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 ２９ 日現在

機関番号：１２７０１
研究種目：基盤研究(B)（一般）
研究期間：2018～2020
課題番号：１８Ｈ０３２３８

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深化、発展とその応用

研究課題名（英文）Developing a Paradigm for Constructions 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）　　13,300,000円

研究成果の概要（和文）：情報理論的暗号理論を更に発展させるため、本研究の目的は情報理論と暗号理論の両分野からの俯瞰的かつ体系的なパラダイムにより、情報理論的安全性を有する複雑かつ高機能なプロトコルを新たに構築すること、そしてそこから得られる手法や成果の幅広い応用を開発することである。本研究の理論的成果として、情報理論的に安全な高機能暗号（完全準同型暗号等）を新たに構成したこと、マルチパーティ計算、カードベースプロトコルを新たに構成したことが挙げられる。また、応用研究成果として、物理的に制限のあるデバイスにおける乱数生成と完全準同型暗号の実装評価、計算量的に安全な様々な高機能暗号に対する新たな構成法の提案が挙げられる。

研究成果の学術的意義や社会的意義
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新しい計算技術の登場に対しても安全性を保証できる暗号技術の開発は重要である。情報理論的安全性に基づく暗号技術はそれを可能とするため、そのニーズは今後の情報社会で益々求められ、またその応用範囲も広がっていくと考えられる。したがって、本研究成果は、多様で複雑な情報システムであふれる現代及び未来の情報社会のセキュリティ設計（クラウド計算，IoT等のセキュリティ等）において、時代の計算機技術に依存しない強力な安全性をもつ暗号技術開発の基盤となることが期待できる。

研究成果の概要（英文）：In order to develop information-theoretic cryptography, the purpose of this research is to construct complicated and advanced cryptographic protocols with information-theoretic security by a broad and systematic paradigm from both information theory and modern cryptography, and to apply resulting techniques to other research topics including construction of protocols with complexity-based security. The contribution of this research includes new constrictions of information-theoretically secure advanced protocols including fully homomorphic encryption and MPC including card-based protocols. In addition, from viewpoints of applications, our contribution includes new constructions of various advanced protocols with complexity-based security, and implementation analysis of randomness extractors and fully homomorphic encryption in resource-constrained devices.

研究分野：暗号理論

キーワード：暗号理論　情報理論的安全性　高機能暗号　情報理論

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

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、一定規模の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。最近の世界の動きでみても、米国および欧州では、量子コンピュータに耐性をもつ暗号技術の標準化へ向けた取り組みが進められている。特に、米国立標準技術研究所（NIST）は、「現在主流の RSA 暗号を数時間で解読可能な量子コンピュータが 2030 年までに実現できる可能性がある」との見解を示している。

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。そのため、情報理論的安全性をもつ暗号技術のニーズは今後の情報社会で益々求められ、またその応用範囲も広がっていくと考えられる。したがって、本研究が目標とする情報理論的暗号理論の深化・発展は、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代及び未来の情報社会のセキュリティ設計全般(クラウド計算，IoT 等のセキュリティを含む)において、時代の計算機技術に依存しない強力な安全性をもつ暗号技術開発の基盤となることが期待できる。

２．研究の目的

従来の情報理論的暗号理論の研究成果は、情報理論主体の研究アプローチと、暗号理論主体の研究アプローチの 2 つに大別することが出来る。特に、両者の特徴として、以下の点が挙げられる。

Ⅰ．情報理論的見地からの安全性定義では、確率分布の独立性（正規ユーザのもつ情報と攻撃者が得られる情報の独立性）を基準にした安全性尺度で定式化しており、Shannon（シャノン）エントロピーや統計的距離を用いて安全性を記述する。このメリットとして、これまでの情報理論における多くの学術成果と同様にして、達成できる安全性と効率性の限界やトレードオフが理論的に解析できる。しかし、上記の定式化に対して、暗号学的見地からはどのような現実的モデルの数学的定式化なのか明確ではなく、想定する攻撃者モデルは能動的でなく静的な攻撃者であることが多い。

ⅠⅠ．暗号理論的見地からの安全性定義では、無制限の計算能力を有する攻撃者（時間計算量に制限の無いチューリング機械）による攻撃のアドバンテージで記述される。特に、攻撃者の強弱（能動的攻撃者から静的攻撃者まで）に関する階層的攻撃モデルを考えた上で、達成すべき安全性を定式化する。この立場からの安全性定式化のメリットは、暗号学的な操作的意味づけが明確であり、1 つの暗号システムに対しても、多様かつ階層的な安全性を定義できることである。しかし、情報理論的安全性をこの枠組みで議論する場合、攻撃者として時間計算量に制限の無いチューリング機械が想定され、安全性と効率性の限界やそのトレードオフが理論的に明確でない場合が多い。

以上より、本研究の目的は、上記（Ⅰ)、(ⅠⅠ）のメリットが両立できるよう、つまり、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複雑かつ高機能な暗号プロトコルに対して適切に定義し、それら多様な安全性と効率性の限界またはトレードオフを理論的に示すことである。この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）は、既に応募者らが暗号化方式や鍵共有方式のような暗号基礎技術に対して構築しているが、複雑で高機能な暗号技術に対しては未解決である。本研究では、複雑かつ高機能な暗号プロトコルに対して適切な安全性指標(定式化)を新たに導入し、効率的な構成法を研究開発する。また、安全性の強弱と効率性とのトレードオフがある場合にはそれも解析する。さらに、情報理論的手法や理論的成果を様々な応用技術に活かす、またはその効果的な応用先に関する技術研究を行う。本研究の特色は、前述した(Ⅰ)，(ⅠⅠ）のメリットが両立できるような、情報理論的暗号理論における新たな統一的な理論的枠組みを更に深化・発展させることであり、当該分野において学術的にも実用的にも非常に重要な問題に取り組む。本研究

は、(I)，(II)に関わる分野の多様な概念を統一的に扱う俯瞰的かつ体系的な理論研究のアプローチにより、情報理論的安全性を有する複雑かつ高機能なプロトコル（特に、完全準同型暗号）を新たに構成すること、そしてその幅広い応用を行うことである。

３．研究の方法

本研究では、既に述べた通り、現存する情報理論的暗号理論に対して、情報理論及び暗号理論の両見地からの統一的枠組み（パラダイム）を更に発展させ、複雑かつ高機能な暗号プロトコルを研究対象にすることである。また、本研究における理論的成果を利用した応用技術や、その効果的な応用先に関しても研究する。具体的には以下の研究を行う。

- 情報理論的暗号理論における統一的パラダイムを深化・発展させて、複雑かつ高機能な暗号プロトコルを研究対象にする理論研究を行う。特に、計算量的安全性概念の枠組みでの高機能暗号（特に、完全準同型暗号）を新たに情報理論的暗号理論において構築し、出来るだけ効率性の高い構成を探求する。また、マルチパーティ計算やカードベースプロトコル等の複雑な暗号プロトコルも研究対象とする。
- 上記の理論研究で得られた成果を、様々な応用技術に活かすこと、またはその効果的な応用先の研究を行う。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、構築した技術の実用性を数値実験的に実証するための計算機実装実験とその評価等を行う。

４．研究成果

（1）情報理論的安全性をもつ高機能暗号の構築とその応用（論文①、②など）

完全準同型暗号はデータを暗号化したまま任意の演算処理が可能な高機能暗号技術である。任意のエンティティが復号処理を行わずに演算処理することが可能なため安全に外部サーバに演算を委託することができることから、その応用としてクラウド計算での利活用が期待できる。高機能暗号の中でも、完全準同型暗号は特に注目されていることから、本研究では情報理論的に安全な完全準同型暗号を新たに構築した。既存研究においても情報理論的に安全な完全準同型暗号が存在するが、その安全性の定式化は計算量的安全性を有する完全準同型暗号の定義から見れば不自然である。そのため、情報理論的暗号理論における統一的パラダイムの観点から新しくモデルや安全性の定式化を行った。また、完全準同型暗号の構成を提案し、我々が定式化した情報理論的安全性を達成することを示した。また、上記の情報理論的安全性をもつ完全準同型暗号の応用先として、情報銀行のシステム構成を提案した。特に、情報銀行に預託した個人情報データの漏えいや不正な利用等のリスクに対する懸念が利用に際してのハードルになると考えられるため、本研究では典型的な情報銀行のモデルを定義した上で、想定される脅威やリスクについての対策を考察し、そのシステム構成に上記の完全準同型暗号の利用を提案した。また、完全準同型暗号から派生することが知られている高機能暗号の構成も上記の成果から導かれる。これ以外にも、調停者付き認証符号やロバストファジー抽出器の構成法の提案も行った。

（2）秘密分散、マルチパーティ計算、カードベースプロトコルの構築（論文③～⑧など）

本研究では、一般アクセス構造に対する秘密分散を構成するための手法を、従来よりも更に一般化して発展させた。また、秘密分散ベースの 3 入力マルチパーティ計算（べき乗演算ベース）に対して従来よりも効率的なプロトコルを構築した。さらに、本研究では様々なカードベースプロトコルに関して新たな構築を行った。カードベースプロトコルはマルチパーティ計算の一種であり、Public model と Private model の 2 種のモデルに大別される。カードベースプロトコルに関する研究では、プロトコルを実行するためのカード枚数を出来るだけ少なくすることが目標とされる。Public model では n ビット入力に対して 2n 枚のカードが必要であることが知られているが、本研究では Private model において、しきい値関数に対するプロトコルに対して、n+1 枚のカードで実行可能であることを示した。また、n 入力の Majority Voting Protocol を n 枚のカードで構築する手法も提案した。上記以外にも様々な機能をもつカードベースプロトコルの提案を行った。また、PEZ プロトコルも、カードベースプロトコルと同様に物理的手段で実装可能なマルチパーティ計算の一種である。既存研究として、n 入力関数に対する PEZ プロトコルが知られているが、本研究では n 入力対称関数に対して従来よりも効率的に実行可能な PEZ プロトコルを構築した。

（3）物理的に制限されたデバイスにおける乱数生成と完全準同型暗号の実装評価（論文⑨、⑩）

IoT デバイスのような物理的に制限されたデバイスにおいて、情報理論的観点からの乱数生成に関する実用的実装とその評価を行った。非一様分布をもつ物理的乱数に対して情報理論的な変換を行って一様乱数を生成する手法の代表的なものとして、von Neumann による手法、Peres による手法、Elias による手法が挙げられるが、それらに対する理論的評価と実装評価を行った。その結果、Peres による手法が最も実用的で有効であることを示した。また、物理的に制限されたデバイスにおいて、計算量的安全な完全準同型暗号の複数方式を実装し、そのパフォーマンスを評価した。具体的には、ウェアラブルデバイス（物理的に制限されたデバイス）によって構成されるヘルスケアシステムを想定し、上記の完全準同型暗号としてよく知られている HElib と SEAL を対象として PC および Raspberry Pi 上で実装し、そのパフォーマンスを評価した。その結果、両者ともに有効であることを示し、特に、SEAL は物理的に制限されたデバイスにおいて

も優れたパフォーマンスを示した。

（4）計算量的安全性をもつ高機能暗号の構成と安全性評価への応用（論文⑪、⑫など）
情報理論的な仕組みの応用研究として、計算量的安全性をもつ高機能暗号の構成と安全性評価へ適用する研究を様々な視点から行った。特に本応用研究では帰着という技法において活かされていることが多い。まず、耐量子計算機暗号（PQC）の安全性基盤となる格子問題に対する代表的な解法アルゴリズムにおける計算量の下界を世界で初めて導出した。また、様々な高機能暗号の構成への応用として、階層的 ID ベース暗号、（動的）検索可能暗号、しきい値暗号、匿名放送暗号、内積暗号、認証暗号（署名付き暗号）、フォワード安全暗号、漏洩耐性鍵隔離暗号、アグリゲート署名、グループ署名等を研究対象とし、これら高機能暗号における新たな構成法を示した。

＜引用文献＞

① 佐藤慎悟，四方順司，“情報理論的に安全な完全準同型暗号に関する考察”，情報処理学会 CSEC 研究会，研究報告コンピュータセキュリティ（CSEC），2021-CSEC-92，No.69，pp.1-6，2021 年 3 月.
② 清藤武暢，四方順司，“情報銀行のセキュリティに関する一考察”，情報処理学会 CSEC/DPS 合同研究会，研究報告コンピュータセキュリティ（CSEC），2022-CSEC-96，No.29，pp. 1-7， 2022 年 3 月.
③ T. Nakai, S. Shirouchi, Y. Tokushige, M. Iwamoto, K. Ohta, “Secure Computation for Threshold Functions with Physical Cards: Power of Private Permutations,” New Generation Computing, 40, pp.95-113, 2022.
④ Y. Abe, T. Nakai, Y. Kuroki, S. Suzuki, Y. Koga, Y. Watanabe, M. Iwamoto, K. Ohta, “Efficient Card-Based Majority Voting Protocols,” New Generation Computing, 40, pp.173-198, 2022.
⑤ Y. Abe, M. Iwamoto, K. Ohta, “Efficient Private PEZ Protocols for Symmetric Functions,” Theory of Cryptography Conference (TCC 2019), LNCS 11891, Springer, pp.372-392, 2019.
⑥ R. Eriguchi, N. Kunihiro, M. Iwamoto, “Optimal Multiple Assignment Schemes Using Ideal Multipartite Secret Sharing Schemes,” IEEE International Symposium on Information Theory (ISIT 2019), pp.3047-3051, 2019.
⑦ K. Ohara, Y. Watanabe, M. Iwamoto, K. Ohta, “Multi-Party Computation for Modular Exponentiation Based on Replicated Secret Sharing,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, pp.1079-1090, 2019.
⑧ Y. Watanabe, Y. Kuroki, S. Suzuki, Y. Koga, M. Iwamoto, K. Ohta, “Card-Based Majority Voting Protocols with Three Inputs Using Three Cards,” International Symposium on Information Theory and Its Applications (ISITA 2018), pp. 218-222, 2018.
⑨ A. Prasitsupparote, N. Konno, J. Shikata, “Numerical and Non-Asymptotic Analysis of Elias’s and Peres’s Extractors with Finite Input Sequences,” Entropy 2018, 20 (10), 2018.
⑩ A. Prasitsupparote, Y. Watanabe, J. Sakamoto, J. Shikata, T. Matsumoto, “Implementation and Analysis of Fully Homomorphic Encryption in Resource-Constrained Devices,” International Journal of Digital Information and Wireless Communications, pp.288-303, 2019.
⑪ Y. Aono, P. Q. Nguyen, T. Seito, J. Shikata, “Lower Bounds on Lattice Enumeration with Extreme Pruning,” Advances in Cryptology - CRYPTO 2018, LNCS 10992, pp. 608-637, Springer, 2018.
⑫ S. Sato, J. Shikata, “Lattice-Based Signcryption without Random Oracles,” International Conference on Post-Quantum Cryptography (PQCrypto 2018), LNCS 10786, pp. 331-351, Springer, 2018.

５．主な発表論文等

〔雑誌論文〕　計45件（うち査読付論文　18件／うち国際共著　2件／うちオープンアクセス　2件）

１．著者名 清藤武暢，四方順司	４．巻 2022-CSEC-96
２．論文標題 情報銀行のセキュリティに関する一考察	５．発行年 2022年
３．雑誌名 情報処理学会 研究報告コンピュータセキュリティ（CSEC）	６．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 Junichi Ida, Junji Shikata, Yohei Watanabe	４．巻 －
２．論文標題 On the Power of Interaction in Signcryption	５．発行年 2020年
３．雑誌名 2020 International Symposium on Information Theory and Its Applications (ISITA), IEEE	６．最初と最後の頁 348-352
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 佐藤慎悟，四方順司	４．巻 2021-CSEC-92, No.69
２．論文標題 情報理論的に安全な完全準同型暗号に関する考察	５．発行年 2021年
３．雑誌名 情報処理学会 研究報告コンピュータセキュリティ（CSEC）	６．最初と最後の頁 1-6
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 宮澤智輝，佐藤慎悟，四方順司	４．巻 －
２．論文標題 効率的な格子問題に基づくSemi-Adaptive安全な内積暗号	５．発行年 2020年
３．雑誌名 情報処理学会 コンピュータセキュリティシンポジウム2020論文集	６．最初と最後の頁 310-315
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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. Takemure, Y. Sakai, B. Santoso, G. Hanaoka, K. Ohta	4．巻 E104-A(9)
2．論文標題 Achieving Pairing-Free Aggregate Signatures using Pre-Communication between Signers	5．発行年 2021年
3．雑誌名 IEICE Transactions	6．最初と最後の頁 1188-1205
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020DMP0023	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 T. Nakai, S. Shirouchi, Y. Tokushige, M. Iwamoto, K. Ohta	4．巻 40
2．論文標題 Secure Computation for Threshold Functions with Physical Cards: Power of Private Permutations	5．発行年 2022年
3．雑誌名 New Generation Computing	6．最初と最後の頁 95-113
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-022-00153-7	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 Y. Abe, T. Nakai, Y. Kuroki, S. Suzuki, Y. Koga, Y. Watanabe, M. Iwamoto, K. Ohta	4．巻 40
2．論文標題 Efficient Card-Based Majority Voting Protocols	5．発行年 2022年
3．雑誌名 New Generation Computing	6．最初と最後の頁 173-198
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-022-00161-7	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 岩成慶太，中井雄士，渡邉洋平，栃窪孝也，岩本貢	4．巻 －
2．論文標題 一様で閉じたシャッフルの効率的な実装	5．発行年 2022年
3．雑誌名 暗号とセキュリティシンポジウム 2022 (SCIS2022)論文集	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） なし	査読の有無 無
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 淺野京一，岩本貢，渡邉洋平	4．巻 －
2．論文標題 効率的な漏洩耐性鍵隔離暗号	5．発行年 2022年
3．雑誌名 暗号とセキュリティシンポジウム 2022（SCIS2022)論文集	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） なし	査読の有無 無
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 清水聖也，中井雄士，渡邉洋平，岩本貢	4．巻 －
2．論文標題 出力埋め込み可能な紛失擬似ランダム関数に基づく多者間秘匿積集合プロトコルの効率化	5．発行年 2022年
3．雑誌名 暗号とセキュリティシンポジウム 2022（SCIS2022)論文集	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） なし	査読の有無 無
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 土井アナスタシヤ，中井雄士，品川和雅，渡邉洋平，岩本貢	4．巻 －
2．論文標題 カードを用いた秘匿共通集合プロトコル	5．発行年 2021年
3．雑誌名 暗号とセキュリティシンポジウム 2021（SCIS2021)論文集	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） なし	査読の有無 無
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 淺野京一，岩本貢，渡邉洋平	4．巻 －
2．論文標題 秘密鍵の漏洩耐性を有する鍵隔離暗号	5．発行年 2021年
3．雑誌名 暗号とセキュリティシンポジウム 2021（SCIS2021)論文集	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） なし	査読の有無 無
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 J. Shikata, Y. Watanabe	4．巻 Volume 87, Issue 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, Springer	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 S. Sato, J. Shikata	4．巻 LNCS 11929
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 Cryptography and Coding, Springer	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 Y. Abe, M. Iwamoto, K. Ohta	4．巻 LNCS 11891
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), Springer	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 R. Eriguchi, N. Kunihiro, M. 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 K. Ohara, Y. Watanabe, M. Iwamoto, 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 K. Ohara, K. Emura, G. Hanaoka, A. Ishida, K. Ohta, Y. Sakai	4．巻 E102.A
2．論文標題 Shortening the Libert-Peters-Yung Revocable Group Signature Scheme by Using the Random Oracle Methodology	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 1101-1117
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1101	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 宮澤智輝，佐藤慎悟，四方順司	4．巻 2019-CSEC-87, no.1
2．論文標題 格子問題に基づくSemi-Adaptive安全な内積暗号	5．発行年 2019年
3．雑誌名 情報処理学会，研究報告コンピュータセキュリティ(CSEC)	6．最初と最後の頁 1-8
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 竹牟禮薫，坂井祐介，Bagus Santoso，花岡悟一郎，太田和夫	4．巻 -
2．論文標題 事前通信モデルにおけるペアリングを用いない集約署名	5．発行年 2020年
3．雑誌名 2020年暗号と情報セキュリティシンポジウム（SCIS2020）論文集	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） なし	査読の有無 無
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 安部芳紀，岩本貢，太田和夫	4．巻 -
2．論文標題 任意の始集合を持つ関数を計算するprivate PEZプロトコル	5．発行年 2020年
3．雑誌名 2020年暗号と情報セキュリティシンポジウム（SCIS2020）論文集	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） なし	査読の有無 無
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 安部芳紀，岩本貢，太田和夫	4．巻 -
2．論文標題 任意の関数を計算するprivate PEZプロトコルの改善	5．発行年 2019年
3．雑誌名 2019年コンピューターセキュリティシンポジウム（CSS2019)論文集	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） なし	査読の有無 無
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 渡邉洋平，大原一真，岩本貢，太田和夫	4．巻 -
2．論文標題 (強)フォワード安全な動的検索可能暗号の効率的な構成	5．発行年 2019年
3．雑誌名 2019年コンピューターセキュリティシンポジウム（CSS2019)論文集	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） なし	査読の有無 無
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 LNCS 10786
2．論文標題 Lattice-Based Signcryption Without Random Oracles	5．発行年 2018年
3．雑誌名 Proceedings of International Conference on Post-Quantum Cryptography, PQCrypto 2018: Post-Quantum Cryptography, Springer	6．最初と最後の頁 331～351
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-79063-3_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 Aono Yoshinori、Nguyen Phong Q.、Seito Takenobu、Shikata Junji	4．巻 LNCS 10992
2．論文標題 Lower Bounds on Lattice Enumeration with Extreme Pruning	5．発行年 2018年
3．雑誌名 Advances in Cryptology - CRYPTO 2018, Springer	6．最初と最後の頁 608～637
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-96881-0_21	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 Prasitsupparote Amonrat、Konno Norio、Shikata Junji	4．巻 20
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 729～729
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 Sato Shingo、Shikata Junji	4．巻 LNCS 11192
2．論文標題 Signcryption with Quantum Random Oracles	5．発行年 2018年
3．雑誌名 Proc. of The 12th International Conference on Provable Security (ProvSec 2018), Springer	6．最初と最後の頁 406～414
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-01446-9_24	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 Prasitsupparote Amonrat, Watanabe Yohei, Shikata Junji	4．巻 -
2．論文標題 Implementation and Analysis of Fully Homomorphic Encryption in Wearable Devices	5．発行年 2018年
3．雑誌名 Proc. of The Fourth International Conference on Information Security and Digital Forensics (ISDF 2018), The Society of Digital Information and Wireless Communications	6．最初と最後の頁 1～14
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Prasitsupparote Amonrat, Watanabe Yohei, Sakamoto Junichi, Shikata Junji, Matsumoto Tsutomu	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） なし	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 Watanabe Yohei、Kuroki Yoshihisa、Suzuki Shinnosuke、Koga Yuta、Iwamoto Mitsugu、Ohta Kazuo	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. of 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 Espejel-Trujillo Angelina、Iwamoto Mitsugu、Nakano-Miyatake Mariko	4．巻 77 (12)
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 海老名将宏，渡邉洋平，四方順司	4．巻 -
2．論文標題 CBDH仮定に基づく効率的な閾値公開鍵暗号	5．発行年 2018年
3．雑誌名 第21回コンピュータセキュリティシンポジウム（CSS2018）論文集	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） なし	査読の有無 無
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 小川善功，田中亮大，四方順司	4．巻 -
2．論文標題 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	5．発行年 2018年
3．雑誌名 第21回コンピュータセキュリティシンポジウム（CSS2018）論文集	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） なし	査読の有無 無
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 山田憲一，四方順司	4．巻 -
2．論文標題 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	5．発行年 2019年
3．雑誌名 2019年暗号と情報セキュリティシンポジウム（SCIS 2019)論文集	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） なし	査読の有無 無
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 小林大輝，四方順司	4．巻 -
2．論文標題 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	5．発行年 2019年
3．雑誌名 2019年暗号と情報セキュリティシンポジウム（SCIS 2019)論文集	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） なし	査読の有無 無
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 海老名将宏，渡邉洋平，四方順司	4．巻 -
2．論文標題 探索問題の困難性に基づく効率的なしきい値公開鍵暗号の構成	5．発行年 2019年
3．雑誌名 2019年暗号と情報セキュリティシンポジウム（SCIS 2019)論文集	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） なし	査読の有無 無
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 打越忠宏，四方順司	4．巻 -
2．論文標題 KEM/DEMフレームワークを利用したフォワード安全公開鍵暗号と匿名放送型暗号の構成	5．発行年 2019年
3．雑誌名 2019年暗号と情報セキュリティシンポジウム（SCIS 2019)論文集	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） なし	査読の有無 無
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 安部 芳紀，山本 翔太，岩本 貢，太田 和夫	4．巻 118（478）
2．論文標題 初期文字列が29 文字の4入力多数決Private PEZプロトコル	5．発行年 2019年
3．雑誌名 電子情報通信学会信学技報	6．最初と最後の頁 223～228
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 渡邉洋平，岩本貢，太田 和夫	4．巻 -
2．論文標題 効率的でフォワード安全な動的検索可能暗号	5．発行年 2019年
3．雑誌名 2019年暗号と情報セキュリティシンポジウム（SCIS 2019)論文集	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） なし	査読の有無 無
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 安部 芳紀，山本 翔太，岩本 貢，太田 和夫	4．巻 -
2．論文標題 不正検知可能な3入力多数決カードプロトコル	5．発行年 2019年
3．雑誌名 2019年暗号と情報セキュリティシンポジウム（SCIS 2019)論文集	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） なし	査読の有無 無
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 山本 翔太，安部 芳紀，岩本 貢，太田 和夫	4．巻 -
2．論文標題 4入力多数決を計算する効率的なPrivate PEZプロトコル	5．発行年 2019年
3．雑誌名 2019年暗号と情報セキュリティシンポジウム（SCIS 2019)論文集	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） なし	査読の有無 無
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 平野 貴人，川合 豊，小関 義博，岩本 貢，太田 和夫	4．巻 -
2．論文標題 共通鍵型マルチユーザ検索可能暗号の検索機能拡張	5．発行年 2019年
3．雑誌名 2019年暗号と情報セキュリティシンポジウム（SCIS 2019)論文集	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） なし	査読の有無 無
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 Wang Wenjia, Abe Yoshiki, Iwamoto Mitsugu, Ohta Kazuo	4．巻 -
2．論文標題 Three-Party Private Set Operation Protocols Using Polynomials and OPPRF	5．発行年 2019年
3．雑誌名 2019年暗号と情報セキュリティシンポジウム（SCIS 2019)論文集	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） なし	査読の有無 無
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 江利口礼央，國廣昇，岩本貢	4．巻 -
2．論文標題 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	5．発行年 2018年
3．雑誌名 第41回情報理論とその応用シンポジウム論文集	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） なし	査読の有無 無
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 渡邉洋平，大原一真，岩本貢，太田和夫	４．巻 118（151）
２．論文標題 現実的な結託者のもとで最もシェア長の短いロバスト秘密分散法	５．発行年 2018年
３．雑誌名 電子情報通信学会信学技報	６．最初と最後の頁 1〜8
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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36件（うち招待講演　6件／うち国際学会　10件）

１．発表者名 清藤武暢，四方順司
２．発表標題 情報銀行のセキュリティに関する一考察
３．学会等名 情報処理学会CSEC/DPS合同研究会
４．発表年 2022年

１．発表者名 Junichi Ida, Junji Shikata, Yohei Watanabe
２．発表標題 On the Power of Interaction in Signcryption
３．学会等名 2020 International Symposium on Information Theory and Its Applications (ISITA)（国際学会）
４．発表年 2020年

１．発表者名 佐藤慎悟，四方順司
２．発表標題 情報理論的に安全な完全準同型暗号に関する考察
３．学会等名 情報処理学会CSEC/DPS合同研究会
４．発表年 2021年

１．発表者名
宮澤智輝，佐藤慎悟，四方順司

２．発表標題
効率的な格子問題に基づくSemi-Adaptive安全な内積暗号

３．学会等名
情報処理学会 コンピュータセキュリティシンポジウム2020

４．発表年
2020年

１．発表者名
岩成慶太，中井雄士，渡邉洋平，栃窪孝也，岩本貢

２．発表標題
一様で閉じたシャッフルの効率的な実装

３．学会等名
暗号とセキュリティシンポジウム 2022 (SCIS2022)

４．発表年
2022年

１．発表者名
淺野京一，岩本貢，渡邉洋平

２．発表標題
効率的な漏洩耐性鍵隔離暗号

３．学会等名
暗号とセキュリティシンポジウム 2022 (SCIS2022)

４．発表年
2022年

１．発表者名
清水聖也，中井雄士，渡邉洋平，岩本貢

２．発表標題
出力埋め込み可能な紛失擬似ランダム関数に基づく多者間秘匿積集合プロトコルの効率化

３．学会等名
暗号とセキュリティシンポジウム 2022 (SCIS2022)

４．発表年
2022年

１．発表者名
土井アナスタシヤ，中井雄士，品川和雅，渡邉洋平，岩本貢

２．発表標題
カードを用いた秘匿共通集合プロトコル

３．学会等名
暗号とセキュリティシンポジウム 2021 (SCIS2021)

４．発表年
2021年

１．発表者名
淺野京一，岩本貢，渡邉洋平

２．発表標題
秘密鍵の漏洩耐性を有する鍵隔離暗号

３．学会等名
暗号とセキュリティシンポジウム 2021 (SCIS2021)

４．発表年
2021年

１．発表者名
M. Ebina, Y. Watanabe, J. Shikata

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

３．学会等名
14th International Workshop on Security (IWSEC2019)（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
K. Ohta

２．発表標題
Strong Forward Privacy for Dynamic Searchable Encryption

３．学会等名
Seminar at Google; Searchable Encryption Talk（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
K. Ohta

２．発表標題
Card-based Majority Voting Protocols with Three Inputs Using Three Cards

３．学会等名
The International Secure Multi-party Computation Forum（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
S. Sato, J. Shikata

２．発表標題
SO-CCA secure PKE in the Quantum Random Oracle Model or the Quantum Ideal Cipher Model

３．学会等名
17th IMA International Conference on Cryptography and Coding（国際学会）

４．発表年
2019年

１．発表者名
Y. Abe, M. Iwamoto, K. Ohta

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

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

４．発表年
2019年

１．発表者名
竹牟禮薫，坂井祐介，Bagus Santoso，花岡悟一郎，太田和夫

２．発表標題
事前通信モデルにおけるペアリングを用いない集約署名

３．学会等名
2020年暗号と情報セキュリティシンポジウム（SCIS2020）

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
2020年暗号と情報セキュリティシンポジウム（SCIS2020）

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
2019年コンピューターセキュリティシンポジウム（CSS2019）

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
2019年コンピューターセキュリティシンポジウム（CSS2019）

４．発表年
2019年

１．発表者名
Shikata Junji

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
Sato Shingo

２．発表標題
Lattice-based Signcryption without Random Oracles

３．学会等名
International Conference on Post-Quantum Cryptography (PQCrypto 2018)（国際学会）

４．発表年
2018年

１．発表者名
Sato Shingo

２．発表標題
Signcryption with Quantum Random Oracles

３．学会等名
The 12th International Conference on Provable Security (ProvSec 2018)（国際学会）

４．発表年
2018年

１．発表者名
Prasitsupparote Amonrat

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)（国際学会）

４．発表年
2018年

１．発表者名
海老名将宏

２．発表標題
CBDH仮定に基づく効率的な閾値公開鍵暗号

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（CSS2018）

４．発表年
2018年

１．発表者名
小川善功

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（CSS2018）

４．発表年
2018年

１．発表者名
山田憲一

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
小林大輝

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
海老名将宏

２．発表標題
探索問題の困難性に基づく効率的なしきい値公開鍵暗号の構成

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
打越忠宏

２．発表標題
KEM/DEMフレームワークを利用したフォワード安全公開鍵暗号と匿名放送型暗号の構成

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
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
太田和夫

２．発表標題
現代暗号研究の事始め ～ 1つのケーススタディ ～

３．学会等名
電子情報通信学会 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（招待講演）

４．発表年
2019年

１．発表者名
安部 芳紀

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
電子情報通信学会 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

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
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
安部芳紀

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
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
山本翔太

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
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
Wang Wenjia

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

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 渡邉洋平
２．発表標題 現実的な結託者のもとで最もシェア長の短いロバスト秘密分散法
３．学会等名 電子情報通信学会情報セキュリティ研究会
４．発表年 2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

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	松本　勉 (Matsumoto Tsutomu) (40183107)	横浜国立大学・大学院環境情報研究院・教授 (12701)	
研究分担者	岩本　貢 (Iwamoto Mitsugu) (50377016)	電気通信大学・大学院情報理工学研究科・准教授 (12612)	
研究分担者	太田　和夫 (Ohta Kazuo) (80333491)	電気通信大学・大学院情報理工学研究科・特命教授 (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