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　 ５ 日現在

機関番号：３２６３９
研究種目：基盤研究(B)（一般）
研究期間：2021～2023
課題番号：２１Ｈ０１３２９

研究課題名（和文）量子雑音マスキングを用いた光・無線統合物理レイヤ暗号化通信

研究課題名（英文）Quantum-noise randomized secure optical fiber and microwave wireless communications

研究代表者
谷澤　健（TANIZAWA, Ken）

玉川大学・量子情報科学研究所・教授

研究者番号：１０７０９４８９

交付決定額（研究期間全体）：（直接経費）　　11,400,000円

研究成果の概要（和文）：超スマート社会を支えるために，通信システムのセキュリティ向上は重要課題の一つである．光の量子雑音の存在により信号の盗聴を直接的に防ぐ物理レイヤ暗号化を，光有線と電波無線伝送を統合した通信システムにて実現する研究を実施した．アナログ光強度変調による短距離の光ファイバ伝送後に，直接検波により電波帯にて暗号化信号を発生し，これをミリ波帯に変換して無線通信する実験を行った．暗号化により光と電波の双方の信号に対して定量的に安全性を保証したうえで，ギガビット毎秒以上の高速通信が実現できることを実証した．送信機構成の簡略化にも成功するなど，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と電波でシームレスに高い安全性を実現できる物理レイヤ暗号化は，情報通信の盗聴に対するセキュリティを飛躍的に高めるものであり，我々の生活を基盤として支えるインターネットの安全性の向上に将来的に貢献することが期待される．将来の高速通信に応用可能であるため，実用的な価値が高い．本研究を通じて，量子雑音による暗号化の電波帯における安全性を評価する基盤を構築することができた．これはこの暗号技術の工学的な体系化に貢献するものである．

研究成果の概要（英文）：Improving security is an important challenge in communication systems that will support future smart society. We have studied physical layer encryption that utilizes quantum uncertainty of light to directly prevent signal interception in communication systems where optical fiber and radio wireless transmissions are converged. After short-reach fiber transmission using analog optical intensity modulation, the encrypted signal was generated at radio frequencies via direct detection. This encrypted signal is upconverted to a millimeter wave band for wireless communication. High-speed communications at gigabits per second or faster was achieved while quantitatively guaranteeing security of both optical and radio signals seamlessly. We also succeeded in simplifying the transmitter configuration, which is an achievement beyond the scope of the original research.

研究分野：光通信

キーワード：物理レイヤ暗号化　無線通信　ミリ波　光ファイバ通信

※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

IoT 技術によって実現される超スマート社会(Society5.0)では，個人情報等の多くの重要なデータが，端末・クラウド間や分散クラウド内で通信される．盗聴などで通信情報が第三者に漏洩すると時に莫大な被害を及ぼすため，通信システムのセキュリティの向上は重要課題である．図1(a)に無線通信を例に現状の通信システムの盗聴に対するセキュリティを示す．盗聴者は，受信機を正しい周波数に設定すれば，物理層でやりとりしている信号を受信しデジタルデータを正しく復調できる．現在のセキュリティポリシーは，「物理層からはデジタルデータを取得できるが，上位層で AES （米国標準技術研究所が制定した共通鍵暗号）等の暗号化が施されているため，データを解析しても情報を復元できない」というものである．この状況は，物理層からの盗聴の可能性を残しており改善の余地がある．我々は，物理層からの盗聴を直接的に防ぐことができる物理レイヤ暗号化に着目している．図 1(b)に示すように，何らかの手段で「物理層でやりとりされる信号を盗聴者が正しく受信できない」状況を作り出す．盗聴者はデジタルデータをそもそも正しく取得できないため，既存の上位層に実装される暗号技術と併用することで，極めてセキュアな通信システムを実現できる．

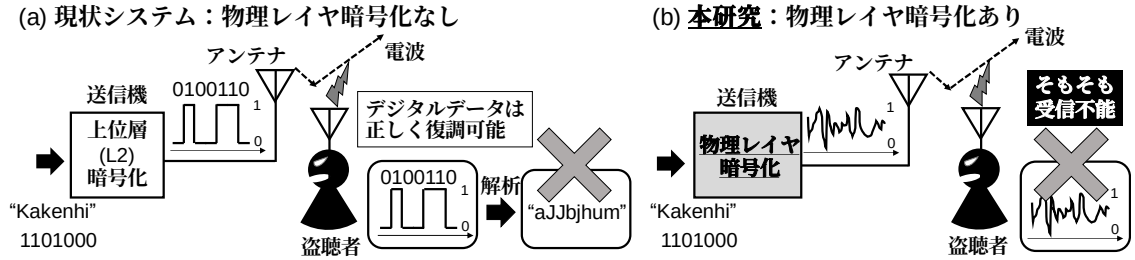

図 1. 無線通信システムにおける盗聴に対するセキュリティ

我々は，短い共有鍵を用いて送信データを多値光信号に変換することで，受信時に不可避な量子（ショット）雑音により隣接信号が覆われる効果（以下，マスキング効果）により秘匿を実現する光ファイバ通信のための物理レイヤ暗号化(G. A. Barbosa, et al., Phys. Rev. Lett., 2003)に着目して研究を進めてきた．図 2 に暗号化のための信号マスキングの原理を示す．(a)は光位相の 0 とπに 0 と 1 を割り当てる一般的な 2 値変調である．暗号化のために，共有鍵から生成した乱数を送信データに加えて多値光変調する．(b)は 8 値光位相に変調した例である．黒丸の直径が量子雑音による不確定性を表す．8 値の位相変調は雑音の重なりがなく正しく判別できる．適切な暗号化では，(c)に示すように位相変調の多値数 M を大きな数(>1,000)にする．このとき拡大図に示すように量子雑音により隣接信号が覆われるため，共有鍵なしで誤りのない信号判別が困難になる．量子雑音は不可避かつ真にランダムであるため，盗聴者がどれだけ完璧な受信や解析をしても除去できない．安全性を定量的に保証できるというユニークな特徴をもつ．申請者は，極めて大きな M を実現する光位相変調技術を提案し，光ファイバ通信においてこの物理レイヤ暗号化の安全性を向上する研究を行ってきた．

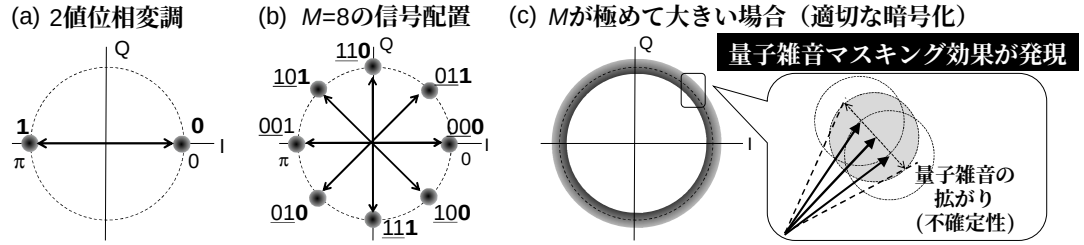

図 2. 物理レイヤ暗号化のための量子雑音による隣接信号のマスキング

物理レイヤ暗号化は，光ファイバ有線通信に比べて，電波が空間にブロードキャストされる無線通信においてより必要性が高い．しかし，近赤外の光波より周波数が 4~5 桁程度低い電波帯で同様の多値変調を行っても，量子雑音による十分なマスキング効果を得ることは難しい．マスキング効果が信号のキャリア周波数の平方根に反比例するためである．よって，この物理レイヤ暗号化を無線通信へ応用することは，不可能と考えられてきた．最近，我々は，図 3 に示すように，量子雑音のマスキング効果による信号の秘匿を光波から電波までシームレスに実現する画期的な手法を考案した．光で発生した多値信号（光波物理暗号）を局発光と光ヘテロダイン検波することで，光の量子雑音のマスキング効果を保ったまま信号を電波帯の周波数に変換する．この提案手法は，電波帯の無線通信の物理レイヤの暗号化に有効であり，将来の無線通信システムのセキュリティを質的に向上することが期待できる．

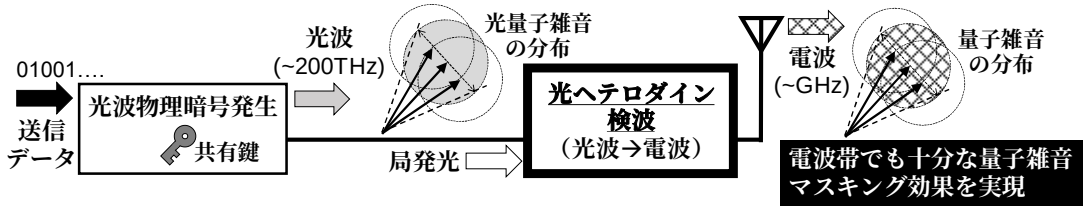

図 3: 光ヘテロダインを用いた量子雑音マスキング効果の電波帯への展開

２．研究の目的

本研究では，超スマート社会(Society5.0)を支える大容量アクセスネットワークへの応用を念頭に，量子雑音マスキング効果を用いた物理レイヤ暗号化を光波から電波帯に展開し，物理層のセキュリティが格段に向上した光・無線統合通信システムを実現することを目的とする．我々が提案した光ヘテロダインを用いた暗号化手法を発展し，直交周波数分割多重(OFDM)が用いられる本格的な無線通信への応用を探求する．その際，安全性や通信性能を実験・理論の両面から明らかにする．さらに，光波と電波の双方でマスキング効果をシームレスに実現できるという特徴を，将来の通信システムでどのように活用できるかを探求する．

具体的な目標として以下を定める．

(1) 量子雑音マスキングによる物理レイヤ暗号化の OFDM への適用検討
(2) 物理レイヤ暗号化 OFDM 信号を光波で発生し，光ファイバ伝送を実証
(3) 光受信により無線周波数帯へと変換し，物理レイヤ暗号化無線通信を実証

３．研究の方法

(1)〜(4)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) 量子雑音マスキングによる物理レイヤ暗号化の OFDM への適用検討

OFDM への適用は，既存の変復調技術の延長にある．送信したいデータと共有鍵から暗号化プロトコルに従って多値変調信号を発生した後，逆フーリエ変換およびガードインターバルの挿入を行う．本研究では，暗号化のため多値変調した OFDM 信号を 1.5μm 帯の光で発生したときの量子雑音によるマスキングの効果を明らかにする．光ヘテロダイン検波の半古典/量子理論を応用することで OFDM 信号におけるマスキングを定量的に表す式を導く．この式に基づいて数値解析を行い，実験に向けて適切なマスキング効果が得られる条件（変調方式，変調多値数，信号帯域，光パワー範囲等）を検討する．最終的にはミリ波による高速通信を目的とするため，信号帯域は数 GHz 程度を目指す．

(2) 物理レイヤ暗号化 OFDM 信号の光発生と光ファイバ伝送の実証

図 4 に示すように，(1)にて明らかにした条件で暗号化のため多値変調した OFDM 信号の光発生と光ファイバ伝送を実証する．まず OFDM 信号を生成し，電気中間周波数(IF)にアップコンバージョンする．その後，電気・光変換して光強度変調信号とする．電気 IF を経由することで，局発光が不要なシンプルで実用的な構成で電波帯への変換が実現できる．この光信号を，アクセス系を想定して短距離（50km 以下）の光ファイバを伝送した後に，光・電気変換する．結果，量子雑音マスキング効果が電気 IF の周波数にて発現する．この方式はアナログ伝送であるため，光ファイバ伝送に伴う各種の歪の影響を実験により検証し，電気 IF での暗号化 OFDM 信号が適切な信号品質を保てる条件（伝送距離，信号帯域，光領域での補償の有無）を明らかにする．

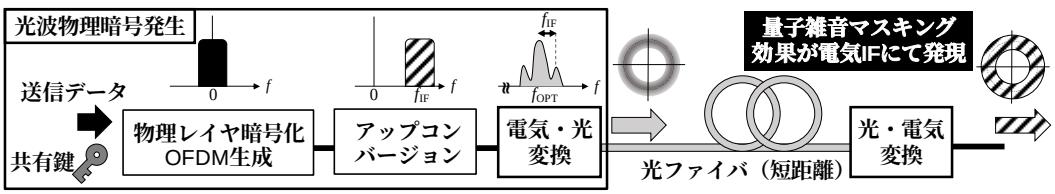

図 4. 物理レイヤ暗号化 OFDM 信号の光発生と光ファイバ伝送実験の構成

(3) 物理レイヤ暗号化 OFDM 信号のミリ波帯へのアップコンバージョンと無線通信の実証

図 5 に示すように，(2)にて発生した電気 IF の暗号化 OFDM 信号を，ミキサを用いてミリ波帯へとアップコンバージョンし，無線通信する実験を行う．ミリ波の周波数として，ライセンスフリーである 60GHz 帯を採用して，実際にアンテナを用いた送受信を行う．復号後の信号品質と安全性を評価し，物理レイヤ暗号化通信がミリ波帯で有効であることを実証する．アンテナ間距離は，実験環境（室内を予定）の制限で数 m 程度に限られると想定される．より現実的な見積もりとしてリンクバジェットを計算し，期待される通信性能を明らかにする．

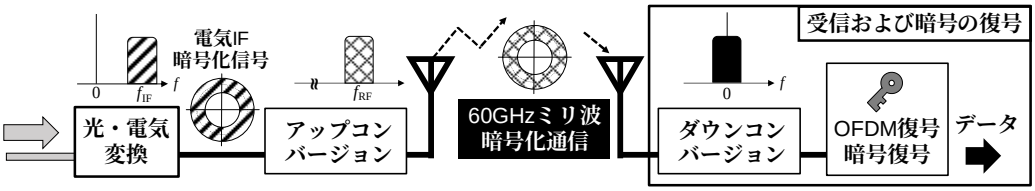

図 5. 物理レイヤ暗号化 OFDM 信号のミリ波無線伝送実験の構成

４．研究成果

(1) 量子雑音マスキングによる物理レイヤ暗号化の OFDM への適用検討

量子雑音マスキング効果を用いた物理レイヤ暗号化では，暗号化後に量子雑音により覆われる信号の数を量子雑音マスク数として安全性の一次指標として用いている．量子雑音マスク数の逆数程度の不確定性が盗聴者に課されることとなる．これまでに，申請者は光ヘテロダイン検波の半古典/量子理論を用いて単一キャリア変調の場合における量子雑音マスク数の導出を行ってきた．これをマルチキャリア変調である OFDM へと拡張し，マスク数を求める式を導出した．OFDM のサブキャリアの変調方式は PSK および QAM とした．また，電気 IF における暗号化 OFDM 信号を光強度変調で送受する構成を採用した．量子雑音マスク数は単一キャリアの場合と同様に暗号化後の信号の次数に比例し，光パワーに反比例（PSK の場合は光パワーの平方根に反比例）することが明らかになった．一方，光強度変調で IF を送受する今回の構成では変調の深さを表す変調度が新たな自由度（設計パラメータ）として加わる．導出した式を用いて PSK と QAM 暗号化の場合で数値計算を行った．図 6 に変調度を変化させたときの量子雑音マスク数の計算結果を示す．PSK の場合は，データ変調は QPSK として信号帯域は 2.5GHz とした．QAM の場合は，16QAM データ変調として信号帯域は 1.25GHz とした．暗号化後の変調次数と変調度を適切に選択することで信号秘匿に十分な数 10~100 程度の量子雑音マスク数を得ることができる．本検討により得られたマスク数を求める式を用いることで，通信システムの要求に応じて適切な暗号化信号の設計をすることが可能となった．

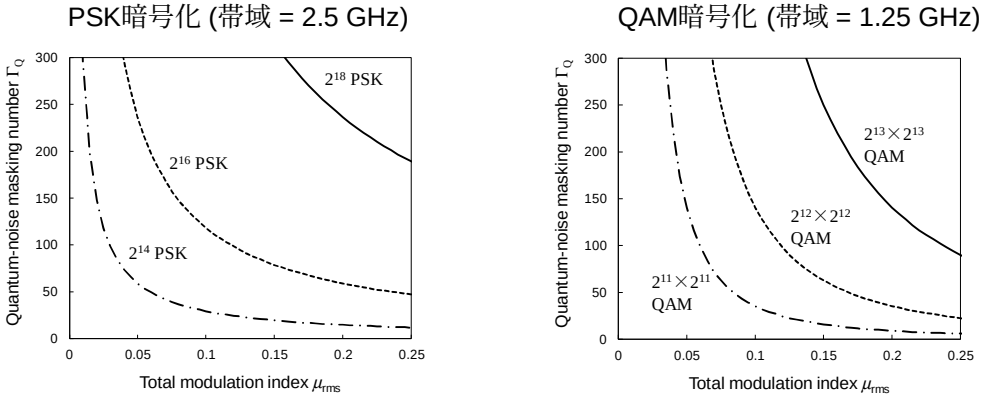

図 6. PSK および QAM 方式の暗号化における量子雑音マスク数と変調度の関係

(2) 物理レイヤ暗号化 OFDM 信号の光発生と光ファイバ伝送の実証

上記検討で明らかにした変調次数と変調度等の諸条件で，暗号化のため多値変調した OFDM 信号の光発生と受信による暗号化 IF 信号発生の実験を行った．電気・光変換にレーザと光強度変調器を用いたときの実験結果を図 7 に示す．PSK 暗号化（データ変調 QPSK，帯域 2.4GHz）と QAM 暗号化（データ変調 16QAM，帯域 1.25GHz）の場合における電気スペクトルとコンス

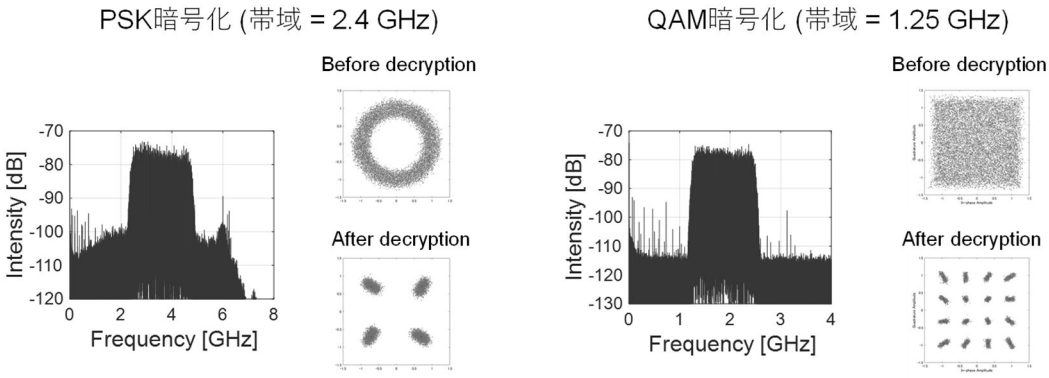

図７．レーザと光強度変調器を用いた PSK および QAM 方式の IF 信号暗号化実験結果

タレーションを示した．PSK 暗号化においては，3.6GHz の電気 IF に 2^{16} PSK を発生した．変調度は 0.08 として，100 を超える秘匿に十分な量子雑音マスク数を実現した．鍵を用いて復号化することで QPSK データ変調が適切に復元できた． QAM 暗号化においては，1.875GHz の電気 IF に $2^{12}\times2^{12}$ QAM を発生した．変調度 0.10 のとき量子雑音マスク数は 138 となった．復号化により 16QAM データ変調が適切に復元できることを確認した．このように，約 5Gbit/s のラインレートにおいて提案方式で適切な暗号化と復号が実現できることを実験で実証した．

次に，より簡素な送信機構成を目指して，直接変調半導体レーザを用いて IF 帯の信号を QAM 暗号化（データ変調 16QAM，帯域 1.25GHz）する実験を行った．図 8 に実験結果である電気スペクトルとコンスタレーションを示す．1.875GHz の電気 IF に $2^{12}\times2^{12}$ QAM を発生した．変調度 0.12 のとき量子雑音マスク数は 50 を超えており，盗聴者が到達可能なシンボルエラーレートは，>0.99 となり高い安全性を実現できる．また，復号化により 16QAM データ変調が適切に復元できることを確認した．受信側の補償アルゴリズムを工夫することで，光強度変調器と比較して変調線形性が劣る直接変調半導体レーザを使用したにも関わらず，EVM = 3%程度の極めて良好な信号受信ができた．

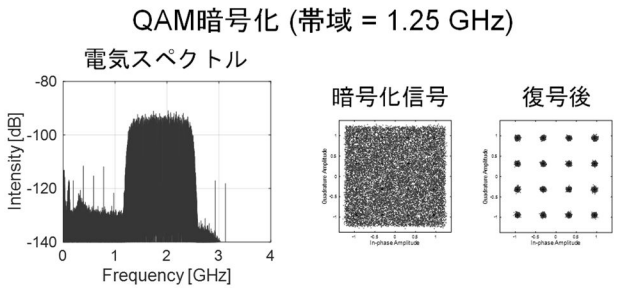

図 8. 直接変調半導体レーザを用いた QAM 方式の IF 信号暗号化実験結果

(3) 物理レイヤ暗号化 OFDM 信号のミリ波帯へのアップコンバージョンと無線通信の実証

上記の直接変調半導体レーザを用いた IF 信号の暗号化に続いて，ミキサを用いてライセンスフリーのミリ波帯 60GHz へとアップコンバージョンし，無線通信する実験を行った．アンテナを用いて実験室環境にて 3m 送受信を行った．図 9 にミリ波を受信しダウンコンバージョンした後の電気スペクトルとコンスタレーションを示す．復号後の信号品質は誤り訂正符号閾値を上回っており，適切な暗号化ミリ波無線通信が実現できた．なお、この実験における伝送距離はミリ波へのアップコンバージョン後の送信パワーが約−20dBm と低いことにより制限されており，送信機側にミリ波帯の高周波増幅器を導入することで改善が見込まれる．20dB 程度のゲインの増幅器を用いることで，ミリ波通信の損失バジェットとして約 50dB が確保できることが明らかとなった．

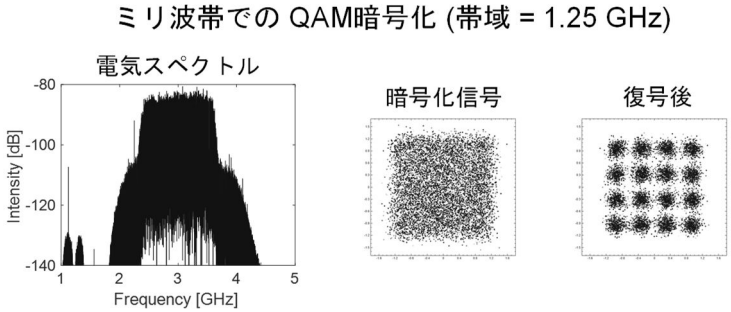

図 9. QAM 方式の 60GH 帯ミリ波信号の暗号化実験結果

以上に示したように，本研究では量子雑音マスキングによる無線信号の物理レイヤ暗号化における安全性と通信性能を理論と実験の両面から検討した．安全性と信号品質のトレードオフを考慮してシステムを設計するための理論を確立したのに加えて，これらを両立できることをミリ波帯の通信実験により実証した．光波と電波の双方で量子雑音マスキング効果をシームレスに実現できるという特徴は，アクセス系システムにおいて局舎とアンテナサイト間を光ファイバで接続する所謂 Radio-over-fiber システムとの相性が良い．6G に代表される次世代の通信システムにおいてセキュリティの向上は重要な課題であり，本技術の貢献が期待される．本研究での実証はオフラインであり，実用化に向けてリアルタイムでの動作実証が今後の課題である．また，光電融合実装技術を用いた送受信機の小型化も社会実装に向けて重要な研究展開と考えられる．

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　2件）

１．著者名 Ken Tanizawa, and Fumio Futami	４．巻 42
２．論文標題 Photonic-Assisted Secure Millimeter Wave Communication with Quantum Noise Randomized Stream Cipher	５．発行年 2024年
３．雑誌名 IEEE/Optica Journal of Lightwave Technology	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） 10.1109/JLT.2024.3387431	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 35
２．論文標題 Tradeoff between Reach and Security in Nyquist WDM Transmission of PSK Y-00 Quantum Stream Cipher	５．発行年 2023年
３．雑誌名 IEEE Photonics Technology Letters	６．最初と最後の頁 1147-1150
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/LPT.2023.3306357	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 12429
２．論文標題 Photonic-Assisted Microwave Quantum-Noise Randomized Cipher Generation for Signal Security of Wireless Communications	５．発行年 2023年
３．雑誌名 Proceedings SPIE, Next-Generation Optical Communication: Components, Sub-Systems, and Systems XII	６．最初と最後の頁 124291G
掲載論文のDOI（デジタルオブジェクト識別子） 10.1117/12.2648630	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 40
２．論文標題 IF-over-Fiber Transmission of OFDM Quantum-Noise Randomized PSK Cipher for Physical Layer Encryption of Wireless Signals	５．発行年 2022年
３．雑誌名 IEEE/OSA Journal of Lightwave Technology	６．最初と最後の頁 1698-1704
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JLT.2021.3119603	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 －

〔学会発表〕　計9件（うち招待講演　2件／うち国際学会　6件）

１．発表者名
Ken Tanizawa

２．発表標題
Secure optical communications and random number generation utilizing quantum property of coherent light

３．学会等名
Optics & Photonics Japan 2023（招待講演）（国際学会）

４．発表年
2023年

１．発表者名
谷澤 健

２．発表標題
直接変調レーザを用いた光IF伝送による電波帯OFDM量子雑音マスキング暗号の発生

３．学会等名
電子情報通信学会 2023年ソサイエティ大会

４．発表年
2023年

１．発表者名
石島 樹

２．発表標題
光位相共役と乱数による信号ランダマイゼーションを用いた高RFリンクゲイン・高セキュリティなアナログRoF伝送システム

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
2023年

１．発表者名
Tatsuki Ishijima, Shuhei Otsuka, Shun Harada, Takahide Sakamoto, Ken Tanizawa, and Fumio Futami

２．発表標題
Nonlinear Tolerant Conjugated RoF System Secured by Physical Layer Encryption with Deliberate Signal Randomization

３．学会等名
Optical Fiber Communication Conference and Exhibition (OFC 2023)（国際学会）

４．発表年
2023年

１．発表者名
Ken Tanizawa, and Fumio Futami

２．発表標題
Photonic-Assisted Microwave Quantum-Noise Randomized Cipher Generation for Signal Security of Wireless Communications

３．学会等名
SPIE Photonics West（招待講演）（国際学会）

４．発表年
2023年

１．発表者名
Ken Tanizawa, and Fumio Futami

２．発表標題
Microwave OFDM Quantum-Noise Randomized QAM Cipher Generation via Analog IFoF Transmission with a DML

３．学会等名
48th European Conference on Optical Communications (ECOC 2022)（国際学会）

４．発表年
2022年

１．発表者名
Ken Tanizawa, and Fumio Futami

２．発表標題
Analog IM/DD IFoF Transmission of OFDM Quantum-Noise Randomized QAM Cipher for Wireless Signal Encryption

３．学会等名
27th Opto-Electronics and Communications Conference (OECC 2022)（国際学会）

４．発表年
2022年

１．発表者名
谷澤 健，二見史生

２．発表標題
アナログ光強度変調・直接検波による電波帯でのOFDM量子雑音マスキングPSK暗号の発生

３．学会等名
電子情報通信学会 2022年総合大会

４．発表年
2022年

１．発表者名 Ken Tanizawa, and Fumio Futami
２．発表標題 Photonic-Assisted Microwave OFDM Quantum-Noise Randomized Cipher Generation via IM/DD IFoF Transmission
３．学会等名 Optical Fiber Communication Conference and Exhibition (OFC 2021)（国際学会）
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

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