様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　２１　日現在

機関番号：　１２７０１
研究種目：　挑戦的萌芽研究
研究期間：　2014～2016
課題番号：　２６５４００５６

研究課題名（和文）公開鍵暗号メカニズムと情報量的安全性構築メカニズムの共存と限界に関する研究

研究課題名（英文）Research on Coexistence of Computational and Information-Theoretic Security Mechanisms for Long-term Security

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・教授

研究者番号：３０３４５４８３

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：高機能暗号の危殆化に備えて、計算量的安全性と情報量的安全性の高機能性がそれぞれどのような数理構造に基づいているのか明らかにすることで、両安全性の共存可能性を解析した。なお、その高機能性には、タイムリリース機能、無効化機能、検索機能等が含まれる。また、上記の数理構造の解析から、公開鍵暗号メカニズムが危殆化した場合でも、情報量的安全性だけでセキュリティ機能をそのまま保つ構造は、ある種の追加の仮定がなければ実現困難であるという知見も得られた。

研究成果の概要（英文）：In this research project, we investigated (im)possibility of coexistence of computational and information-theoretic security for advanced cryptographic systems with long-term security. Our approach is to analyze various computational or information-theoretic advanced functionalities in cryptographic systems by means of several mathematical structures, and such advanced functionalities include timed-release functionality, revocable functionality, and searchable functionality. In addition, the analysis results tell us that, in a cryptographic system in which computational and information-theoretic security coexist, it seems to be difficult to maintain long-term security only by information-theoretic security without any additional assumption if computational security is compromised.

研究分野：　暗号理論

キーワード：　暗号理論　情報量的安全性　高機能暗号　長期的安全性　暗号・認証等

１．研究開始当初の背景

近年、インターネットの利用は世界的規模で展開され、現在も更に拡大している。それに伴い、電子商取引等を安全に実現するため暗号基礎技術の利用は必要不可欠であり、特に公開鍵暗号は世界中で広く利用されている有用な暗号技術である。公開鍵暗号メカニズムの最大の利点は、2 者間のセキュア通信において、一方の鍵を公開できることにある。例えば、暗号化方式においては暗号化鍵を公開でき、ディジタル署名方式においては検証鍵を公開できる。これにより、世界中のユーザらはユーザ間で事前に秘密鍵を共有することなくセキュア通信を行える。しかしながら、公開鍵暗号メカニズムの安全性は数学的問題の計算困難性（素因数分解問題等）に依存しており、この安全性は計算量的安全性とよばれている。従って、計算機技術の発達、アルゴリズムの高速化等により計算困難性を確保するため公開鍵暗号メカニズムの鍵長は今後も何年かごとに見直され、同じシステムパラメータで長期にわたって安全性を保証することは困難である。更には、量子コンピュータ等の新しい計算技術が実用化されれば現存するほとんどの公開鍵暗号は崩壊してしまうことも知られている。これらの問題は「公開鍵暗号の危殆化問題」ともよばれ、公開鍵暗号メカニズムだけでは長期の安全性を実現することは困難である。

２．研究の目的

本研究の目的は、公開鍵暗号の危殆化問題に対する実現可能な本質的解決法を求めて、現存の公開鍵暗号メカニズム（計算量的安全性）を基盤にして長期間の高い安全性をどれだけ達成し得るかのメカニズムを解明することである。具体的には、研究期間内に以下の研究課題に取り組むことを目的としていた。

(ア) 公開鍵暗号メカニズムと情報量的安全性構築メカニズムを共存させることにより、公開鍵暗号メカニズムが危殆化したときにも重要なセキュリティ機能を保てる高機能暗号の仕組み及びその実現可能性（または不可能性）を解明する。

(イ) さらに可能であれば、計算量的安全性から情報量的安全性への暗号学的移行メカニズムを探求する。

ここで、情報量的安全性とは、情報理論の創始者シャノン（C. Shannon）によって発見された安全性の概念であり、文字通りその安全性が情報理論または確率論の立場から定式化され、それは素因数分解問題等、如何なる計算困難な数学的問題に依拠しない形で、時代の計算技術とは無関係に保証できる安全性概念である。

３．研究の方法

通常、システム内に計算量的安全性と情報量的安全性が共存する場合、複数の安全性（セキュリティ）要件がそのシステムに求められ、かつ、各安全性要件が計算量的安全性または情報量的安全性の構築技術により実現されている。このことから、高機能暗号技術において、計算量的安全性と情報量的安全性の高機能性がそれぞれどのような数理構造に基づいているのか明らかにすることで、両安全性の共存可能性（あるいは不可能性）を解析することにした。さらに、幅広く高機能性を解析することで、計算量的安全性と情報量的安全性を構築可能な体系を俯瞰的にみることにより、研究目的で記述した（ア）（イ）の解決に繋がる成果を得ることを目指した。

４．研究成果

本研究成果として、広範に計算量的安全性と情報量的安全性それぞれの高機能性が、どのような数理構造から実現できるかに関して、多くの様々な成果を得ることができた。具体的には、高機能性として、タイムリリース機能（論文①,⑦,⑭,⑮）、無効化機能（論文②,⑤,⑫）、検索機能（論文③,④,⑥,⑩,⑪）、鍵隔離機能（論文⑨）、アグリゲーション機能（論文⑧）、匿名化機能（論文⑬）を実現可能な数理構造を示し、これらの研究成果を国内外の学会または論文誌で発表した。

さらに、上記の各種実現可能な高機能性の数理構造を解析してみると、公開鍵暗号メカニズム自体が危殆化したときにでも、情報量的安全性だけでセキュリティ機能をそのまま保つ構造は、ある種の追加の仮定がなければ実現困難であるという知見も得ている。今後の研究活動では、どのような合理的かつ実用上自然な仮定があれば、そのような構造を実現可能なのかを解明して行きたい。また、そのような構造を実現することは、暗号学的移行メカニズムを探求するという課題の解にも繋がると考えられるため、このテーマに関しても今後の研究活動で解明して行きたいと考えている。

５．主な発表論文等

〔雑誌論文〕（計 15 件）

① Y. Watanabe and J. Shikata, “Timed-Release Computational Secret Sharing Scheme and Threshold Encryption”, Designs, Codes and Cryptography, 2017.（To appear）（査読有）

② Y. Ishida, J. Shikata, and Y. Watanabe, “CCA-secure Revocable Identity-based Encryption Schemes with Decryption Key Exposure Resistance," International Journal on Applied Cryptography (IJACT), 2017. (To appear)（査読有）

③ T. Yoshizawa, Y. Watanabe, and J. Shikata, “Unconditionally Secure Searchable Encryption”, Proc. of The

51st Annual Conference on Information Systems and Sciences (CISS 2017), IEEE Xplore, March 2017. **（査読有）**

④ **吉澤貴博, 渡邉洋平, 四方順司, “推測秘匿性に基づく情報理論的に安全な検索可能暗号”, 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017)論文集, 1D1-4, 2017 年 1 月. （査読無）**

⑤ Y. Watanabe, G. Hanaoka, and J. Shikata, “Unconditionally Secure Revocable Storage: Tight Bounds, Optimal Construction, and Robustness”, Information Theoretic Security, LNCS 10015, pp.213-237, Springer, November 2016. **（査読有）**

⑥ **吉澤貴博, 渡邉洋平, 四方順司, “情報理論的に安全な検索可能暗号の構成法について”, コンピュータセキュリティシンポジウム 2016 (CSS2016)論文集, 2C3-2, 2016 年 10 月. （査読無）**

⑦ Y. Watanabe and J. Shikata, “Information-Theoretically Secure Timed-Release Secret Sharing Schemes," Journal of Information Processing, Vol.24, No.4, pp.680-689, July 2016. **（査読有）**

⑧ S. Tomita, Y. Watanabe, and J. Shikata, “Sequential Aggregate Authentication Codes with Information Theoretic Security,” Proc. of 50th Annual Conference on Information Sciences and Systems (CISS 2016), pp. 192-197, IEEE Xplore, March 2016,. **（査読有）**

⑨ Y. Watanabe and J. Shikata, “Identity-based Hierarchical Key-insulated Encryption without Random Oracles," Public-Key Cryptography (PKC 2016), LNCS 9614, pp. 255-279, Springer, March 2016.

⑩ **吉澤貴博, 渡邉洋平, 四方順司, “情報理論的安全性を持つ検索可能暗号の一般的モデルとその構成法,”暗号と情報セキュリティシンポジウム 2016 (SCIS 2016)論文集, 2A1-3, 2016 年 1 月. （査読無）**

⑪ **吉澤貴博, 渡邉洋平, 四方順司, “情報理論的に安全な検索可能暗号,”コンピュータセキュリティシンポジウム 2015 (CSS 2015)論文集, 3C4-4, 2015 年 10 月. （査読無）**

⑫ Y. Ishida, Y. Watanabe, and J. Shikata, “Constructions of CCA-secure Revocable Identity-based Encryption”, Information Security and Privacy, LNCS 9144, pp. 174-191, Springer, June 2015. **（査読有）**

⑬ N. Takei, Y. Watanabe, and J. Shikata, “Information-Theoretically Secure Blind Authentication Codes without Verifier's Secret Keys”, Statistical Science and Related Topics, Josai Mathematical Monograph, vol. 8, pp. 115-133, January 2015. **（査読有）**

⑭ Y. Watanabe and J. Shikata, “Timed-Release Secret Sharing Schemes with Information-Theoretic Security”, Cryptography and Information Security in the Balkans (BalkanCryptSec2014), LNCS 9024, pp. 219-236, Springer, 2015. **（査読有）**

⑮ Y. Watanabe and J. Shikata, “Timed-Release Computational Secret Sharing Scheme and Its Applications”, Proc. of the 8th International Conference on Provable Security (ProvSec 2014), LNCS 8782, pp.326-333, Springer, October 2014. **（査読有）**

〔学会発表〕（計 12 件）

① T. Yoshizawa, Y. Watanabe, and J. Shikata, “Unconditionally Secure Searchable Encryption”, The 51st Annual Conference on Information Systems and Sciences (CISS 2017), Baltimore, Maryland, USA, March 2017.

② **吉澤貴博, 渡邉洋平, 四方順司, “推測秘匿性に基づく情報理論的に安全な検索可能暗号”, 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017), 1D1-4, 沖縄, 日本, 2017 年 1 月.**

③ **吉澤貴博, 渡邉洋平, 四方順司, “情報理論的に安全な検索可能暗号の構成法について”, コンピュータセキュリティシンポジウム 2016 (CSS2016), 2C3-2, 秋田, 2016 年 10 月.**

④ Y. Watanabe, G. Hanaoka, and J. Shikata, “Unconditionally Secure Revocable Storage: Tight Bounds, Optimal Construction, and Robustness”, The 9th International Conference on Information Theoretic Security (ICITS 2016), Tacoma, Washington, USA, August 2016.

⑤ S. Tomita, Y. Watanabe, and J. Shikata, “Sequential Aggregate Authentication Codes with Information Theoretic Security,” The 50th Annual Conference on Information Sciences and Systems (CISS 2016), Princeton, USA, March 2016.

⑥ Y. Watanabe and J. Shikata, “Identity-based Hierarchical Key-insulated Encryption without Random Oracles," 19th International Conference on the Theory and Practice

of Public-Key Cryptography (PKC 2016), Tapei, Taiwan, March 2016.

⑦ **吉澤貴博，渡邉洋平，四方順司，“情報理論的安全性を持つ検索可能暗号の一般的モデルとその構成法，”暗号と情報セキュリティシンポジウム** 2016 (SCIS 2016)，2A1-3，**熊本，日本，**2016 **年** 1 **月.**

⑧ **吉澤貴博，渡邉洋平，四方順司，“情報理論的に安全な検索可能暗号，”コンピュータセキュリティシンポジウム** 2015 (CSS 2015)，3C4-4，**長崎，日本，**2015 **年** 10 **月.**

⑨ Y. Ishida, Y. Watanabe, and J. Shikata, “Constructions of CCA-secure Revocable Identity-based Encryption”, 20th Australasian Conference on Information Security and Privacy (ACISP 2015), Brisbane, Australia, June 2015

⑩ **四方順司**, “ Information-Theoretically Secure Blind Authentication Codes without Verifier's Secret Keys ”, **城西大学ワークショップ** Annual Workshop on Statistical Science and Related Topics, 2014 **年** 12 **月（招待講演）**.

⑪ Y. Watanabe and J. Shikata, “Timed-Release Secret Sharing Schemes with Information-Theoretic Security”, Cryptography and Information Security in the Balkans (BalkanCryptSec 2014), Istanbul, Turkey, October 2014.

⑫ Y. Watanabe and J. Shikata, “Timed-Release Computational Secret Sharing Scheme and Its Applications”, 8th International Conference on Provable Security (ProvSec 2014), Hong Kong, China, October 2014.

〔その他〕
ホームページ等
http://www.slab.ynu.ac.jp/index.html

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・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