

令和 5 年 6 月 19 日現在

機関番号：18001

研究種目：基盤研究(C) (一般)

研究期間：2017～2022

課題番号：17K05181

研究課題名(和文) 跡公式とゼータ関数を用いた素測地線とスペクトルの分布に関する研究

研究課題名(英文) Research on distributions of prime geodesics and spectrum using trace formula and zeta functions

研究代表者

橋本 康史 (Hashimoto, Yasufumi)

琉球大学・理学部・准教授

研究者番号：30452733

交付決定額(研究期間全体)：(直接経費) 3,200,000円

研究成果の概要(和文)：実階数1の半単純リー群の離散部分群によって与えられる体積有限な双曲多様体の素測地線とラプラシアン・スペクトルの分布との間には密接な関係がある。本研究では、セルバーグの跡公式を用いて2つの分布を関連づけて調べることで、対応する多様体の特徴づけを行うことを目的としている。本研究期間中には、合同部分群や不定値四元数環から与えられる余コンパクト群を含む広い範囲の基本群に対して、セルバーグゼータ関数の非絶対収束域における値の評価を行った。加えて、セルバーグゼータ関数の値の普遍性についても、既存の研究成果を大幅に一般化し、適用範囲を拡張した。

研究成果の学術的意義や社会的意義

セルバーグゼータ関数については、リーマンゼータ関数との類似性が強調されることが多いが、有理型関数としての位数や非自明零点の分布、素元の分布などで大きな相違があるため、従来の解析数論的な手法では解析が必ずしも簡単ではないことが少なくない。本研究では、既知のセルバーグゼータ関数の値の評価や、値分布の普遍性に関する結果を改良することで、この研究分野における素元の分布を丁寧に解析することの重要性の一端に触れることができたと思う。

研究成果の概要(英文)：There are deep connections between the distributions of the spectra of the Laplacian and the prime geodesics of hyperbolic manifolds of finite volume derived from discrete subgroups of a semi-simple Lie group of real rank one. The aim of this study is to characterize the corresponding manifolds by studying the two distributions in relation to each other using Selberg's trace formula. During the course of this study, we evaluated the values of the Selberg zeta functions in the non-absolute convergence region for various arithmetic groups, including congruence subgroups and co-compact groups derived from indefinite quaternion algebras. We also generalized and extended the universality theorems of the Selberg zeta function from existing researches.

研究分野：数物系科学

キーワード：セルバーグ跡公式 セルバーグゼータ関数 双曲多様体 length spectrum ラプラシアン・スペクトル

科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

1. 研究開始当初の背景

実階数 1 の半単純リー群の離散部分群によって与えられる双曲多様体において、素測地線の分布とスペクトルの分布との間には密接な関係があり、それぞれが多様体を特徴づける重要な要素である。これら 2 つの分布の間のある種の良い性質をみたくテスト関数を含む形で明示的に記述する公式として、セルバーグの跡公式が有名だが、この跡公式において、テスト関数のとり方を工夫することで一方の分布の性質からもう一方の分布の性質を知ることができる。さらにこの公式は、解析数論における素数とリーマンゼータ関数の非自明零点との間の関係性を表わすヴェイユの明示公式や、数理物理における古典系の周期軌道と量子系の固有エネルギーとの間の関係をあらわすグッツヴィラーの跡公式にもよく似ていることから、一見あまり関連がなさそうな分野で用いられてきた手法の応用によって予期できないほどの研究の進展が得られることも期待できる。実際に、多様体(の基本群)の数論性・非数論性 (arithmeticity, non-arithmeticity) に関しては、ラプラシアン例外固有値の存在・非存在性、非コンパクト多様体上のラプラシアンのスペクトルに関する cuspidality、スペクトルのばらつきをあらわす number variance とよばれる関数の挙動、length spectrum (素測地線から長さの情報をとりだしたものの重複度分布、など、いずれも完全には解決されていないが、1980 年代以降(数値実験的なものを含めて)少なくない研究成果が得られており、セルバーグ跡公式やセルバーグゼータ関数を用いて新たな視点からの研究成果が得られることも期待できる。

2. 研究の目的

(1) 素測地線分布について: 素測地線とその長さの集合である length spectrum (以下 LS) は多様体を特徴づける重要な要素のひとつである。実際に、数論的(arithmetic)な多様体においては、非数論的(non-arithmetic)なものに比べて LS の重複度が高くなる傾向にあることが、数値実験を含む Bogomolny et al.(1997) や Marklof (1997), Schmutz (2001) らの研究によって示唆されている。とくに、モジュラー群の合同部分群によって与えられるリーマン面に対しては、LS の重複度が不定値 2 元 2 次形式の類数で記述できることが知られており、これらの平均的な増大度が、重複度のべき和に関する漸近公式という形で与えられている(Bogomolny et al., 1996, Peter, 2002, Lukianov, 2007, Hashimoto, 2013)。本研究では、この結果をより一般的な多様体に対して拡張するとともに、セルバーグゼータ関数やラプラシアンのスペクトル分布の研究へと応用することを目的とする。

(2) セルバーグゼータ関数について: 素測地線の長さに関するオイラー積で定義されるセルバーグゼータ関数は、素数に関するオイラー積で定義されるリーマンゼータ関数との類似性が着目されることが多いが、有理型関数としての位数や素元のノルムの重複度などに相違がある。このような相違は、従来の解析数論的な手法をセルバーグゼータ関数に適用するうえで困難を生じることが少なくない。例えば、素数定理については、リーマン予想を仮定すれば誤差項の最良評価が得られる一方、素測地線定理については、セルバーグゼータ関数に関するリーマン予想がほぼ成り立っているにもかかわらず、誤差項評価は最良にほど遠い状況にある。本研究では、セルバーグ跡公式や(1)で得られた LS に関する研究成果を利用して、セルバーグゼータ関数の解析を行うことを目的とする。

(3) ラプラシアンのスペクトル分布について: セルバーグゼータ関数の非自明零点がラプラシアンのスペクトルを用いて記述できることはよく知られている。本研究では、(1),(2)で得られた素測地線分布やセルバーグゼータ関数に関する成果を跡公式に適用することで、ラプラシアンのスペクトル分布を明らかにすることを目的とする。

3. 研究の方法

(1) 素測地線分布について: 2・3 次元の双曲多様体において、LS は基本群の共役類の跡(トレース)の集合として表わせるため、一見初等的であるようにみえるが、一般的には必ずしも簡単ではない。ただ、モジュラー群やその合同部分群を基本群とするリーマン面に対しては、LS とその重複度を不定値 2 元 2 次形式の狭義類数と基本単数を用いて記述できる(Sarnak, 1982, Hashimoto, 2007, 2013)ことが知られている。この表示は非常に有用であり、LS の重複度の漸近的な挙動だけでなく、素測地線定理の誤差項評価にも使われている(Soundararajan-Young, 2013)。本研究では、このような LS の「よりわかりやすい」表示を他の基本群に対して拡張することで、素測地線分布に関する知見を得る手掛かりとする。

(2) セルバーグゼータ関数について: セルバーグゼータ関数の研究には、従来から跡公式が大きな役割を果たしている。実際に、セルバーグゼータ関数の解析接続や関数等式は跡公式から得られている。本研究では、(1)で得られた素測地線分布に関する成果と跡公式、さらにリーマンゼータ関数などの他のゼータ関数に適用されてきた解析数論的なアプローチを組み合わせるこ

とで、セルバーグゼータ関数の解析性や値分布を調べる。

(3) ラプラシアンの特値について: スペクトルの分布に関しては, (1), (2) で得られた研究成果を跡公式に応用することで研究を進める。加えて、跡公式に適用するテスト関数を工夫し、計算アルゴリズムを改良することで、計算機を用いたより精密な固有値評価を行う。

4. 研究成果

(1) セルバーグゼータ関数の値評価: 一般的に、ゼータ関数の非絶対収束域における値の分布を調べることは、絶対収束域と比べて難しい。とくにセルバーグゼータ関数は有理型関数としての位数が大きいため、リーマンゼータ関数などの位数が小さいゼータ関数と比較しても問題は深刻である。本研究(Hashimoto, Math. Nachr. 2021)では、モジュラー群に関するセルバーグゼータ関数に対して、その非絶対収束域における評価を改良した。モジュラー群に関する LS が 2 次形式の類数と基本単数を用いて記述できるため、絶対収束域においてセルバーグゼータ関数も類数と基本単数によって記述できることはすぐにわかるが、これを非絶対収束域に拡張することで、セルバーグゼータ関数の値の評価を指数和評価や指標和評価へ帰着させた。そして、古典的に知られている van der Corput の評価や Weil の評価を適用することで、モジュラー群に関するセルバーグゼータ関数の対数微分の評価を改良させることに成功した。この成果は、従来の評価(Hejhal, 1970s, Iwaniec, 1980s etc.)のおそらく初めての改良であると考えられる。さらに、Hashimoto (Internat. J. Number Theory, 2023) では、セルバーグゼータ関数の対数微分の 2 乗積分の評価を行った。先の研究と比べると、それほど緻密な指数和や指標和の評価を行う必要なくなったため、モジュラー群だけでなく、合同部分群や不定値四元数環から定義される余コンパクトな群などより一般的な基本群に対して解析が可能になった。加えて、前年の評価を直接 2 乗積分して得られる評価を大幅に改良することができた。

(2) セルバーグゼータ関数の普遍性: 1970 年代に Voronin がリーマンゼータ関数の値分布に関する普遍性定理を証明して以降、ゼータ関数の普遍性に関する研究は活発に行われているが、そのほとんどはリーマンゼータ関数やディリクレ級数を含む位数が 1 のゼータ関数に対するもので、セルバーグゼータ関数に対しては、Drungilas-Garunkstis-Kacenas(2013)と見正(2021)によるモジュラー群と主合同部分群に関する研究しかない。本研究では、モジュラー群と主合同部分群だけでなく、もっと一般的にモジュラー群と不定値四元数環から定義される余コンパクトな群の部分群に対して、セルバーグゼータ関数に関する普遍性定理が成り立つことを証明した。さらに(1)で得られたセルバーグゼータ関数の非絶対収束域における値評価の研究を応用することで、これまでの研究よりも普遍性定理が成り立つ非絶対収束域内の領域を広げることができた。この成果については、すでに e-print arXive で公表済みで、国際学術誌に投稿中である。

(3) Length Spectrum: これまでに、モジュラー群の合同部分群に関する LS とその重複度が不定値 2 元 2 次形式の単数と類数を用いて記述されることが知られていた(Sarnak, 1981, Hashimoto, 2007, 2013 etc.)。実は、非余コンパクトで数論的(arithmetic)な基本群は、モジュラー群と commensurable なものしかなく、さらにそれらの中で極大なものはモジュラー群の合同部分群のひとつと類似性がある。本研究では、このような数論的な基本群に対して、モジュラー群や合同部分群との類似性を調べることで、LS とその重複度が同様に 2 次形式の類数と基本単数を用いて記述できることを突き止めた。この成果については、研究集会における講演で公表済みだが、考えうる応用例について未決着な部分があるため、今のところ論文としての公表には至っていない。

(4) ラプラシアンの特値: ラプラシアンの特値は、セルバーグゼータ関数の非自明零点としてあらわれることから、リーマンゼータ関数の非自明零点と比較されることが多い。リーマンゼータ関数の非自明零点の重複度は全て 1 であると予想されており、Montgomery (1972) が pair correlation を用いた手法で重複度 1 の零点の割合を評価したのを皮切りに、これまでも少なからぬ研究成果が得られている。一方で、ラプラシアンの特値について、Peter (1995) による pair correlation の類似の研究(1995)があるが、重複度の評価という観点からは、それほど強い結果が得られているとは言い難い。本研究では、素数定理と素測地線定理の誤差項評価の相違に着目し、pair correlation の手法をセルバーグゼータ関数に適用することで、素測地線定理の誤差項の最良に近い評価を仮定することで、ラプラシアンの特値に関する非自明な評価が得られることがわかった。この成果については、すでに研究集会における講演で公表済みだが、テスト関数のとり方を工夫することで、より良い評価が得られることが期待できるため、研究を継続し、改良・修正の後に国際学術誌への掲載を目指す予定である。

5. 主な発表論文等

〔雑誌論文〕 計18件（うち査読付論文 14件 / うち国際共著 0件 / うちオープンアクセス 11件）

1. 著者名 Yasufumi Hashimoto	4. 巻 19
2. 論文標題 Square integrals of the logarithmic derivatives of Selberg's zeta functions in the critical strip	5. 発行年 2023年
3. 雑誌名 International Journal of Number Theory	6. 最初と最後の頁 747,756
掲載論文のDOI (デジタルオブジェクト識別子) 10.1142/S1793042123500379	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 Yasufumi Hashimoto	4. 巻 E106.A
2. 論文標題 Solving the Problem of Blockwise Isomorphism of Polynomials with Circulant Matrices	5. 発行年 2023年
3. 雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6. 最初と最後の頁 185,192
掲載論文のDOI (デジタルオブジェクト識別子) 10.1587/transfun.2022CIP0002	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 Yasufumi Hashimoto	4. 巻 14
2. 論文標題 Key recovery attack on Hufu-UOV	5. 発行年 2022年
3. 雑誌名 JSIAM Letters	6. 最初と最後の頁 1,4
掲載論文のDOI (デジタルオブジェクト識別子) 10.14495/jsiaml.14.1	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 Yasufumi Hashimoto	4. 巻 294
2. 論文標題 Selberg's zeta function for the modular group in the critical strip	5. 発行年 2021年
3. 雑誌名 Mathematische Nachrichten	6. 最初と最後の頁 1899,1904
掲載論文のDOI (デジタルオブジェクト識別子) 10.1002/mana.202000268	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 Yasufumi Hashimoto	4. 巻 12835
2. 論文標題 Solving the Problem of Blockwise Isomorphism of Polynomials with Circulant Matrices	5. 発行年 2021年
3. 雑誌名 Springer LNCS	6. 最初と最後の頁 137,150
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_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 Yasufumi Hashimoto	4. 巻 34
2. 論文標題 Vulnerability of Diene-Thabet-Yusuf's cubic multivariate signature scheme,	5. 発行年 2021年
3. 雑誌名 Ryukyu Mathematical Journal	6. 最初と最後の頁 1,5
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 オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 Yasufumi Hashimoto	4. 巻 -
2. 論文標題 Recent Developments in Multivariate Public Key Cryptosystems	5. 発行年 2020年
3. 雑誌名 International Symposium on Mathematics, Quantum Theory, and Cryptography	6. 最初と最後の頁 209,229
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/978-981-15-5191-8_16	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 Yasufumi Hashimoto	4. 巻 292
2. 論文標題 Asymptotic behaviors of class number sums associated with Pell-type equations	5. 発行年 2019年
3. 雑誌名 Mathematische Zeitschrift	6. 最初と最後の頁 641,654
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/s00209-018-2139-5	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 Yasufumi Hashimoto	4. 巻 11
2. 論文標題 Key recovery attack on Circulant UOV/Rainbow	5. 発行年 2019年
3. 雑誌名 JSIAM Letters	6. 最初と最後の頁 45,48
掲載論文のDOI (デジタルオブジェクト識別子) 10.14495/jsiaml.11.45	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 Yasufumi Hashimoto, Y. Ikematsu, T. Takagi	4. 巻 27
2. 論文標題 Chosen Message Attack on Multivariate Signature ELSA at Asiacrypt 2017	5. 発行年 2019年
3. 雑誌名 Journal of Information Processing	6. 最初と最後の頁 517,524
掲載論文のDOI (デジタルオブジェクト識別子) 10.2197/ipsjnip.27.517	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 Yasufumi Hashimoto	4. 巻 81
2. 論文標題 Recent developments in multivariate public key cryptosystems	5. 発行年 2019年
3. 雑誌名 MI Lecture Notes	6. 最初と最後の頁 187,205
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 Yasufumi Hashimoto	4. 巻 10
2. 論文標題 High-rank attack on HMFev	5. 発行年 2018年
3. 雑誌名 JSIAM Letters	6. 最初と最後の頁 21,24
掲載論文のDOI (デジタルオブジェクト識別子) 10.14495/jsiaml.10.21	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 -

1. 著者名 Yasufumi Hashimoto, Y. Ikematsu, T. Takagi	4. 巻 11049
2. 論文標題 Chosen Message Attack on Multivariate Signature ELSA at Asiacrypt 2017	5. 発行年 2018年
3. 雑誌名 Springer LNCS	6. 最初と最後の頁 3, 18
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/978-3-319-97916-8_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 Yasufumi Hashimoto	4. 巻 31
2. 論文標題 On the security of Zhang-Tan's variants of multivariate signature schemes	5. 発行年 2018年
3. 雑誌名 Ryukyu Mathematical Journal	6. 最初と最後の頁 1, 5
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 オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 Yasufumi Hashimoto	4. 巻 1
2. 論文標題 Multivariate public key cryptosystems	5. 発行年 2017年
3. 雑誌名 Mathematical Modelling for Next-Generation Cryptography	6. 最初と最後の頁 17, 42
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/978-981-10-5065-7_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 Yasufumi Hashimoto	4. 巻 9
2. 論文標題 Chosen ciphertext attack on ZHFE	5. 発行年 2017年
3. 雑誌名 JSIAM Letters	6. 最初と最後の頁 21, 24
掲載論文のDOI (デジタルオブジェクト識別子) 10.14495/jsiaml.9.21	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 -

1. 著者名 Yasufumi Hashimoto	4. 巻 100-A
2. 論文標題 Key recovery attacks on multivariate public key cryptosystems derived from quadratic forms over an extension field	5. 発行年 2017年
3. 雑誌名 IEICE Transactions Fundamentals	6. 最初と最後の頁 18,25
掲載論文のDOI (デジタルオブジェクト識別子) 10.1587/transfun.E100.A.18	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 Yasufumi Hashimoto	4. 巻 30
2. 論文標題 Weaknesses of cubic UOV and its variants	5. 発行年 2017年
3. 雑誌名 Ryukyu Mathematical Journal	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 オープンアクセスとしている (また、その予定である)	国際共著 -

〔学会発表〕 計20件 (うち招待講演 0件 / うち国際学会 3件)

1. 発表者名 橋本康史
2. 発表標題 セルバーグゼータ関数に関する普遍性定理
3. 学会等名 2023年度日本数学会年会代数学分科会
4. 発表年 2023年

1. 発表者名 橋本康史
2. 発表標題 有限体上の under-defined な多変数連立2次方程式の解法について
3. 学会等名 日本応用数理学会第19回研究部会連合発表会
4. 発表年 2023年

1. 発表者名 Yasufumi Hashimoto
2. 発表標題 Universality of the Selberg zeta function
3. 学会等名 Zeta Functions in OKINAWA 2022
4. 発表年 2022年

1. 発表者名 橋本康史
2. 発表標題 Simple matrix signature scheme の安全性について
3. 学会等名 日本応用数理学会第18回研究部会連合発表会
4. 発表年 2022年

1. 発表者名 Yasufumi Hashimoto
2. 発表標題 Solving the problem of Blockwise Isomorphism of Polynomials with Circulant matrice
3. 学会等名 16th International Workshop on Security (IWSEC2021) (国際学会)
4. 発表年 2021年

1. 発表者名 橋本康史
2. 発表標題 セルバーグゼータ関数の臨界領域における2乗積分について
3. 学会等名 2021年度日本数学会秋季総合分科会
4. 発表年 2021年

1. 発表者名 橋本康史
2. 発表標題 Hufu-UOVの安全性について
3. 学会等名 日本応用数理学会年会第17回研究部会連合発表会
4. 発表年 2021年

1. 発表者名 橋本康史
2. 発表標題 モジュラー群に関するセルバーグゼータ関数の臨界領域での値について
3. 学会等名 2020年度日本数学会秋季総合分科会代数学分科会
4. 発表年 2020年

1. 発表者名 橋本康史
2. 発表標題 Diene-Thabet-Yusuf の3次多変数署名方式の安全性について
3. 学会等名 2020年度日本応用数理学会年会
4. 発表年 2020年

1. 発表者名 Yasufumi Hashimoto
2. 発表標題 Recent developments in multivariate public key cryptosystems
3. 学会等名 International Symposium on Mathematics, Quantum Theory, and Cryptography (国際学会)
4. 発表年 2019年

1. 発表者名 Yasufumi Hashimoto
2. 発表標題 An error term estimation of the prime geodesic theorem for the modular group
3. 学会等名 Zeta Functions in OKINAWA 2019
4. 発表年 2019年

1. 発表者名 Yasufumi Hashimoto
2. 発表標題 On multiplicities of eigenvalues of Laplacians on hyperbolic surfaces
3. 学会等名 Zeta Functions in OKINAWA 2018
4. 発表年 2018年

1. 発表者名 Yasufumi Hashimoto, Y. Ikematsu, T. Takagi
2. 発表標題 Chosen Message Attack on Multivariate Signature ELSA at Asiacrypt 2017
3. 学会等名 The 13th International Workshop on Security (IWSEC 2018) (国際学会)
4. 発表年 2018年

1. 発表者名 橋本康史
2. 発表標題 Circulant UOV/Rainbow の安全性について
3. 学会等名 2018年度日本応用数学会年会
4. 発表年 2018年

1. 発表者名 橋本康史
2. 発表標題 A survey on Multivariate Public key Cryptosystem
3. 学会等名 代数的手法による数理論号解析
4. 発表年 2018年

1. 発表者名 橋本康史
2. 発表標題 多変数多項式暗号の暗号化の効率化
3. 学会等名 2018年度暗号と情報セキュリティシンポジウム
4. 発表年 2018年

1. 発表者名 Yasufumi Hashimoto
2. 発表標題 Multiplicities in length spectra for congruence subgroups
3. 学会等名 Zeta functions and trace formulas in Fukuoka
4. 発表年 2017年

1. 発表者名 Yasufumi Hashimoto
2. 発表標題 Multiplicities in length spectra for non-compact arithmetic surfaces
3. 学会等名 Zeta Functions in OKINAWA 2017
4. 発表年 2017年

1. 発表者名 橋本康史
2. 発表標題 HMFev の安全性について
3. 学会等名 日本応用数理学会2017年度年会
4. 発表年 2017年

1. 発表者名 橋本康史
2. 発表標題 拡大体型多変数多項式暗号に対するランク攻撃
3. 学会等名 CREST暗号数理 平成29年度第2回全体会議
4. 発表年 2017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

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