキュリティ技術である長期署名が非常に重要であり，現在その仕様の標準化が行われている．

しかし，標準仕様では電子文書の真正性を長期間保つために必要となる項目は示されても，その仕様によって保証される安全性が示されて(定式化されて)いない．保証する安全性が定式化されておらず，実用上十分な安全性をもつか明らかでなく，安全に利用できる環境が明らかでない．

２．研究の目的

本研究では，標準仕様の問題点を解決するために次の三つを目的とする．

(A) 既存の標準仕様（XAdES および CAdES）が保証する安全性を評価．

(B) 長期署名が目標とすべき安全性を適切に定式化．

(C) 目標とすべき安全性を保証できる長期署名を設計し実装．

長期署名はインターネット上の様々なアプリケーションの電子文書に対して利用されるため，どのような環境において，どのよう

なセキュリティ技術と共に利用（結合）されるかを限定できない．そこで，三つの目的を達成するに当たって，任意の利用環境における任意のセキュリティ技術との結合を想定する．

３．研究の方法

三つの目的を達成するための次の方法に従う．

目的(A)：既存の標準仕様（XAdES および CAdES）が保証する安全性を評価．

既存の標準仕様の安全性を評価では，電子商取引実証推進協議会(ECOM)の推奨プロファイルをもとにする．標準仕様では，多くの選択的な定義が含まれており，長期署名を実現する際にはそのサブセットを選ぶことになる．現在，ECOM によって推奨プロファイルの検討がなされており，本研究では，常に最新の推奨プロファイルで示された選択可能なサブセット全てに対して安全性の評価を行い，満たすべき安全性の検討を行う．

目的 (B)：長期署名が目標とすべき安全性を適切に定式化．

長期署名の安全性とは，電子文書の真正性を長期に渡って保証することである．定式化では，まず必須安全性として，電子文書に対して長期署名を「作成した時」に電子文書の真正性「誰が」「何を書いたか」を確認できること(生成時真正性)を定式化する．次に，時間の概念を導入し，長期間経過後に「いつ」「誰が」「何を書いたか」を確認できること（長期真正性）を定式化する．そして，それらの定式化に基づき，推奨プロファイルで示された様々な項目に対応する安全性の定式化を行う．

目的 (C)：目標とすべき安全性を保証する長期署名の設計および実装．

長期署名の設計では，その方式が速やかに実用化できるように設計することが重要である．よって，利用するセキュリティ技術を XAdES と同様，既に実用化されたセキュリティ技術を利用する．具体的には，ハッシュ関数，電子署名，タイムスタンプの三つとする．

４．研究成果

研究成果は，既存技術の安全性評価，安全性の適切な定式化，新たな方式の設計，実装の四つからなる．本研究では，長期署名に加えて，長期署名の核となるセキュリティ技術である電子署名について，多くの成果を得た．具体的には，真正性と秘匿を保証する Signcryption，電子カルテ情報のための電子署名を中心に研究した．以下では，主要な研究成果を示す．

成果 1：既存技術の安全性評価．既存の標準仕様の安全性を評価では，電子商取引実証推進協議会(ECOM)の推奨プロファイルをもとにした．標準仕様では，多くの選択的な定義が含まれており，長期署名を実現する際にはそのサブセットを選ぶことになる．本研究では，最新の ECOM の推奨プロファイルで示されたサブセットに対して安全性の評価を行った．さらに，Signcryption の安全性について，署名対象メッセージの秘匿を同時に考えた場合，既存の定義では不十分であることを指摘し，国際会議で発表した．

成果 2：安全性の適切な定式化．長期署名の安全性として，生成時真正性と長期真正性を定式化した．その際，タイムスタンプに関する汎用的結合可能安全性の定式化を参照とした．また，成果 1 において問題点を指摘した Signcryption について，その問題点を解消する適切な安全性を定式化し，国際会議で発表した．さらに，電子カルテのための電子署名に関する安全性を定式化した．近年，電子カルテの利用によって医療サービスの効率化が進んでいるが，さらに患者が自身のカルテ情報を保持できれば，災害や事故遭遇時などに適切な処置を受けることができ，医療サービスの更なる充実につながる．そこで患者が自身のカルテ情報を保持し，それを適切な形で利用するための安全性に関する要求を分析した．その結果，セキュリティに関する要求は二つあることが分かった．一つは部分的な開示制御の要求であり，患者が見てもよい情報は開示し，そうでない情報は患者には秘匿され，医師や救急隊員等の適切な相手（開示対象者と呼ぶ）には開示したいという要求である．もう一つは全体の真正性保証の要求であり，カルテ情報を医師が作成した後，改ざんされていない（正しい）ことを，患者を含む誰もが確認できるようにしたいという要求である．これまでに，一部の要求を満たす暗号技術として墨塗り署名が知られている．墨塗り署名は情報を全員に公開するか完全に秘匿するかのいずれかの場合だけを対象としており，元の文書を知るためにはそれをもつ人と通信する必要がある．よって，そのままでは緊急時の使用には適さない．そこで，電子カルテ情報自己管理のための電子署名の安全性として，部分的な開示制御と全体の真正性保証を定式化した．

成果 3：新たな方式の設計． 長期署名の核となる電子署名として，成果 2 で定式化した安全性を満たす Signcryption と電子カルテ情報のための電子署名を設計した．前者の提案方式は，従来と同程度の効率でより強い安全性を満たす．そして，後者の提案方式は，新しい二つの安全性を，元の電子文書をもつ人と通信することがないという点で効率よく満たす．なお，基本設計方針は既存の墨塗り署名に基づく．そして，開示対象者だけが単独で開示できるように暗号化データを付与する（部分的な開示制御の実現）．その上で

誰でも単独で秘匿された内容と暗号化データの内容が同じであることを確認できるように証拠データも付与する（全体の真正性保証）．証拠データの生成には知識の証明に基づく署名を利用する．ここで，提案法の安全性は利用した暗号技術の安全性により保証される．提案法を用いることで患者は適切かつ安心なカルテ情報自己管理を行うことができる．

さらに，汎用的結合可能性の枠組みにおける安全性を記号的手法に基づき形式的に検証する手法を提案した．今後さまざまな暗号機能の汎用的結合可能な安全性を検証可能とするために，記述能力の高い我々の研究グループが提案した記号的手法（公理的安全性検証法と呼ぶ）を用いた．

成果 4：実装．成果 2 の形式的検証法が基づく公理的安全性検証法の高速実装を目標とし，本手法で繰り返し実行される主要処理を改良して実装した．そして検証例としてよく用いられるプロトコルに対して検証時間を実測し，有効性と実用性を確認した．

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 11 件）

1. Maki Yoshida and Toru Fujiwara, ``Flexible Timed-release Encryption,'' IEICE Transactions on Fundamentals, Vol.E92-A, No.1, pp.222-225 (2009-01), 査読あり.
2. Kazuhiro Haramura, Maki Yoshida, and Toru Fujiwara, ``Anonymous Fingerprinting for Predelivery of Contents,'' Proceedings of the 11th International Conference on Information Security and Cryptography (ICISC2008), LNCS 5461, pp.134-151 (2008-12), 査読あり.
3. Mohamed Layouni, Maki Yoshida, and Shingo Okamura, ``Efficient Multi-Authorizer Accredited Symmetrically Private Information Retrieval,'' Proceedings of the 10th International Conference on Information and Communications Security (ICICS2008), LNCS 5308, pp.387-402 (2008-10), 査読あり.
4. Maki Yoshida and Toru Fujiwara, ``Expiration-dated Fingerprinting,'' Proceedings of the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2008), pp.147-150 (2008-08), 査読あり.
5. Maki Yoshida and Toru Fujiwara, ``Global Timed-release Encryption,'' to appear in Proceedings of the 26th International Conference on Consumer Electronics 2008 (ICCE2008) (2008-01), 査読あり.
6. Maki Yoshida, Itaru Kitamura, and Toru Fujiwara, ``A New Scheme for Optimum Decoding of Additive Watermarks in Spatial Domain,'' to appear in Proceedings of the 3rd International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP2007) (2007-11), 査読あり.
7. Maki Yoshida and Toru Fujiwara, ``A Secure Construction for the Nonlinear Function Threshold Ramp Secret Sharing Scheme,'' Proceedings of the 2007 IEEE International Symposium on Information Theory (ISIT2007) (2007-07), 査読あり.
8. Satoshi Nakayama, Maki Yoshida, Shingo Okamura, and Toru Fujiwara, ``A Private and Consistent Data Retrieval Scheme with Log-Squared Communication,'' IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E90-A, No.1, pp.204-215 (2007-01), 査読あり.
9. Takaaki Fujita, Maki Yoshida, and Toru Fujiwara, ``A New Scheme to Realize the Optimum Watermark Detection for the Additive Embedding Scheme with the Spatial Domain,'' IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E90-A, No.1, pp.216-225 (2007-01), 査読あり.
10. Junya Asano, Shingo Okamura, Maki Yoshida, and Toru Fujiwara, ``Towards Secure C2C Contents Distribution Services,'' Proceedings of the 1st Joint Workshop on Information Security (JWIS2006), pp.347-360 (2006-09), 査読あり.
11. Maki Yoshida and Toru Fujiwara, ``On the Security of Tag-KEM for Signcryption,'' Proceedings of the 2nd Workshop on Cryptography for Ad hoc Networks (WCAN'06), Electronic Notes in Theoretical Computer Science 171, No.1, pp.83-91 (2006-07), 査読あり.

〔学会発表〕（計 10 件）

1. 鈴木 斎輝, 吉田 真紀, 藤原 融, ``汎用的結合可能な鍵交換の安全性検証法,'' 日本応用数理学会 2009 年春の研究部会連合発表会，数理的技法による情報セキュ

リティ(FAIS), (2009-03).
2. 鎌野 善樹, 鈴木 斎輝, 吉田 真紀, 藤原 融, ``暗号プロトコルに対する公理的安全性検証法の主要処理の改良と実装,'' 日本応用数理学会 2009 年春の研究部会連合発表会, 数理的技法による情報セキュリティ(FAIS), (2009-03).
3. 鈴木 斎輝, 吉田 真紀, 藤原 融, ``相互認証の汎用的結合可能な安全性の解析のための形式的手法,'' 2009年暗号と情報セキュリティシンポジウム予稿集, 4C2-4, CD-ROM (概要集 p.345) (2009-01).
4. 原村 和裕, 吉田 真紀, 藤原 融, ``コンテンツ事前配信における不正配布抑止力の強い匿名フィンガープリンティング,'' 2009 年暗号と情報セキュリティシンポジウム予稿集, 1B2-3, CD-ROM (概要集 p.39) (2009-01).
5. Maki Yoshida, Toru Fujiwara, and Marc Fossorier, ``Optimum General Threshold Secret Sharing,'' Proceedings of the 31th Symposium on Information Theory and Its Applications (SITA2008), CD-ROM (6 pages) (2008-10).
6. 冨士 由奈, 吉田 真紀, 藤原 融, ``カルテ情報自己管理のための墨塗り署名,'' 電子情報通信学会 2008 年総合大会, BS5-6, CD-ROM (2008-03).
7. 原村 和裕, 吉田 真紀, 藤原 融, ``利便性の高いコンテンツ事前配信のための匿名フィンガープリンティング,'' 2008年暗号と情報セキュリティシンポジウム予稿集, 1D1-4, CD-ROM (概要集 p.18) (2008-01).
8. 原村 和裕, 吉田 真紀, 藤原 融, ``コンテンツ事前配信のための匿名フィンガープリンティング,'' 電子情報通信学会技術研究報告 (ISEC2007-92), Vol.107, No.345, pp.23-30 (2007-11).
9. Maki Yoshida and Toru Fujiwara, ``Efficiency Analysis of the Nonlinear Function Ramp Secret Sharing Schemes,'' Proceedings of the 2007 Hawaii and SITA Joint Conference on Information Theory (HISC'07), Honolulu, Hawaii, CD-ROM (2007-05).
10. 浅野 順也, 岡村 真吾, 吉田 真紀, 藤原 融, ``C2C コンテンツ配信仲介サービスのための協調型非対称フィンガープリンティング,'' 2007年暗号と情報セキュリティシンポジウム予稿集, 1B2-3, CD-ROM (概要集 p.37) (2007-01).

６．研究組織

(1)研究代表者

吉田　真紀 (YOSHIDA MAKI)

大阪大学・大学院情報科学研究科・助教

研究者番号：50335387

(2)研究分担者

なし

(3)連携研究者

なし