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 ２０ 日現在

機関番号：１２６０８
研究種目：基盤研究(B)（一般）
研究期間：2017～2020
課題番号：１７Ｈ０１６９５

研究課題名（和文）インセンティブを考慮した暗号基盤技術の構築

研究課題名（英文）Constructions for Cryptographic Primitives with Incentives

研究代表者
田中　圭介（Tanaka, Keisuke）

東京工業大学・情報理工学院・教授

研究者番号：２０３３４５１８

交付決定額（研究期間全体）：（直接経費）　　12,200,000円

研究成果の概要（和文）：インセンティブ設計技法に関する調査と研究を行った。詳細な調査や手法の比較を行ない、インセンティブを用いた電子署名・相手認証のモデルと技術の設計を試みた。特に、これらの要素に密接に関わるSecure Message Transmission (SMT) と呼ばれる要素に着目し、複数ある通信路がすべての敵に支配されたとしても、合理的な敵を考える場合には、安全に通信を行うことができることを示した。さらに、ブロックチェーンに関する調査と研究を行った。特にproof-of-workの原点に立ち戻り、証明者と検証者で時間とメモリのギャップを生じる状況についての考察を行った。

研究成果の学術的意義や社会的意義
インセンティブ付与の重要性が、ナカモトサトシによる原論文(2008)でも言及されている。ビットコインでは、ブロックをチェーンに接続させることに対して報酬が付与され、その額は4年毎に半減する。このような報酬設定は、直観的なアイディアにもとづいて行われており、適切か否かに 関する厳密な議論は行われていない。本研究は、直観的なアイディアによるものではではなく、理論的な考察によりある種の妥当性を示すことに成功している。具体的に、合意形成に用いるための計算において、証明者と検証者で時間とメモリのギャップを生じる状況についての考察に成功している。

研究成果の概要（英文）：We conducted a survey and research on incentive design techniques. Through detailed surveys and comparisons of techniques, we attempted to design models and techniques for incentive-based digital signatures and authentication. In particular, we focused on an element called Secure Message Transmission (SMT), which is closely related to these elements, and showed that even if multiple communication channels are all controlled by an adversary, communication can be performed securely when a rational adversary is considered. In addition, we conducted a survey and research on blockchain. In particular, we returned to the origin of proof-of-work and examined the situation where a time and memory gap occurs between the prover and the verifier.

研究分野：暗号理論、情報セキュリティ、暗号通貨・ブロックチェーン

キーワード：暗号　安全性　インセンティブ設計　ゲーム理論　ブロックチェーン　暗号通貨

１．研究開始当初の背景

ゲーム理論と暗号技術：従来の暗号理論では、暗号技術・プロトコルの参加者は基本的に、正直者か攻撃者のどちらかであると考えられてきた。例えば、公開鍵暗号方式では、メッセージの送信者と受信者は正しく計算を行うと仮定し、攻撃者はその内容を入手・改竄するため出来る限りの手段を取る。しかしながら、このような設定は必ずしも現実的とはいえない。現実世界では、攻撃者も攻撃のためのコストや不正発覚のリスクを考慮する。攻撃によって得られる利益がコストやリスクに見合わなければ攻撃するとは考えにくい。また、正直者も、常に決められた計算を行うとは考えにくい。例えば、組み込みシステムやモバイル端末などの計算資源が限られた状況では、 自身の不利益にならない範囲で計算の手間を省き、本来の手順に従わない可能性がある。 そこで、Halpern と Teague (STOC 2004) により、参加者がある種の合理性に従って行動する状況における暗号技術の研究、すなわち、ゲーム理論にもとづく暗号技術の研究が始められた。

国内・国外の研究動向：2004 年に Halpern と Teague が考察対象にしたのは秘密分散法であった。その後、毎年論文が発表されているが、初期の論文はほとんどが秘密分散を対象としており、他の暗号技術は扱っていなかった。2010 年から少しずつ対象を広げ、リーダー選出問題を対象とした Gradwohl の研究(TCC 2010)や、真鍋らによるケーキカット問題の研究 (MFCS 2010)、二者間計算に関する Asharov らの研究 (Eurocrypt 2011)などがある。 研究代表者の田中と研究分担者の安永は、平成 22 年度から平成 26 年度まで、基盤研究(C) 「ゲーム理論にもとづく暗号プロトコル」として研究を行い、ゲーム理論を用いた暗号技術研究の対象を、紛失通信・コミットメント・公開鍵暗号などの重要な暗号技術に広げることに成功している (ACISP2012, SCN2012, IWSEC2013, IEICE Trans. 2016)。

２．研究の目的

ゲーム理論にもとづく暗号技術では、各参加者がその技術を利用することを「ゲーム理論的に」保証する。つまり、各参加者には複数の取りうる行動があり、その中から自身の利益に合うものを選ぶことができるが、暗号技術・プロトコルで指定された(推奨された)行動を選択することが経済原理的な意味で最適な(インセンティブのある)選択であることを保証している。一連の研究の中で、従来的な方法ではインセンティブ設定が難しい状況が存在することがわかった。公開鍵暗号に対する安永の研究(SCN 2012, IEICE Trans. 2016)では、送受信者が計算コストを考える場合、送受信者間の対話や送信者用の秘密鍵など、従来の設定では不要な要素を追加することで安全な方式を設計している。これらを用いない従来設定での実現方法は未解決である。また、秘密分散においても、同時同報通信等の強い仮定を用いずに実現する方法が存在しないなど、インセンティブ設定の困難さに直面している。

2012 年、Azar と Micali(STOC 2012)は合理的証明を導入した。合理的証明では、正しい証明に高い報酬を与えることで、正しく証明することのインセンティブを与えている。彼らの研究は、合理的証明が認識可能な言語クラスの特徴づけを目的としており、計算複雑さ理論の研究であった。しかし、注目すべき点は、合理的証明では、報酬を「技術的に」付与していることである。証明の正しさを検証して報酬を与えるという率直な方法ではなく、報酬の最大化のために正しく証明をする必要がある仕組みを構築している。このようなインセンティブ付与方法はこれま

でになく画期的であり、結果として、非常に効率的な対話証明の実現に成功している。
2014 年、Guo ら(ITCS 2014)は、合理的証明における報酬付与の仕組みを利用した委託計算を 提案した。対話証明にもとづく委託計算研究は、Goldwasser ら(STOC 2008)の研究を契機に、暗号理論分野で注目され始めたが、報酬を利用した研究は Guo らの研究が初めてである。暗号通貨ビットコインの基盤技術として注目されているブロックチェーンでは、インセンティブ付与の重要性が、ナカモトサトシによる原論文(2008)でも言及されている。ビットコインでは、ブロックをチェーンに接続させることに対して報酬が付与され、その額は 4 年毎に半減する。このような報酬設定は、直観的なアイディアにもとづいて行われており、適切か否かに 関する厳密な議論は行われていない。実際に、Eyal と Sirer(FC2014)は、各参加者がグループを組んで運用することで各参加者の利益が高くなるという問題点を指摘した。これは、中央集権的でない暗号通貨の実現を目指したビットコインの目的に反しており、ある意味で、ビットコインのインセンティブ設計が成功していない証拠と言える。上記を踏まえ、ブロックチェーン技術を含む暗号基盤技術に対するインセンティブ設計の重要性、およびその技術発展の必要性を認識するに至った。

３．研究の方法

本研究ではインセンティブの設計を様々な暗号技術(電子署名・相手認証・ブロックチェー ン技術)に拡張することを目的としている。この目的のため、研究課題を 2 つ設定し、各課題に対して研究期間を大きく 3 つに分ける。課題(A)では、合理的証明にもとづいた委託計算で利用されている報酬の技術的な設定手法を電子署名や相手認証などへ応用し、さらにその手法をその他の技術へ適用可能な形へ一般化させる。課題(B)では、ブロックチェーンに対して適切にインセンティブを設定する手法を考案し、そのインセンティブの設定を、課題(A)で発展させたインセンティブの技術的設定手法で実現する。

４．研究成果

課題(A)に対しては、インセンティブ設計技法に関する調査と研究をまず行った。特に既存研究を、具体的なプロトコルに対するインセンティブ設計手法と、一般的なインセンティブ設計手法に分類し、詳細な調査やこれら手法の比較を行なった。 ここで得られた知見を活用し、インセンティブを用いた電子署名・相手認証のモデルと技術の設計を試みた。特に、これらの要素に密接に関わる Secure Message Transmission (SMT) と呼ばれる要素に着目し、複数ある通信路がすべての敵に支配されたとしても、合理的な敵を考える場合には、安全に通信を行うことができることを示した。
課題(B)に対しては、ブロックチェーンに関する調査と研究を行った。特に、スマートコントラクトと呼ばれるブロックチェーン上でのある種のプログラミング環境を成り立たせる枠組みについて詳細に調査を行ない、そこで利用されているインセンティブ設計手法を抽出した。この知見を活用し、インセンティブを用いたブロックチェーンのモデルと技術の設計を試みた。典型的な proof-of-work においてはハッシュ関数の特定の要件を満たす値を出力するような入力を見つけることが行われている。これはある種の計算問題を解くことに対応しており、この問題を別の計算問題に置き換えたときのインセンティブ設計についての可能性について考察を行った。さら、proof-of-work の原点に立ち戻り、証明者と検証者で時間とメモリのギャップを生じる状況についての考察を行った。

５．主な発表論文等

〔雑誌論文〕　計30件（うち査読付論文　30件／うち国際共著　4件／うちオープンアクセス　1件）

１．著者名 Hara Keisuke、Kitagawa Fuyuki、Matsuda Takahiro、Hanaoka Goichiro、Tanaka Keisuke	４．巻 795
２．論文標題 Simulation-based receiver selective opening CCA secure PKE from standard computational assumptions	５．発行年 2019年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 570～597
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2019.08.016	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 Egashira Shohei、Wang Yuyu、Tanaka Keisuke	４．巻 LNCS11923
２．論文標題 Fine-Grained Cryptography Revisited	５．発行年 2019年
３．雑誌名 ASIACRYPT2019	６．最初と最後の頁 637～666
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34618-8_22	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、Tanaka Keisuke	４．巻 LNCS11923
２．論文標題 Simple and Efficient KDM-CCA Secure Public Key Encryption	５．発行年 2019年
３．雑誌名 ASIACRYPT2019	６．最初と最後の頁 97～127
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34618-8_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 Yoshida Yusuke、Kitagawa Fuyuki、Tanaka Keisuke	４．巻 LNCS11923
２．論文標題 Non-Committing Encryption with Quasi-Optimal Ciphertext-Rate Based on the DDH Problem	５．発行年 2019年
３．雑誌名 ASIACRYPT2019	６．最初と最後の頁 128～158
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34618-8_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 Tezuka Masayuki、Su Xiangyu、Tanaka Keisuke	4．巻 LNCS11829
2．論文標題 A t-out-of-n Redactable Signature Scheme	5．発行年 2019年
3．雑誌名 CANS2019	6．最初と最後の頁 470～489
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-31578-8_26	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 Ishida Ai、Sakai Yusuke、Emura Keita、Hanaoka Goichiro、Tanaka Keisuke	4．巻 NA
2．論文標題 Proper Usage of the Group Signature Scheme in ISO/IEC 20008-2	5．発行年 2019年
3．雑誌名 AsiaCCS2019	6．最初と最後の頁 515～528
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3321705.3329824	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、Tanaka Keisuke	4．巻 LNCS11694
2．論文標題 CCA Security and Trapdoor Functions via Key-Dependent-Message Security	5．発行年 2019年
3．雑誌名 CYRPTO2019	6．最初と最後の頁 33～64
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-26954-8_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 Kitagawa Fuyuki、Nishimaki Ryo、Tanaka Keisuke、Yamakawa Takashi	4．巻 LNCS11694
2．論文標題 Adaptively Secure and Succinct Functional Encryption: Improving Security and Efficiency, Simultaneously	5．発行年 2019年
3．雑誌名 CRYPTO2019	6．最初と最後の頁 521～551
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-26954-8_17	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 Yasunaga Kenji、Koshiba Takeshi	4．巻 LNCS11836
2．論文標題 Perfectly Secure Message Transmission Against Independent Rational Adversaries	5．発行年 2019年
3．雑誌名 GameSec2019	6．最初と最後の頁 563～582
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-32430-8_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 KAWACHI Akinori、KAWANO Kenichi、LE GALL Francois、TAMAKI Suguru	4．巻 E102.D
2．論文標題 Quantum Query Complexity of Unitary Operator Discrimination	5．発行年 2019年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 483～491
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018FCP0012	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 Kotoko Yamada, Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, Keisuke Tanaka	4．巻 101-A(9)
2．論文標題 Generic Constructions for Fully Secure Revocable Attribute-Based Encryption	5．発行年 2018年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1456-1472
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.1456	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 Masayuki Tezuka, Yusuke Yoshida, Keisuke Tanaka	4．巻 -
2．論文標題 Weakened Random Oracle Models with Target Prefix	5．発行年 2018年
3．雑誌名 SecITC 2018	6．最初と最後の頁 344-357
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-12942-2_26	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 Keisuke Hara, Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka	４．巻 -
２．論文標題 Simulation-Based Receiver Selective Opening CCA Secure PKE from Standard Computational Assumptions	５．発行年 2018年
３．雑誌名 SCN 2018	６．最初と最後の頁 140-159
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-98113-0_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 Ai Ishida, Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Keisuke Tanaka	４．巻 -
２．論文標題 Fully Anonymous Group Signature with Verifier-Local Revocation	５．発行年 2018年
３．雑誌名 SCN 2018	６．最初と最後の頁 23-42
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-98113-0_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 Fuyuki Kitagawa, Keisuke Tanaka	４．巻 -
２．論文標題 A Framework for Achieving KDM-CCA Secure Public-Key Encryption	５．発行年 2018年
３．雑誌名 ASIACRYPT (2) 2018	６．最初と最後の頁 127-157
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-03329-3_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 Yuyu WANG, Keisuke TANAKA	４．巻 E100-A
２．論文標題 Generic Transformation for Signatures in the Continual Leakage Model	５．発行年 2017年
３．雑誌名 IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1857-1869
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E100.A.1857	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 Ai ISHIDA, Keita EMURA, Goichiro HANAOKA, Yusuke SAKAI, Keisuke TANAKA	4．巻 E100-A
2．論文標題 Group Signature with Deniability: How to Disavow a Signature	5．発行年 2017年
3．雑誌名 IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1825-1837
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E100.A.1825	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 Kawachi Akinori、Okamoto Yoshio、Tanaka Keisuke、Yasunaga Kenji	4．巻 60
2．論文標題 General Constructions of Rational Secret Sharing with Expected Constant-Round Reconstruction	5．発行年 2017年
3．雑誌名 The Computer Journal	6．最初と最後の頁 711-728
掲載論文のDOI（デジタルオブジェクト識別子） 10.1093/comjnl/bxw094	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 Thanh Ta Minh、Tanaka Keisuke	4．巻 76
2．論文標題 An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information	5．発行年 2017年
3．雑誌名 Multimedia Tools and Applications	6．最初と最後の頁 13455～13471
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11042-016-3750-2	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 該当する

1．著者名 Thanh Ta Minh、Tanaka Keisuke、Dung Luu Hong、Tai Nguyen Tuan、Nam Hai Nguyen	4．巻 77
2．論文標題 Performance analysis of robust watermarking using linear and nonlinear feature matching	5．発行年 2017年
3．雑誌名 Multimedia Tools and Applications	6．最初と最後の頁 2901～2920
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11042-017-4435-1	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 該当する

1．著者名 Yoshida Yusuke、Morozov Kirill、Tanaka Keisuke	4．巻 LNCS10346
2．論文標題 CCA2 Key-Privacy for Code-Based Encryption in the Standard Model	5．発行年 2017年
3．雑誌名 International Conference on Post-Quantum Cryptography	6．最初と最後の頁 35～50
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-59879-6_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 Yamada Kotoko、Attrapadung Nuttapong、Emura Keita、Hanaoka Goichiro、Tanaka Keisuke	4．巻 LNCS10493
2．論文標題 Generic Constructions for Fully Secure Revocable Attribute-Based Encryption	5．発行年 2017年
3．雑誌名 European Symposium on Research in Computer Security	6．最初と最後の頁 532～551
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-66399-9_29	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、Nishimaki Ryo、Tanaka Keisuke	4．巻 LNCS10770
2．論文標題 Simple and Generic Constructions of Succinct Functional Encryption	5．発行年 2018年
3．雑誌名 IACR International Workshop on Public Key Cryptography	6．最初と最後の頁 187～217
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-76581-5_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 Kitagawa Fuyuki、Tanaka Keisuke	4．巻 LNCS10769
2．論文標題 Key Dependent Message Security and Receiver Selective Opening Security for Identity-Based Encryption	5．発行年 2018年
3．雑誌名 IACR International Workshop on Public Key Cryptography	6．最初と最後の頁 32～61
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-76578-5_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 Saha Tushar Kanti、Koshiba Takeshi	4．巻 LNCS10723
2．論文標題 Privacy-Preserving Equality Test Towards Big Data	5．発行年 2018年
3．雑誌名 The 10th International Symposium on Foundations & Practice of Security (FPS 2017)	6．最初と最後の頁 95～110
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-75650-9_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 Ito Tomohiro、Koizumi Hayato、Suzuki Nobumitsu、Kakesu Izumi、Iwakawa Kento、Uchida Atsushi、Koshiba Takeshi、Muramatsu Jun、Yoshimura Kazuyuki、Inubushi Masanobu、Davis Peter	4．巻 7
2．論文標題 Physical implementation of oblivious transfer using optical correlated randomness	5．発行年 2017年
3．雑誌名 Scientific Reports	6．最初と最後の頁 12ページ
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41598-017-08229-x	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 Saha Tushar Kanti、Mayank、Koshiba Takeshi	4．巻 LNCS10359
2．論文標題 Efficient Protocols for Private Database Queries	5．発行年 2017年
3．雑誌名 The 31st IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2017)	6．最初と最後の頁 337～348
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-61176-1_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 該当する

1．著者名 Keita INASAWA, Kenji YASUNAGA	4．巻 E100-A
2．論文標題 Rational Proofs against Rational Verifiers	5．発行年 2017年
3．雑誌名 IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 2392-2397
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E100.A.2392	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 Kawachi Akinori、Kawano Kenichi、Le Gall Francois、Tamaki Suguru	4．巻 LNCS10392
2．論文標題 Quantum Query Complexity of Unitary Operator Discrimination	5．発行年 2017年
3．雑誌名 23rd International Conference, COCOON 2017	6．最初と最後の頁 309～320
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-62389-4_26	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 Akinori Kawachi, Mitsunori Ogihara, Kei Uchizawa	4．巻 LIPICS83
2．論文標題 Generalized Predecessor Existence Problems for Boolean Finite Dynamical Systems	5．発行年 2017年
3．雑誌名 42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017)	6．最初と最後の頁 8:1-8:13
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.MFCS.2017.8	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

〔学会発表〕　計0件

〔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	河内　亮周 (Kawachi Akinori) (00397035)	三重大学・工学研究科・教授 (14101)	
研究分担者	安永　憲司 (Yasunaga Kenji) (50510004)	東京工業大学・情報理工学院・准教授 (12608)	
研究分担者	小柴　健史 (Koshiba Takeshi) (60400800)	早稲田大学・教育・総合科学学術院・教授 (32689)	

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