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

令和　４ 年　 ６ 月 ２４ 日現在

機関番号：１２６１２
研究種目：基盤研究(B)（一般）
研究期間：2017～2020
課題番号：１７Ｈ０１７５２

研究課題名（和文）推測秘匿性に基づく情報理論的暗号理論の新展開

研究課題名（英文）Development of Information-Theoretic Security Based on Guessing Secrecy

研究代表者
岩本　貢（Iwamoto, Mitsugu）

電気通信大学・大学院情報理工学研究科・教授

研究者番号：５０３７７０１６

交付決定額（研究期間全体）：（直接経費）　　14,100,000円

研究成果の概要（和文）：本研究では，近年提案された情報理論的安全性概念である推測秘匿性を深く追求することで，関連分野を含めた暗号理論に新たな展開をもたらすことを目指した．はじめに，推測秘匿性に関するいくつかの定義をあたえ，それらの関係性を調べた．推測秘匿性を満足するいくつかの暗号プロトコルを提案した結果，プロトコルごとに安全性間のギャップの有無が異なることを明らかにした．また，AES暗号にプロービング攻撃を行って鍵を推測するときに必要となる計算時間を計測し，推測と計算量の関係を明らかにした．その他，推測秘匿性を研究するために，完全秘匿性を満たす暗号方式，特に秘密分散法や秘密計算に関するプロトコルをいくつか提案した．

研究成果の学術的意義や社会的意義
情報理論的暗号において近年提案された推測秘匿性をテーマとした理論研究を行った．情報理論的暗号は通常，完全秘匿性を要求することが多い．その強力な安全性の代償として，機能や効率に問題がある．そこで完全秘匿性を緩めた安全性概念として推測秘匿性を研究することは重要である．本研究では，推測秘匿性の基礎的・基本的性質やプロトコルを明らかにし，鍵を実際に推測する際の計算時間なども検討した．このように，推測と安全性という暗号理論における基本的な関係を多角的に考察することができた点に学術的な意義がある．推測秘匿性の研究に関連して，完全秘匿性をもつ暗号プロトコルもいくつか提案することができたことも有意義であった．

研究成果の概要（英文）：In this study, we investigated the recently proposed information-theoretic security notion called guessing secrecy for developing information-theoretic security. First, we proposed several definitions of guessing secrecy and investigated their relationship. Then, by proposing several cryptographic protocols satisfying guessing secrecy, we found that the existence of the security gap depends on the protocols. We also measured the computation time required to guess a key of AES under a probing attack and clarified the relationship between guessing and computation time. Besides the study of guessing secrecy, we proposed several cryptographic protocols that satisfy perfect secrecy, especially secret sharing and multi-party computation.

研究分野：暗号理論

キーワード：推測秘匿性　情報理論的安全性　暗号理論

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

情報理論的暗号とは，無制限の計算能力をもつ攻撃者に対しても安全な暗号方式である．解読に要する時間が十分に長いことを安全性の根拠とする計算量的暗号と比べ，高い安全性が約束できる一方で，効率性や機能性に改善すべき点が多い．非効率性の例として，情報理論的安全性の最も基本的な安全性概念である完全秘匿性(Perfect Secrecy，PS)のもとでは，任意の共通鍵暗号方式において鍵長が平文長以上になる，というシャノンの悲観的結果はよく知られている．攻撃者の計算能力に依存しない安全性を定義しつつ，効率性や機能性を高めることは，理論的に興味深いだけでなく，情報理論的暗号の実用のためにも極めて重要な課題である．

このような観点から有益な安全性概念として，推測確率に基づく新しい情報理論的安全性(Guessing Secrecy，推測秘匿性，Alimomeni，Safavi-Naini,[ICITS 2012])が提案された．推測秘匿性は，攻撃者が確率的推測によって暗号文から平文を当てる確率（推測確率）が，暗号文の有無によって変化しないことを安全の根拠としており，攻撃者の計算能力に依存しないという意味で情報理論的な安全性概念といえる．

本研究の背景として，このような推測に基づく安全性の重要性がより強く認識されてきたことがあげられる．

２．研究の目的

本研究では，以下のように目的を設定し，推測秘匿性に対してより深い理解を得ることを目指した．

(A) 安全性概念の相互関係の体系化：
　暗号理論において，様々な安全性概念間の相互関係（強弱や等価性）を明らかにすることは，基本的かつ重要な課題である．本研究では，PS および GS の 2 つの分類である平均推測秘匿性(Average GS，A-GS)や(Worst-case GS，W-GS）だけでなく，様々なレベルの安全性との関係を明らかにし，暗号理論的な広い立場から，GS の保証する安全性の位置づけをより精密な形で明らかにする．

(B) 安全性ギャップに着目した暗号プリミティブ構成の基本原理：
　我々は既に安全性概念のギャップ PS が A-GS より強い共通鍵暗号や秘密分散法の例を得ている．しかし，PS と W-GS あるいは W-GS と A-GS の間に明らかなギャップがある方式は見つかっていない．一方で申請者らは，共通鍵暗号においてはある条件の下で，PS と W-GS にはギャップが存在せず，両者は同値となることを明らかにしている．共通鍵暗号だけでなく，秘密分散法・鍵共有・認証などの基本的な暗号プリミティブに対して，安全性概念のギャップの有無に着目して W-GS，A-GS を満足する暗号プリミティブの構成法を明らかにする．

(C) 情報量を用いた暗号方式の効率性評価：
　構築する暗号プリミティブや暗号プロトコルに対して，情報量に基づく効率評価を行い，暗号プロトコルの効率化を図る．

(D) 暗号プロトコルへの展開・高効率化と高性能化：
　現在の所，GS の研究は共通鍵暗号や秘密分散法といった秘匿性をもつ暗号方式にとどまっている．本研究では(A)，(C) の知見をもとに，A-GS/W-GS を満たす，暗号プロトコルへの拡張を議論し，高効率化や高機能化を図る．

３．研究の方法

本研究では，上記の課題(A)～(D)を相互に関連付けて研究を進めた．研究初期には(A),(B)などの基本的問題を扱い，(C),(D)の発展的課題の解決の基盤とした．実際の研究遂行にあたっては，必ずしも順番に成果は得られなかったが，得られた研究成果を検討しつつ，計画当初に想定した課題間の関係に従って研究を進めた．また，情報理論的暗号だけでなく，計算量的暗号についても鍵の推測アルゴリズムを提案することで，推測と計算量の関係について考察した．

推測秘匿性は情報理論的な安全性概念である．様々な暗号プロトコルに対して推測秘匿性を検討するため，情報理論的安全性の基本的安全性概念である完全秘匿性を満たす暗号プロトコルについても研究を進めた．特に，秘密分散法やマルチパーティ計算(Multi-Party Computation，MPC)についての研究を多く行った．

４．研究成果

課題(A)～(D)についての成果について年度ごとに記述し，それ以外の関連成果について最後に説明する．

【平成２９年度】
課題(A),(B)に関連して得られた成果を国際会議で発表した．それ以外に，(D)に関連して，推測秘匿性を満たす放送型暗号プロトコルとその諸性質を解明することに成功し，国際会議で発表した．(A),(B)について：平均推測秘匿性(Average GS)を満足するが最悪推測秘匿性(Worst-case GS)を満たさない暗号プリミティブとして，共通鍵暗号があげられる．ここで共通鍵暗号に最悪推測秘匿性を要求すると，その共通鍵暗号は完全秘匿性を満たすことが分かっている．すなわち，共通鍵暗号における最悪推測秘匿性は，平均推測秘匿性と完全秘匿性の中間の安全性としての意味をもたない．我々は，秘密分散法においては最悪推測秘匿性が平均推測秘匿性と完全秘匿性の中間の安全性として意味をもつことを明らかにし，その成果を ICITS2017 の workshop track にて発表した．ここで報告した事実は一つの例であって，一般的な構成法については今後の課題となっている．(D)について：推測秘匿性をもつ放送型暗号プロトコルを提案し，符号化効率について評価した．この中で，放送型暗号においては，平均・最悪推測秘匿性の variant として，強い平均推測秘匿性(strong Average GS，sAGS)および弱い最悪推測秘匿性を新しく提案し，それらの関係を明らかにした．さらに，sAGS を満足する放送型暗号の構成法を示し，それが暗号文と鍵のサイズに関してある種の最適性を満足することも示した．この成果を ICITS2017 の conference track で発表した．

【平成 30 年度】
認証符号のうち，調停者が必ずしも信用できる存在ではなく，攻撃することも考慮した認証符号(A^3-code)について，推測秘匿性をもつプロトコルを提案し，その最適性を示した．また，推測秘匿性に重要な役割を果たす乱数生成（今回は Peres の乱数生成）についても新しい知見を得た．また，秘密分散法に関して，埋め込み画像を推測出来ないような画像秘密分散(Secret Image Sharing; SIS)について研究し，埋め込み画像が機械学習攻撃による推測に対しても頑健な Proactive SIS を提案している．この場合の推測は「推測秘匿性」の数学的な定義通りではないが，機械学習という形の推測が SIS に与える影響を検討したことになっており，本研究課題としては重要な成果であると考えている．

【令和元年度】
平成 30 年度までは，推測秘匿性の基礎的な性質の探求やプロトコルの構築を行ってきたが，課題(A)のサブテーマとして予定していた，推測秘匿性と攻撃計算量との関係について検討が行われていなかったので，令和元年度はこの点について研究を行った．この課題にアプローチする一つの方法として，プロービング攻撃による情報漏洩時に鍵の推測を行うことを考え，情報漏洩と推測秘匿性の関係を考察した．具体的には AES(Advanced Encryption Standard) について，鍵スケジュールのうち何割かが攻撃者に盗聴されている場合を考え，推測するためにはどの程度の計算量（計算時間）が必要となるかについて明らかにした．鍵スケジュールから攻撃者に漏洩する割合を決めたときに，攻撃者が真の鍵をどれくらい推測できるかについて，Tsow [SAC2009]や Tanigaki-Kunihiro [ICISC2016]などをもとにして攻撃方法を提案し，攻撃時間を計算機実験で算出した．結果としては，鍵スケジュールの 15%が漏洩すると非常に高い確率で鍵が復元されてしまうことが明らかになり，確率的に定義された推測秘匿性と，実際の AES 鍵スケジュールに対する推測秘匿性の関係を考える重要なデータが得られた．この成果は，国内シンポジウム SCIS で発表した．

【令和 2 年度】
令和元年度から検討している AES(Advanced Encryption Standard) に対する鍵推測アルゴリズムに関して，鍵スケジュールから攻撃者に漏洩する割合を決めたときに，攻撃者が真の鍵をどれくらい推測できるかについて実験精度を向上させたものを国際会議 ISITA2022 で発表した．ここでの研究は，盗聴がビット毎に一定の確率で起きていることを仮定して実験を行っている．
得られた結果を考察したところ，この仮定は推測アルゴリズムの理論的限界を考える場合には有効であるが，盗聴されるビット数がばらつくことで，実験の精度が悪くなることが分かった．そのため，ビットが確率的に盗聴されるのではなく，鍵全体に対して盗聴される割合を定めることで，実験の精度を高めることを試みた．結果として，鍵の漏洩量が 13%である場合にはほぼ確率 1 で鍵を復元でき，一方で鍵の漏洩量が 11%である場合には鍵を復元できる確率はほぼ 0 であることが明らかになった．確率的漏洩モデルにおける性能評価と比べ，復元成功確率がほぼ 1 となるために必要な漏洩量が減り，またほぼ 0 となるような漏洩量は増えたということから，評価精度が向上していることが分かる．本研究は推測アルゴリズムの評価がより現実的になった面では成功といえるが，より強い攻撃を考えることができるので，今後も研究を続ける予定である．

【その他の研究】

推測秘匿性の研究は，共通鍵暗号・秘密分散法・放送型暗号，認証符号に対して成果を得ることができた．それ以外のプロトコルとしてマルチパーティ計算(Multi-Party Computation; MPC)における推測秘匿性を考えるために，まずは完全秘匿性を保証する MPC を様々な角度から検討した．MPC に関する推測秘匿性の研究は期間内に完成させることはできなかったが，その過程で，完全秘匿性をもつ MPC に関連する幾つかの成果が得られた．

具体的にはカードで MPC を行うカード暗号で，2 入力の XOR/AND/NOR を同時に計算する非常に効率の良いプロトコル（semi-honest モデル）やその不正検知手法（malicious モデル），PEZ dispenser を用いて private MPC を行う PEZ プロトコルの大幅な効率化などである．また，MPC の安全性に関するチュートリアルを行った（招待講演）．特に private PEZ プロトコルには大きな進展があった，従来研究として，この研究を開始した Balogh et al.の成果（任意の関数に対する private PEZ プロトコルの実現法）を，計算する関数を対称関数に限定することで指数的に改善した．さらに，一般の関数に対しても，入力をバイナリでなく一般的な始集合に対する関数計算が行えるようなプロトコルを提案し，従来研究から大幅な効率化に成功した．

その他に，完全秘匿性と計算量的安全性の関係に関する多角的な考察，シェアサイズの小さな秘密分散法の実現手法，マルチパーティ計算の高速な実現手法といった，情報理論的暗号の構成法を中心とした暗号理論に関する幾つかの成果を得て，国際会議や論文誌で発表を行った．これらの暗号方式に対しても，推測秘匿性のもとでの安全性を考えることが出来るが，それは今後の課題としたい．

５．主な発表論文等

〔雑誌論文〕　計16件（うち査読付論文　16件／うち国際共著　1件／うちオープンアクセス　2件）

１．著者名 Y. Abe, M. Iwamoto, and K. Ohta	４．巻 LNCS11891
２．論文標題 Efficient Private PEZ Protocols for Symmetric Functions	５．発行年 2019年
３．雑誌名 Proc. Theory of Cryptography Conference (TCC2019)	６．最初と最後の頁 372-392
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-36030-6_15	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 K. Emura, S. Katsumata, and Y. Watanabe	４．巻 LNCS11736
２．論文標題 Identity-Based Encryption with Security against the KGC: A Formal Model and Its Instantiation from Lattices	５．発行年 2019年
３．雑誌名 Proc. European Symposium on Research in Computer Science (ESORICS2019)	６．最初と最後の頁 113-133
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-29962-0_6	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Reo Eriguchi, Noboru Kunihiro, and Mitsugu Iwamoto	４．巻 -
２．論文標題 Optimal Multiple Assignment Schemes Using Ideal Multipartite Secret Sharing Schemes	５．発行年 2019年
３．雑誌名 Proc. IEEE International Symposium on Information Theory (ISIT2019)	６．最初と最後の頁 3047-3051
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISIT.2019.8849591	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 H. Anada, A. Kanaoka, N. Matsuzaki, and Y. Watanabe	４．巻 19
２．論文標題 Key-Updatable Public-Key Encryption with Keyword Search (Or: How to Realize PEKS with Efficient Key Updates for IoT Environments)	５．発行年 2020年
３．雑誌名 International Journal of Information Security	６．最初と最後の頁 15-38
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10207-019-00441-2	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 K. Ohara, Y. Watanabe, M. Iwamoto, and K. Ohta	4．巻 E102.A
2．論文標題 Multi-Party Computation for Modular Exponentiation Based on Replicated Secret Sharing	5．発行年 2019年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1079-1090
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1079	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Junji Shikata and Yohei Watanabe	4．巻 87-5
2．論文標題 Identity-based Encryption with Hierarchical Key-insulation in the Standard Model	5．発行年 2019年
3．雑誌名 Designs, Codes and Cryptography	6．最初と最後の頁 1005-1033
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-018-0503-4	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Sato Shingo、Shikata Junji	4．巻 LNCS11929
2．論文標題 SO-CCA Secure PKE in the Quantum Random Oracle Model or the Quantum Ideal Cipher Model	5．発行年 2019年
3．雑誌名 Proc. Cryptography and Coding (IMACC 2019)	6．最初と最後の頁 317～341
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-35199-1_16	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Yohei Watanabe, Yoshihisa Kuroki, Shinnosuke Suzuki, Yuta Koga, Mitsugu Iwamoto, Kazuo Ohta	4．巻 -
2．論文標題 Card-Based Majority Voting Protocols with Three Inputs Using Three Cards	5．発行年 2018年
3．雑誌名 Proc. International Symposium on Information Theory and Its Applications (ISITA2018)	6．最初と最後の頁 218-222
掲載論文のDOI（デジタルオブジェクト識別子） 10.23919/ISITA.2018.8664324	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Anjelina Espejel-Trujillo, Mitsugu Iwamoto, and Mariko Nakano-Miyatake	4．巻 77
2．論文標題 A Proactive Secret Image Sharing Scheme with Resistance to Machine Learning Based Steganalysis	5．発行年 2018年
3．雑誌名 Multimedia Tools And Applications	6．最初と最後の頁 15161-15179
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11042-017-5097-8	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Amonrat Prasitsupparote, Norio Konno, and Junji Shikata	4．巻 20 (10)
2．論文標題 Numerical and Non-Asymptotic Analysis of Elias's and Peres's Extractors with Finite Input Sequences	5．発行年 2018年
3．雑誌名 Entropy	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/e20100729	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Amonrat Prasitsupparote, Yohei Watanabe, Junichi Sakamoto, Junji Shikata, and Tsutomu Matsumoto	4．巻 8 (4)
2．論文標題 Implementation and Analysis of Fully Homomorphic Encryption in Resource-Constrained Devices	5．発行年 2019年
3．雑誌名 International Journal of Digital Information and Wireless Communications (IJDIWC)	6．最初と最後の頁 288-303
掲載論文のDOI（デジタルオブジェクト識別子） 10.17781/P002535	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Iwamoto Mitsugu、Ohta Kazuo、Shikata Junji	4．巻 64
2．論文標題 Security Formalizations and Their Relationships for Encryption and Key Agreement in Information-Theoretic Cryptography	5．発行年 2018年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 654～685
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2017.2744650	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Watanabe Yohei	4．巻 LNCS100681
2．論文標題 Broadcast Encryption with Guessing Secrecy	5．発行年 2017年
3．雑誌名 Information Theoretic Security	6．最初と最後の頁 39～57
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-72089-0_3	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Nakai Takeshi、Shirouchi Satoshi、Iwamoto Mitsugu、Ohta Kazuo	4．巻 LNCS100681
2．論文標題 Four Cards Are Sufficient for a Card-Based Three-Input Voting Protocol Utilizing Private Permutations	5．発行年 2017年
3．雑誌名 Information Theoretic Security	6．最初と最後の頁 153～165
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-72089-0_9	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Shikata Junji	4．巻 ITW2017
2．論文標題 Tighter bounds on entropy of secret keys in authentication codes	5．発行年 2017年
3．雑誌名 IEEE International Workshop on Information Theory	6．最初と最後の頁 259～263
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ITW.2017.8278016	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Watanabe Yohei、Shikata Junji	4．巻 86
2．論文標題 Timed-release computational secret sharing and threshold encryption	5．発行年 2017年
3．雑誌名 Designs, Codes and Cryptography	6．最初と最後の頁 17～54
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-016-0324-2	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計32件（うち招待講演　5件／うち国際学会　8件）

１．発表者名
植村友紀，李陽，三浦典之，岩本貢，崎山一男，太田和夫

２．発表標題
鍵のランダムな漏洩に対するAES鍵スケジュール復元アルゴリズム

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
品川和雅，三浦典之，岩本貢，崎山一男，太田和夫

２．発表標題
気泡検出器を用いたゼロ知識非破壊検査

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
安部芳紀，岩本貢，太田和夫

２．発表標題
任意の始集合を持つ関数を計算するprivate PEZプロトコル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
渡邉洋平

２．発表標題
フォワード安全かつ検索時通信量が最適な動的検索可能暗号

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
安部芳紀，岩本貢，太田和夫

２．発表標題
任意の関数を計算するprivate PEZプロトコルの改善

３．学会等名
コンピューターセキュリティシンポジウム（CSS）2019

４．発表年
2019年

１．発表者名
渡邉洋平，大原一真，岩本貢，太田和夫

２．発表標題
(強)フォワード安全な動的検索可能暗号の効率的な構成

３．学会等名
コンピューターセキュリティシンポジウム（CSS）2019

４．発表年
2019年

１．発表者名
Yoshiki Abe, Mitsugu Iwamoto, Kazuo Ohta

２．発表標題
How to improve the private PEZ protocol for general functions

３．学会等名
The 14th International Workshop on Security (IWSEC2019), poster session（国際学会）

４．発表年
2019年

１．発表者名
宮澤智輝，佐藤慎悟，四方順司

２．発表標題
格子問題に基づくSemi-Adaptive安全な内積暗号

３．学会等名
情報処理学会，研究報告コンピュータセキュリティ(CSEC)

４．発表年
2019年

１．発表者名
Masahiro Ebina, Yohei Watanabe, Junji Shikata

２．発表標題
Efficient Threshold Public-Key Encryption from CBDH

３．学会等名
International Workshop on Information Security (IWSEC 2019)（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
岩本貢

２．発表標題
秘密計算の安全性～プライバシーを保ちつつどこまで計算できるか

３．学会等名
第8回バイオメトリクスと認識・認証シンポジウム(SBRA)（招待講演）

４．発表年
2018年

１．発表者名
安部 芳紀，山本 翔太，岩本 貢，太田 和夫

２．発表標題
初期文字列が29 文字の4 入力多数決Private PEZプロトコル

３．学会等名
情報理論・情報セキュリティ・ワイドバンドシステム合同研究会

４．発表年
2019年

１．発表者名
渡邉洋平，岩本貢，太田 和夫

２．発表標題
効率的でフォワード安全な動的検索可能暗号

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
安部 芳紀，山本 翔太，岩本 貢，太田 和夫

２．発表標題
不正検知可能な3入力多数決カードプロトコル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
山本 翔太，安部 芳紀，岩本 貢，太田 和夫

２．発表標題
4入力多数決を計算する効率的なPrivate PEZプロトコル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
Wenjia Wang, Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta,

２．発表標題
Three-Party Private Set Operation Protocols Using Polynomials and OPPRF

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
江利口礼央，國廣昇，岩本貢

２．発表標題
いくつかの理想的な秘密分散法を用いた最適な複数割り当て法

３．学会等名
情報理論とその応用シンポジウム（SITA2018）

４．発表年
2018年

１．発表者名
Amonrat Prasitsupparote, Yohei Watanabe, and Junji Shikata

２．発表標題
Implementation and Analysis of Fully Homomorphic Encryption in Wearable Devices

３．学会等名
The Fourth International Conference on Information Security and Digital Forensics (ISDF 2018), The Society of Digital Information and Wireless Communications（国際学会）

４．発表年
2018年

１．発表者名
小林大輝，四方順司

２．発表標題
非一様ランダム鍵を用いた情報理論的に安全な信頼性の低い調停者付き認証符号について

３．学会等名
2019年暗号と情報セキュリティシンポジウム（SCIS 2019）

４．発表年
2019年

１．発表者名
山田憲一，四方順司

２．発表標題
エントロピーロスの小さいロバストファジー抽出器の構成に関する一考察

３．学会等名
2019年暗号と情報セキュリティシンポジウム（SCIS 2019）

４．発表年
2019年

１．発表者名
小川善功，田中亮大，四方順司

２．発表標題
相関のある情報を用いたMultiple Access Wiretap Channelにおける秘匿通信について

３．学会等名
第21回コンピュータセキュリティシンポジウム（CSS 2018）

４．発表年
2018年

１．発表者名
Junji Shikata

２．発表標題
Toward Lightweight Authentication: Application of Aggregate MACs for IoT

３．学会等名
The 4th French-Japanese Cybersecurity Workshop（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Mitsugu Iwamoto

２．発表標題
Worst-case guessing secrecy is meaningful in secret sharing schemes

３．学会等名
International Conference on Information Theoretic Security (ICITS)（国際学会）

４．発表年
2017年

１．発表者名
Watanabe Yohei

２．発表標題
Broadcast Encryption with Guessing Secrecy

３．学会等名
International Conference on Information Theoretic Security (ICITS)（国際学会）

４．発表年
2017年

１．発表者名
Nakai Takeshi、Shirouchi Satoshi、Iwamoto Mitsugu、Ohta Kazuo

２．発表標題
Four Cards Are Sufficient for a Card-Based Three-Input Voting Protocol Utilizing Private Permutations

３．学会等名
International Conference on Information Theoretic Security (ICITS)（国際学会）

４．発表年
2017年

１．発表者名
Mitsugu Iwamoto

２．発表標題
Secret sharing schemes under guessing secrecy

３．学会等名
Cryptographic Technologies for Securing Network Storage and Their Mathematical Modeling, Kyushu University.（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
岩本貢

２．発表標題
情報理論的安全性 ―さまざまな視点から―

３．学会等名
誤り訂正符号のワークショップ（招待講演）

４．発表年
2017年

１．発表者名
鈴木慎之介，渡邉洋平，岩本 貢，太田和夫

２．発表標題
ロバスト秘密分散法 CFOR 方式における精密な安全性解析

３．学会等名
暗号と情報セキュリティシンポジウム (SCIS2018)

４．発表年
2018年

１．発表者名
黒木慶久，古賀優太，渡邉洋平，岩本 貢，太田和夫

２．発表標題
3 枚のカードで実現可能な 3 入力多数決プロトコ ル

３．学会等名
暗号と情報セキュリティシンポジウム (SCIS2018)

４．発表年
2018年

１．発表者名
古賀優太，鈴木 慎之介，渡邉 洋平，岩本 貢，太田 和夫

２．発表標題
カードを用いた複数人でのマッチングプロト コル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2018）

４．発表年
2018年

１．発表者名
田中亮大，四方順司

２．発表標題
Wiretap Channel IIにおける能動的攻撃を考慮した暗号通信について

３．学会等名
コンピュータセキュリティシンポジウム2017（CSS2017）

４．発表年
2017年

１．発表者名
石川美穂，四方順司

２．発表標題
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

３．学会等名
電子情報通信学会，ISEC

４．発表年
2017年

１．発表者名
飯塚寛貴，田中亮大，四方順司

２．発表標題
Cooperative Jammingを用いた主通信路に雑音のあるWiretap Channel IIにおける暗号通信について

３．学会等名
電子情報通信学会，ISEC

４．発表年
2018年

〔図書〕　計1件

1．著者名	4．発行年
Junji Shikata (ed.)	2017年
2．出版社	5．総ページ数
Springer-Verlag	233
3．書名	
Information Theoretic Security	

〔産業財産権〕

〔その他〕

岩本・渡邉研究室
https://iw-lab.jp
電気通信大学 教員総覧
http://kjk.office.uec.ac.jp/Profiles/11/0001044/profile.html
岩本貢ホームページ
https://iw-lab.jp/users/mitsugu/index.html

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	四方　順司 (Shikata Junji) (30345483)	横浜国立大学・大学院環境情報研究院・教授 (12701)	
研究分担者	渡邉　洋平 (Yohei Watanabe) (40792263)	電気通信大学・大学院情報理工学研究科・助教 (12612)	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関