様式 C-19

科学研究費補助金研究成果報告書

平成 22 年 5 月 28 日現在

研究種目：若手研究（B）
研究期間：2007～2009
課題番号：19700008
研究課題名（和文）情報理論的に安全性が保証される暗号・署名技術とその応用に関する研究

研究課題名（英文）Research on Encryption and Signatures with Information-theoretic Security and Their Application

研究代表者
四方　順司（SHIKATA　JUNJI）
横浜国立大学・大学院環境情報研究院・准教授
研究者番号：30345483

研究成果の概要（和文）：今日の情報化社会において、暗号・電子署名技術は情報セキュリティ技術の根幹を支える重要な技術である。将来の情報関連システムの安全性を考えると、たとえ時代の計算技術が発達しても、長期間安全性が保証できる暗号・電子署名技術を構築できることが理想的である。本研究では、そのような新たな暗号・署名及びその応用技術を開発することに成功した。本研究成果は、時代の計算技術に依存せず原理的に安全な暗号・署名及びその関連技術の構築に関するものであり、将来の社会の情報セキュリティ基盤技術の構築に大きく貢献することが期待される。

研究成果の概要（英文）：Today, cryptographic primitives such as encryption and digital signature schemes are fundamental and important to establish various and complex systems in the modern society of computers and networks. Considering security of the systems in the future, it is desirable to provide cryptographic primitives whose security can be guaranteed for a long time. In this research project, we successfully developed such cryptographic primitives concerning to encryption, signatures and their applications. Since our contribution lies in proposing new mechanisms of cryptographic primitives whose security does not depend on any computational model, we hope that our research results can contribute to the development of construction of security systems in the future.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	1,100,000	0	1,100,000
2008 年度	1,200,000	360,000	1,560,000
2009 年度	900,000	270,000	1,170,000
年度			
年度			
総　計	3,200,000	630,000	3,830,000

研究分野：暗号理論，情報セキュリティ，理論計算機科学，計算数論
科研費の分科・細目：情報学・情報学基礎
キーワード：情報セキュリティ，暗号理論，情報理論的安全性，暗号，ステガノグラフィ，認証，署名

１．研究開始当初の背景

今日の情報化社会において、暗号・電子署名技術はインターネット等を利用した様々なサービス（電子商取引等）の安全性を支え、多くの人々が安心して通信・契約等を行うための核となる技術である。現在は公開鍵暗号をはじめとする計算量理論的安全性に基づく暗号・署名技術及びその応用技術が普及しているが、将来の計算アルゴリズムの発展や新たな計算機技術の登場（量子計算機等）の可能性を考えると、時代の計算技術に依存せず原理的に安全な暗号・署名技術を開発することが重要である。このような技術の開発のアプローチとして、情報理論的安全性に基づく暗号・署名技術の提案があげられる。時代の計算技術に依存せず原理的に安全な暗号・署名及びその関連技術の構築方法が確立すれば、将来の社会の情報セキュリティ基盤技術の構築に大きく貢献することが期待される。

２．研究の目的

本研究の目的は、情報理論的立場から、暗号・署名技術およびその応用技術の安全性の概念の理論構築を行うと共に、その効率の良い実現方法を提案することである。具体的にいえば、本研究では次に挙げる内容に取り組んだ。

(1)情報理論的に安全性が保証される署名及び署名関連技術の研究：情報理論的に安全性が保証される署名及び署名関連技術を更に発展させるために、従来よりも効率的な署名の実現方法や、署名に関連する新たなシステム技術（グループ認証・署名システム、ブラインド認証・署名システム等）を開発する。新たなシステムを開発する際には、その数理モデル、安全性の定式化を適切に行い、そして実際にそれをみたす実現方法を提案する。また、効率的な実現方法を提案するにあたっては、ユーザが保持する秘密情報及び通信路を流れるデータサイズが少なくて済む実現方法を目指す。

(2)情報理論的に安全性が保証されるステガノグラフィの研究：従来の情報理論的安全性を有するステガノグラフィの理論研究を発展させるために、それに関するこれまでの数理モデルを整理し、その上で理論的立場から最強の安全性をもち、実用的といえる実現方法を提案する。

３．研究の方法

情報理論的安全性を有する各種システムの数理モデルの提案や安全性の定式化にあたっては、従来の情報理論的安全性を有するシステムのモデリング手法に加えて、（公開鍵暗号技術を代表とする）計算量理論的安全性を有するシステムの数理モデルの諸概念を、新たに情報理論の枠組みで表現する方法をとる。このことによって、強い安全性をもつ対象システムの数理モデル化、安全性の定式化を適切に行う。これまで、情報理論的安全性を有するシステムと計算量理論的安全性を有するシステムの構築理論は、基礎とする理論がそれぞれ異なることから両者は各々独自に発展してきたが、本研究では、上記のように柔軟に後者のモデルでの諸概念を前者に取り入れることで、前者の立場から安全性の定式化を目指し、それに基づいて構築理論を発展させることを目指す。このように、既に熟成した計算理論ベースの諸概念を横断的に情報理論的立場の定式化に取り入れる点が最も独創的な研究方法といえる。

４．研究成果　（成果・インパクト・展望）

上記の「研究の目的」に示した２つの項目に対して、それぞれの成果を記述する。

(1)情報理論的に安全性が保証される署名及び署名関連技術の研究成果：ブラインド認証符号を世界で初めて提案し、その数理モデル、安全性の定式化、構成法、そしてそれを利用したコミットメントの構成法に関する研究の集大成を査読有の論文集において発表した。また、情報理論的安全性を有するブラインド署名システムに対しても、数理モデル、安全性の定式化、構成法に関する先駆的成果を査読有の国際会議論文集にて発表した。これらの成果により、情報理論的安全性を有するブラインド認証及びブラインド署名システムは実現可能であることが初めて示され、その具体的実現方法も明らかになった。

そして、以下の認証・署名に関する成果は先駆的研究成果として国内会議で発表を行った。まず、情報理論的安全性を有する（鍵の漏洩に対して耐性のある）鍵更新型認証方式に関して、数理モデル、安全性の定式化を世界で初めて提案し、その最も効率的な構成法（最適構成法）を明らかにした。更にその拡張である鍵更新型署名方式の構成法も提案した。これらの成果により、秘密にすべき鍵情報が多少漏えいしても安全性が保たれ

る認証・署名方式が構成できたことになる。また一方で、情報理論的観点から、認証・署名技術に匿名性を汎用的に付与できる暗号基礎技術に関しても提案した。この匿名性を付与する技術は、将来のプライバシー保護の核となる技術として今後の更なる発展が期待される。

(2)情報理論的に安全性が保証されるステガノグラフィの研究成果：能動的攻撃を行う攻撃者に対して、情報理論的立場から安全性が保証されるステガノグラフィの数理モデル、安全性の概念とその定式化、そして構成法について、完成度の高い研究成果が得られた。これはこの分野で最も権威ある学術論文誌である IEEE 情報理論論文誌にて発表した。これにより、最強の安全性を有するステガノグラフィのモデルとその実現方法が明確になった。また、ステガノグラフィの安全性の定式化を Bhattacharyya Distance により与えた場合の有効性についても、論文誌 T. Data Hiding and Multimedia Security にて発表した。これら成果は、情報理論的安全性を有するステガノグラフィ理論の発展に大きく貢献したといえる。

以上の２つの項目に関する成果は、いずれも現在の「情報理論的に安全性が保証できる情報セキュリティ技術」の発展に大きく貢献しており、将来のセキュリティ基盤技術構築に貢献することが期待できる。

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 16 件）
①相河正，清藤武暢，四方順司，“情報理論的に安全な Key-Insulated 署名方式”，2010 年暗号と情報セキュリティシンポジウム論文集(CDROM)，3A1-4，2010，査読無.
②小林大樹，四方順司，“情報理論的安全性に基づいて匿名性・追跡性を付与するプリミティブの提案”，2010 年暗号と情報セキュリティシンポジウム論文集(CDROM)，2B4-3，2010，査読無.
③T. Seito, T. Aikawa, J. Shikata, T. Matsumoto, “Information-Theoretically Secure Key-Insulated Multireceiver Authentication Codes”，2010 年暗号と情報セキュリティシンポジウム論文集(CDROM)，2B2-4，2010，査読無.
④Y. Hara, T. Seito, J. Shikata, T. Matsumoto, “Unconditionally Secure Blind Signatures”, Information Theoretic Security, ICITS 2007 - Selected Papers, LNCS 4883, pp.23-43, Springer, December 2009，査読有.
⑤Y. Hara, T. Ishiwata, J. Shikata, T. Matsumoto, “Unconditionally Secure Blind Authentication Codes: The Model, Constructions, and Links to Commitment”, Formal to Practical Security, LNCS 5458, pp.116-137, Springer, May 2009，査読有.
⑥清藤武暢，四方順司，松本勉，“メンバーの秘密鍵を無効化できる情報理論的に安全な署名方式について”，2009 年暗号と情報セキュリティシンポジウム論文集(CDROM)，3B3-3，2009，査読無.
⑦ Junji Shikata, Tsutomu Matsumoto, “Unconditionally Secure Steganography Against Active Attacks”, IEEE Transactions on Information Theory 54(6), pp.2690-2705, June 2008，査読有.
⑧Valery I. Korzhik, Hideki Imai, Junji Shikata, Guillermo Morales-Luna, Ekaterina Gerling, “On the Use of Bhattacharyya Distance as a Measure of the Detectability of Steganographic Systems”, T. Data Hiding and Multimedia Security 3, Springer, pp.23-32, Jan. 2008，査読有.
⑨清藤武暢，二井将太，四方順司，松本勉，メンバーの秘密鍵を無効化できる情報理論的に安全な認証方式について，2008 年暗号と情報セキュリティシンポジウム論文集(CDROM)，1E1-5，2008，査読無.

〔学会発表〕（計 13 件）
①相河正，清藤武暢，四方順司，情報理論的に安全な Key-Insulated 署名方式，2010 年暗号と情報セキュリティシンポジウム，2010 年 1 月 21 日，サンポートホール高松（香川県）.
②清藤武暢，四方順司，松本勉，Information-theoretically Secure Key-Insulated Multireceiver Authentication Codes，2010 年暗号と情報セキュリティシンポジウム，2010 年 1 月 20 日，サンポートホール高松（香川県）.
③小林大樹，四方順司，情報理論的安全性に基づいて匿名性・追跡性を付与するプリミティブの提案，2010 年暗号と情報セキュリティシンポジウム，2010 年 1 月 20 日，サンポートホール高松（香川県）.
④清藤武暢，四方順司，松本勉，メンバーの秘密鍵を無効化できる情報理論的に安全な署名方式について，2009 年暗号と情報セキュリティシンポジウム，2009 年 1 月 22 日，滋賀県大津.
⑤清藤武暢，四方順司，松本勉，メンバーの秘密鍵を無効化できる情報理論的に安全な認証方式について，2008 年暗号と情報セキュリティシンポジウム，2008 年 1 月 22 日，宮崎.

⑥Junji Shikata, Construction Methodology of Unconditionally Secure Signature Schemes, International Conference on Information Theoretic Security (ICITS 2007), May 26, 2007, Madrid, Spain.
⑦ Y. Hara, T. Seito, J. Shikata, T. Matsumoto, Unconditionally Secure Blind Signatures, International Conference on Information Theoretic Security (ICITS 2007), May 25, 2007, Madrid, Spain.

〔その他〕
ホームページ等
(1)http://er-web.jmk.ynu.ac.jp/html/SHIKATA_Junji/ja.html

(2)http://ipsr.ynu.ac.jp/

６．研究組織
(1)研究代表者
四方　順司（SHIKATA　JUNJI）
横浜国立大学・大学院環境情報研究院・
准教授
研究者番号：30345483