量子雑音マスキングを用いた物理暗号によるセキュア無線通信システム

代表研究者　　谷澤　健　　玉川大学　量子情報科学研究所　准教授

1 研究の背景と目的

情報通信におけるセキュリティの担保は，IoT に代表される超情報化社会において喫緊の課題である．無線通信では電波帯の信号がブロードキャストされるため，信号の傍受が平易である．よって，信号の盗聴に対するセキュリティ対策が重要になる．図 1(a)に無線通信における現状の盗聴に対するセキュリティ対策を示す．現用の通信システムでは，L2 以上のレイヤに Advanced Encryption Standard(AES)に代表される計算量的に安全性を確保する現代暗号技術を導入する．AES ではあらかじめ共有された秘密鍵を使って送信するデジタルデータを変換する．盗聴者は傍受した信号を正しく復調し，暗号化されたデジタルデータを得ることは可能であるが，このデータをコンピュータで解析しても秘密鍵（AES の場合は 128 や 256 ビット程度の鍵長が通常用いられる）をもたない限り元（暗号化前）のデータを得ることが困難である．一方，本研究では，図 1(b)に示すように，傍受した信号を正しく復調すること自体を防ぐような物理レイヤ暗号技術を将来の無線通信システムに導入することを目的とする．現代暗号と併用することで，盗聴に対して極めて高い安全性を実現できる．

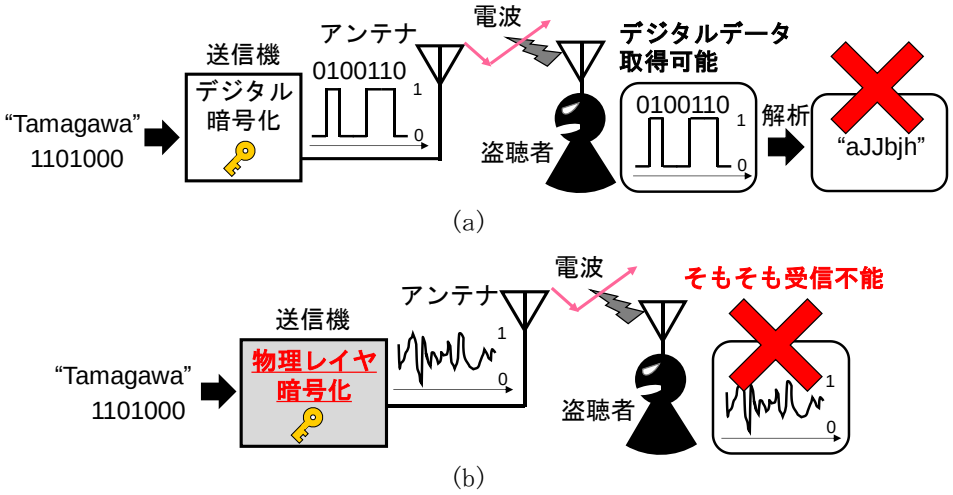

図 1：無線通信における盗聴に対するセキュリティ：(a)現代暗号によるレイヤ 2 暗号化システム，(b)物理レイヤ暗号化システム（本研究）

本研究では，秘密鍵を使って信号を変調することで，量子雑音（ショット雑音）の存在により安全性を担保する物理レイヤ暗号化に着目する．光通信への応用を念頭に 2000 年初頭に提案された暗号化であり[1]，アルファ・エータ(αη)[2]，Y-00 光通信量子暗号[3]等と呼ばれている．この物理レイヤ暗号化では，あらかじめ共有した短い秘密鍵を用いて送りたいデータ（平文）を直接暗号化する．具体的な暗号化の方法としては，鍵の情報に基いて電磁波の位相と振幅，もしくはその一方をシンボル毎に「極めて」多値に変調（ランダム化）する．鍵を共有する正規の受信者はこの多値変調信号をデータ変調に戻して平文を正しく受信・復調できる．一方で，鍵を持たない非正規の受信者（盗聴者）は，多値変調信号を受信する必要があるため，量子雑音の影響が顕著となりエラーのない正しい受信・復調ができない．この信号秘匿の効果を量子雑音マスキングと呼ぶ（詳細は次章で示す）．量子雑音は真にランダムかつ不変・不可避であるため，この物理レイヤ暗号化は安全性を定量的に担保できるという優れた特徴をもつ．これまでに光ファイバ通信への応用に向けた検討が精力的に行われてきた．光の位相を多値化してランダム化する位相変調(PSK)方式[2]，[4],[5]光の強度（振幅）をランダム化する強度変調(IM)方式[6]-[8]，その両方を用いる直交振幅変調(QAM)方式[9]-[11]にて，暗号化を実現することができる．近年は，チャネル当たり 160Gbit/s の高速伝送[11]や，10,000km を超える太平洋横断級の伝送距離[12]が実証されている．また，波長多重化を実現できるため，既

公益財団法人電気通信普及財団
研究調査助成報告書　第36号　2021年度

存の光ファイバ通信システムと非常に相性が良い[8].

本研究では，この量子雑音マスキングによる物理レイヤ暗号化を電波帯の無線通信に応用することを目指す．しかしながら，量子雑音によるマスキングの効果は電磁波の周波数の平方根に比例するため，単純に数100THz の周波数の光から 100GHz 以下の電波帯にこの暗号化手法を拡張して同等の安全性を実現することはできない．図 2 に約 200THz の光と 30GHz の電波における量子雑音による信号の不確定性の比較を示す．灰色の円が量子雑音の拡がり，つまり不確定性を表している．電波帯では極めて小さく，光と同程度の秘匿効果を得ることが困難である．そこで，研究代表者は，光の周波数で発生した暗号化信号を光ヘテロダインにより所望の電波帯に周波数変換することで，光の周波数での秘匿性を維持したまま電波帯で適切な物理レイヤ暗号化を実現する手法を提案した．

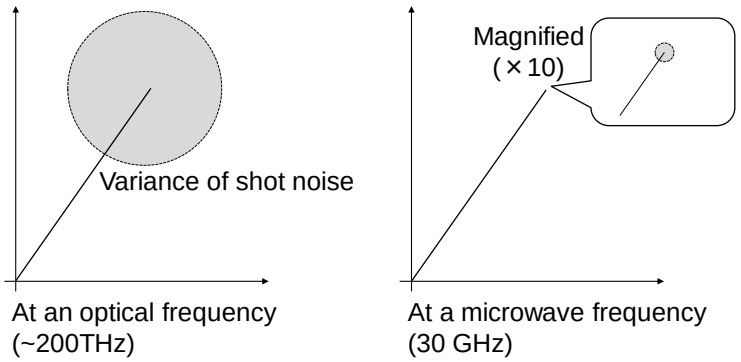

図 2：光と電波の周波数における量子雑音による不確定性の比較

本研究では，この光ヘテロダインを用いて電波帯の信号を量子雑音マスキングにより秘匿化する提案を原理実証し，ミリ波帯で物理レイヤ暗号化無線通信実験を行うことを目標とする．具体的には，以下の 3 つの課題に取り組んだ．

[1] ミリ波帯での物理レイヤ暗号化信号の発生
提案する光ヘテロダインによる暗号化を実現する送信系を構築し，ミリ波帯にて適切に暗号化信号が発生できることを実証する．また，暗号の復号を伴う受信系を構築し，物理レイヤ暗号化システムとして正しく動作することを確認する．
[2] 物理レイヤ暗号化信号のミリ波無線伝送
発生したミリ波帯の物理レイヤ暗号化信号を，アンテナを用いて無線伝送できることを実験により示す．このときの物理レイヤ暗号化通信システムとしての性能，つまり伝送品質と安全性を評価する．
[3] 安全性と伝送特性の理論検討
この物理レイヤ暗号化の安全性の評価指標の一つは量子雑音によるマスキング効果の量である．光ヘテロダインによりミリ波帯へと周波数変換されたとき,マスキングの量がどうなるのかを量子/半古典理論を用いて検討する．そして，マスキング量と信号品質の関係を明らかにする．

2 量子雑音マスキングによる電波帯信号の物理レイヤ暗号化

2-1 量子雑音マスキングによる信号秘匿化の原理

ここでは，秘密鍵を用いて位相を変調する PSK 方式の物理レイヤ暗号化方式にて，量子雑音マスキングによる信号秘匿の原理を示す．暗号化のために，通常の M-ary PSK データ変調の位相を秘密鍵に従ってシンボル毎にランダムに回転する．以下，簡単のために M=4 である QPSK 変調をデータ変調として採用した場合の動作原理を示す．図 3(a)に暗号化のために QPSK のシンボル点を IQ 平面上でθ_{basis}回転させる様子を示す．回転角度θ_{basis}は $-\pi/4$~$\pi/4$の間で，シンボル毎にあらかじめ共有した秘密鍵から生成される疑似ランダムビット列の情報によって決める．次節にて詳細な信号処理を示す．回転角度の分解能が$\pi/2^{(m+1)}$（m ビット）のとき，QPSK データ変調が暗号化されたコンスタレーションは $M \cdot 2^m$ PSK 信号となる．m を十分に大きくした場合，コンスタレーションは図 3(b)に示すようにドーナツ状になる．このとき，拡大図に示すように，量子雑音の

広がり角度$\Delta\phi_{shot}$が隣接するシンボル間角度$\Delta\theta_{basis}$より大きくなり，受信時に避けられない量子雑音により観測した信号に不確定性が生じる．つまり，秘密鍵をもたない盗聴者は，暗号化された M・2^m PSK 信号を正しく受信・復調することが困難である．一方，秘密鍵をもつ正規の受信者は，暗号化で行った位相回転の逆回転をシンボル毎に施すことで，QPSK データ変調信号として量子雑音の影響を大きく受けない受信が可能となる．これを量子雑音によるマスキング効果と呼んでおり，信号の秘匿化（秘密鍵をもつ受信者の有利性）を実現できる．量子雑音によるマスキングは，真にランダムかつ除去できない（理論的に保証）という点において信号秘匿に理想的である．

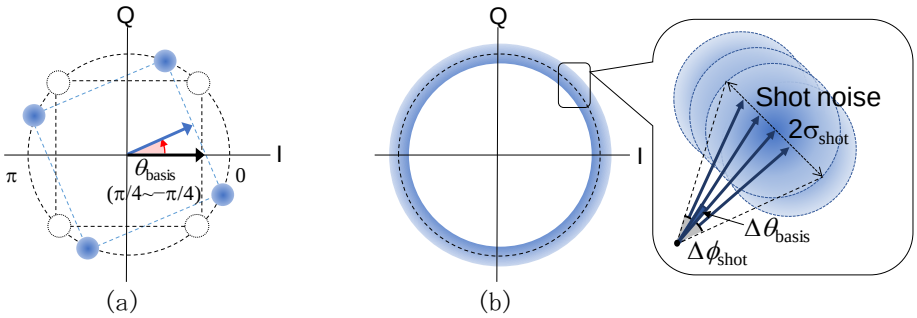

図 3：PSK 方式の物理レイヤ暗号化における量子雑音マスキング

2- 2 暗号化と復号化

前節に示したように，暗号化は低次のデータ変調信号を秘密鍵に基づいて多値信号に変換する部分と，量子雑音による真にランダムな不確定性が付与されるマスキング部分からなる．マスキングは，高い周波数をもつ光波の場合，信号受信時にごく自然かつ不可避に実施される．安全性を高めるためには，位相回転のビット分解能 m を大きくして量子雑音による十分なマスキングを実現することに加えて，前者の多値信号への変換を適切に行うことも大切である．図 4 に暗号化のための多値信号への変換処理を示す．秘密鍵は通常 256 ビット程度である．疑似乱数発生器を用いてこの鍵を伸長する．伸長された鍵（以下，ストリーム鍵）は，m ビット毎に区切られ，マッパーを通じてシンボル毎の位相の回転角度θ_{basis}へと変換される．一方，データビットは，まずストリーム鍵と排他的論理和（XOR）をとることでランダマイズされる（Overlap Selection Keying）．次に，シンボルごとにストリーム鍵の下位 2 ビット情報に従ってランダマイズされたマッピングが行われ，データ変調の位相角度θ_{data}が決まる．信号変調では，基準位相からθ_{basis}+θ_{data}の位置に信号がマッピ

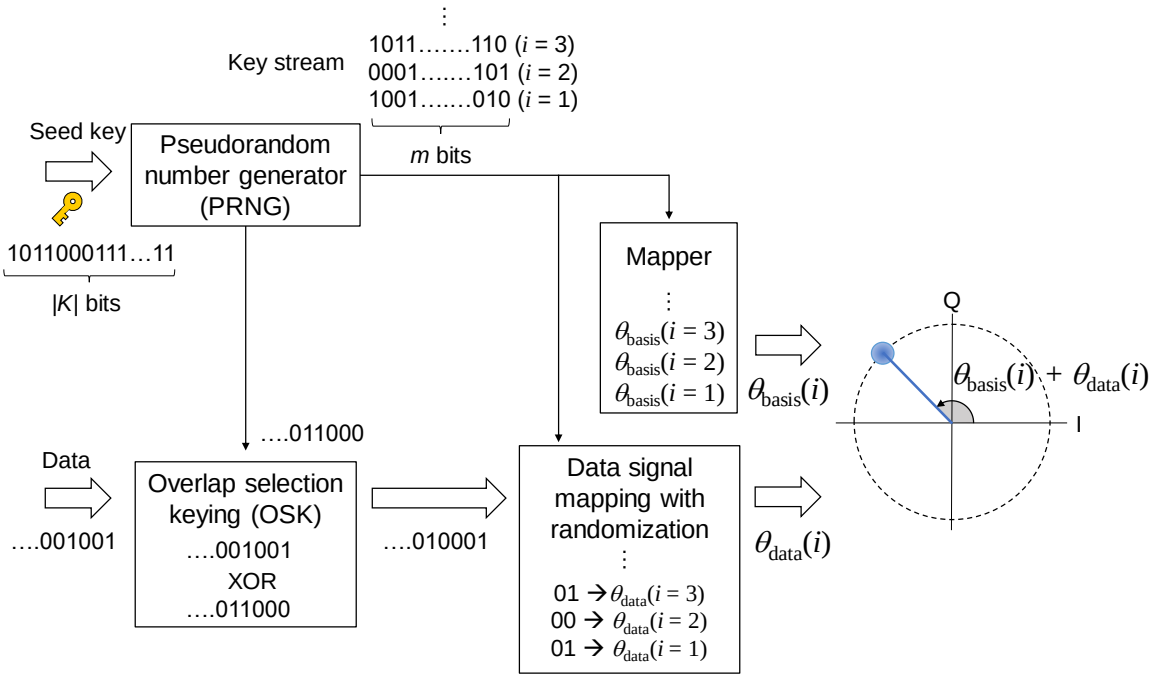

図 4：暗号化のための多値信号への変換処理

ングされる．θ_{basis} はシンボル毎に異なることから十分に長い時間観測するとドーナツ形状のコンスタレーションになる．

量子雑音によるマスキング効果は，m が大きいほど大きくなる．よって，信号変調に用いるデジタル・アナログ変換（DA 変換）の分解能のビット数は大きいほど良い．しかしながら，DA 変換のビット数とアナログ変調帯域にはトレードオフの関係があり，10Gbaud の変調に用いられる DA 変換のビット数は 10 ビット程度である．そこで，より大きなマスキング効果を得るために，複数の DA 変換器と変調器を組み合わせて，m=16 程度の信号変調を実現している[12]-[14]．

正規の受信者は秘密鍵を共有しているのに加えて，送信側と同じ疑似乱数発生器およびマッパーを持っている．よって，シンボル毎の位相回転角度 θ_{basis} を知ることができる．暗号の復号化は，シンボル毎に受信した多値信号の位相から θ_{basis} を減ずることで実現できる．この後，キャリア位相の回復等の適切なデジタル信号処理[15]-[17]を施すことで低次のデータ変調，例えば QPSK を復元できる．ビットに復調後に，再度ストリーム鍵との排他的論理和をとることで，元のデータビットを得ることができる．なお，位相の減算（逆回転）は本研究ではデジタル信号処理の一環として行ったが[18]，変調器などを用いてアナログ的に行うことも可能である．

2-3 光ヘテロダインを用いた電波帯への展開

量子雑音のマスキング効果を定量的に評価するために，量子雑音の拡がりに含まれる多値信号数である量子雑音マスク数とよばれる指標を導入する．量子雑音マスク数は大きいほど盗聴者に課される不確定性が大きいことを表しており，安全性が高まる．量子雑音の拡がりは信号周波数の平方根に比例するため，図 2 にそのイメージを示した通り，電波帯では光と比べて著しく小さくなる．具体的には，比較的周波数の高いミリ波帯でも量子雑音マスキング数は，光波帯の 1/100 程度であり，十分な秘匿を実現できない．そこで，研究代表者は，図 5 に示すように，光ヘテロダインによる周波数の変換を用いて量子雑音のマスキングによる秘匿効果を電波帯にて実現する画期的な手法を考案した．まず送信データを前節で示した暗号化プロトコルに従って多値信号へと変換し，光波で物理レイヤ暗号化信号を発生する．信号のキャリア周波数は近赤外であり秘匿に十分なマスキング効果が得られる．次に，信号光と局発光（周波数がわずかに異なる光）を合波し，それらを光ヘテロダイン検波することで，信号を電波の周波数に変換する．信号光と局発光の周波数の差を所望の電波の周波数に設定する．このとき，量子雑音のマスキング効果は光波の周波数で決まり，電波への変換後も保持されるため，電波帯でも十分な秘匿が実現できる．3 章で本手法を用いたミリ波帯の物理レイヤ暗号化の実験について示す．また，本手法により実現される量子雑音マスク数の定量的な評価は 4 章に示す．

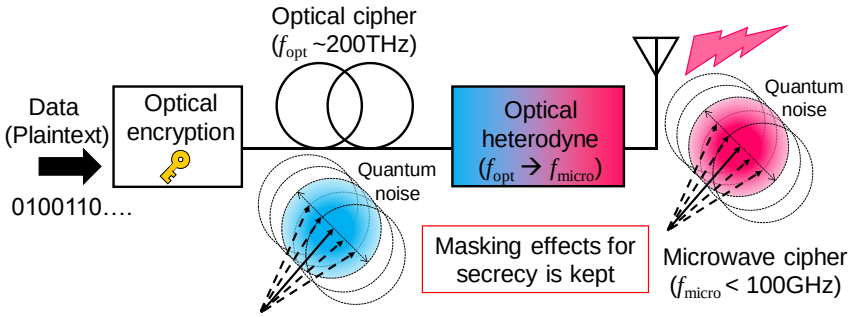

図 5：光ヘテロダインによる電波帯での量子雑音マスキングによる物理レイヤ暗号化の提案

3 実験

3-1 30-GHz 帯信号の量子雑音マスキングによる物理レイヤ暗号化

提案した電波帯の量子雑音マスキングによる物理レイヤ暗号化の原理実証を行った．高速の無線通信への適用を念頭に，キャリア周波数はミリ波帯とした．はじめに，30GHz のミリ波帯で 6-Gbit/s の暗号化信号を発生する実験を行った．図 6 に実験系を示す．オフラインで実装される Y-00 数理暗号化部に，PRBS データと秘密鍵を入力して多値信号への変換を行った．これを DA 変換として用いる 6Gsample/s の任意波形発生器（AWG）に入力して，対応する電圧を発生した．AWG からの出力電圧を増幅器とアッテネータを用いて適切に

調整して，3 つの変調器を時間同期して駆動した．可変波長レーザからの 1550.12nm のコヒーレント光は，まず IQ 変調器により QPSK 変調される．その後，一段目と二段目の位相変調器にて，それぞれ 6 ビット，10 ビットの分解能で位相変調した．こうして 2^{18} の位相値をもつ暗号化信号を光で発生させた．次に，別のレーザから出力された 1549.87nm の連続光である局発光と光カプラで合波した．二つのレーザの周波数差は，発生したいミリ波の周波数である約 30GHz である．発生する電波の周波数を正確に設定するには，二つのレーザの周波数をロックする必要があるが，今回は原理確認のために行わなかった．これら 2 波長の光をフォトディテクタで検波することで，ビート信号であるキャリア周波数約 30GHz の暗号化信号を発生した．本実験では，ミリ波の空間伝送を行わない B-to-B 構成とした．1.5m 程度の RF ケーブルを通じて IQ ミキサにてダウンコンバージョンし，リアルタイムオシロスコープにて波形を取り込んだ．その後，オフラインにて暗号の復号化を含むデジタル信号処理を行い，信号品質を測定した．

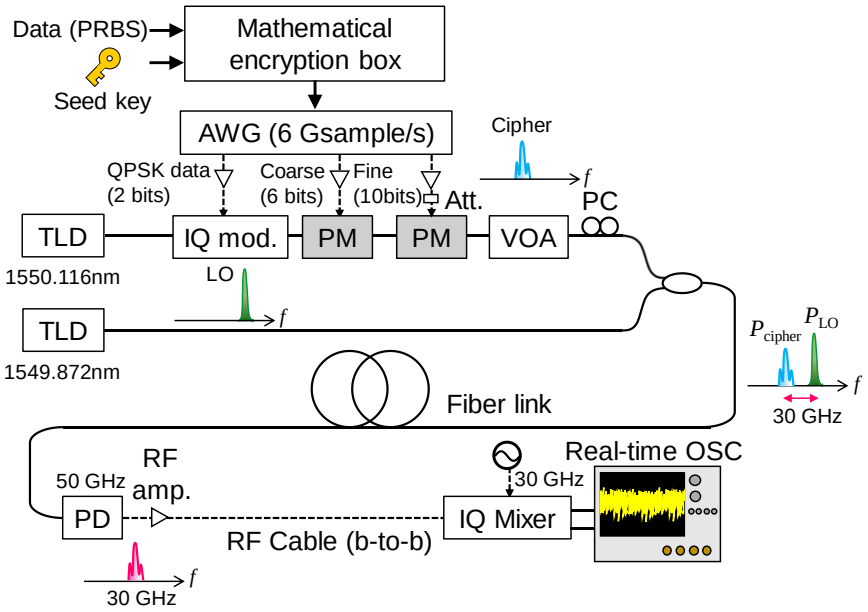

図 6：30GHz 帯 RF 信号の量子雑音マスキングによる物理レイヤ暗号化実験系

図 7(a)に光カプラにて暗号化信号光と局発光を合波した直後の光スペクトルを示す．約 30GHz 離れた波長に光の信号が正しく配置されていることがわかる．図 7(b)に光ヘテロダイン後の電気スペクトルを示す．約 30GHz を中心に信号が発生していることが見てとれる．図 8(a)の上段に暗号の復号化とキャリア位相推定前の受信コンスタレーションを示す．位相がランダム化されてコンスタレーションがドーナツ形状となっており，想定通りの暗号化がミリ波帯で実現できたことを確認できた．(a)の下段は，デジタル信号処理により暗号の復号化とキャリア位相推定を行った後のコンスタレーションである．デジタル信号処理が正しく動作して QPSK のコンスタレーションが復元している様子が確認できる．図 8(b)には，暗号化信号光の入力パワー

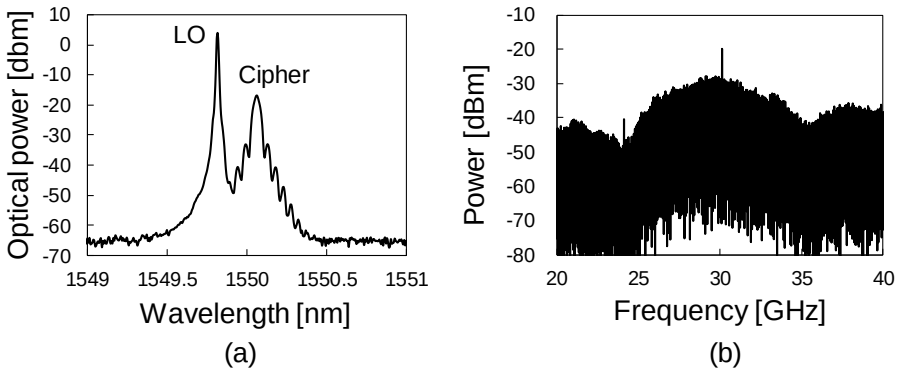

図 7：(a) 光スペクトルおよび(b)ヘテロダイン検波後の電気スペクトル

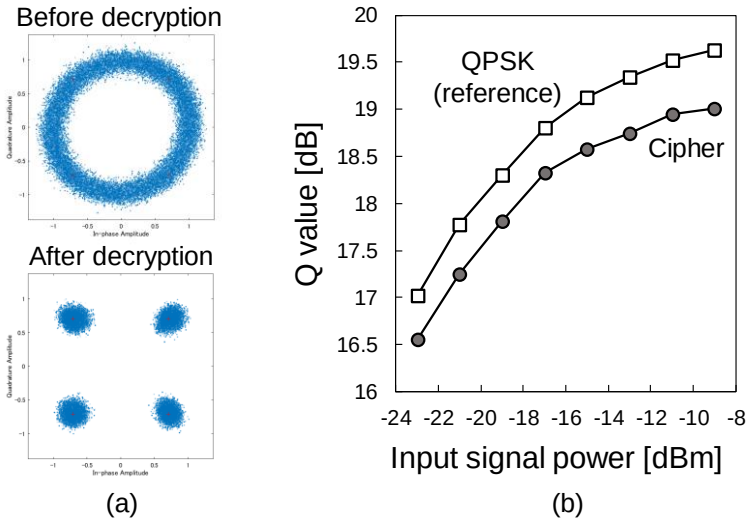

図 8: RF B-to-B の実験結果: (a)暗号復号化前後のコンスタレーション, (b)BER 特性

を変化させたときに Q 値の測定結果を示している. リファレンスとして同じビットレートで暗号化を行っていない QPSK 信号の測定結果も示している. この結果との比較より, 暗号化と復号化によって生じる Q 値ペナルティは, 最大でも 0.6dB 程度と小さいということが確認できた. また, Q 値は信号光パワーが-20dBm 以下と小さい場合でも 16.5dB 程度となり,軟判定判定誤り訂正符号の Q 閾値である 7.3dB から 9dB 以上のマージンがあることがわかる. このマージンはある程度の距離の無線伝送が可能であることを示唆している.

4- 2 12-Gbit/s 物理レイヤ暗号化信号の無線伝送

次に, ミリ波帯のアンテナペアを用いてシールド環境下において約 0.3m の 30-GHz 帯ミリ波の暗号化無線伝送の実験を行った. 伝送距離は実験環境により制限されている. また, 送信機側と送信アンテナが離れて設置されており, その間を光ファイバでつなぐ所謂 Radio-over-Fiber(RoF)構成を想定して, 1km の光ファイバを伝送する実験も実施した. 図 9 に実験系を示す. オフラインで実装される Y-00 数理暗号化部に, PRBS データと秘密鍵を入力して多値信号への変換を行った. これを DA 変換として用いる 6Gsample/s の任意波形

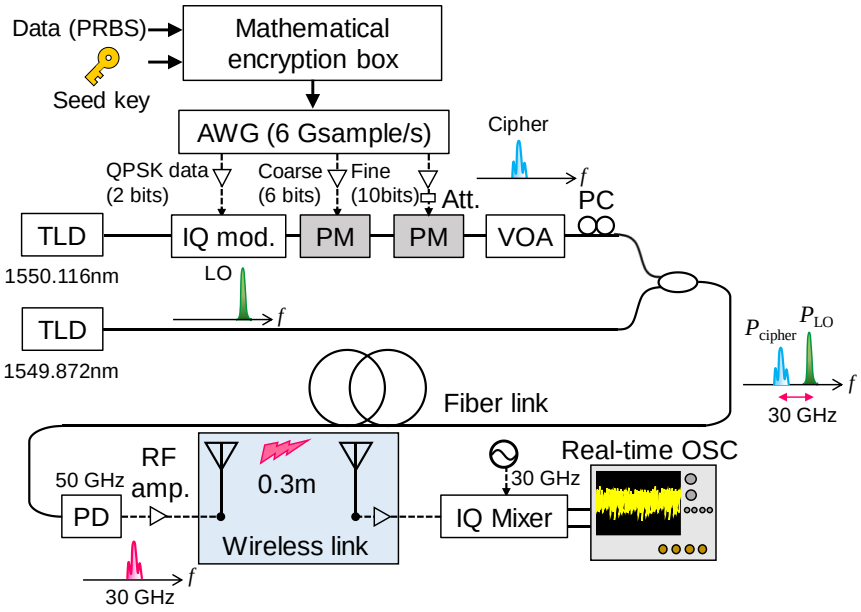

図 9: 量子雑音マスキング物理レイヤ暗号化信号の 30-GHz 帯無線通信実験系

発生器（AWG）に入力して，対応する電圧を発生した．AWG からの出力電圧を増幅器とアッテネータを用いて適切に調整して，3 つの変調器を時間同期して駆動した．可変波長レーザからの 1550.12nm のコヒーレント光は，まず IQ 変調器により QPSK 変調される．その後，一段目と二段目の位相変調器にて，それぞれ 6 ビット，10 ビットの分解能で位相変調した．この 2^{18} の位相値をもつ暗号化光信号は，6Gbaud/s で QPSK データ変調であるため，12Gbit/s のラインレートである．次に，別のレーザから出力された 1549.87nm の連続光である局発光と光カプラで合波した．二つのレーザの周波数差は，発生したいミリ波の周波数である約 30GHz である．これら 2 波長の光をフォトディテクタで検波することで，ビート信号であるキャリア周波数約 30GHz の暗号化信号を発生した．本実験では，発生したミリ波の暗号化信号を増幅後に，ホーンアンテナペアを用いて無線伝送した．受信側で再び増幅した後，IQ ミキサにてダウンコンバージョンし，リアルタイムオシロスコープにて波形を取り込んだ．最後に，オフラインにて暗号の復号化を含むデジタル信号処理を行い，信号品質を測定した．

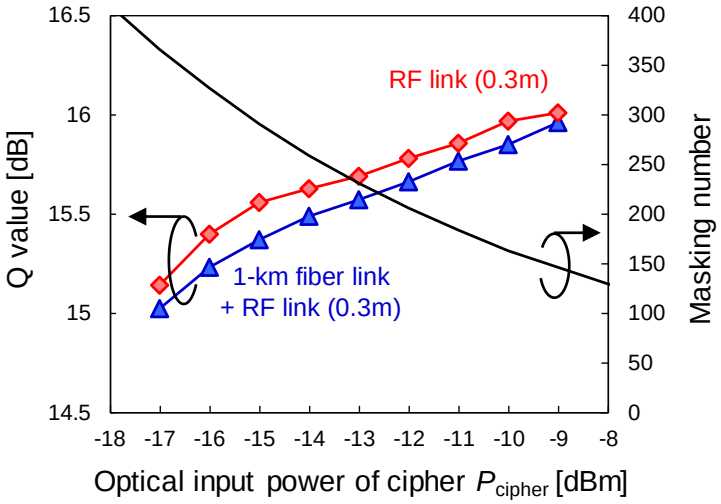

図 10：30-GHz 帯無線通信の受信 Q 値と量子雑音マスク数の見積もり

図 10 に信号光のパワーを変化させたときの Q 値の測定結果と量子雑音マスク数の見積もりを示す．赤線は 0.3m の無線通信後，青線は 1km のファイバ伝送と 0.3m の無線通信を行った後の Q 値である．どちらの場合においても 15dB 以上の高い Q 値が得られており，十分な信号品質で通信を行うことができている．軟判定誤り訂正符号閾値から 7.5dB 以上ある Q 値マージンは，より長距離の光ファイバと無線伝送が可能であることを示唆している．また，黒線は右縦軸に対応し，量子雑音マスク数を計算した値である．（計算の方法については 4 章で示す。）信号光パワーが上がるにつれてマスク数は減少するが，測定範囲において 100 を超えるマスク数が実現できる．一例として，光パワーが-9dBm でマスク数が 146 のときに秘密鍵をもたない盗聴者が実現可能な多値信号の受信について考察する．このとき，盗聴者が付加雑音のない理想的な受信をした場合に到達可能なシンボルエラー率は>0.994 となる．シンボルエラー率は 1 に近づくにつれて受信時の誤りが増えることとなる．つまり，0.994 というシンボルエラー率は極めて高く，盗聴者が多値信号を正しく受信・復調することは実質的に不可能であることを示している．さらに，この値は盗聴者がすべての信号パワーを傍受したという仮定におけるものである．つまり，下限であり現実的にこの値より優れた受信をするとはできない．このように，提案手法を用いてミリ波帯の信号の適切な物理レイヤ暗号化が実現できる．

ここまで，ミリ波信号の安全性について議論したが，この暗号の特徴として送信機とアンテナを結ぶ RoF リンクにおいても物理レイヤ暗号化が実現できるというメリットがある．図 11 に量子雑音マスク数がどのように変化するかを示す．ただし，RoF リンクは短いために光増幅器はないものと仮定している．図に示すようにマスク数は RoF リンクの入口で最小となり，光の伝搬に伴い信号光パワーが減少するためにマスク数が増加する．光ヘテロダインのためにフォトディテクタで受信した段階で一定となり電波帯の無線信号となる．これは，RoF のリンク長に従って適切に信号光の入力パワーを設定することで，システム全体として一貫した物理レイヤ暗号化を実現できることを示している．

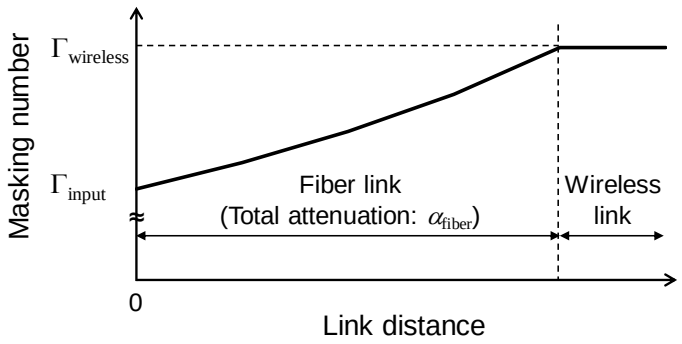

図 11：光ファイバおよび無線伝送における量子雑音マスク数

4 安全性と通信性能の理論検討

3-1 量子雑音による信号マスキングと伝送品質

光ヘテロダインを用いた提案手法により電波帯で実現できる量子雑音マスキングの効果を見積もる理論検討を行った．図 12 にモデルを示す．信号光は秘密鍵を用いた所定の手続きで得られる多値位相変調信号であり，角周波数ω_Sである．局発光は連続光であり，角周波数ω_Lとする．$|\omega_S-\omega_L|=\omega_{RF}$が発生する電波帯の信号の角周波数となる．量子雑音マスキング数Γ_Qは，量子雑音の拡がりで覆われる信号数として定義する．図 3(b)の拡大図中に示す量子雑音の拡がり角度$\Delta\phi_{shot}$と隣接するシンボル間角度$\Delta\theta_{basis}$の比として，

$$\Gamma_Q = \frac{\Delta\phi_{shot}}{\Delta\theta_{basis}} \tag{1}$$

と表される．隣接するシンボル間角度$\Delta\theta_{basis}$は，データ変調次数 M と位相変調の分解能 m から

$$\Delta\theta_{basis} = \frac{2\pi}{M\cdot 2^m} \tag{2}$$

となる．量子雑音の拡がり角度$\Delta\phi_{shot}$は理想的なヘテロダイン検波として，半古典理論で求める．まず量子雑音の分散σ_{shot}^2は

$$\sigma_{shot}^2 = 2ei_{bias}B \tag{3}$$

となる．e は電荷素量，i_{bias}はバイアス電流（直流成分），B は電気信号帯域である．直流バイアス電流 i_{bias}は，PD のレスポンシビティ S，信号光と局発光のパワーP_Sと P_L から，

$$i_{bias} = S(P_S + P_L) \tag{4}$$

と求められる．一方，信号電流 i_{sig}は，以下の式で表せる．

$$i_{sig} = 2S\sqrt{P_S\cdot P_L}\cos[(\omega_S-\omega_L)t+\varphi(t)] \tag{5}$$

$\varphi(t)$は信号の位相変調成分である．信号光と局発光の位相差の項は簡単化のため省略した．(3)−(5)より，

$$\tan\left(\frac{\Delta\phi_{shot}}{2}\right)\sim\frac{\Delta\phi_{shot}}{2} = \frac{\sigma_{shot}}{2S\sqrt{P_S\cdot P_L}} \tag{6}$$

$$\Delta\phi_{shot} = \sqrt{\frac{2eB}{SP_S}} \tag{7}$$

となり，量子雑音の拡がり角度$\Delta\phi_{shot}$を求めることができる．このとき，PD のレスポンシビティ S は以下となる．

$$S = \frac{\eta_q e}{h\nu_0} \tag{8}$$

η_q, h, ν_0 は量子効率，プランク定数，光信号の周波数である．以上より，マスク数Γ_Q は，

$$\Gamma_Q = \frac{M \cdot 2^m}{2\pi}\sqrt{\frac{2h\nu_0 B}{\eta_q P_S}} \tag{9}$$

となる．量子雑音マスク数は信号の周波数の平方根に比例する．つまり，高い周波数である光波においてマスキングの効果は大きくなる．また，マスク数は暗号化後の多値数 $M{\cdot}2^m$ に比例する一方で，信号パワーの平方根に反比例する．マスク数は上げるためには位相変調の分解能ビット数 m を上げて信号多値数を増加するか，信号パワーP_s を減少させる必要がある．信号パワーは信号品質に関連する．信号品質を示す指標である信号対雑音比 SNR は，信号パワーP_s の関数として以下で求められる．

$$\mathrm{SNR} = \frac{SP_S}{eB} \tag{10}$$

SNR は信号パワーに比例することがわかる．この式(9)(10)は，量子雑音マスク数と SNR，つまり安全性と信号品質にトレードオフがあることを示している．このトレードオフを考慮して暗号通信システムを構築することが重要である．

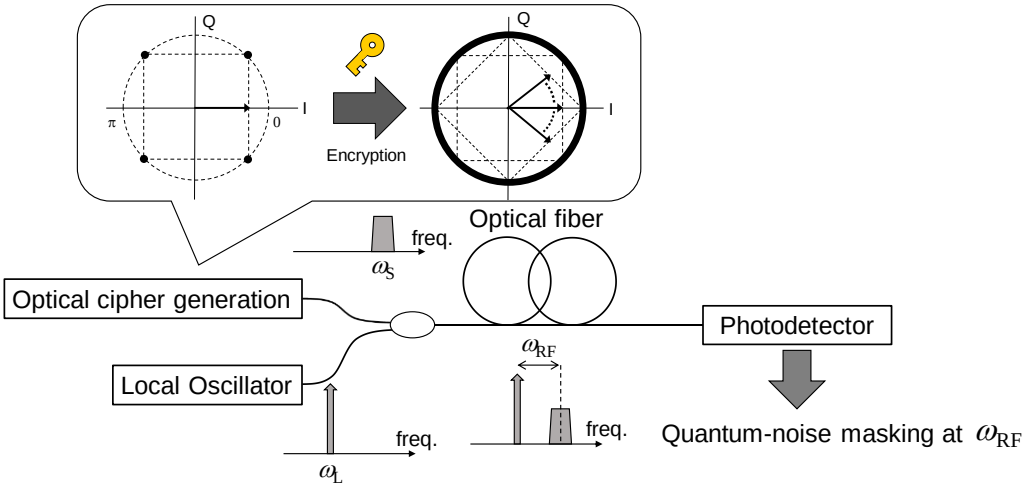

図 12：光ヘテロダインによる物理レイヤ暗号化の解析モデル

3-2 数値計算結果

前節で示した量子雑音マスク数と信号品質を示す SNR のトレードオフを，4-1 および 4-2 節で実験に用いた具体的なシステムパラメータを用いて計算した．表 1 にパラメータの詳細を示す．データ変調次数は 4(QPSK)，信号帯域は 6GHz，光周波数は 193THz とした．PD の量子効率は 1 とした．位相変調の分解能は 12, 14, 16 ビットと変化させた．

表 1：数値計算のためのシステムパラメータ

Item	Value
Order of data modulation: M	4
Bit number of the resolution of phase randomization: m	12, 14, 16
Bandwidth of cipher: B	6 GHz
Optical frequency of cipher: ν_0	193 THz
Quantum efficiency of PD: η_q	1

図 13 に暗号光信号のパワーを変化させたときの量子雑音マスク数（黒の 3 つのカーブ）と SNR（赤線）の計算結果を示す．式(9)からも明らかなように，位相変調分解能 m を上げるか，信号パワーを減少するこ

とで大きなマスク数を実現できる．−10dBm 程度の現実的な光パワーで 100 以上のマスク数を実現するには，*m*=16 以上とする必要があることがわかる．また，このとき SNR は 50dB 以上あり，十分な信号品質を確保できていることがわかる．本検討結果より，提案する光ヘテロダインを用いた電波帯の物理レイヤ暗号化無線通信において，*m*=16 とすることで高い安全性と十分な信号品質が両立できることがわかった．

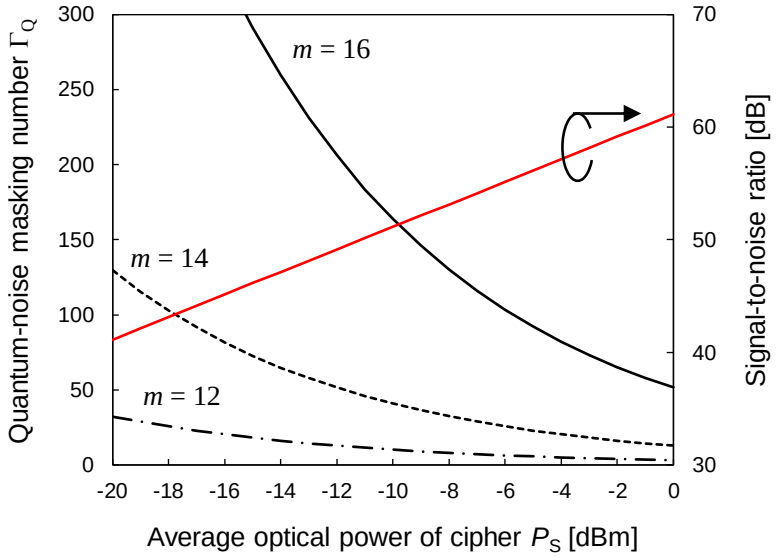

図 13：光信号パワーを変化したときの電波帯での量子雑音マスク数と信号対雑音比の関係

5 まとめと今後の展望

本助成による研究では，光ヘテロダインを用いて電波帯にて量子雑音マスキングを実現する研究代表者の提案を，ミリ波帯の無線通信に応用展開することに取り組んだ．まず，ミリ波帯約 30GHz で 12Gbit/s の暗号化信号を発生し，これを復号化する実験を実施した．暗号化と復号化による Q 値ペナルティは最大で 0.6dB 程度と信号品質に大きな影響を与えることなく物理レイヤ暗号化が実現できることを示した．次に，この暗号化信号をアンテナペアを用いて無線伝送する実験を行った．シールド環境のサイズで無線伝送距離は 0.3m に限られたが，軟判定誤り訂正符号閾値からは 7.5dB 以上のマージンがあり，より長距離の伝送に適用可能であることが示唆された．また，このとき量子雑音によるマスク数は 100 を超えており，高い安全性と両立できることがわかった．さらに，光信号パワーを変化させたときの，量子雑音マスク数と SNR の関係を光ヘテロダインの理論から導出した．量子雑音マスク数は光パワーの平方根に反比例する一方で，SNR は光パワーに比例する．つまり安全性と信号品質にはトレードオフの関係性があることがわかった．このトレードオフ関係を実験の条件にて数値計算した．その結果，暗号化のための位相変調の分解能を 16 ビット以上とすれば十分に安全性と信号品質を両立できることが確認できた．このトレードオフの関係式は，量子雑音マスキングを用いた物理レイヤ暗号化システムの設計に有用である．

今後の展望としては，より本格的な無線通信への適用に向けて，現用の無線通信システムで耐フェージング性を考慮して採用されている直交周波数分割多重変調への適用や，直接的に無線周波数を発生することなく中間周波数を利用するなどが考えられる．

【参考文献】

1. G. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, “Secure communication using mesoscopic coherent states,” Phys. Rev. Lett. 90, 227901 (2003).
2. E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen “Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks,” Phys. Rev. A. 71, 062326 (2005).
3. O. Hirota, M. Sohma, M. Fuse, and K. Kato, “Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme,” Phys. Rev. A, 72(2), 022335, 2005.
4. C. Liang, G. S. Kanter, E. Corndorf, and P. Kumar, “Quantum Noise Protected Data Encryption in a WDM Network,” IEEE Photon. Technol. Lett, 17, 1573-1575, (2005).
5. G. S. Kanter, S. X. Wang, R. A. Lipa, and D. Reilly, "Self-Coherent Differential Phase Detection for Optical Physical-Layer Secure Communications," in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2013, OSA Technical Digest (online) (Optical Society of America, 2013), paper JW2A.41.
6. Y. Doi, S. Akutsu, M. Honda, K. Harasawa, O. Hirota, S. Kawanishi, K. Ohhata, and K. Yamashita, “360 km field transmission of 10 Gbit/s stream cipher by quantum noise for optical network,” in Proc. Optical Fiber Communication Conference (OFC), OWC4, 2010.
7. F. Futami and O. Hirota, " 100 Gbit/s (10 × 10 Gbit/s) Y-00 Cipher Transmission over 120 km for Secure Optical Fiber Communication between Data Centers," in Opto-Electronics and Communications Conference (OECC2014), paper MO1A2.
8. F. Futami, K. Guan, J. Gripp, K. Kato, K. Tanizawa, C. Sethumadhavan, and P. J. Winzer, “Y-00 quantum stream cipher overlay in a coherent 256-Gbit/s polarization multiplexed 16-QAM WDM system,” Optics Express, 25, 33338-33349, (2017).
9. K. Kato and O. Hirota, “Quantum quadrature amplitude modulation system and its applicability to coherent state quantum cryptography,” Proc. SPIE 5893, 589303 (2005).
10. M. Nakazawa, M. Yoshida, T. Hirooka, and K. Kasai, “QAM quantum stream cipher using digital coherent optical transmission,” Opt. Express 22, 4098-4107 (2014).
11. X. Chen, K. Tanizawa, P. Winzer, P. Dong, J. Cho, F. Futami, K. Kato, A. Melikyan, and KW Kim, “Experimental demonstration of 4,294,967,296-QAM based Y-00 quantum stream cipher template carrying 160-Gb/s 16-QAM signals,” Optics Express, 29, 5658-5664 (2021)
12. K. Tanizawa, and F. Futami, “Ultra-long-haul digital coherent PSK Y-00 quantum stream cipher transmission system,” Optics Express, 29, 10451-10464 (2021).
13. K. Tanizawa, and F. Futami, “Digital coherent PSK Y-00 quantum stream cipher with 2^{17} randomized phase levels,” Optics Express, 27, 1071-1079 (2019).
14. K. Tanizawa, and F. Futami, “Single channel 48-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 400- and 800-km SSMF,” Optics Express, 27, 25357-25363 (2019).
15. Seb J. Savory, "Digital filters for coherent optical receivers," Opt. Express 16, 804-817 (2008).
16. B. Szafraniec, B. Nebendahl, and T. Marshall, "Polarization demultiplexing in Stokes space," Opt. Express 18, 17928-17939 (2010).
17. D.-S. Ly-Gagnon, S. Tsukamoto, K. Katoh, and K. Kikuchi, “Coherent detection of optical quadrature phase-shift keying signals with carrier phase estimation,” J. Lightwave Technol., 24, 12-21 (2006).
18. K. Tanizawa, F. Futami, and O. Hirota, “Digital feedforward carrier phase estimation for PSK Y-00 quantum-noise randomized stream cipher,” IEICE Communications Express, 7, 1-6 (2018).

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Quantum Noise-Assisted Coherent Radio-over-Fiber Cipher System for Secure Optical Fronthaul and Microwave Wireless Links	*IEEE/OSA Journal of Lightwave Technology*	2020 年　8 月
Quantum-Noise Signal Making at Microwave Frequency in PSK Y-00 Quantum Stream Cipher with Optical Heterodyne Frequency Conversion	*Tamagawa University Quantum ICT Research Institute Bulletin*	2021 年　3 月
Photonic-Assisted Microwave OFDM Quantum-Noise Randomized Cipher Generation via IM/DD IFoF Transmission	*Optical Fiber Communication Conference and Exhibition (OFC 2021)*	2021 年　6 月
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	電子情報通信学会 2021 年総合大会	2021 年　3 月