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　 ５ 月 １８ 日現在

機関番号：３２６３９
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ０４３９７

研究課題名（和文）超多値変調を用いた物理暗号によるセキュア光無線通信の研究

研究課題名（英文）Secure free-space optical communication using physical cipher signals with ultra-high order modulation

研究代表者

二見　史生（FUTAMI, Fumio）

玉川大学・量子情報科学研究所・教授

研究者番号：２０４１７６９５

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、高い安全性、低遅延性やプロトコル無依存動作を特徴とする光無線通信の実現を目的に、物理暗号を用いたセキュア光無線通信方式を新たに提案し、その特性評価に取り組んだ。物理暗号に雑音を利用し、通信データの高い安全性と低遅延性を実現でき、同時に、光のまま空間と光ファイバを相互変換することにより通信データのプロトコル無依存性を達成した。更に、本方式の暗号鍵更新への応用も実証し、当初計画を越える成果が得られた。

研究成果の学術的意義や社会的意義
本研究では、物理現象を用いた物理暗号を利用して光無線通信の安全性を高めるセキュア光無線通信方式を提案し、実証した。本方式は、空間通信の安全性を高められる上に、通信で生じる遅延時間が小さく、様々な変調方式の信号を扱うことができる特長があり、将来的には安全な通信手段としての日常的な利用が期待される。物理暗号を空間通信に応用する研究は、比較的新しい研究領域であり、新領域の研究分野の開拓やその発展に貢献するものと考えられる。

研究成果の概要（英文）：This study proposed a novel secure optical wireless communication scheme using a physical cipher for highly secure optical wireless communication with low latency and protocol-free operation. High security and low latency were achieved using noise in the physical cipher. In addition, protocol-free communication was achieved by all-optical conversion with free space and optical fibers. Furthermore, we successfully applied this scheme to the updating of secret keys.

研究分野：光通信

キーワード：セキュア通信　光無線通信　物理暗号

１．研究開始当初の背景

ネットが発展し機微な情報を扱うアプリやサービスの実現に伴い、ネット全体のセキュリティ担保が喫緊の課題になっていた。光無線通信は天候依存性や通信距離が比較的短い課題があるものの、高速・大容量、電波と共存可能など特徴があり、企業、学校、自治体等の建物間通信や防犯/監視カメラとの通信等で利用され、秘密情報や個人情報も通信されているため、光無線通信にも高いセキュリティが求められていた。指向性が高いため光無線通信は秘匿性が高いと一般に考えられているが、空間を信号が伝搬する以上、第三者が通信光を傍受可能である。そのため、通信光を盗まれてもなお通信情報は漏洩しない安全性を実現する学術的な方法論とその実現技術が求められていた。特に最近ではストレスのないネット利用のために低遅延性や様々なプロトコルで動作するプロトコル無依存動作も通信全般に求められており、これらの要求も満たすことが望まれていた。

２．研究の目的

本研究では、高い安全性を担保し、低遅延性やプロトコル無依存動作を特徴とする光無線通信を実現するために、物理暗号を用いたセキュア光無線通信方式を新たに提案し、安全性、通信特性を実験検証することを目的とする。

３．研究の方法

一般的な暗号では、暗号鍵を用いて 2 値のディジタル信号で構成されるデータを、2 値のディジタル信号で構成される暗号信号に変換し、正規受信者は同じ暗号鍵を用いて、暗号信号から元のデータを復号する。暗号信号が 2 値ディジタル信号なので、盗聴者は暗号信号を正しく読み取ることができる。そのため、暗号信号解析により、データや鍵が漏洩する危険がある。安全性を高めるためには暗号化と復号のための複雑な演算処理が必要になり、遅延時間が増大する。一方、本研究では、雑音によるマスキング効果を利用して安全性を実現する物理暗号を利用する。雑音の中に暗号信号を埋めることにより、暗号信号が正しく読み取られることを妨げる。その結果、従来の暗号にはない高い安全性を達成できる。雑音の利用により暗号化・復号の演算は簡単なものでよくなるために、暗号化・復号化の過程で発生する遅延時間を小さく抑えることができる。この物理暗号を光無線通信に適用し、高い安全性と低遅延性を両立するセキュア光無線通信方式を検証する。研究の目的を達成するために、光ファイバと空間を相互変換する全光型アンテナ、安全性向上・低遅延性、セキュア光通信方式の三つの課題を設定し研究を実施した。全光型アンテナは電子回路を介在せずに光のまま変換することを特徴とし、広帯域性、低遅延性、プロトコル無依存性など優れた性能につながる。

４．研究成果

全光型アンテナは、応用形態として光ファイバ通信との接続性を重視し、光ファイバ通信で広く用いられる光ファイバ伝搬の損失が小さい波長 1.55 μm 帯の光で動作すること、また、通信距離は 50 メートル程度を目標とした。ビーム広がりから受光レンズの所要径を導き、通信距離延伸への可能性も残し、直径 50 mm とした。このレンズを組み込んだ全光型アンテナの入出力特性を評価した。二つの全光型アンテナを向かい合わせた構成の評価系で、一方から波長 1.55 μm の光を入力し、他方から出力される光を光パワーメータで測定した。過剰損失が残っているものの、光ファイバと空間を相互変換できること、および、同時に双方向から光を入力して動作することを検証した。

次に、通信特性の評価を実施し、ビット誤りなく暗号通信を行えることを実証した。実証実験では、擬似乱数で構成されるディジタル信号を通信データとして用意した。このデータを事前に送受信機で共有している 256 ビットの暗号鍵で暗号化した。はじめに送信端で、鍵長が 256 ビットの暗号鍵を線形フィードバックレジスタ(LFSR)を用いて拡張し、鍵長が 2^{256} のランニング鍵を

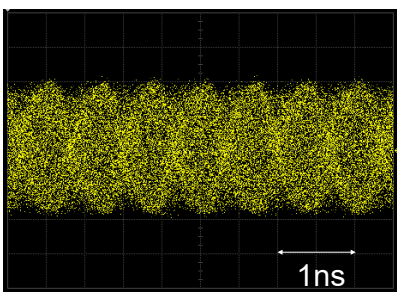

図１　4096 値の強度変調型暗号信号光の波形

生成した。この鍵長はおよそ 10^{77} で、鍵が繰り返し利用されることがないほど長い。このランニング鍵を 11 ビット毎にブロック化し、2 値データを暗号化する基底選択信号を生成した。基底信号と 2 値データを合わせて 12 ビットの電気信号で、強度変調器を介して波長 1550.12nm の連続光を 1.5 Gb/s で変調し、多値数が 4096 値の暗号信号（強度変調、変調速度 1.5 Gb/s）を発生させた。図 1 にそのサンプリング波形を示す。4096 値という超多値変調なので各強度レベルが雑音に埋もれていることが見て取れる。次に送信機に直結した受信端で、暗号信号を共有している暗号鍵を用いて元のデータに復号し、ビット誤り率(BER)を測定した。まず、送信端と同様に 256 ビットの共通鍵を LFSR で拡張し、基底選択信号を生成した。次に、光検出器で電気信号に変換した 4096 値の多値信号を、基底選択信号で 2 値識別し、元のデータである擬似乱数に復号した。これらの一連の処理はリアルタイムで実施した。復号したディジタル信号と送信したディジタル信号を比較し、BER を算出した。BER は 10^{-9} を下回っており、リアルタイム暗号通信でセキュア光無線通信実験に成功した。次に、この暗号信号の安全性評価を実施した。暗号信号が雑音に埋もれ暗号信号を正しく読み取ることができなくなることが本暗号の安全性の根拠となる。従って、暗号信号がどの程度、雑音に埋もれているかが安全性の指標になる。本研究では、雑音にマスクされている多値信号数を雑音マスキング量として評価した。光パワーが 2mW の時に、雑音マスキング量は 190 だった。雑音により暗号信号のレベルに 190 の不確定性を生じさせることができた。一般的なディジタル信号の暗号では、暗号信号は”0”か”1”なので、確率 0.5 で正しい暗号文を推定できるのに対して、本暗号では正しい暗号文を推定できる確率は 0.005 と桁違いに小さい。この確率は 1 ビットの暗号信号を正しく推定できる確率であり、本暗号の安全性が高いことが分かる。次に、鍵の推定確率についても評価した。4096 値の強度変調信号から 256 ビットの鍵を正しく推定できる鍵推定成功確率は 10^{-55} と算出でき、雑音が除去できないので、この成功確率が大きくなることはない。本暗号信号が高い安全性を実現していることを検証できた。

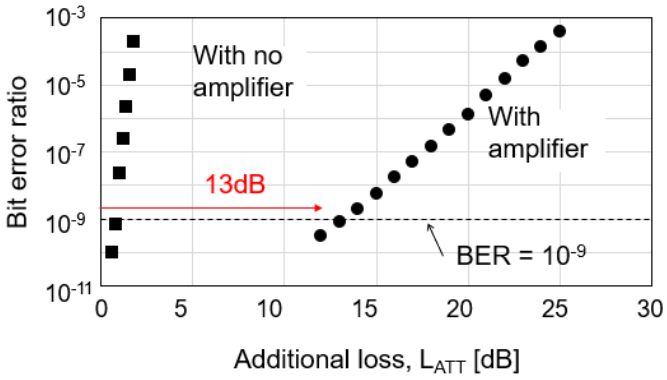

図 2　空間伝送による伝搬損失を模擬した付加損失量と BER の関係

これまでの実験評価では、送信機と受信機を直接接続した構成で実施した。次に、対向させた全光型アンテナを 30 メートル離れた場所に設置し、セキュア光無線通信を実施した。光増幅器を使用することなく、リアルタイム暗号通信で BER が 10^{-9} を下回るセキュア通信実験に成功した。通信距離は本暗号通信システムの伝送限界ではなく、実験可能な場所で見通せる距離が最大 30 メートルだった。そこで、通信可能な距離について実験検討を行った。通信距離を延伸するためには、送信端の光パワーを大きくする方法と受信端でプリアンプを利用する方法が考えられる。本物理暗号は、光パワーを大きくすると安全性が低下する傾向があることが分かっているため、受信端でプリアンプを用いる手法で検討した。実験構成は、受信機の前に可変光減衰器と光直接増幅器を直列に接続した。可変光減衰器は、空間伝送の損失を模擬するために設置した。光可変減衰器の減衰量を増加させ光増幅器に入力する光パワーを小さくし、光増幅器で光パワーを増幅後、受信機に暗号信号を入力し BER を測定した。受信機入力パワーは、可変光減衰器の減衰量に関わらず一定値に保持した。BER 測定結果を図 2 に示す。●で表しているのが光増幅器を使った場合の BER で、■は光増幅器を使用しない場合の BER を表している。BER=10^{-9} を達成する条件で、光増幅器の利用により 13 dB 程度の過剰損失が許容されることが分かった。この結果は、1 キロメートル程度の通信可能性を示唆している。以上により、高い安全性を実現するセキュア光無線通信を実証することができた。

最後に、残りの課題である低遅延性およびプロトコル無依存性の実験検証を実施した。低遅延性はシグナルクオリティアナライザのギガビット・イーサネット(GbE)のフレーム解析機能を利用して評価した。アナライザから出力される GbE フレームを送信機に入力し物理暗号信号光に変換し、直結した受信機で再び GbE フレームに復号しアナライザに入力した。信号伝搬経路は極めて短いので、GbE フレームが出力されてからアナライザに戻ってくるまでに要する時間を暗号化・復号により生じる遅延時間とした。一時間程度の測定で、平均時間は 4.8 マイクロ秒程度で、一般的なブロック暗号と比較して遅延時間が極めて小さかった。プロトコロル無依存性は、

異なるフォーマットのデータを暗号通信することにより検証した。検証実験では、全てのデータが擬似乱数で構成されるディジタル信号、代表的な通信規格である GbE 信号を用いて暗号化・復号の過程で発生する誤り率を測定した。受信機への入力パワーは十分大きな値に設定し、伝送により通信エラーが発生する可能性は排除した。測定結果は、どちらの信号も BER が 10^{-9} よりも小さく、ビット誤りが発生していないとみなせる結果だった。

以上で当初の目標は全て達成した。更に、当初の計画にはなかったが、データの暗号通信のみならず、暗号鍵の更新にも利用できることを実験検証に成功し、計画以上の成果を得られた。本研究ではデータ容量は 1.5 Gb/s、通信距離は 30 メートルだったが、単一の波長のみで 100Gb/s など高速化が可能である。更に長分割多重方式を利用すると、Tb/s を越えるデータ通信も実現できる。光増幅器の利用、光アンテナの改良などにより、通信距離の延伸も可能である。今後の課題としては、本研究では室内で実験を行ったために、空間の揺らぎによる通信特性の劣化は発生しなかったが、屋外環境では空間通信路の環境は時々刻々と変化する上、雨や霧など天候により伝送路損失が大きく変わるために、暗号信号の空間伝搬特性の研究が今後重要になると考えられる。

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Futami Fumio、Tanizawa Ken、Kato Kentaro	４．巻 38
２．論文標題 Y-00 Quantum-Noise Randomized Stream Cipher Using Intensity Modulation Signals for Physical Layer Security of Optical Communications	５．発行年 2020年
３．雑誌名 Journal of Lightwave Technology	６．最初と最後の頁 2774～2781
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JLT.2020.2985709	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 二見史生	４．巻 42
２．論文標題 量子技術を用いた暗号通信の最近の進展	５．発行年 2019年
３．雑誌名 O plus E	６．最初と最後の頁 57-63
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 －

〔学会発表〕　計9件（うち招待講演　2件／うち国際学会　3件）

１．発表者名 Fumio Futami, and Ken Tanizawa
２．発表標題 Key Update using Y-00 Quantum Noise Stream Cipher with 20-bit Intensity Levels in a 1,000-km Optical Fiber Link
３．学会等名 Conference on Lasers and Electro‐Optics (CLEO 2021)（国際学会）
４．発表年 2021年

１．発表者名 二見史生, 谷澤 健
２．発表標題 Y-00光通信量子暗号によるセキュア光データ通信
３．学会等名 電子情報通信学会 2021年ソサイエティ大会
４．発表年 2021年

１．発表者名
二見史生，谷澤 健

２．発表標題
Y-00光通信量子暗号をもちいた高セキュリティ光データ通信

３．学会等名
レーザー学会学術講演会第42回年次大会（招待講演）

４．発表年
2021年

１．発表者名
二見史生

２．発表標題
Y-00光通信量子暗号トランシーバとその応用　～暗号鍵の更新～

３．学会等名
第20回量子情報ミニワークショップ

４．発表年
2022年

１．発表者名
Fumio Futami, Ken Tanizawa, Abdelmoula Bekkali, and Hideo Fujita

２．発表標題
Secure Free-Space Optical Transmission of Y-00 Quantum Stream Cipher with 4096-Level Intensity Modulated Signals

３．学会等名
14th Pacific Rim Conference on Lasers and Electro-Optics（国際学会）

４．発表年
2020年

１．発表者名
二見史生，谷澤 健，ベッカリアブデルモウラ，藤田日出生

２．発表標題
強度変調型Y-00光通信量子暗号を用いたセキュア空間光通信

３．学会等名
電子情報通信学会 2020年ソサイエティ大会

４．発表年
2020年

１．発表者名
二見史生

２．発表標題
Y-00光通信量子暗号トランシーバとその応用　～光空間通信応用と鍵更新～

３．学会等名
第19回量子情報ミニワークショップ

４．発表年
2021年

１．発表者名
二見史生

２．発表標題
Y-00光通信量子暗号トランシーバとその応用 ～1,000㎞伝送と光空間通信～

３．学会等名
第18回 量子情報ミニワークショップ

４．発表年
2020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

〔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	谷澤　健 (TANIZAWA Ken) (10709489)	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