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 ２５ 日現在

機関番号：３２６６０
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ０４４７３

研究課題名（和文）論理機能切替え可能な全光論理回路と大容量光通信への応用

研究課題名（英文）Multifunctional all-optical logic gate using quantum-dot semiconductor optical amplifiers

研究代表者

八嶋　弘幸（Yashima, Hiroyuki）

東京理科大学・工学部情報工学科・教授

研究者番号：３０２３０１９７

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究では量子ドット半導体光増幅器に着目し、論理機能切替え可能な全光論理回路を提案し、その諸特性を求め、大容量光通信への応用を検討する。提案する全光論理回路はゼロ復帰2値位相変調を入力とし、2入力および3入力に切替え可能で、さらに論理演算子切替機能を有する。提案回路は160Gbpsで動作し、4種類の論理演算を切り替えることが可能である。シミュレーションにより、出力信号品質は消光比12.28dBが得られた。また、自然放出雑音および位相誤差耐性を検討し、提案回路の諸特性を求めた。検討の結果、提案回路は論理機能切替可能な全光論理回路として有効なものであることを明らかにした。

研究成果の学術的意義や社会的意義
通信の大容量化に向けて全光信号処理のための全光論理回路を実現する必要があり、AND,OR,NOR,XORなどいくつか提案されているが、いずれもその構成が大きく異なり、入出力信号強度が異なるため、これらを組み合わせた回路を構成するのは難しいという問題がある。
提案する全光論理回路は、一つの回路で論理演算子を切替可能な機能を有しており、各論理演算に対する特性も均一で、組み合わせ論理回路の設計が容易になり、全光信号処理の実現に向けて大きな意義がある。また、提案回路は位相変調された信号に対するものであり、コヒーレント光通信の全光受信機の実現にも寄与できる可能性がある。

研究成果の概要（英文）：In this paper, we propose and investigate the reconfigurable all optical multifunctional logic gates using quantum-dot (QD) semiconductor optical amplifiers (SOA). An all-optical switchable logic gate using a single QD-SOA for return to zero binary phase shift keying signal inputs is proposed. The proposed gate can switch the two and three input operations and can also switch the four logical operators. This multifunctionality is achieved by introducing the external control signal. To evaluate the quality of the proposed logic gates, we perform numerical simulations. The quality of the output signal is approximately 12.28 dB in the extinction ratio. We also investigate the effect of amplified spontaneous emission noise and phase error tolerance. We have revealed the effectiveness of the all-optical logic gates introducing QD-SOAs for RZ BPSK inputs. This reserach contributes to improving the development of the multifunctional all optical signal processing using QD-SOAs.

研究分野：通信工学

キーワード：光論理回路　QS-SOA

様　式　C－１９、F－１９－１（共通）

１．研究開始当初の背景

現代の高度情報化社会における通信ネットワークにおいては、「大容量化」および「情報セキュリティの保持」がますます重要となっている。

通信の大容量化においては、高速化のため電気信号処理を排除した全光信号処理を用いた光通信に向けて様々な挑戦が行われているが、光信号処理はまだほんのわずかしか用いられていない。全光信号処理を行うには、全光論理回路を実現する必要があり、AND、OR、NOR、XOR などいくつか提案されているが、いずれもその構成が大きく異なり、入出力信号強度が異なるため、これらを組み合わせた回路を構成するのは難しいという問題がある。

また、現状の基幹通信網では位相に情報をのせるデジタルコヒーレント技術が実用化され、100Gbps 級の伝送を可能にしているが、デジタルコヒーレント技術では、電気信号による超高速信号処理が必要であり、さらなる高速化にも限度がある。このような問題を回避する将来の超高速通信を実現策として、位相変調信号の全光受信機の実現が望まれている。

一方、光 CDMA　は全光信号処理を用いるアクセス系の多重通信方式として注目されているが、各ユーザが異なる符号を用いて多重化を行っているため、符号を工夫すれば光 CDMA そのものにセキュリティ効果を持たせることができるという特徴がある。よって、光 CDMA と暗号技術を併用することにより二重の暗号化を施した高度なセキュリティ通信が可能となり、大きな意義を有することになる。

２．研究の目的

本研究の目的は、位相変調された信号に対する論理機能を切り替え可能な全光論理回路を提案し、その有効性を明らかにすることと、提案素子を高速な全光通信に適用し、大容量化と情報セキュリティの向上に役立てることである。具体的には次のようなものである。

(1) 位相変調信号に対する論理機能切り替え可能な全光論理回路

一つの回路構成で複数の論理演算素子として切り替え可能な全光論理演算回路を提案し、その諸特性を求め、有効性を示すことを目的とする。このような発想の演算機能を切り替える光論理演算回路はなく、提案方式は極めて独自性・創造性の高いものである。

(2) 光位相変調信号のコヒーレント全光復調器

図１の提案回路を組み合わせることにより、位相変調されたコヒーレント光信号を電気信号処理を用いずに光信号から直接復調できる受信器を提案し、提案方式の有効性を明らかにすることを目的とする。

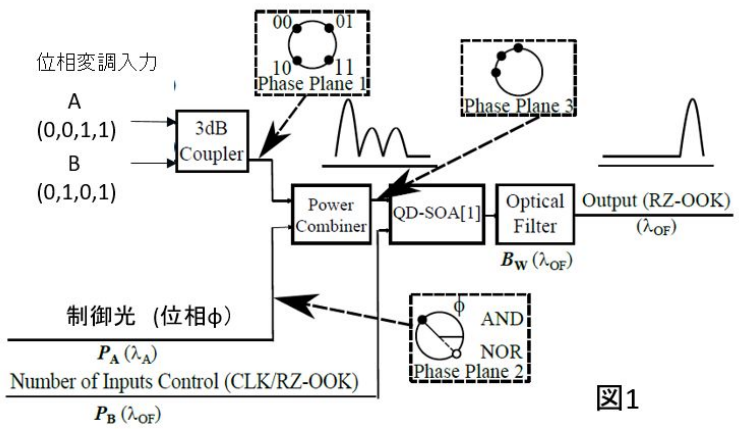

図1

(3) 光 CDMA の全光干渉除去と暗号との併用による情報セキュリティの向上

提案する図１の全光論理演算回路を全光 CDMA システムの受信器の干渉抑圧に適用して多重度を上げるとともに、長い２次元符号系列を用いることによるセキュリティ効果を向上させる全光 CDMA システムを提案し、暗号と併用して強固なセキュリティ強度を持たせ、その諸特性を評価し、有効性を明らかにすることを目的とする。光 CDMA はユーザごとに異なる符号を用いるため、符号を工夫することにより光 CDMA 自身にセキュリティ効果を持たせることができる。そこで、光 CDMA と暗号と組み合わせ二重のセキュリティを施した通信システムを提案し、そのセキュリティ強度を評価する。

３．研究の方法

(1) 位相変調信号に対する論理機能切り替え可能な全光論理回路

提案する全光回路は図１の構成とし、位相変調された入力 A および入力 B をカプラで合波し、制御光と組み合わせて量子ドット半導体増幅器(QD-SOA : Quantum Dot-Semiconductor Optical Amplifier）に入力すると、QD-SOA の非線形性により出力スペクトルが歪み、出力を光フィルタで切り取ることにより光信号のまま論理演算結果が得られる。制御光の位相を 90°毎に 4 通りに変化させることにより、入力 A、B に対して$\overline{A}\,\overline{B}$, $\overline{A}B$, $A\overline{B}$, AB の４通りの演算結果が得られる。シミュレーションによりアイパターン、消光比、Q 値などの諸特性を求め、入力信号光、制御光のレベル、QD-SOA への注入電流などを最適化し、制御光の位相誤差の許容度も求め、有効性を示す。

A	B	$\overline{A}\,\overline{B}$	$\overline{A}B$	$A\overline{B}$	AB
0	0	1	0	0	0
0	1	0	1	0	0
1	0	0	0	1	0
1	1	0	0	0	1

制御光の位相により切り替え可能

(2) 光位相変調信号のコヒーレント全光復調器

図１の回路で 3dB Coupler を取り除き、コントロールパルスの位相をπ/2 ずつ４通りに変えた４つの並列回路に 4 値位相変調(QPSK)信号を入力すると、位相が一致した回路のみから出力が得られるため、電気信号を用いずに光領域で直接復調できる。この復調回路において、波動方程式とレート方程式の数値解析およびシミュレーションによりアイパターンを求め、消光比、Q 値など提案受信機の諸特性を求める。

(3) 光 CDMA の全光干渉除去と暗号との併用による情報セキュリティの向上

光 CDMA は他ユーザからの干渉による性能劣化があり、多重度があまり高くできないという問題点がある。図１の論理演算回路の後半部分(QD-SOA 以下)は、QD-SOA の相互位相変調および相互振幅変調と呼ばれる非線形効果を利用したアナログ入力信号の弁別効果、すなわち、０，１のデジタル出力とする機能を持つ。干渉で劣化した光 CDMA の出力信号をこの回路（図１の後半部分）に通し、波形整形し干渉の除去を行い多重度を実用レベルまで上げる。

一方、光 CDMA はユーザごとに異なる符号を用いるため、長い符号を用いれば光 CDMA 自身がセキュリティ効果を有する。そこで、暗号と組み合わせ二重のセキュリティを持たせ、そのセキュリティ強度を評価する。光 CDMA の符号として、波長領域と時間領域の２次元符号とし、なおかつ、N 情報ビット毎に LN チップの長さ（L は１ビット当りの符号長）かつ多値系列のユーザ符号（多値・長符号）を用いる。また、暗号としては種々の共通鍵暗号（KASUMI, Midori64,128 等）とし、最も解読されやすい条件として、単一送信者の送信端で送信信号が盗聴されたと仮定し、高階差分攻撃、中間一致攻撃、補間攻撃等の最新の攻撃法を適用し、符号長と多値数等のパラメータと安全性の関係を求め、定量的にセキュリティ強度を評価し、提案法が高いセキュリティ機能を有することを明らかにする。

４．研究成果

論理演算子および入力数の全ての組み合わせに対してアイダイアグラムおよび消光比を求める。2 入力動作における4 種類の論理演算に対するアイダイアグラムをもとめたところ、消光比はそれぞれ12.28 dB、12.29 dB、12.28 dB、12.27 dB が得られた。さらに、3 入力動作における4 種類の論理演算に対するアイダイアグラムより、消光比は12.28 dB が得られた。 ASE 雑音を考慮しない場合、論理演算子間での出力信号品質の変動および2入力動作および3入力動作での出力信号品質の変動は観測されなかった。ASE 雑音を考慮した場合の動作特性を調査するため、論理演算子および入力数の全ての組み合わせに対して$2 \leq n_{sp} \leq 8$ の範囲で消光比を求め、図２に示す。図２より、n_{sp}の値が大きくなるにつれて消光比の値は減少する傾向を持つ。また、3 入力動作の消光比は2 入力動作の消光比と比べて良好な値を観測した。

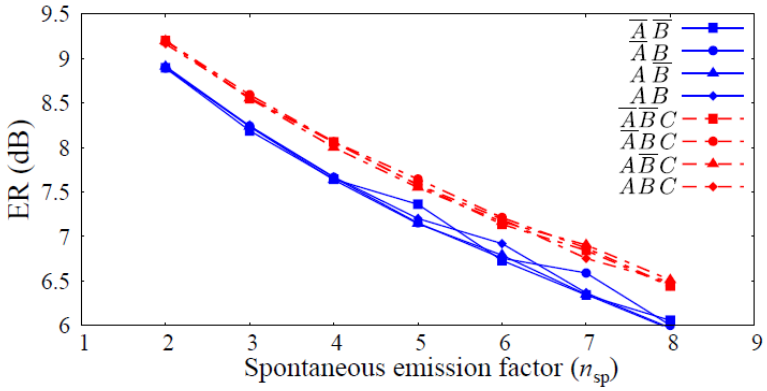

図２　提案する論理演算回路の消光比

シミュレーションの結果、アイダイアグラムおよび消光比から良好な信号品質を有することを明らかにした。特に、消光比は入力数および論理演算のいずれの組み合わせに対しても約12.28 dB が得られた。従って、ASE 雑音を考慮しない場合、入力数や論理演算子は出力信号品質に影響を与えない特性を持つことを明らかにした。次に、ASE 雑音の影響下における消光比およびQ値の特性を検討した。いずれもASE 雑音電力が大きくなるにつれて出力信号品質は単調減少する傾向を持つことを明らかにした。また、消光比の観点で、3 入力動作は2 入力動作と比べて良好な信号品質となることを明らかにした。最後に提案回路の位相誤差耐性を調査し、LOC信号の位相変化$-5^\circ < \Delta\phi_{LOC} < 15^\circ$の範囲で良好な出力信号品質となることを確認した。

一方、セキュリティ関連については、2022年に提案された64ビットブロック暗号であるLBC-3について検討した。鍵長は80ビット、ラウンド数は20であり、まず、混合整数線形計画法を用いたBit-Based Division Propertyによって積分特性を調査した。その結果、63階差分を用いた特性の網羅的な調査から、最良の特性として既存の60階差分特性を上回る特性が存在しない ことがわかった。また、新しい16ラウンドの48階差分特性を発見し、これを利用したフルラウンドのLBC-3に対する攻撃の高速化により、必要な選択平文数及び 計算量は従来に比べて大幅に削減できることを示した。

＜引用文献＞

① All-optical switchable logic gate using a single QD-SOA for RZ-BPSK signal inputs, Akira Nabeyama and Hiroyuki Yashima, OPTICAL AND QUANTUM ELECTRONICS, vol.53-5 (244), pp.1-16, 2021.4.

５．主な発表論文等

〔雑誌論文〕　計12件（うち査読付論文　12件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Shibata Ryo、Yashima Hiroyuki	４．巻 59
２．論文標題 Symbol-Level Detection With Matched Non-Binary LDPC Codes for Position Errors in Racetrack Memories	５．発行年 2023年
３．雑誌名 IEEE Transactions on Magnetics	６．最初と最後の頁 1～9
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TMAG.2022.3214932	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 Shibata Ryo、Yashima Hiroyuki	４．巻 11
２．論文標題 Windowed-based synchronization error-correction for spatially coupled codes	５．発行年 2022年
３．雑誌名 IEICE Communications Express	６．最初と最後の頁 697～702
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/comex.2022XBL0121	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 久保田 悟、雨車 和憲、田中 勇帆、古川 利博、八嶋 弘幸	４．巻 J105-C
２．論文標題 NMRS信号及びその差分信号のスパース性に基づいたデノイジング手法の提案	５．発行年 2022年
３．雑誌名 電子情報通信学会論文誌 C	６．最初と最後の頁 376～383
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transelej.2022JCP5006	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 SUGIO Nobuyuki、IGARASHI Yasutaka、HONGO Sadayuki	４．巻 E105.A
２．論文標題 Integral Cryptanalysis on Reduced-Round KASUMI	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 1309～1316
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021EAP1124	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 Usui Jumpei、Shibata Ryo、Yashima Hiroyuki	４．巻 11
２．論文標題 Deep-learning-aided design of LDPC coding scheme for two-user Gaussian multiple access channels	５．発行年 2022年
３．雑誌名 IEICE Communications Express	６．最初と最後の頁 111～116
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/comex.2021XBL0200	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 SHIBATA Ryo、YASHIMA Hiroyuki	４．巻 E105.A
２．論文標題 Design and Performance of Low-Density Parity-Check Codes for Noisy Channels with Synchronization Errors	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 63～67
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021EAL2013	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 Nabeyama Akira、Yashima Hiroyuki	４．巻 53
２．論文標題 All-optical switchable logic gate using a single QD-SOA for RZ-BPSK signal inputs	５．発行年 2021年
３．雑誌名 Optical and Quantum Electronics	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/s11082-021-02892-1	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 Shibata Ryo、Hosoya Gou、Yashima Hiroyuki	４．巻 56.9
２．論文標題 Concatenated LDPC/2-D-Marker Codes and Non-Iterative Detection/Decoding for Recovering Position Errors in Racetrack Memories	５．発行年 2020年
３．雑誌名 IEEE Transactions on Magnetics	６．最初と最後の頁 1～9
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TMAG.2020.3011447	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 SHIBATA Ryo、HOSOYA Gou、YASHIMA Hiroyuki	4．巻 E103.A
2．論文標題 Design and Construction of Irregular LDPC Codes for Channels with Synchronization Errors: New Aspect of Degree Profiles	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 1237～1247
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020EAP1004	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 SHIBATA Ryo、HOSOYA Gou、YASHIMA Hiroyuki	4．巻 E103.B
2．論文標題 A Novel Concatenation Scheme of Protograph-Based LDPC Codes and Markers for Recovering Synchronous Errors	5．発行年 2020年
3．雑誌名 IEICE Transactions on Communications	6．最初と最後の頁 1318～1330
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transcom.2019EBP3244	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 SHIBATA Ryo、HOSOYA Gou、YASHIMA Hiroyuki	4．巻 E103.A
2．論文標題 Concatenated LDPC/Trellis Codes: Surpassing the Symmetric Information Rate of Channels with Synchronization Errors	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 1283～1291
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020EAP1019	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 Igarashi Yasutaka、Nakazawa Shun、Kaneko Toshinobu	4．巻 10
2．論文標題 Differential Cryptanalysis of Block Cipher Halka	5．発行年 2020年
3．雑誌名 International Journal of Information and Electronics Engineering	6．最初と最後の頁 40～43
掲載論文のDOI（デジタルオブジェクト識別子） 10.18178/IJIEE.2020.10.2.718	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15件（うち招待講演　0件／うち国際学会　3件）

1．発表者名
杉尾信行，五十嵐保隆，本郷節之

2．発表標題
ブロック暗号KASUMIに対するBit-Based Division Propertyの適用に向けた解析(III)

3．学会等名
令和4年度 電気・情報関係学会北海道支部連合大会

4．発表年
2022年

1．発表者名
Naoki Shibayama and Yasutaka Igarashi

2．発表標題
A New Higher Order Differential of RAGHAV

3．学会等名
Proc. of The Tenth International Symposium on Computing and Networking（国際学会）

4．発表年
2022年

1．発表者名
山﨑　寛斗、五十嵐　保隆

2．発表標題
軽量ブロック暗号ALLPCに対する中間一致攻撃

3．学会等名
2023年　暗号と情報セキュリティシンポジウム

4．発表年
2023年

1．発表者名
杉尾信行，五十嵐保隆，本郷節之

2．発表標題
ブロック暗号MISTY2に対するBit-Based Division Propertyを用いた積分特性探索

3．学会等名
令和4年度 電気・情報関係学会北海道支部連合大会

4．発表年
2022年

１．発表者名
野畑開、五十嵐保隆

２．発表標題
MILPを用いた軽量ブロック暗号SHADOW-32の線形攻撃耐性評価

３．学会等名
2023年　暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
樋口 智大，柴田 凌，八嶋 弘幸

２．発表標題
非正則Multi-Kernel Polar符号の提案と性能調査

３．学会等名
第44回情報理論とその応用シンポジウム

４．発表年
2021年

１．発表者名
平川竜之・柴田　凌・八嶋弘幸

２．発表標題
FSK信号を入出力としたAND/OR切替可能な全光論理回路

３．学会等名
電子情報通信学会　総合大会

４．発表年
2022年

１．発表者名
杉尾信行，本郷節之，五十嵐保隆

２．発表標題
ブロック暗号KASUMIに対するBit-Based Division Propertyの適用に向けた解析

３．学会等名
電気・情報関係学会北海道支部連合大会

４．発表年
2021年

１．発表者名
Naoki Shibayama, Yasutaka Igarashi

２．発表標題
A New Higher Order Differential of Enocoro-128v2

３．学会等名
2021 Ninth International Symposium on Computing and Networking Workshops（国際学会）

４．発表年
2021年

１．発表者名
阿部友美，五十嵐保隆

２．発表標題
Fibonacci数列を利用したS-box及び転置関数によるAESへの有効性調査

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2022年

１．発表者名
Usui, J.; Hosoya, G.; Yashima, H.

２．発表標題
All-Optical Multi-Logic Gate Based on Four-Wave-Mixing in a Highly Nonlinear Fiber for Frequency-Shift-Keying Signal Inputs

３．学会等名
OSA Advanced Photonics Congress (AP) 2020（国際学会）

４．発表年
2020年

１．発表者名
金川創治郎、五十嵐保隆、金子敏信

２．発表標題
改良されたDLBCAブロック暗号アルゴリズムのFull-Round 差分特性による暗号識別

３．学会等名
2021年暗号と情報セキュリティシンポジウム

４．発表年
2021年

１．発表者名 芝山直喜、五十嵐保隆、金子敏信
２．発表標題 ストリーム暗号Enocoro-128v2の高階差分特性
３．学会等名 2021年暗号と情報セキュリティシンポジウム
４．発表年 2021年

１．発表者名 小松宏輝・五十嵐保隆・金子敏信
２．発表標題 軽量ブロック暗号MANTRAに対するBit-BasedDivisionPropertyを用いたIntegral攻撃
３．学会等名 電子情報通信学会技術研究報告
４．発表年 2021年

１．発表者名 勝田耕作、五十嵐保隆、金子敏信
２．発表標題 ニューラルネットワークを用いた軽量ブロック暗号PRESENTの解析
３．学会等名 研究報告コンピュータセキュリティ（CSEC）
４．発表年 2021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	五十嵐　保隆 (Igarashi Yasutaka) (80434025)	東京理科大学・創域理工学部電気電子情報工学科・准教授 (32660)	

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