

令和 3 年 5 月 21 日現在

機関番号：32639

研究種目：基盤研究(C)（一般）

研究期間：2018～2020

課題番号：18K04290

研究課題名（和文）高速物理暗号光通信のための多段変調素子構成による超多値光位相変調

研究課題名（英文）Extremely high-order optical phase modulation with multi-stage modulators for physical layer encryption of high-speed optical communications

研究代表者

谷澤 健（TANIZAWA, Ken）

玉川大学・量子情報科学研究所・准教授

研究者番号：10709489

交付決定額（研究期間全体）：（直接経費） 3,400,000円

研究成果の概要（和文）：本研究では、高速かつセキュアな光ファイバ通信のための物理暗号の実現を目指して、極めて多値に光位相を変調する新たな手法を提案し、その動作を実証することに取り組んだ。光変調素子を多段に接続して高分解能な光位相変調を実現し、これを10Gbit/sを超える高速の物理暗号へと応用展開し、光集積デバイス構成を検討するという目標を達成した。提案する光位相の高分解能変調により、安全性と通信性能を両立した物理暗号が実現できることを明らかにした。高速な物理暗号の長距離光ファイバ通信実験にも成功するなど、当初想定を超える成果を挙げることができた。

研究成果の学術的意義や社会的意義

本研究で実証した光位相の高分解能変調を応用した物理暗号は、光ファイバ通信のセキュリティを高めるものであり、我々の生活を基盤として支えるデータ通信技術の安全性の向上に将来的に貢献することが期待される。高速の光通信に応用可能であるため、実用的な価値も高い。研究成果の一部である物理暗号の安全性と通信性能のトレードオフに関する知見は、この暗号技術の学問的な体系化に貢献するものである。また、光位相の高分解能変調は物理暗号以外にも応用できる汎用的な技術であり、将来的に様々な研究への展開が期待できる。

研究成果の概要（英文）：In this research, we proposed a novel method of cascading optical phase modulators for a high bit resolution and demonstrated extremely high-order phase modulation for physical layer encryption of high-speed fiber-optic communications. Proof-of-concept experiments of the proposed method were achieved. The method was successfully applied to physical layer encryption of optical signals at 10 Gbit/s or higher. Furthermore, optical devices that integrate multiple phase modulators were studied. We showed that the physical layer encryption with the proposed method simultaneously realized high security and adequate signal quality. Physical-layer encrypted high-speed optical signal transmission over a long-haul fiber was experimentally demonstrated.

研究分野：光ファイバ通信

キーワード：光ファイバ通信 物理暗号 変調方式

## 1. 研究開始当初の背景

情報通信におけるセキュリティの担保は、IoT 等の発展により益々重要な課題となっている。近年は通信のバックボーンである光ファイバ伝送でもセキュリティの重要性が高まっている。光ファイバからの盗聴を防ぐ技術として、2000 年初頭に光の量子雑音の存在によりその安全性を保証する物理暗号（以下、「光通信物理暗号」）が提案され(G. A. Barbosa, et al., Phys. Rev. Lett., 2003)、その原理実証や安全性の議論が行われてきた(O. Hirota, Phys. Rev. A. 2007 等)。最近では、1Gbit/s を超える光通信物理暗号装置が試作され実データの伝送も実証されている(F. Futami, et al., Proc. of SPIE, 9980, 2016)。光通信物理暗号は、あらかじめ共有した短い秘密鍵を用いて[0 or 1]のデータを、光の領域で連続的なアナログ量に「極めて」多値に変調することで暗号化する。データを雑音、究極的には真にランダムかつ絶対に取り除けない光受信で生じる量子雑音で覆うことで秘匿化が実現できる。秘密鍵をもたない非正規の受信者は雑音により暗号を正確に読み取ることができない。この物理暗号では、どれだけ多値にデータを変調できるかが安全性の指標になる。研究代表者は、安全性と高い通信性能の両立を目指して、光の位相変調とデジタル信号処理を融合する光通信物理暗号の高速・高機能化を検討してきた(K. Tanizawa, et al., Communications Express, 2017)。この光通信物理暗号で量子雑音による秘匿の効果を十分に得るには、 $2^{12}=4096$  値以上の変調多値数が求められることがわかっている。光の多値変調は、通常、D/A コンバータで光変調器を駆動することで実現できる。しかしながら、一般に D/A コンバータのサンプリング速度と分解能にはトレードオフ(例、10Gsample/s では、多値数が最大 1024 値程度)があるため、10Gbit/s 超の高速で物理暗号化のためにそのような高い多値信号で作り出すことができなかった。

## 2. 研究の目的

本研究では、極めて多値の光位相の変調を実現するために「光位相変調素子を多段に接続・制御する超高分解能の位相変調技術」を新たに提案し、これを多値変調による光通信物理暗号に応用し、その動作を実験実証することを目的とする。また、将来的な光集積デバイスでの実現を念頭に基礎検討を行う。以下に示す 3 つの具体的な目標を掲げて研究を進めた。

- (1) 提案方式にて位相変調の多値数が向上することを 10Gbit/s の変調速度で示す
- (2) 10Gbit/s の光通信物理暗号を多値数  $2^{12}=4096$  以上で発生する
- (3) 提案方式を光集積デバイスで実現するための基礎検討を行う

## 3. 研究の方法

(1) ~ (3)のそれぞれの目標に対して以下の方法で研究を進めた。

### (1) 光位相変調素子の多段接続・制御による変調多値数向上の実証

提案する光位相変調素子の多段接続による高分解能の位相変調では、初段で荒い位相変調を行った後に二段目で密な位相変調を実施する。これにより、例えば、位相変調素子を駆動する D/A コンバータの分解能がそれぞれ M, N ビットとしたとき、M+N ビットの分解能を実現できる。研究では、まずどのように変調量を設定すればこのような分解能の向上を実現できるかの設計論を確立した。次に、10Gbit/s 以上で動作する LiNbO<sub>3</sub> 位相変調器を 2 つ直列に接続する実験系を構築し、実験を行った。位相変調器間に距離があるため、前後段の変調が同期するように、後段の D/A コンバータ出力に電気段で適切な遅延を与えた。また、光学素子と高周波デバイスに高い線形性が求められるため、電気段での補償技術についても検討した。10Gsample/s の速度で M および N を 1, 2 など比較的小さな値として、変調多値数の向上を確認する実験を行った。最終的には、M=6, N=10 として一段の変調では実現できない 16 ビットの高分解能な位相変調を行った。

### (2) 多値数 $2^{12}=4096$ (分解能 12 ビット) 以上の 10Gbit/s 光通信物理暗号の発生

次に、直列接続した位相変調器への入力を 10Gbit/s の 2 値位相変調データ信号とし、位相変調器の駆動を秘密鍵から生成したランダムな信号とすることで、光通信物理暗号を発生した。2 値のデータと共有する秘密鍵から光通信物理暗号を生成するための数学的な前処理をソフトウェアで実装し、この信号を用いて D/A コンバータを同期・協調して制御した。先の原理確認で採用した M=6, N=10 とすることで、BPSK 信号を  $2^{17}$  の位相レベルをもつ暗号に変換できる。並行して暗号の復号化を含む受信のための信号処理をソフトウェアで実装し、オフラインで暗号を復号し、受信品質を評価できるようにした。さらに、多値データ変調や偏波多重技術を適用する高速化の検討を行った。

### (3) 光集積デバイスの実現に向けた基礎検討

提案方式は、複数(最低 2 つ)の位相変調素子が必要になるという構成上の複雑さをとまなう。よって、これらの位相変調素子を集積化した光デバイスをシリコンフォトリソグラフィにて実現するための検討を行った。まず、位相変調器、強度変調器、IQ 変調器の 3 つのパターンで複数位相変調素子を用いる集積化変調器の構成を考案した。次に、シリコンフォトリソグラフィにおける代表的な高速位相変調機構である pn 構造によるキャリアプラズマ効果を用いた光デバイスの設計方針に

ついて検討した。さらに、共同研究により実際に多段の位相変調素子を配した IQ 変調器を作製し、その評価を行った。

#### 4. 研究成果

##### (1) 光位相変調素子の多段接続・制御による変調多値数向上の実証

図 1 にマツツェンダ変調器で BPSK 変調を行った後に、二段の光位相変調器をそれぞれ 1 ビットの信号で駆動した原理確認実験の結果を示す。最終段では、 $1+1+1=3$  ビット、つまり  $2^3=8$  値の位相変調信号となることが実験的に確認できた。本実験に先立ち、それぞれの位相変調器による変調量をどのように設定すれば分解能が向上するかという設計論を確立した。それに従って駆動電圧を適切に調整することで、このように 8 値の位相が等間隔に配される分解能の向上を実現できた。

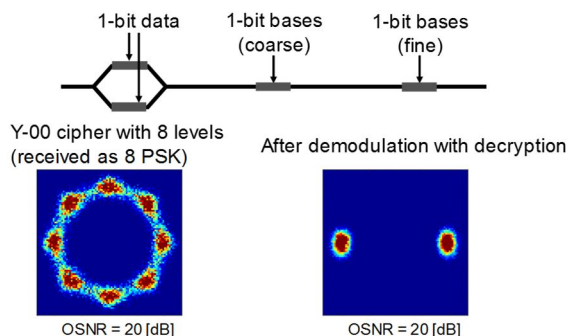


図 1 位相変調素子の多段接続による位相多値数向上の原理確認実験結果

##### (2) 多値数 $2^{12}=4096$ (分解能 12 ビット) 以上の 10Gbit/s 光通信物理暗号の発生

図 2 に提案手法において  $M=6$ ,  $N=10$  とした  $2^{17}$  値の光位相をもつ物理暗号を発生・受信した結果を示す。(a)に示すように、暗号化により上段のドーナツ形状のコンスタレーションが得られた。秘密鍵を用いた復号化により、下段に示す暗号化前の BPSK 信号を復元することができた。このように適切に暗号化・復号化が実施できることを確認した。光ファイバを 400km 伝送した後で復号化したコンスタレーションと信号品質の評価として BER を測定した結果を、(b)と(c)にそれぞれ示す。光ファイバの伝送にともない生じる波長分散による線形な波形劣化を補償する信号処理を行うことで、長距離伝送後も劣化のない信号品質を実現した。暗号化・復号化により生じるペナルティは極めて小さく、高い通信性能を保ったまま安全性の向上を実現できた。

図 3 にデータ変調を QPSK とし、偏波多重を導入したときの実験結果を示す。これらの多重技術の導入によりビットレートは 48Gbit/s となる。(a)に示したコンスタレーションから、両偏波について適切な暗号化と復号化が実施できていることがわかる。(b)に 400 と 800km 伝送を行ったときの光ファイバへの入力パワーと受信した信号の Q 値 (左縦軸) および量子雑音による信号マスクの数を示す。信号マスク数は大きいほど秘密鍵をもたない受信における不確実性が大きくなり、安全性が高い。この結果より、長距離伝送においては信号品質と安全性にトレードオフの関係があることがわかる。400km と 800km の光ファイバ伝送においては、誤り訂正符号閾値を満たす適切な信号品質と実際的に十分な安全性を実現できる数 100 程度のマスク数を両立できることを実証した。

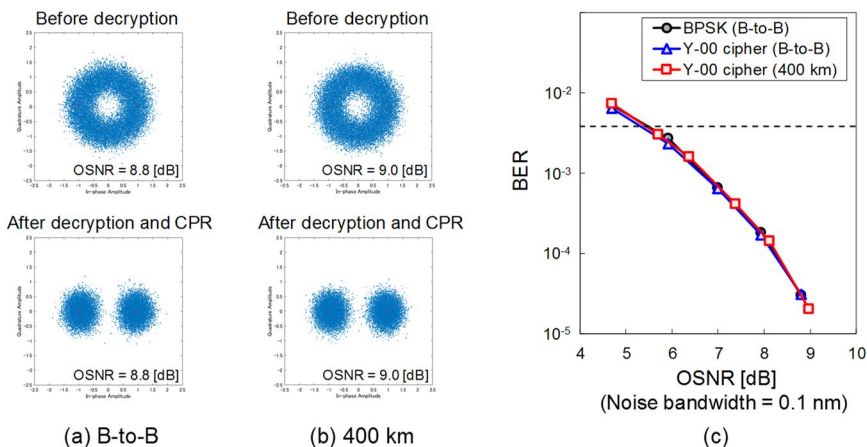


図 2 10Gbit/s の光通信物理暗号の発生および受信実験結果

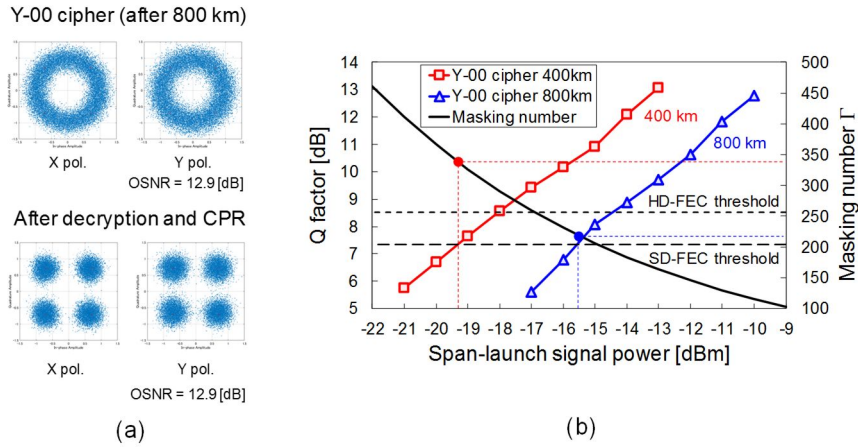


図3 48Gbit/s の光通信物理暗号の光ファイバ伝送実験結果

### (3) 光集積デバイスの実現に向けた基礎検討

位相変調器，強度変調器，IQ 変調器の 3 つのパタンで複数位相変調素子を用いる集積化変調器の構成について考案した．位相変調器については単純に直列接続すれば良いが，強度変調器と IQ 変調器についてはその配置に設計の自由度がある．マッハツェンダ干渉計を構成する両アームに直列に接続した位相変調素子を配し，これらをプッシュ・プルで駆動する構成がチャープを防ぐために好適であることがわかった．次に，シリコンフォトニクスにおけるキャリアプラズマ効果を用いた位相変調素子については，ファウンドリが提供するデザインを用いることで概ね所望の特性が得られることがわかった．最後に，共同研究により実際に二段の位相変調素子を配した IQ 変調器を作製し，その評価を行った．I および Q の双方の成分に対して想定通りに変調多値数を向上できることを実験により確認した．

以上に示すように，当初の目標を十分に達成し，高速の物理暗号光ファイバ通信実験や光デバイス試作にも成功するなど，当初想定を超える成果を挙げることができた．本研究で提案・実証した光位相変調の分解能向上の手法は，秘密鍵による多値変調を用いる光通信物理暗号の通信性能と安全性の両立に貢献することが実証できた．より高速・長距離というような今後の研究進展に加えて，光ファイバ通信以外への応用展開やさらなる安全性向上の追求などが今後重要な研究となると考えられる．

## 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 1件/うちオープンアクセス 5件）

1. 著者名 Xi Chen, Ken Tanizawa, Peter Winzer, Po Dong, Junho Cho, Fumio Futami, Kentaro Kato, Arishti Melikyan, and KW Kim	4. 巻 29
2. 論文標題 Experimental demonstration of 4,294,967,296-QAM based Y-00 quantum stream cipher template carrying 160-Gb/s 16-QAM signals	5. 発行年 2021年
3. 雑誌名 Optics Express	6. 最初と最後の頁 5658-5664
掲載論文のDOI (デジタルオブジェクト識別子) 10.1364/OE.405390	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 Ken Tanizawa, and Fumio Futami	4. 巻 29
2. 論文標題 Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system	5. 発行年 2021年
3. 雑誌名 Optics Express	6. 最初と最後の頁 10451-10464
掲載論文のDOI (デジタルオブジェクト識別子) 10.1364/OE.418302	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 Ken Tanizawa, and Fumio Futami	4. 巻 38
2. 論文標題 Quantum Noise-Assisted Coherent Radio-over-Fiber Cipher System for Secure Optical Fronthaul and Microwave Wireless Links	5. 発行年 2020年
3. 雑誌名 IEEE/OSA Journal of Lightwave Technology	6. 最初と最後の頁 4244-4249
掲載論文のDOI (デジタルオブジェクト識別子) 10.1109/JLT.2020.2987213	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 Ken Tanizawa, and Fumio Futami	4. 巻 27
2. 論文標題 Single channel 48-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 400- and 800-km SSMF	5. 発行年 2019年
3. 雑誌名 Optics Express	6. 最初と最後の頁 25357-25363
掲載論文のDOI (デジタルオブジェクト識別子) 10.1364/OE.27.025357	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 Ken Tanizawa, and Fumio Futami	4. 巻 27
2. 論文標題 Digital coherent PSK Y-00 quantum stream cipher with $2^{17}$ randomized phase levels	5. 発行年 2019年
3. 雑誌名 Optics Express	6. 最初と最後の頁 1071-1079
掲載論文のDOI (デジタルオブジェクト識別子) 10.1364/OE.27.001071	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 Ken Tanizawa, and Fumio Futami	4. 巻 30
2. 論文標題 $2^{14}$ Intensity-Level 10-Gbaud Y-00 Quantum Stream Cipher Enabled by Coarse-to-Fine Modulation	5. 発行年 2018年
3. 雑誌名 IEEE Photonics Technology Letters	6. 最初と最後の頁 1987-1990
掲載論文のDOI (デジタルオブジェクト識別子) 10.1109/LPT.2018.2874236	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 Ken Tanizawa, and Fumio Futami	4. 巻 10946
2. 論文標題 Digital-coherent PSK Y-00 quantum stream cipher for secure fiber-optic transmission	5. 発行年 2019年
3. 雑誌名 Proceedings SPIE 10946, Metro and Data Center Optical Networks and Short-Reach Links II	6. 最初と最後の頁 109460B
掲載論文のDOI (デジタルオブジェクト識別子) 10.1117/12.2506835	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14件(うち招待講演 4件/うち国際学会 9件)

1. 発表者名 Ken Tanizawa, and Fumio Futami
2. 発表標題 Security-Enhanced 10,118-km Single-Channel 40-Gbit/s Transmission Using PSK Y-00 Quantum Stream Cipher
3. 学会等名 46th European Conference on Optical Communications (ECOC 2020) (国際学会)
4. 発表年 2020年

1. 発表者名 Ken Tanizawa, and Fumio Futami
2. 発表標題 Multi-Channel Simultaneous Encryption in WDM Systems of PSK Y-00 Quantum Stream Cipher
3. 学会等名 25th Opto-Electronics and Communications Conference (OECC 2020) (国際学会)
4. 発表年 2020年

1. 発表者名 谷澤 健, 二見史生
2. 発表標題 デジタルコヒーレント位相変調Y-00光通信量子暗号を用いたセキュア光ファイバ伝送
3. 学会等名 電子情報通信学会 光ファイバ応用技術研究会 (招待講演)
4. 発表年 2020年

1. 発表者名 谷澤 健, 二見史生
2. 発表標題 位相変調Y-00光通信量子暗号におけるWDM信号の一括暗号化実験
3. 学会等名 電子情報通信学会 光通信システム研究会
4. 発表年 2020年

1. 発表者名 谷澤 健, 二見史生
2. 発表標題 光ヘテロダイン検波を用いたミリ波無線信号の量子雑音マスキングによる秘匿化の提案・実証
3. 学会等名 電子情報通信学会 2021年総合大会
4. 発表年 2021年

1. 発表者名 Ken Tanizawa, and Fumio Futami
2. 発表標題 Digital coherent PSK Y-00 quantum stream cipher for secure and high-capacity optical transmission systems
3. 学会等名 Asia Communications and Photonics Conference 2019 (ACP2019) (招待講演) (国際学会)
4. 発表年 2019年

1. 発表者名 Ken Tanizawa, and Fumio Futami
2. 発表標題 48-Gbit/s Dual-Polarization PSK Y-00 Quantum Stream Cipher Based on QPSK Data Modulation
3. 学会等名 24th Opto-Electronics and Communications Conference (OECC 2019) (国際学会)
4. 発表年 2019年

1. 発表者名 Fumio Futami, Ken Tanizawa, and Kentaro Kato
2. 発表標題 Y-00 Quantum Stream Cipher for Physical Layer Security of Optical Communications
3. 学会等名 45th European Conference on Optical Communications (ECOC 2019) (招待講演) (国際学会)
4. 発表年 2019年

1. 発表者名 谷澤 健, 二見史生
2. 発表標題 48-Gbit/s PSK Y-00光通信量子暗号の800-km光ファイバ伝送
3. 学会等名 電子情報通信学会 2020年総合大会
4. 発表年 2020年



1. 発表者名 Ken Tanizawa, and Fumio Futami
2. 発表標題 Digital Coherent 20-Gbit/s DP-PSK Y-00 Quantum Stream Cipher Transmission over 800-km SSMF
3. 学会等名 Optical Fiber Communication Conference and Exhibition (OFC 2019) (国際学会)
4. 発表年 2019年

1. 発表者名 Ken Tanizawa, and Fumio Futami
2. 発表標題 Digital-coherent PSK Y-00 quantum stream cipher for secure fiber-optic transmission
3. 学会等名 SPIE Photonics West (招待講演) (国際学会)
4. 発表年 2019年

1. 発表者名 Ken Tanizawa, and Fumio Futami
2. 発表標題 PSK Y-00 Quantum Stream Cipher with $2^{17}$ Levels Enabled by Coarse-to-Fine Modulation Using Cascaded Phase Modulators
3. 学会等名 44th European Conference on Optical Communications (ECOC 2018) (国際学会)
4. 発表年 2018年

1. 発表者名 Ken Tanizawa, and Fumio Futami
2. 発表標題 Digital Coherent Detection with Decryption in PSK Y-00 Quantum Stream Cipher
3. 学会等名 23rd Opto-Electronics and Communications Conference (OECC 2018) (国際学会)
4. 発表年 2018年

1. 発表者名 谷澤 健, 二見史生
2. 発表標題 波多重PSK Y-00光通信量子暗号のデジタルコヒーレント受信
3. 学会等名 電子情報通信学会 2019年総合大会
4. 発表年 2019年

〔図書〕 計0件

〔出願〕 計1件

産業財産権の名称 信号処理装置	発明者 谷澤 健, 二見史生	権利者 同左
産業財産権の種類、番号 特許、PCT/JP2019/010997	出願年 2019年	国内・外国の別 国内

〔取得〕 計0件

〔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
連携研究者	二見 史生  (FUTAMI Fumio)  (20417695)	玉川大学・量子情報科学研究所・教授    (32639)	

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
---------	---------