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　３０　年　　６　月　２０　日現在

機関番号：　１２７０１
研究種目：　基盤研究(B)（一般）
研究期間：　2015～2017
課題番号：　１５Ｈ０２７１０

研究課題名（和文）情報理論的暗号理論における統一的パラダイムの構築とその応用

研究課題名（英文）A Unified Paradigm in Information Theoretic Cryptography and Its Applications

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）　　13,900,000円

研究成果の概要（和文）：暗号理論や情報理論に跨る多様な安全性概念を俯瞰的かつ体系的に扱うことのできる統一的パラダイムを研究した。計算量的安全性概念、情報理論的安全性概念を様々な角度から俯瞰的にみることで、様々な安全性概念の定式化、システム構成法及びそれらの関係性を明らかにした。特に、操作的意味付けのある様々な安全性概念を情報理論的観点から定式化し、従来の安全性概念も含めて、安全性概念間の関係性を示した。また、偏りのある分布の秘密鍵や乱数による情報理論的安全性の実現性や効率性の限界を示した。さらに、本パラダイムにより、様々な高機能暗号やプロトコルの安全性定式化や構成法に関する新たな成果を得た。

研究成果の概要（英文）：In this research project, we studied a unified paradigm in information theoretic cryptography which can deal with various security notions in cryptography and information theory from systematic and bird's-eye viewpoints. By overlooking security notions of computational security and information-theoretic security from various aspects, we showed new formalizations of security, construction of cryptographic systems, and their relationships. In particular, we formalized various security notions of encryption and key agreement which have meaningful operations, and showed relationships among security formalizations including the existing ones. We also showed (im)possibility of information theoretic security for encryption, authentication and secret sharing only from biased randomness. Furthermore, as applications of this paradigm, we showed new security formalizations and/or new construction methodology for advanced cryptographic systems.

研究分野：　暗号理論

キーワード：　暗号理論　情報理論　情報理論的安全性　暗号　鍵共有　認証

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、今日、電子商取引等におけるセキュア通信や安全な情報処理技術実現のため暗号基礎技術の利用は必要不可欠である。暗号技術の中でも公開鍵暗号は世界中で広く利用されており、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、素因数分解問題または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等により、十分な安全性を確保するために必要な鍵長は年々急速な勢いで大きくなっており、長期的安全性が保証されるべき電子データに関しては、現存の公開鍵暗号技術を利用するのは好ましくない（暗号技術の危殆化問題）。さらに重要なことには、近い将来、量子計算機が実現されれば、素因数分解問題や離散対数問題は高速に解けることが理論的に示されており、現存するほとんどすべての公開鍵暗号は崩壊してしまう。以上より、暗号理論研究において、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全く新しい計算技術の登場に対しても十分な安全性を確保できるメカニズムは非常に重要である。このためのアプローチとして、情報理論的安全性に基づく暗号技術の提案があげられる。ここで、情報理論的安全性とは、文字通りその安全性が情報理論または確率統計論の立場から定式化される安全性概念を意味し、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、原理的に安全であると言える安全性概念である。

２．研究の目的

現在の多くの暗号技術は計算困難な数学的問題に基づいて設計されている。一方、計算困難な問題に依拠しない形で、原理的に安全といえる強固な安全性として情報理論的安全性がある。従来の情報理論的安全性には、その定式化において暗号学的観点からの操作的意味づけが不明確である場合や、安全性と効率性の限界・それらのトレードオフが理論的に不明確である場合が多い。本研究では、暗号理論と情報理論に跨る多様な安全性概念を俯瞰的かつ体系的に扱うことのできる統一的パラダイムを構築することを目的とする。これにより、暗号学的に明確な操作的意味づけをもつ階層的な情報理論的安全性指標の導入、安全性と効率性の限界・それらのトレードオフの明確化、幅広いシステム構成法の展開が可能になる。従って、本研究は当該理論を更に飛躍的に発展させるための基礎研究である。

３．研究の方法

本研究の目的は、暗号学的立場から操作的意味づけが明確であり、多様かつ階層的な安全性を定義できる情報理論的安全性指標を適切に定義し、それら多様な安全性と効率性の限界やトレードオフを理論的に示すことができるような、情報理論的暗号理論における新たな統一的枠組み（パラダイム）を構築することである。そのための研究方法として、具体的には、次の理論研究および応用研究に取り組んだ。

- 理論研究：暗号化、鍵共有、認証等の暗号基礎技術を対象として、多様かつ適切な安全性指標（安全性の定式化）を新たに導入する。達成できる安全性の限界及び効率性とのトレードオフ等を理論的に明らかにする。その限界を達成する構成法を研究開発する。
- 応用研究：得られた理論的成果を様々な応用技術に生かす、またはその効果的な応用先（応用するシナリオ）の技術研究を行う。具体的には、計算量的安全性をもつ暗号技術構成への応用、長期間の安全性が必要とされる暗号技術への応用、実用性の観点からの計算機実装実験による解析等を行う。

４．研究成果

情報理論的暗号理論における統一的枠組み（パラダイム）の観点から、暗号理論における計算量的安全性概念、情報理論における情報理論的安全性概念を様々な角度から俯瞰的にみることで、暗号化方式、鍵共有方式、認証方式、秘密分散法等に対して、様々な安全性概念の定式化、効率的なシステム構成法、及びそれらの関係性等を明らかにした。具体的な成果については以下の通りである。

まず、情報理論的安全性を有する暗号化方式および鍵共有方式に対して、計算量的安全性の観点から操作的意味付けのある様々な安全性概念を情報理論的観点から定式化し、従来の安全性概念も含めて、様々な情報理論的安全性の概念間の関係を理論的に解析した（論文①）。また、一様ランダムな秘密鍵や乱数を仮定せず、多少偏りのある分布の秘密鍵や乱数による情報理論的安全性の実現性に関して研究した。このテーマに関しては、理論的観点から、暗号化（論文⑮）、認証（論文③,⑯）、秘密分散（論文⑥）に対して、それらの情報理論的安全性の実現可能性や効率性の限界を示すことができた。実装面では、非一様な物理乱数から真性乱数を生成する手法に対して、その実用性を非漸近的立場から評価するため、計算機実験を行った（論文④）。

また、計算量的安全性概念、情報理論的安全性概念を俯瞰的にみることで、様々な高機能暗号やプロトコルの安全性の定式化、効率的構成法、それらの関係性等に関して研究成果を得ることができた。特に、暗号化状態での検索機能（論文⑤）、暗号化の無効化機能（論文⑦,⑧）、鍵隔離機能（⑬）、ブロード

キャスト機能（論文⑩）、認証のアグリゲート機能（論文⑫）、秘密分散のタイムリリース機能（論文⑨）、そして効率的なカードプロトコルの構成（論文②）の成果等が含まれる。また、情報理論的指標（エントロピー等）を利用して、ネットワークセキュリティへ応用する成果も得られた（論文⑪,⑭）。

今後の研究活動では、暗号理論と情報理論に跨る多様な概念を俯瞰的かつ体系的に扱うことのできる統一的パラダイムをさらに発展させることにより、本研究で得られた成果を、より複雑かつ高機能な暗号プロトコルに拡張するとともに、統一的パラダイムのさらに幅広い応用を目指したい。

５．主な発表論文等

〔雑誌論文〕（計１６件）

① M. Iwamoto, K. Ohta, and J. Shikata, “Security Formalizations and Their Relationships for Encryption and Key Agreement in Information Theoretic Cryptography”, IEEE Transactions on Information Theory, Vol. 64, No. 1, pp. 654-685, January 2018, 査読有.

② T. Nakai, S. Shirouchi, M. Iwamoto and K. Ohta, “Four Cards Are Sufficient for a Card-Based Three-Input Voting Protocol Utilizing Private Permutations”, Information Theoretic Security (ICITS 2017), pp.153-165, Springer, 2017, 査読有.

③ J. Shikata, “Tighter Bounds on Entropy of Secret Keys in Authentication Codes”, Proc. of 2017 IEEE Information Theory Workshop (ITW2017), November 2017, Taiwan, pp.259-263, IEEE Xplore, 査読有. DOI: 10.1109/ITW.2017.8278016

④ A. Prasitsupparote, N. Konno, and J. Shikata, “Numerical Analysis of Elias's and Peres's Deterministic Extractors”, Proc. of 2017 Annual Conference on Information Science and Systems (CISS), Baltimore, Maryland, March 2017, IEEE Xplore, 査読有. DOI: 10.1109/CISS.2017.7926129

⑤ T. Yoshizawa, Y. Watanabe, and J. Shikata, “Unconditionally Secure Searchable Encryption”, Proc. of 2017 Annual Conference on Information Science and Systems (CISS), Baltimore, Maryland, USA, March 2017, pp.1-6, IEEE Xplore, 査読有. DOI: 10.1109/CISS.2017.7926154

⑥ 岩本貢, 四方順司, “最悪推測秘匿性を満たす秘密分散法に関する基本的性質”, 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017)論文集, 1A1-4, 2017 年１月, 査読無.

⑦ 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), vol.3, no.3, pp.288-311, 2017, 査読有.

⑧ Y. Watanabe, G. Hanaoka, and J. Shikata, “Unconditionally Secure Revocable Storage: Tight Bounds, Optimal Construction, and Robustness”, Information Theoretic Security (ICITS 2016), LNCS 10015, pp.213-237, Springer, November 2016, 査読有.

⑨ 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.

⑩ Y. Watanabe and J. Shikata, “Unconditionally Secure Broadcast Encryption Schemes with Trade-offs between Communication and Storage,” Special Section on Discrete Mathematics and Its Applications, IEICE Transactions, vol.99-A, no.6, pp.1097-1106, June 2016, 査読有.

⑪ J. Su, K. Yoshioka, J. Shikata, T. Matsumoto, “An Efficient Method for Detecting Obfuscated Suspicious JavaScript Based on Text Pattern Analysis”, Proc. of the 2016 ACM International Workshop on Traffic Measurements for Cybersecurity (WTMC 2016), pp.3-11, ACM, May 2016, 査読有.

⑫ S. Tomita, Y. Watanabe, and J. Shikata, “Sequential Aggregate Authentication Codes with Information Theoretic Security,” Proc. of 2016 Annual Conference on Information Science and Systems (CISS), Princeton, USA, March 2016, pp. 198-203, IEEE Xplore, 査読有. DOI: 10.1109/CISS.2016.7460500

⑬ 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, 査読有.

⑭ J. Su, K. Yoshioka, J. Shikata, T. Matsumoto, “Detecting Obfuscated Suspicious JavaScript Based on Information-Theoretic Measures and Novelty Detection”, Information

Security and Cryptology – ICISC 2015, LNCS 9558, pp. 278–293, Springer, November 2015, 査読有.

⑮ M. Iwamoto and J. Shikata, “Constructions of Symmetric-key Encryption with Guessing Secrecy”, Proc. of 2015 IEEE International Symposium on Information Theory (ISIT 2015), pp. 725-729, June 2015, 査読有.

⑯ 石川美穂, 四方順司, “非一様ランダム鍵を用いた情報理論的に安全な調停者付き認証符号について”, 電子情報通信学会, 信学技報, vol. 117, no. 488, ISEC2017-130, pp. 231-236, 2018 年 3 月, 査読無.

〔学会発表〕(計１２件)

① M. Iwamoto, “Four Cards Are Sufficient for a Card-Based Three-Input Voting Protocol Utilizing Private Permutations”, ICITS 2017, Conference Track, Hong Kong, December 2017.

② M. Iwamoto, “Worst-case Guessing Secrecy Is Meaningful in Secret Sharing Schemes”, ICITS 2017, Workshop Track, Hong Kong, December 2017.

③ J. Shikata, “Tighter Bounds on Entropy of Secret Keys in Authentication Codes”, 2017 IEEE Information Theory Workshop (ITW 2017), Taiwan, November 2017.

④ A. Prasitsupparote, “Numerical Analysis of Elias's and Peres's Deterministic Extractors”, 2017 Annual Conference on Information Science and Systems (CISS), Baltimore, Maryland, March 2017.

⑤ T. Yoshizawa, “Unconditionally Secure Searchable Encryption”, 2017 Annual Conference on Information Science and Systems (CISS), Baltimore, Maryland, USA, March 2017.

⑥ Y. Watanabe, “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.

⑦ J. Su, “An Efficient Method for Detecting Obfuscated Suspicious JavaScript Based on Text Pattern Analysis”, 2016 ACM International Workshop on Traffic Measurements for Cybersecurity (WTMC 2016), Xi’an, China, May 2016.

⑧ S. Tomita, “Sequential Aggregate Authentication Codes with Information Theoretic Security,” 2016 Annual Conference on Information Science and Systems (CISS), Princeton, USA, March 2016.

⑨ Y. Watanabe, “Identity-based Hierarchical Key-insulated Encryption without Random Oracles,” Public-Key Cryptography (PKC 2016), March 2016.

⑩ Y. Watanabe, “Constructions of Unconditionally Secure Broadcast Encryption from Key Predistribution Systems with Trade-offs between Communication and Storage”, ProvSec 2015, Kanazawa, Japan, November 2015.

⑪ J. Su, “Detecting Obfuscated Suspicious JavaScript Based on Information-Theoretic Measures and Novelty Detection”, ICISC 2015, Seoul, South Korea, November 2015.

⑫ J. Shikata, “Constructions of Symmetric-key Encryption with Guessing Secrecy”, 2015 IEEE International Symposium on Information Theory (ISIT 2015), Hong Kong, June 2015.

〔図書〕(計１件)

① J. Shikata (Editor), Information Theoretic Security - 10th International Conference, ICITS 2017, Hong Kong, China, November 29 - December 2, 2017, Proceedings. LNCS 10681, Springer 2017. ISBN 978-3-319-72088-3

〔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)研究分担者
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

太田　和夫（OHTA, Kazuo）
電気通信大学・大学院情報理工学研究科・教授
研究者番号：80333491

岩本　貢（IWAMOTO, Mitsugu）
電気通信大学・大学院情報理工学研究科・
准教授
研究者番号：50377016