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　２ 年　 ６ 月 １１ 日現在

機関番号：３２６６０
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ０６４４３

研究課題名（和文）干渉抑圧機能とセキュリティ機能を有する全光CDMA

研究課題名（英文）All Optical CDMA with interference cancellation and security

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）　　3,600,000円

研究成果の概要（和文）：本論文では，SSFBGを用いたOCDMAシステムにおいて，相関値出力における干渉抑圧を目的とした，QD-SOA based MZIで構成する干渉抑圧器を提案した．提案デバイスにより，他ユーザからの干渉や自己相関のピーク強度以外の光が混在している相関器の出力光から，ピーク強度の光のみを抽出し，さらに干渉を抑圧した．また提案デバイスが全光CDMAに適用可能か検証するた め、光CDMAのクロックと信号のタイミングのずれの影響も評価した.
一方、セキュリティ対策として、暗号分野で注目を集めている超軽量暗号に 着目し、超軽量ブロック暗号QTL-64の不能差分攻撃耐性の評価を行った.

研究成果の学術的意義や社会的意義
量子ドット半導体のような小型・省電力・低雑音の素子で構成され、かつ全光処理が可能な干渉 抑圧機能を備えた全光 CDMA はこれまでになく、本研究は独創性の高いものである。これによ り、小型、低消費電力な素子で干渉を抑圧し、高速・高多重度の全光 CDMA システムの構築が 可能となるという意義がある。また、通常の暗号とセキュリティ機能を持つ全光 CDMA との併用という選択肢が生じ、提案する全光CDMAは、超高速で高いセキュリティ機能を有する通信方式として安心・安全な情報化社 会を支える手段として考えられ、大きな意義を有する。

研究成果の概要（英文）：In this research, we propose a method for suppressing interference in a SSFBG OCDMA(Super Structured Fiber Bragg Grating Optical Code Division Multiple Access) system. The proposed suppressor comprises Quantum-dot Semiconductor Optical Amplifier and can be composed as a small and power-efficient device. The proposed device suppresses interference in chip positions (except at the auto-correlation peak) through time gate processing, and it enhances eye opening through threshold processing. These reduce multiple access interference and significantly improve power contrast ratio and extinction ratio. The performance of this device is verified through numerical analysis and simulation.
In addition, we apply the MILP method to the symmetric key block ciphers M6 and M8. M6 is a 10-round Feistel-type cipher with a block size of 64 bits. We found the 4-round 63rd-order integral distinguisher of M6 and 5-round 63rd-order integral distinguisher of M8 for the first time.

研究分野：通信工学

キーワード：光CDMA　量子ドット半導体光増幅器　セキュリティ

様　式　C－１９、F－１９－１、Z－１９（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。光 CDMA(Code Division Multiple Access) はアクセス系ネットワークの多重通信方式として、現状の波長分割多重(WDM)との 共存が可能かつ構成が簡単でフレキシブルな光ネットワークの構築が可能である。特に、 SSFBG(Super-Structured Fiber Bragg Grating)による２次元符号を用いる光 CDMA は、周波数利用効率が高く、次世代のアクセス系ネットワークの多重通信方式として期待され、近年、企業や独立行政法人の研究所等でも研究が進められ、実験段階に至っている.

２．研究の目的

本研究では、大容量かつ高度な情報セキュリティ機能を有する全光 CDMA を提案し、その有効性を明らかにすることを目的とする。具体的な研究目的は次の２点である。光 CDMA において、電気信号処理を用いず全光処理 が可能な干渉抑圧手法を用いた全光 CDMA システムを提案し、その諸特性を評価し、周波数 利用効率が高く、大容量の伝送が可能であることを明らかにする。さらに、提案する全光 CDMA に長周期で多値のユーザ符号を用いることによりセキュリティ効果を持たせ、その安全性を評価し、高いセキュリティ効果を有することを明らかにする。

３．研究の方法

本研究では、大容量の全光 CDMA を目指し、他ユーザからの干渉信号を光信号のまま抑圧する機能を持つ全光 CDMA を提案する。提案する干渉抑圧器は量子ドット光増幅器で構成され、波動方程式とレート方程式を数値解析することにより動作を解析し、さらに計算機シミュレーションにより、相関出力波形と消光比および Q 値等の諸特性を求め、その有効性を示す。また、多値・長符号を全光 CDMA のユーザ符号に用いることにより、セキュリティ機能を 有する全光 CDMA システムを提案する。提案した全光 CDMA に対し、相互情報量解析および解読までに要するデータ量、計算量等の諸特性を解析とシミュレーションにより定量的に評価し、提案する全光 CDMA システムが高いセキュリティ強度を有することを明らかにする。評価検討項目としては、全光 CDMA の受信器に用いる干渉抑圧器の提案と基礎特性の評価、多値・長周期符号を用いた光 CDMA システムの符号の構築および相互情報量特性の評価、干渉を抑圧した全光 CDMA システムの特性評価などがある。

４．研究成果

図１ に提案する SSFBG と干渉抑圧器を用いた光 CDMA システムのブロック図を示す．まず，各送信ユーザは送信情報を与えられた拡散符号に基づいて，SSFBG で構成された符号器により符号化を行う．符号化された光信号はパワーコンバイナにより合成され，一本の光ファイバで伝送される．光ファイバを通った受信信号はスプリッタにより各ユーザに分配され，SSFBG で構成された相関器を用いて受信した信号と各ユーザの拡散符号との相関値を求め，相関器の出力とする．最後に提案する干渉抑圧器を用いて相関器の出力から自己相関の干渉抑圧器を用いて相関器の

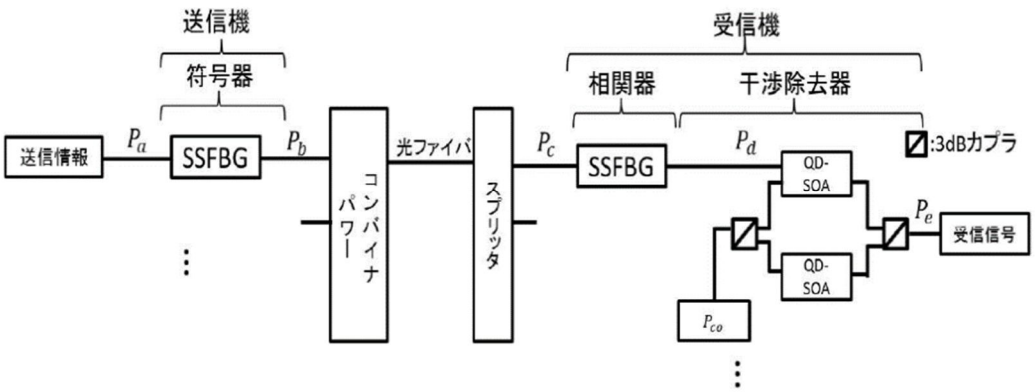

図１　提案する SSFBG と干渉抑圧器を用いた光 CDMA

出力から自己相関のピーク値のみを抽出し，これを受信情報とする．本干渉抑圧器は自己相関のピーク強度の信号以外の信号を除去する時間ゲート処理，かつ閾値強度をこえた信号のみを増

幅させる閾値処理を同時に行い，MAI を軽減する．

ユーザ数を 8 人として多重通信を行った場合の解析結果を示す．図２はユーザ数 N = 8，符号長 F = 31 プリファードゴールド符号を用いた場合の送受信信号の波形である．図２(a)～(c) の光強度は各図における最大強度で正規化されている．またユーザ 1 に注目して解析を行い，ユーザ 1 は 1, 0 を送信し，その他のユーザは 1, 1 を送信するものとし，ユーザ間の同期はとっていない．図２(a) はユーザ 1 の送信信号，図２(b) は相関器出力の光信号，図２(c) は干渉抑圧器の出力の光信号である．干渉抑圧器の制御光は相関器の自己相関のピーク強度のタイミングに合わせて光信号を入射するため，ピーク強度のタイミングの光信号のみが出力されている．図２(a), (c) より，送受信が正しく行われていることが確認できる．

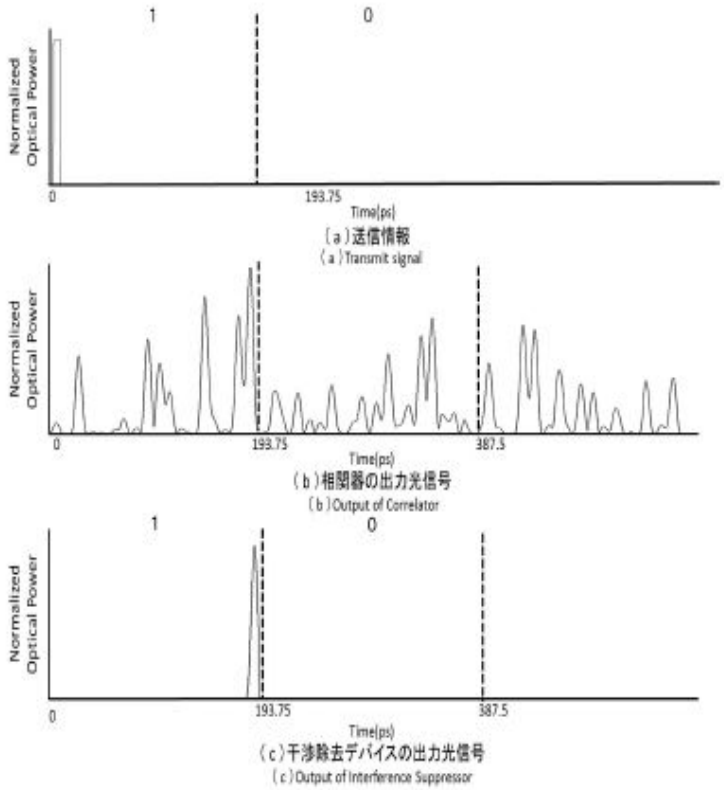

図２　ユーザ数 N = 8，符号長 F = 31 の符号を用いた場合の送受信信号の波形

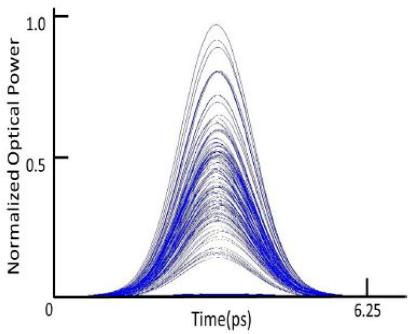

図３は N = 4,F = 31 のときの送信信号とユーザ間の遅延をランダムにしたときの干渉抑圧器の出力におけるアイダイアグラムである．干渉抑圧器を用いることで MAI が軽減されている．また光強度の高い信号程増幅されている．消光比は 13dB で，干渉抑圧器適応前と比較して 7dB ほど改善されることがわかる．

図３　N = 4,F = 31 のときの干渉抑圧器の出力におけるアイダイアグラム

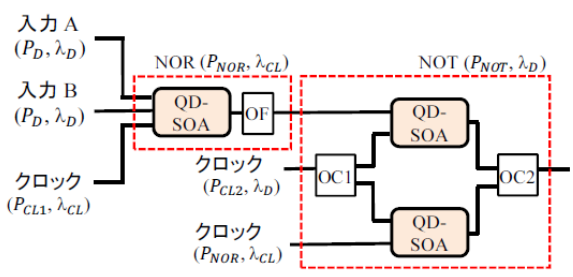

図４　干渉抑圧器を応用した全光 OR ゲート

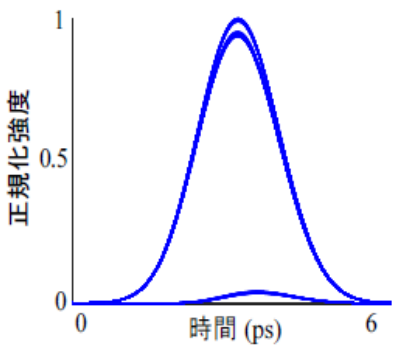

図５　出力信号のアイダイアグラム

干渉抑圧器の応用として、図４のように、全光 OR ゲートの一部に用いることができる。図５は図４の全光 OR ゲートの出力信号のアイダイアグラムであり、良好な消光比を示している。

また、情報セキュリティについては、軽量ブロック暗号μ2 に対する Bit-Based Division Property を用いた積分攻撃、ブロック暗号 SIT に対する差分攻撃、Division Property と MILP を利用したブロック暗号 CHAM 積分特性及び鍵回復などの検討を行った。

５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　7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 R. Shibata, G. Hosoya, and H. Yashima	４．巻 E101-A
２．論文標題 Joint iterative decoding of spatially coupled low-density parity-check codes for position errors in racetrack memories	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 2055-2063
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.2055	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 Tadashi Sasaki, Yasutaka Igarashi, and Toshinobu Kaneko	４．巻 24.3
２．論文標題 MILP-Aided Bit-Based Division Property for M6 and M8	５．発行年 2018年
３．雑誌名 Advanced Science Letters	６．最初と最後の頁 1571-1574
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 Komatsu K.、Hosoya G.、Yashima H.	４．巻 51
２．論文標題 Ultrafast all-optical digital comparator using quantum-dot semiconductor optical amplifiers	５．発行年 2019年
３．雑誌名 Optical and Quantum Electronics	６．最初と最後の頁 1-16
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11082-019-1756-5	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 Matsumoto T.、Komatsu K.、Hosoya G.、Yashima H.	４．巻 54.9
２．論文標題 Performance of all-optical AND gate using photonic-crystal QDSOA at 160 Gb/s	５．発行年 2018年
３．雑誌名 Electronics Letters	６．最初と最後の頁 580-582
掲載論文のDOI（デジタルオブジェクト識別子） 10.1049/el.2018.0371	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. Komatsu, G. Hosoya, and H. Yashima	４．巻 50-131
２．論文標題 All-Optical Logic NOR Gate Using a Single Quantum-Dot SOA-Assisted an Optical Filter	５．発行年 2018年
３．雑誌名 Optical and Quantum Electronics	６．最初と最後の頁 1-18
掲載論文のDOI（デジタルオブジェクト識別子） org/10.1007/s11082-018-1384-5	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 SHIBATA Ryo、HOSOYA Gou、YASHIMA Hiroyuki	４．巻 E102.A
２．論文標題 Protograph-Based LDPC Coded System for Position Errors in Racetrack Memories	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 1340～1350
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1587/transfun.E102.A.1340	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 -
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 -
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/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 －

〔学会発表〕　計11件（うち招待講演　1件／うち国際学会　9件）

１．発表者名 M. Yuri, R. Shibata, G. Hosoya, and H. Yashima
２．発表標題 Probabilistic shaping for BICM with pseudorandom sequence
３．学会等名 Proc. 2018 International Symposium on Information Theory and its Applications (ISITA2018)（国際学会）
４．発表年 2018年

１．発表者名
K. Komatsu, G. Hosoya, and H. Yashima

２．発表標題
Multiple-input all-optical OR gate by cascaded logic gates based on quantum-dot semiconductor optical amplifier

３．学会等名
Latin America & Optics and Photonics Conference（国際学会）

４．発表年
2018年

１．発表者名
K. Komatsu, G. Hosoya, and H. Yashima

２．発表標題
All-optical two-bit magnitude comparator using quantum-dot semiconductor optical amplifier

３．学会等名
Proc. Asia Communications and Photonics Conference（国際学会）

４．発表年
2018年

１．発表者名
T. Matsumoto, G. Hosoya, and H. Yashima

２．発表標題
All-optical AND gate with photonic crystal quantum-dot semiconductor optical amplifiers

３．学会等名
2018 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing（国際学会）

４．発表年
2018年

１．発表者名
R. Shibata, G. Hosoya, and H. Yashima

２．発表標題
Performance analysis of spatially-coupled low-density parity-check codes based on reading ratio in racetrack memory

３．学会等名
2018 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing（国際学会）

４．発表年
2018年

１．発表者名
G. Hosoya and H. Yashima

２．発表標題
Spatially-coupled LDPC codes for two dimensional erasure channel

３．学会等名
2017 IEEE Information Theory Workshop (ITW2017)（国際学会）

４．発表年
2017年

１．発表者名
K. Komatsu, G. Hosoya, and H. Yashima

２．発表標題
Simulation of All-Optical NOR Gate Using Single Quantum-Dot And Optical Filter

３．学会等名
CLEO PR, OECC & PGC 2017（国際学会）

４．発表年
2017年

１．発表者名
Gou Hosoya

２．発表標題
Recent Studies on Error Correction for Insertion/Deletion/Substitution Channels

３．学会等名
2017 Society Symposium, The Institute of Electronics, Information and Communication Engineers , AT-1-4（招待講演）

４．発表年
2017年

１．発表者名
芝山直喜，五十嵐保隆，金子敏信

２．発表標題
ブロック暗号Fewの高階差分特性

３．学会等名
電子情報通信学会、技術報告

４．発表年
2017年

１．発表者名
Akira Nabeyama, Kosuke Komatsu, Gou Hosoya, and Hiroyuki Yashima

２．発表標題
2-Input/3-Input All-Optical Switchable AND/NOR Logic Gate

３．学会等名
OSA Advanced Photonics Congress (AP) 2019（国際学会）

４．発表年
2019年

１．発表者名
Hiroyuki Yashima, Kosuke Komatsu and Gou Hosoya

２．発表標題
SIMULATION ON APPLICATION OF QD-SOA TO SOME ALL OPTICAL LOGIC GATES

３．学会等名
2nd International Congress on Photonics Research（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	細谷　剛 (Hosoya Gou) (60514403)	東京理科大学・工学部情報工学科・講師 (32660)	
研究分担者	五十嵐　保隆 (Igarashi Yasutaka) (80434025)	東京理科大学・理工学部電気電子情報工学科・講師 (32660)	