科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　６　日現在

機関番号：　１２７０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５０００１２

研究課題名（和文）情報理論的結合可能安全性を有する暗号基礎技術の研究

研究課題名（英文）Research on Information-Theoretically Composable Security for Cryptographic Primitives

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

交付決定額（研究期間全体）：（直接経費）　　3,800,000円、（間接経費）　　1,140,000円

研究成果の概要（和文）：本研究では情報理論的結合可能安全性を有する暗号基礎技術に関する理論研究を行った。ここで情報理論的結合可能安全性は、時代の計算技術に依存せず原理的に安全であると言える安全性で、複数のシステムとも自由に組み合わせ可能な高い安全性である。主要な研究成果は、暗号基礎技術（暗号化、鍵共有、認証）に対して、従来の情報理論的安全性と情報理論的結合可能安全性が本質的に同値であることを理論的に示せた点である。本成果は、暗号理論分野における学術的重要性だけに留まらず、多様で複雑な情報システムを構成する際、情報理論的に安全な基礎技術を自由に組み合わせても良いことを示しており実用的観点からも意義は大きいと考えられる。

研究成果の概要（英文）：In this research project, we studied cryptographic primitives having information-theoretic composable security. Here, information-theoretic composable security implies the strong security which does not depend on any computational model, and cryptographic primitives having such a security can be composed with other ones without losing their security. The main contribution of this research is to show the essential equivalence of information-theoretic composable security and traditional information-theoretic security for cryptographic primitives such as encryption, key-agreement, and authentication codes. This result means that the cryptographic primitives having traditional information-theoretic security can be composed with other ones without losing security in various and complicated systems in information society, and therefore, our results are considered to be important not only from an theoretical aspect but also from a practical viewpoint.

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：　暗号・認証等　暗号理論　情報理論的安全性　結合可能安全性　情報セキュリティ

１．研究開始当初の背景

近年、インターネットを利用した電子市場が急激に拡大している。それらに伴い、電子商取引を安全に実現するための暗号技術の重要性は非常に高くなっている。特に公開鍵暗号は広く用いられており、現在の実用的なほとんどすべての公開鍵暗号の安全性は、素因数分解問題の困難性、あるいは（楕円曲線上の）離散対数問題の困難性に依存している。ところが、近年の計算機技術の発達、ネットワークの拡大、アルゴリズムの高速化により、十分な安全性を確保するために必要とされる暗号システムの鍵サイズは年々急速な勢いで大きくなっている。このように、公開鍵暗号の鍵長は今後も何年かごとに見直され、同じ鍵サイズで長期にわたって安全性を保証することは困難である。さらに重要なことには、仮に、近い将来、量子計算機が実現された場合、素因数分解問題や離散対数問題は高速に（多項式時間で）解けることが理論的に報告されている。これらの経緯から将来のことを考えると、暗号基礎技術の研究において、計算技術の発達、ネットワークの拡大、アルゴリズムの高速化、更には量子計算機のような新しい技術の登場に対しても十分な安全性を確保できるような暗号基礎技術の研究開発は重要である。これを満たす技術として、情報理論的安全性に基づく暗号基礎技術の提案があげられる。ここで、情報理論的に安全性が保証される技術とは、文字通りその安全性が情報理論の立場から完全に保証される技術を意味し、素因数分解問題等の、いかなる計算困難な数学的問題に依拠しない形で、原理的に安全であると言える技術である。

また、一方で、インターネットやPC・モバイル端末で利用されている現在のセキュリティシステムは、多くの暗号基礎技術を組み合わせて実現されている。2000年より前の暗号研究においては、各暗号技術の安全性としてそれ単体で使用する場合の安全性だけを考えていたが、2000年以降はカネッティ（Canetti）を含む多くの研究者により、暗号基礎技術はそれ単体で使用する環境下の安全性だけでなく、他の基礎技術と自由に組み合わせて利用する環境下においても、システムに脆弱性が生じない安全性の定義（以下、結合可能安全性とよぶ）が要求されている。特に、暗号基礎技術は、多様で複雑な情報システム構築の際に、様々な形で自由に組み合わせて利用することが想定されるため、結合可能安全性をもつように設計されることが理想的である。

２．研究の目的

本研究の目的は、数学的な計算問題の困難性に依拠せず、多様で複雑なシステムにも自由に組み込める高い安全性を実現するため、情報理論的結合可能安全性を有する暗号基礎技術の研究を発展させることである。本研究で目標とする情報理論的結合可能安全性を有する暗号基礎技術は、時代の計算技術に依存せず原理的に安全であると言える技術であるだけでなく、多様で複雑なシステムにも自由に組み込める高い安全性を有する。これは学術的にも実用的にも意義のある技術といえる。

上記の目的を達成するため、本研究の核となるのは以下の理論的成果を示すことにある。（１）主要な暗号基礎技術（暗号化、鍵共有、認証等）に対して、情報理論的結合可能安全性を数理的立場から適切に定式化すること、（２）主要な暗号基礎技術に対して、情報理論的結合可能安全性の定式化と従来の情報理論的安全性の定式化との差を理論的に明らかにすること、（３）もしも両者の定式化に差があるならば、情報理論的結合可能安全性をみたす新たな構築法を提案すること、である。

また、実用性の立場から、情報理論的結合可能安全性をみたす暗号基礎技術の構築法の有用性を評価することも重要である。この評価には、机上の理論的評価と、実装実験による評価が挙げられる。特に、情報理論的結合可能安全性が従来の情報理論的安全性より真に強い安全性である場合、前者の安全性を有する暗号技術の構築法は、後者の安全性を有する暗号技術の構築法よりも非効率的になるはずである（秘密鍵の鍵長が長くなる等）。したがって、その非効率性の度合いを正確に評価する必要がある。

３．研究の方法

主要な暗号基礎技術（暗号化、鍵共有、認証）に対して、情報理論的結合可能安全性を数理的に定式化するにあたっては、従来の情報理論的安全性の定式化手法で用いられているメトリックを利用することに加えて、（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結合可能安全性に関する諸概念を、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、情報理論的立場から、結合可能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、既存の計算量理論ベースの結合可能安全性概念を上記のように柔軟に情報理論的暗号理論に取り入れることで、情報理論的結合可能安全性の理論を発展させることを目指す。このように、既に熟成した計算量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。その後は、情報理論的手法あるいは数学的手法を用いて、情報理論的結合可能安全性の定式化と従来の情報理論的安全性の定式化との関係性を数理科学的に明らかにする。

４．研究成果

研究期間全体を通して、暗号基礎技術、特に、暗号化方式、鍵共有方式、メッセージ認証方式（認証符号）に対して、従来の情報理論的安全性と情報理論的結合可能安全性の関係を理論的に示すことができた。

まず、暗号化方式および鍵共有方式においては、用いる情報理論的指標やメトリック（具体的には相互情報量、統計的距離等）によって僅かな差はあるものの、本質的には、従来の情報理論的安全性と情報理論的結合可能安全性は同値であることを示した。このことは、対象の暗号化方式において復号誤りが生じる場合や、暗号化アルゴリズムまたは復号アルゴリズムが確率的アルゴリズムの場合にも適用でき、広範の暗号化方式に対して示されている。また、上記の同値性は、対象の鍵共有方式において共有鍵の一致誤りが生じる場合や、エンティティ間の通信路が一方向又は双方向である場合、ラウンド数が任意の場合すべてに適用可能であり、広範の鍵共有方式に対して示されている。これらに関する成果は、当初、国内会議 SCIS2012 において発表し、次いで国際暗号学会（IACR）のアーカイブによって世界中に広く公表し、それから査読有の国際会議 IEEE ISIT2013 において論文発表を行った。今後は、当該分野において世界的に権威ある論文誌に投稿したいと考えている。

また、メッセージ認証方式（認証符号）においては、従来の情報理論的安全性と情報理論的結合可能安全性は全く同値であることを示した。特別な認証符号の場合（認証子生成アルゴリズムが決定的な場合）には、他の研究者により既に発表されているが、必ずしもそうとは限らない一般の場合に対して示した点に新規性がある。この成果は、国内会議 SCIS2014 における発表内容の一部になっている。今後は、SCIS2014 の成果を更に発展させた成果を査読有の国際会議および論文誌に投稿したいと考えている。

一方、実用的な観点から、もしも情報理論的結合可能安全性と従来の情報理論的安全性の間に本質的な差異がある場合は、情報理論的結合可能安全性をみたす暗号基礎技術の構築方法に対して、当初は、机上の理論的評価と実装実験による評価を行うことを重視していた。しかしながら、上記に記述したように両者の安全性は本質的に同値であることが判明したため、従来から既知の情報理論的安全性をみたす構築方法は、情報理論的結合可能安全性をも有し、それら構築方法の効率性（鍵長等）は既に評価されているため、本研究において、再び、効率性（鍵長等）の評価を行うことを重視はしなかった。

更に、当初の研究目的である上記の情報理論的結合可能安全性に関する成果に加えて、従来の情報理論的暗号理論を拡張するため、Renyi エントロピーを利用した体系的枠組みを提案し、この成果を国内会議 SCIS2013，SCIS2014，査読有の国際会議 ICITS2013 において発表した。この体系的枠組みの中で情報理論的結合可能安全性をどれだけ一般的に扱えるかについては、今後の研究活動の中で明らかにしてゆきたい。

以上の研究成果は、暗号理論分野における学術的重要性だけに留まらず、多様で複雑な情報システムであふれる現在あるいは未来の情報社会において、その構成要素となる暗号基礎技術を自由に組み合わせても情報理論的安全性を実現できることを明確に示しており、実用的観点からもその意義は大きいと考える。

５．主な発表論文等

〔雑誌論文〕（計 18 件）

① J. Shikata, “Revisiting Information Theoretically Secure Authentication Codes by Conditional Renyi Entropies”, Proc. of the 31th Symposium on Cryptography and Information Security (SCIS2014), Jan. 2014, 1E2-2 (CDROM). 査読無.

② M. Iwamoto and J. Shikata, “Optimal Constructions for Information Theoretically Secure Encryptions Based on Renyi Entropies”, Proc. of the 31th Symposium on Cryptography and Information Security (SCIS2014), Jan. 2014, 1E2-3(CDROM). 査読無.

③ M. Iwamoto and J. Shikata, “Information Theoretic Security for Encryption Based on Conditional Renyi Entropies”, Proc. of the 7th International Conference on Information Theoretic Security (ICITS2013), LNCS 8317, pp.103-121, Springer, November 2013. 査読有. The full version is available at http://eprint.iacr.org/2013/440

④ A. Kubai, J. Shikata, Y. Watanabe, “Information Theoretically Secure Aggregate Authentication Code: Model, Bounds, and Constructions”, Proc. of CD-ARES 2013 Workshops, LNCS 8128, pp.16-28, Springer, September 2013. 査読有.

⑤ J. Shikata, “Formalization of Information Theoretic Security for Key-Agreement, Revisited”, Proc. of 2013 IEEE International Symposium on Information Theory (ISIT2013), pp.2720-2724, July 2013. 査読有. Full version is available at http://eprint.iacr.org/2012/383

⑥ M. Iwamoto and J. Shikata, “Revisiting Conditional Renyi Entropy and its Application to Encryption: Part I - Properties of Conditional Renyi Entropy-”, Proc. of the 30th Symposium on Cryptography and Information Security (SCIS2013), Jan. 2013, 1F1-3 (CDROM). 査読無.

⑦ J. Shikata and M. Iwamoto, “Revisiting Conditional Renyi Entropy and its Application to Encryption: Part II -Fano's Inequality and Shannon's Bound-”, Proc. of the 30th Symposium on Cryptography and Information Security (SCIS2013), Jan. 2013, 1F1-4 (CDROM). **査読無**

⑧ Y. Watanabe, T. Seito and J. Shikata, “Information Theoretic Timed-Release Security: Key-Agreement, Encryption and Authentication Codes”, Proc. of the 6th International Conference on Information Theoretic Security (ICITS2012), LNCS 7412, pp. 167–186, Springer, August 2012. **査読有**. Full version is available at http://eprint.iacr.org/2012/460

⑨ **四方順司**, “**情報理論的安全性の定式化の再考：暗号化と鍵共有方式**”, **暗号と情報セキュリティシンポジウム** (SCIS2012) **論文集**（CDROM）, Jan. 2012. **査読無**.

⑩ J. Shikata and D. Yamanaka, “Bit Commitment in the Bounded Storage Model: Tight Bound and Simple Optimal Construction”, Proc. of the 13th IMA International Conference, Cryptography and Coding (IMACC2011), LNCS 7089, pp.112-131, Springer, December 2011. **査読有**.

⑪ T. Seito and J. Shikata, “Information Theoretically Secure Key-Insulated Key Agreement”, Proc. of 2011 IEEE Information Theory Workshop (ITW2011), Oct. 2011, pp. 287 – 291. **査読有**.

〔学会発表〕（計 19 件）

① **四方順司，“情報理論的暗号理論について～サーベイとチャレンジ～”，電子情報通信学会 ISEC-IT-WBS 合同研究会，名古屋，2014 年 3 月（招待講演）．**

② J. Shikata, “Revisiting Information Theoretically Secure Authentication Codes by Conditional Renyi Entropies”, The 31th Symposium on Cryptography and Information Security (SCIS2014), Kagoshima, Japan, Jan. 2014.

③ M. Iwamoto and J. Shikata, “Optimal Constructions for Information Theoretically Secure Encryptions Based on Renyi Entropies”, The 31th Symposium on Cryptography and Information Security (SCIS2014), Kagoshima, Japan, Jan. 2014.

④ M. Iwamoto and J. Shikata, “Information Theoretic Security for Encryption Based on Conditional Renyi Entropies”, The 7th International Conference on Information Theoretic Security (ICITS2013), Singapore, November 2013.

⑤ A. Kubai, J. Shikata, Y. Watanabe, “Information-Theoretically Secure Aggregate Authentication Code: Model, Bounds, and Constructions”, CD-ARES 2013 Workshops, Regensburg, Germany, September 2-6, 2013.

⑥ J. Shikata, “Formalization of Information Theoretic Security for Key-Agreement, Revisited”, 2013 IEEE International Symposium on Information Theory (ISIT2013), Istanbul, Turkey, July 2013.

⑦ M. Iwamoto and J. Shikata, “Revisiting Conditional Renyi Entropy and its Application to Encryption: Part I -Properties of Conditional Renyi Entropy-”, The 30th Symposium on Cryptography and Information Security (SCIS2013), Kyoto, Japan, Jan. 2013.

⑧ J. Shikata and M. Iwamoto, “Revisiting Conditional Renyi Entropy and its Application to Encryption: Part II -Fano's Inequality and Shannon's Bound-”, The 30th Symposium on Cryptography and Information Security (SCIS2013), Kyoto, Japan, Jan. 2013.

⑨ Y. Watanabe, T. Seito and J. Shikata, “Information-Theoretic Timed-Release Security: Key-Agreement, Encryption and Authentication Codes”, The 6th International Conference on Information Theoretic Security (ICITS2012), Montreal, Canada, August 2012.

⑩ **四方順司**, “**情報理論的安全性の定式化の再考：暗号化と鍵共有方式**”, **暗号と情報セキュリティシンポジウム** 2012 (SCIS2012), **金沢**, Jan.30-Feb.3, 2012.

⑪ T. Seito and J. Shikata, “Information-theoretically Secure Key-Insulated Key Agreement ”, 2011 IEEE Information Theory Workshop (ITW2011), Brazil, Oct. 2011.

⑫ J. Shikata and D. Yamanaka, “Bit Commitment in the Bounded Storage Model: Tight Bound and Simple Optimal Construction”, The 13th IMA International Conference, Cryptography and Coding (IMACC2011), Oxford, UK, December 2011.

〔その他〕

ホームページ等

(1) http://www.slab.ynu.ac.jp/index.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

(2) 連携研究者

松本　勉（MATSUMOTO TSUTOMU）
横浜国立大学・大学院環境情報研究院・教授
研究者番号：40183107