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　６ 年　 ６ 月 １４ 日現在

機関番号：８２６２６
研究種目：基盤研究(A)（一般）
研究期間：2019～2023
課題番号：１９Ｈ０１１０９

研究課題名（和文）あらゆる高機能暗号方式の相互変換を可能にするアジャイルクリプト技術

研究課題名（英文）Agilecrypt Frameworks for Advanced Cryptographic Primitive Constructions, Compositions, and Conversions

研究代表者

Ａｔｔｒａｐａｄｕｎｇ　Ｎｕｔｔａｐｏｎｇ（Attrapadung, Nuttapong）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・研究チーム長

研究者番号：４０５１５３００

交付決定額（研究期間全体）：（直接経費）　　34,700,000円

研究成果の概要（和文）：本研究は、複数の高機能暗号方式を組み合わせや変換が可能とする「アジャイルクリプト技術」の実現に向けて、理論的枠組みを設計したものである。本研究の成果には、属性ベース暗号、関数型暗号、準同型暗号、属性ベース署名、秘密計算、ゼロ知識証明、プライバシー保護データ分析技術などが含まれる。特に、複雑なアクセスポリシーに対応可能な属性ベース暗号方式を、単純なポリシーの方式から変換できるモジュラー構成枠組みが代表的な成果である。これらの結果は、Eurocrypt ’19、Asiacrypt ’20、Crypto ’24などで発表された。本プロジェクト全体で発表した論文は40本以上に達する。

研究成果の学術的意義や社会的意義
本研究の学術的意義は、高度な暗号プリミティブの設計と組み合わせを可能にする新しい理論的枠組みを提供する点にある。これにより、複雑な暗号システムの構築が容易になり、暗号理論の発展に寄与する。また、社会的意義としては、安全で柔軟なデータ保護技術を提供することで、プライバシー保護やデータセキュリティの向上が期待される。これにより、医療、金融、行政などの分野でのデータ利用が促進され、社会全体の信頼性と安全性が向上する。

研究成果の概要（英文）：We design theoretical frameworks that compose advanced cryptographic primitives or schemes in secure, compatible, and agile manners, collectively termed Agilecrypt. Our research encompasses composition frameworks for advanced encryption methods such as attribute-based, functional, and homomorphic encryption. Additionally, we have developed frameworks for attribute-based signatures, multi-party computation, proof systems, and privacy-preserving data analysis techniques. A highlight of our work is a series of results on modular compositions for attribute-based encryption (ABE), enabling system adopters to derive complex ABE policies from simpler ones in an agile manner. The security of these composed schemes is generically ensured by a central theorem. Our ABE results have been published in top-tier conferences such as Eurocrypt ’19, Asiacrypt ’20, and Crypto ’24. Overall, we have produced more than 40 papers on this project.

研究分野：情報学

キーワード：暗号理論　情報セキュリティ　高機能暗号

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

情報システムの高度化に伴い、個人の健康、財産、権利、行動履歴等に関するプライバシ情報を幅広い用途に活用し、社会の利便性向上に役立てようとする動きが活発になっている。しかし、これらの情報利用は、深刻なプライバシ侵害に繋がる可能性があるため、高機能暗号の研究が重要視されている。例えば、複雑なアクセス制御が可能な「属性ベース暗号」や、暗号化したままデータの利活用を可能とする「準同型暗号」や「関数暗号」などが代表的である。国内外で高機能暗号の研究開発が進められているが、多くの場合、システム要求に応じた個別設計が必要であり、それぞれのシステムに合わせた専用設計とセキュリティ保証を毎回提供しなければならない。また、異なるシステム間で暗号化データを活用することも困難である。既存の高機能暗号の全ての機能を併せ持つ新しい高機能暗号の設計は考えられるが、その設計は極めて複雑であり、安全性の数学的証明や高い処理性能の提供は非常に困難である。

２．研究の目的

本研究の目的は、システムの機能に応じて複数の暗号プリミティブを容易に組み合わせや変換できる一般的なフレームワークを提案し、専用設計や個別の安全性証明の必要性を軽減することである。このフレームワークの重要なポイントは、安全性の数学的証明を統一的に取り扱える安全性定理を導くことである。また、様々な高機能暗号を扱えるように、組み合わせや変換について様々なレベルを検討する必要がある。具体的には、個別暗号方式間の変換、暗号技術機能間の変換、暗号要素技術間の変換というレベルが挙げられる。また、高機能暗号の基盤理論の確立、属性ベース暗号・関数暗号のフレームワーク確立、準同型暗号・秘密計算・プライバシ保護技術のフレームワーク確立といった課題を設定した。

３．研究の方法

本研究の主な方法は、従来の高機能暗号方式およびその要素技術を適切なクラスを選定および分類し、そのクラス全体の共通点を抽象化することで、多様な機能を持つ高機能暗号を取り扱える設計フレームワークを構築することである。さらに、抽象化した数学的構造を活用して、統一的かつ取り扱い可能な安全性証明を与える。なお、本研究で扱うほとんどの暗号方式は計算量的な安全性も持つものであり、その場合、安全性の証明には数学的困難性仮定が必要であるが、できる限り標準的な計算量仮定に基づく暗号学的証明を行うことが一つの目標となっている。

４．研究成果

本研究成果は、複数の高機能暗号方式を組み合わせや変換が可能な理論的枠組みの提案である。代表的な成果は以下である。

(1) 属性ベース暗号および関数暗号に関して、世界で初めて動的で暗号方式を組み合わせる変換手法の設計フレームワークの構築に成功した。本研究は様々レベルの変換に成功し、暗号研究分野のトップ国際会議である Eurocrypt’19、Eurocrypt’20、Asiacrypt’20 そして Crypto’24（いわゆる暗号三大国際学会）に採録された。最初の Eurocrypt’19 のフレームワークでは、単純な機能のみを取り扱う方式から、動的かつ無制限に組み合わせることで、複雑な述語に対応可能な新しい属性ベース暗号を提案した。これにより、ユーザーは自身の秘密鍵または暗号文に対し任意かつ無制限のサイズの組み合わせポリシーを指定できる。具体的には、任意のスパンプログラム、任意の分岐プログラム、および任意の決定性有限オートマトンの三つの組み合わせポリシークラスに対する変換を提案した。これらの汎用ポリシーは任意の述語に対して定義されており、モジュラーな組み合わせが可能となる。Asiacrypt’20 では、統一的な安全性証明に利用された仮定をより標準的な計算量仮定に改良し、Crypto’24 では、信頼する第三者を必要としない「登録属性ベース暗号」を含む新しい高機能暗号の組み合わせ変換フレームワークを構築した。さらに、Eurocrypt’20 では、属性ベース暗号の組み合わせ変換を行うことで世界初の理論的に最適な放送型暗号の構築にも成功し、Best Paper Award を受賞した。
(2) 秘匿計算という、情報を秘匿したままデータ解析ができる技術に関して、データベース処理に有用な秘密技術変換フレームワークを構築した。これらの成果は、情報セキュリティ分野トップ国際会議である ACM CCS’21、ACM AsiaCCS’22,および ACM CCS’22 に採録された。（なお、ACM CCS は当時 Google Scholar Computer Security and Cryptography subcategory のランク１であった。）特に、秘匿 Shuffle や秘匿 Sort などを含む Linear group action と

呼ばれる代数的な計算クラス、秘匿分割データの並列計算、そして秘匿大小比較計算などの効率的なプロトコルが得られた。また、秘密分散フォームの変換が可能とする方式を提案し、この変換により従来の方式より 効率な秘匿計算プロトコルが得られた。この成果は国際会議 ACISP 2019 にて発表し、Best Paper Award を受賞した。秘密分散の変換技術を応用し、プライバシー保護可能な機械学習プロトコルを提案し、成果は国際論文誌 IEEE Access および IEICE Transaction で発表した。秘匿計算に有用とされる秘匿大小比較プロトコルについて様々なデータフォーマットに対応できる変換を提案し、国際論文誌 IEICE Transactions で発表した。また、効率的な通信ラウンドの秘密計算および準同型秘密分散方式の成果が得られた(国際会議 CRYPTO21、ASIACRYPT21、IWSEC21)。プライバシー保護検索(Private Information Retrieval)の高度化(国際会議 Esorics'20, TCC'22、 ITC'22)、差分プライバシ技術の高度化(国際会議 ACM CCS'22)の成果が得られた。

(3) その他の高機能暗号および暗号プリミティブに関し、以下の成果が得られた。低い安全性を持つ公開鍵暗号から、高い安全性の公開鍵暗号方式に変換可能な技術を提案し、成果は暗号理論分野のトップ国際会議 TCC'19 および国際論文誌 Journal of Cryptology に採録された。また、関数暗号の高度化(国際会議 CRYPTO'21, CRYPTO'22、TCC'22)、ブラインド署名の高効率化(国際会議 Eurocrypt'21)、集約署名の高度化(国際論文誌 IEICE)、ID ベース暗号の高度化(国際論文誌 IEICE, 国際会議 APKC'21)、準同型暗号の高度化・高安全化(国際会議 ACISP'22、IWSEC'22、APKC'22)、関数署名の高度化(国際会議 SCN'22)、ゼロ知識証明技術の変換(国際論文誌 Journal of Cryptology)などの成果が得られた。

５．主な発表論文等

〔雑誌論文〕　計41件（うち査読付論文　41件／うち国際共著　5件／うちオープンアクセス　8件）

１．著者名 Nuttapong Attrapadung, Hiraku Morita, Kazuma Ohara, Jacob C. N. Schuldt, Tadanori Teruya, Kazunari Tozawa	４．巻 -
２．論文標題 Secure Parallel Computation on Privately Partitioned Data and Applications	５．発行年 2022年
３．雑誌名 ACM SIGSAC Conference on Computer and Communications Security CCS 2022	６．最初と最後の頁 151-164
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3548606.3560695	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 Nuttapong Attrapadung, Hiraku Morita, Kazuma Ohara, Jacob C. N. Schuldt, Kazunari Tozawa	４．巻 -
２．論文標題 Memory and Round-Efficient MPC Primitives in the Pre-Processing Model from Unit Vectorization	５．発行年 2022年
３．雑誌名 ACM ASIACCS 2022	６．最初と最後の頁 858-872
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3488932.3517407	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 Nuttapong Attrapadung, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Takahiro Matsuda, Ibuki Mishina, Hiraku Morita, Jacob C. N. Schuldt	４．巻 4
２．論文標題 Adam in Private: Secure and Fast Training of Deep Neural Networks with Adaptive Moment Estimation	５．発行年 2022年
３．雑誌名 Proc. Priv. Enhancing Technol. (PETS) 2022(4)	６．最初と最後の頁 746-767
掲載論文のDOI（デジタルオブジェクト識別子） 10.56553/popets-2022-0131	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 Reo Eriguchi, Kaoru Kurosawa, Koji Nuida	４．巻 -
２．論文標題 On the Optimal Communication Complexity of Error-Correcting Multi-Server PIR	５．発行年 2022年
３．雑誌名 Proceedings of TCC 2022	６．最初と最後の頁 60-88
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-22368-6_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 Yusaku Maeda, Koji Nuida	4．巻 -
2．論文標題 Chosen Ciphertext Secure Keyed Two-Level Homomorphic Encryption	5．発行年 2022年
3．雑誌名 Proceedings of ACISP 2022	6．最初と最後の頁 209-228
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-22301-3_11	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 Hirotomo Shinoki, Koji Nuida	4．巻 -
2．論文標題 On Extension of Evaluation Algorithms in Keyed-Homomorphic Encryption	5．発行年 2022年
3．雑誌名 Proceedings of IWSEC 2022	6．最初と最後の頁 189-207
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-15255-9_10	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, Kaoru Kurosawa, Koji Nuida	4．巻 -
2．論文標題 Multi-Server PIR with Full Error Detection and Limited Error Correction	5．発行年 2022年
3．雑誌名 Proceedings of ITC 2022	6．最初と最後の頁 1:1-1:20
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITC.2022.1	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 Koji Nuida	4．巻 -
2．論文標題 How to Handle Invalid Queries for Malicious-Private Protocols Based on Homomorphic Encryption	5．発行年 2022年
3．雑誌名 Proceedings of The 9th ACM ASIA Public-Key Cryptography Workshop (APKC 2022)	6．最初と最後の頁 15-25
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3494105.3526238	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 Jacob Imola, Takao Murakami, Kamalika Chaudhuri	４．巻 -
２．論文標題 Differentially Private Triangle and 4-Cycle Counting in the Shuffle Model	５．発行年 2022年
３．雑誌名 ACM SIGSAC Conference on Computer and Communications Security CCS 2022	６．最初と最後の頁 1505-1519
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3548606.3560659	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 該当する

１．著者名 Fuyuki Kitagawa, Takahiro Matsuda, Takashi Yamakawa	４．巻 36
２．論文標題 NIZK from SNARGs	５．発行年 2022年
３．雑誌名 Journal of Cryptology	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） 10.1007/s00145-023-09449-3	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 Fuyuki Kitagawa, Takahiro Matsuda, Keisuke Tanaka	４．巻 35
２．論文標題 CCA Security and Trapdoor Functions via Key-Dependent-Message Security	５．発行年 2022年
３．雑誌名 Journal of Cryptology	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） 10.1007/s00145-022-09420-8	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 －

１．著者名 Shweta Agrawal, Anshu Yadav, Shota Yamada	４．巻 -
２．論文標題 Multi-input Attribute Based Encryption and Predicate Encryption	５．発行年 2022年
３．雑誌名 CRYPTO 2022	６．最初と最後の頁 590-621
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-15802-5_21	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 該当する

1．著者名 Shweta Agrawal, Fuyuki Kitagawa, Anuja Modi, Ryo Nishimaki, Shota Yamada, Takashi Yamakawa	4．巻 -
2．論文標題 Bounded Functional Encryption for Turing Machines: Adaptive Security from General Assumptions	5．発行年 2022年
3．雑誌名 TCC (1) 2022	6．最初と最後の頁 618-647
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-22318-1_22	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 該当する

1．著者名 Yusuke Sakai	4．巻 -
2．論文標題 Succinct Attribute-Based Signatures for Bounded-Size Circuits by Combining Algebraic and Arithmetic Proofs	5．発行年 2022年
3．雑誌名 Security and Cryptography for Networks, SCN 2022	6．最初と最後の頁 711-734
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-14791-3_31	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 Yi Lu, Keisuke Hara, Kazuma Ohara, Jacob C. N. Schuldt, Keisuke Tanaka	4．巻 -
2．論文標題 Efficient Two-Party Exponentiation from Quotient Transfer	5．発行年 2022年
3．雑誌名 Applied Cryptography and Network Security - 20th International Conference, ACNS 2022	6．最初と最後の頁 643-662
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-09234-3_32	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 Kittiphop Phalakarn, Nuttapong Attrapadung, Kanta Matsuura	4．巻 -
2．論文標題 Efficient Oblivious Evaluation Protocol and Conditional Disclosure of Secrets for DFA	5．発行年 2022年
3．雑誌名 Applied Cryptography and Network Security - 20th International Conference, ACNS 2022	6．最初と最後の頁 605-625
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-09234-3_30	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 Phalakarn Kittiphop、Suppakitpaisarn Vorapong、Attrapadung Nuttapong、Matsuura Kanta	4．巻 12835
2．論文標題 Evolving Homomorphic Secret Sharing for Hierarchical Access Structures	5．発行年 2021年
3．雑誌名 IWSEC 2021 (Lecture Notes in Computer Science)	6．最初と最後の頁 77～96
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-85987-9_5	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 Attrapadung Nuttapong、Hanaoaka Goichiro、Matsuda Takahiro、Morita Hiraku、Ohara Kazuma、Schuldt Jacob C. N.、Teruya Tadanori、Tozawa Kazunari	4．巻 n/a
2．論文標題 Oblivious Linear Group Actions and Applications	5．発行年 2021年
3．雑誌名 ACM SIGSAC Conference on Computer and Communications Security CCS 2021	6．最初と最後の頁 630-650
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3460120.3484584	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 Kitagawa Fuyuki、Matsuda Takahiro、Tanaka Keisuke	4．巻 35
2．論文標題 CCA Security and Trapdoor Functions via Key-Dependent-Message Security	5．発行年 2022年
3．雑誌名 Journal of Cryptology	6．最初と最後の頁 n/a
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00145-022-09420-8	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 －

1．著者名 TAKEMURE Kaoru、SAKAI Yusuke、SANTOSO Bagus、HANAOKA Goichiro、OHTA Kazuo	4．巻 E104.A
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 on Fundamentals of Electronics, Communications and Computer Sciences	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 Eriguchi Reo、Ohara Kazuma、Yamada Shota、Nuida Koji	4．巻 12826
2．論文標題 Non-interactive Secure Multiparty Computation for Symmetric Functions, Revisited: More Efficient Constructions and Extensions	5．発行年 2021年
3．雑誌名 CRYPTO 2021 (Lecture Notes in Computer Science)	6．最初と最後の頁 305～334
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-84245-1_11	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 Eriguchi Reo、Nuida Koji	4．巻 13091
2．論文標題 Homomorphic Secret Sharing for Multipartite and General Adversary Structures Supporting Parallel Evaluation of Low-Degree Polynomials	5．発行年 2021年
3．雑誌名 ASIACRYPT 2021 (Lecture Notes in Computer Science)	6．最初と最後の頁 191～221
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-92075-3_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 Hara Keisuke、Matsuda Takahiro、Hanaoka Goichiro、Tanaka Keisuke	4．巻 90
2．論文標題 Generic transformation from broadcast encryption to round-optimal deniable ring authentication	5．発行年 2022年
3．雑誌名 Designs, Codes and Cryptography	6．最初と最後の頁 277～316
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-021-00975-4	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 HARA Keisuke、MATSUDA Takahiro、TANAKA Keisuke	4．巻 E105.A
2．論文標題 Receiver Selective Opening Chosen Ciphertext Secure Identity-Based Encryption	5．発行年 2022年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 160～172
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021CIP0006	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 Hara Keisuke、Matsuda Takahiro、Tanaka Keisuke	4．巻 n/a
2．論文標題 Receiver Selective Opening Chosen Ciphertext Secure Identity-Based Encryption	5．発行年 2021年
3．雑誌名 Proceedings of the 8th ACM on ASIA Public-Key Cryptography Workshop (APKC 2021)	6．最初と最後の頁 51-59
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3457338.3458294	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 Agrawal Shweta、Maitra Monosij、Vempati Narasimha Sai、Yamada Shota	4．巻 12828
2．論文標題 Functional Encryption for Turing Machines with Dynamic Bounded Collusion from LWE	5．発行年 2021年
3．雑誌名 CRYPTO (4) 2021: (Lecture Notes in Computer Science)	6．最初と最後の頁 239～269
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-84259-8_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 該当する

1．著者名 Katsumata Shuichi、Nishimaki Ryo、Yamada Shota、Yamakawa Takashi	4．巻 12696
2．論文標題 Round-Optimal Blind Signatures in the Plain Model from Classical and Quantum Standard Assumptions	5．発行年 2021年
3．雑誌名 EUROCRYPT (1) 2021: (Lecture Notes in Computer Science)	6．最初と最後の頁 404～434
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-77870-5_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 Attrapadung Nuttapong、Tomida Junichi	4．巻 12493
2．論文標題 Unbounded Dynamic Predicate Compositions in ABE from Standard Assumptions	5．発行年 2020年
3．雑誌名 ASIACRYPT 2020 (Lecture Notes in Computer Science)	6．最初と最後の頁 405～436
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-64840-4_14	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 Hayata Junichiro、Schuldt Jacob C. N.、Hanaoka Goichiro、Matsuura Kanta	4．巻 12309
2．論文標題 On Private Information Retrieval Supporting Range Queries	5．発行年 2020年
3．雑誌名 ESORICS (2) 2020 (Lecture Notes in Computer Science)	6．最初と最後の頁 674～694
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-59013-0_33	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 Phalakarn Kittiphop、Suppakitpaisarn Vorapong、Attrapadung Nuttapong、Matsuura Kanta	4．巻 12578
2．論文標題 Constructive t-secure Homomorphic Secret Sharing for Low Degree Polynomials	5．発行年 2020年
3．雑誌名 INDOCRYPT 2020 (Lecture Notes in Computer Science)	6．最初と最後の頁 763～785
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-65277-7_34	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 NISHIDA Naohisa、OBA Tatsumi、UNAGAMI Yuji、PAUL CRUZ Jason、YANAI Naoto、TERUYA Tadanori、ATTRAPADUNG Nuttapong、MATSUDA Takahiro、HANAOKA Goichiro	4．巻 E103.A
2．論文標題 Efficient Secure Neural Network Prediction Protocol Reducing Accuracy Degradation	5．発行年 2020年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1367～1380
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020TAP0011	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 Hanaoka Goichiro、Komatsu Misaki、Ohara Kazuma、Sakai Yusuke、Yamada Shota	4．巻 12309
2．論文標題 Semantic Definition of Anonymity in Identity-Based Encryption and Its Relation to Indistinguishability-Based Definition	5．発行年 2020年
3．雑誌名 ESORICS (2) 2020 (Lecture Notes in Computer Science)	6．最初と最後の頁 65～85
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-59013-0_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 Takemure Kaoru、Sakai Yusuke、Santoso Bagus、Hanaoka Goichiro、Ohta Kazuo	４．巻 12505
２．論文標題 Achieving Pairing-Free Aggregate Signatures using Pre-Communication between Signers	５．発行年 2020年
３．雑誌名 ProvSec 2020 (Lecture Notes in Computer Science)	６．最初と最後の頁 65～84
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-62576-4_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 Agrawal Shweta、Yamada Shota	４．巻 12550
２．論文標題 CP-ABE for Circuits (and More) in the Symmetric Key Setting	５．発行年 2020年
３．雑誌名 TCC (1) 2020: (Lecture Notes in Computer Science)	６．最初と最後の頁 117～148
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-64375-1_5	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 Katsumata Shuichi、Nishimaki Ryo、Yamada Shota、Yamakawa Takashi	４．巻 12493
２．論文標題 Adaptively Secure Inner Product Encryption from LWE	５．発行年 2020年
３．雑誌名 ASIACRYPT (3) 2020: (Lecture Notes in Computer Science)	６．最初と最後の頁 375～404
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-64840-4_13	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 Attrapadung Nuttapong	４．巻 11476
２．論文標題 Unbounded Dynamic Predicate Compositions in Attribute-Based Encryption	５．発行年 2019年
３．雑誌名 Eurocrypt 2019 (Lecture Notes in Computer Science)	６．最初と最後の頁 34～67
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-17653-2_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 Kikuchi Ryo、Attrapadung Nuttapong、Hamada Koki、Ikarashi Dai、Ishida Ai、Matsuda Takahiro、Sakai Yusuke、Schuldt Jacob C. N.	4．巻 11547
2．論文標題 Field Extension in Secret-Shared Form and Its Applications to Efficient Secure Computation	5．発行年 2019年
3．雑誌名 ACISP 2019 (Lecture Notes in Computer Science)	6．最初と最後の頁 343～361
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-21548-4_19	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 Kitai Hiromasa、Hanaoka Goichiro、Cruz Jason Paul、Yanai Naoto、Nishida Naohisa、Oba Tatsumi、Unagami Yuji、Teruya Tadanori、Attrapadung Nuttapong、Matsuda Takahiro	4．巻 7
2．論文標題 MOBIUS: Model-Oblivious Binarized Neural Networks	5．発行年 2019年
3．雑誌名 IEEE Access	6．最初と最後の頁 139021～139034
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2939410	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 ATTRAPADUNG Nuttapong、HANAOKA Goichiro、KIYOMOTO Shinsaku、MIMOTO Tomoaki、C. N. SCHULDT Jacob	4．巻 E102.A
2．論文標題 A Taxonomy of Secure Two-Party Comparison Protocols and Efficient Constructions	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 1048～1060
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1048	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 Kitagawa Fuyuki、Matsuda Takahiro	4．巻 11892
2．論文標題 CPA-to-CCA Transformation for KDM Security	5．発行年 2019年
3．雑誌名 TCC 2019 (Lecture Notes in Computer Science)	6．最初と最後の頁 118～148
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-36033-7_5	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 Attrapadung Nuttapong、Tomida Junichi	4．巻 -
2．論文標題 A Modular Approach to Registered ABE for Unbounded Predicates	5．発行年 2024年
3．雑誌名 CRYPTO 2024 (Lecture Notes in Computer Science)	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 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2件（うち招待講演　0件／うち国際学会　2件）

1．発表者名 Attrapadung Nuttapong
2．発表標題 Unbounded Dynamic Predicate Compositions in Attribute-Based Encryption
3．学会等名 Eurocrypt 2019（国際学会）
4．発表年 2019年

1．発表者名 Matsuda Takahiro
2．発表標題 CPA-to-CCA Transformation for KDM Security
3．学会等名 TCC 2019（国際学会）
4．発表年 2019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	縫田　光司 (Nuida Koji) (20435762)	九州大学・マス・フォア・インダストリ研究所・教授 (17102)	

6．研究組織（つづき）

	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	照屋　唯紀 (Teruya Tadanori) (20636972)	国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員 (82626)	
研究分担者	花岡　悟一郎 (Hanaoka Goichiro) (30415731)	国立研究開発法人産業技術総合研究所・情報・人間工学領域・首席研究員 (82626)	
研究分担者	坂井　祐介 (Sakai Yusuke) (40750659)	国立研究開発法人産業技術総合研究所・情報・人間工学領域・研究員 (82626)	
研究分担者	松田　隆宏 (Matsuda Takahiro) (60709492)	国立研究開発法人産業技術総合研究所・情報・人間工学領域・研究チーム長 (82626)	
研究分担者	山田　翔太 (Yamada Shota) (70750834)	国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員 (82626)	
研究分担者	村上　隆夫 (Murakami Takao) (80587981)	統計数理研究所・データ科学研究系・准教授 (62603)	
研究分担者	Ｓｃｈｕｌｄｔ　Ｊａｃｏｂ (Schuldt Jacob) (80750893)	国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員 (82626)	

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