デジタルコヒーレント方式物理暗号光通信（延長）

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．大容量・長距離の情報通信を支える光ファイバ通信システムにおいても，近年は，セキュリティの重要性が高まってきている．光ファイバ伝送路では，タッピング（一部の光パワーを分岐・観測すること）により，光信号が盗聴される危険性が潜在的に存在する．現状の通信システムにおけるセキュリティ対策では，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暗号技術を導入する．盗聴者は，タップした光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共有する鍵（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．将来のより安全な光通信システムの実現のためには，タップした光信号を正しく復調すること自体を防ぐような暗号技術を導入することが一つの解決策となる．

光の量子雑音（ショット雑音）の存在により安全性を担保する光ファイバ通信向けの物理暗号が 2000 年初頭に提案された[1]．この暗号は，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（以下，Y-00 暗号と呼ぶ）．図 1 に示すように，この暗号は，あらかじめ共有した短い鍵を用いて送りたいデータ（平文）を直接暗号化する方式である．具体的な暗号化の方法としては，鍵の情報に基いて光の位相と振幅，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は，多値変調信号を受信する必要があるため，受信時に生じるショット雑音の影響により正しい受信・復調ができない．つまり，鍵なしでは暗号化された光信号を正しく受信すること自体ができないことを特徴としており，前述のタッピング自体を防ぐのに有効な暗号化である．Y-00 暗号は，チャネル当たり Gbit/s 以上の伝送速度，1,000km 級の伝送距離，古典システムと同様の波長多重化を実現できるため，既存の光ファイバ通信システムと非常に相性が良い．

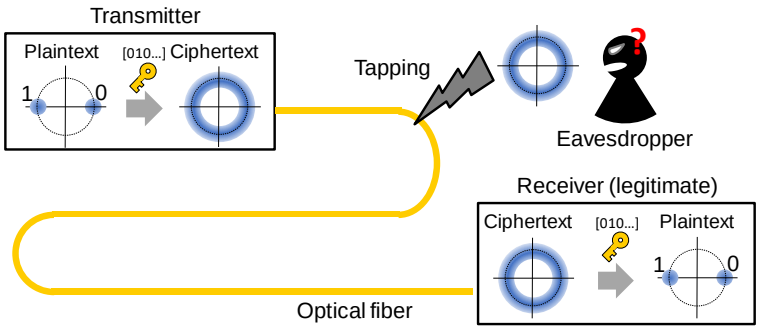


図 1：Y-00 暗号のシステム構成概要

Y-00 暗号は，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]にて実現することができる．本研究では，長距離の伝送に有利である PSK 方式の Y-00 暗号に焦点をあてる．PSK 方式の Y-00 暗号は，αηとして OC-12(622 Mbit/s)の伝送速度で 250-km の伝送距離にて実験実証された[4]．この実験では，鍵の情報に基いて暗号化とは逆の位相回転を施す復号化が，位相変調器を用いて光領域で実現されている．その後，差動の IQ 測定後にデジタル領域で復号化を行うシステムが，2.66Gbit/s のビットレートで実証されている[5]．最近，我々は，イントラダインのコヒーレント受信とデジタル信号処理を組み合わせる，所謂，デジタルコヒーレント方式を利用して PSK Y-00 暗号を実現する方法を提案し，シミュレーションにて 10Gbit/s の伝送速度における検証を行った[12]．また，昨年度には本助成にて，デジタルコヒーレント方式

との融合の核となる受信側のデジタル信号処理に焦点をあて，通信の安定化を実現するキャリア位相推定と伝送により生じる波形歪を補償する波形等化を実験的に検証することに成功した[13].

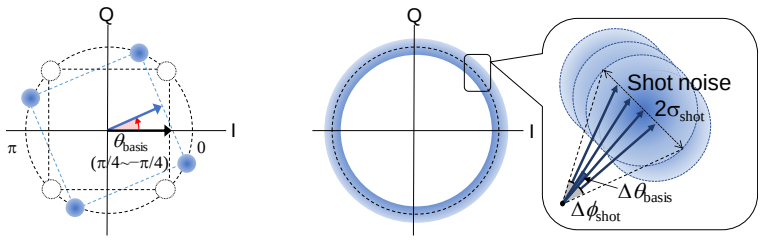
本研究では，この物理暗号のさらなる大容量を目指して，(a)偏波及び波長多重技術を導入した大容量化の実験実証と(b)安全性と通信性能（通信容量，距離など）の理論検討を行った．具体的には，以下の 3 つの課題に取り組んだ.

[1] 偏波多重技術の導入
本助成で購入する偏波多重エミュレータ光回路を用いて，送信側で物理暗号を偏波多重する．受信側では，バタフライ構成のデジタルフィルタをブラインド最適化アルゴリズムで駆動するが，暗号化された信号を扱うという点に注意してアルゴリズムを検討する.
[2] 高密度波長多重技術の導入
雑音マスキングによる物理暗号は信号の変調速度に応じた帯域をもつ．本助成で購入する波長合分波器を用いて波長多重・分離を行う．さらに，送受信端のデジタル信号処理でナイキスト整形を施すことでチャネル間隔を狭めた高密度の多重化を検討する.
[3] 安全性と伝送特性の理論検討
この物理暗号の安全性の評価指標の一つは雑音によるマスキング効果の量である．これは信号パワーに反比例することがわかっている．一方，伝送では，信号パワーは伝送速度と距離に関係する．この二つの関係を整理・統合してトレードオフを明らかにする.

2 Y-00 光通信量子暗号

2-1 原理

PSK Y-00 暗号は，通常の M-ary PSK データ変調の位相を鍵の情報に従ってシンボル毎にランダムに回転することで実現される．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．（本稿で紹介する実験では，データ変調としては BPSK および QPSK を採用している.）図 2(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．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 2(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，ショット雑音の広がり角度$\Delta\phi_{shot}$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ショット雑音により観測した信号に不確定性が生じる．つまり，鍵をもたない盗聴者は，暗号化された $M \cdot 2^m$ PSK 信号を正しく受信・復調することが困難である．一方，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正しい受信が可能となる．これをショット雑音によるマスキング効果と呼んでおり，Y-00 暗号における秘匿性（鍵をもつ受信者の有利性）を実現できる．ショット雑音によるマスキングは，送信端直後でのタッピングにも有効，真にランダムかつ除去できない（理論的に保証）という点において非常に重要である.



(a) (b)

図 2: PSK Y-00 暗号における雑音マスキング

2-2 光位相のランダム化による暗号化

Y-00 暗号は，例えば，IQ 変調器で QPSK 変調を行い，その後段で位相変調器により位相を回転することで発生する．ショット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．つまり，位相変調器を駆動

するデジタル・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，粗密位相ランダマイズ法を提案する．

図 3 に粗密位相ランダマイズ法の構成と動作原理を示す．まず IQ 変調器にて QPSK 変調を行い，次に後段の 2 つの位相変調器で粗な位相回転θ_{basis_c}と密な位相回転θ_{basis_f}を組み合わせて目標とする位相回転θ_{basis}を実現する．それぞれの変調器を駆動する電気信号（電圧）は，疑似乱数発生器(PRNG)とマッパーからなる Y-00 数理暗号化部と DA 変換器から供給される．暗号化部では，典型的には 256 ビットの鍵が PRNG によって現実的に繰り返しが生じない長さ，例えば 2^{256} ビットに伸長され，その疑似ランダムビット列からシンボル毎に基底が選択される．選択された基底とマッパーから位相回転量θ_{basis}が決まる．それが粗な回転量θ_{basis_c}と密な位相回転θ_{basis_f}に分離され，対応する電気信号が出力される．粗な位相回転として K ビット（2^Kの位相レベル），密な位相回転として L ビット（2^Lの位相レベル）が用意され，QPSK データ信号を暗号化する場合は，DA 変換の出力をそれぞれのピーク・ピーク位相回転量θ_{pp_PM-1}とθ_{pp_PM-2}が以下の式を満たすように調整する．

$$\theta_{pp\_PM-1} = \frac{\pi}{\log_2 M}\left(1-\frac{1}{2^K}\right) \tag{1}$$

$$\theta_{pp\_PM-2} = \frac{\pi}{\log_2 M \cdot 2^K}\left(1-\frac{1}{2^L}\right) \tag{2}$$

このとき，m=K+L となり，2^{K+L}のレベルの位相のランダム化が実現できる．例えば，K=L=8 とすることで，8 ビットの DA 変換で 2^{16} の基底数の Y-00 暗号を発生させることができる．なお，前段の QPSK 変調については，Y-00 数理暗号発生部でデータの極性が鍵の情報に基づきランダム化されている．

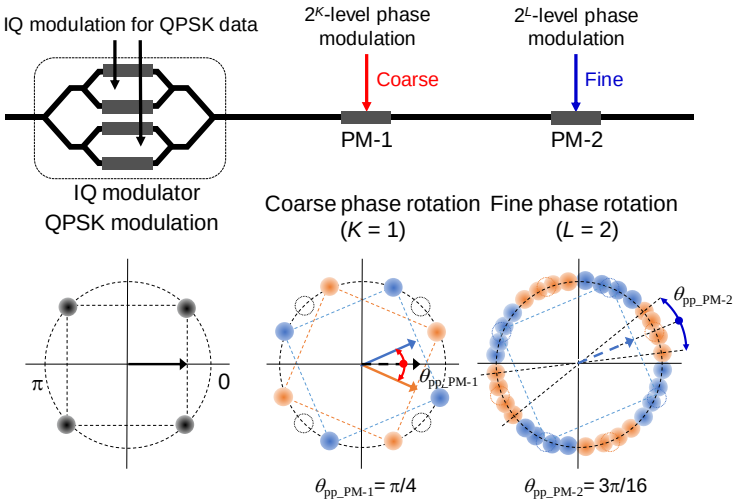


図 3: 粗密位相ランダマイズ法による PSK Y-00 暗号の発生

2-3 デジタル信号処理

暗号は，90 度光ハイブリッド光回路とフリーランの局発光を用いたイントラダイン方式で受信される．典型的なデジタルコヒーレント受信器の構成と全く同一である．その後，デジタル信号処理により，波形等化，暗号の復号化，データの復調を行う．図 4 に信号処理のブロック図を示す．入力は，偏波・位相ダイバーシティコヒーレント受信器で得られる両偏波の信号の電界と正規受信者に共有されている鍵である．まず，有限インパルス応答(FIR)フィルタによって分散補償を行う[14]．その後，偏波処理を行う．単一偏波の場合は，SOP 法により偏波を調整する[15]．偏波多重の場合は，バタフライ構成の FIR フィルタを CMA にて収束させることで偏波分離を行う．次に，鍵と送信側と同一の Y-00 数理暗号化部を用いてシンボル毎の位相回転角をθ_{basis}得て，$\exp(-j\theta_{basis})$を乗じる，つまり，位相の逆回転を与えることで暗号の復号化を行う．最後に累乗法によるキャリア位相推定を行い[16]，データを復調する．本研究では，偏波多重された信号を処理するため

に，偏波分離を新たに実装・検討した．

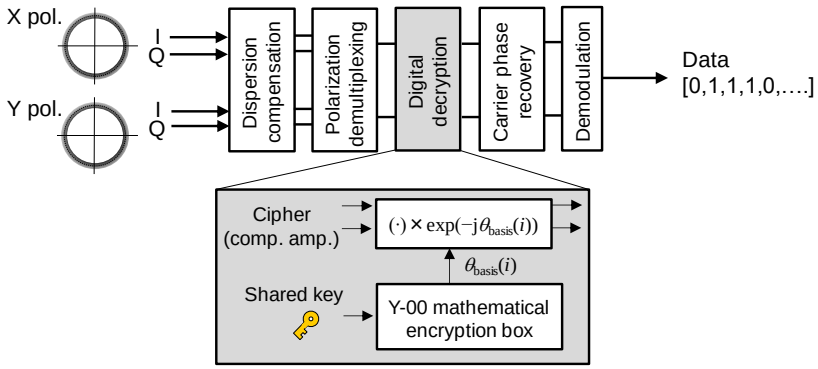


図 4: Y-00 暗号受信のためのデジタル信号処理フロー

3 偏波多重および波長多重実験

3-1 偏波多重 20-Gbit/s PSK Y-00 暗号の伝送実験

はじめに，20Gbit/s の PSK Y-00 暗号の暗号化・復号化の実験を行い，偏波分離の有効性を示した．図 5 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 データと鍵を入力して暗号化を行った．これを DA 変換として用いる 10Gsample/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，粗密位相ランダマイズ法のための 3 つの変調器を駆動した．可変波長レーザからのコヒーレント光は，まずマッハツェンダ変調器により BPSK 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をランダム化する．こうして 2^{17} の光位相値をもつ Y-00 暗号を発生させた．はじめに，偏波分離を含むデジタル信号処理のみを実験検証するために，光ファイバ伝送路のない状態（所謂，バック・トゥー・バック構成）にて実験を行った．可変アッテネータとエルビウム添加光ファイバアンプ(EDFA)によって，受信 OSNR を調整した．受信では，フリーランの可変波長レーザを局発光として用いて，90 度光ハイブリッド回路とバランスディテクタにより，イントラダイン受信を行った．リアルタイムオシロスコープにて波形を取り込み，オフラインにて 2.3.にて示したデジタル信号処理のうち波形等化である分散補償以外の処理を行った．次に，100km ごとに EDFA によって光増幅が行われる 400km と 800km のシングルモードファイバ伝送路を用いて伝送実験を行った．受信はバック・トゥー・バック構成と同様である．デジタル信号処理では，ファイバ長に対応する波長分散補償を行った．

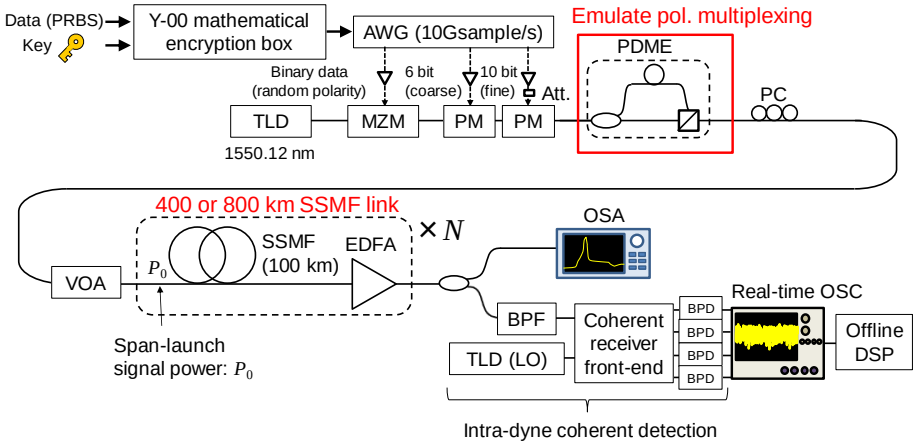
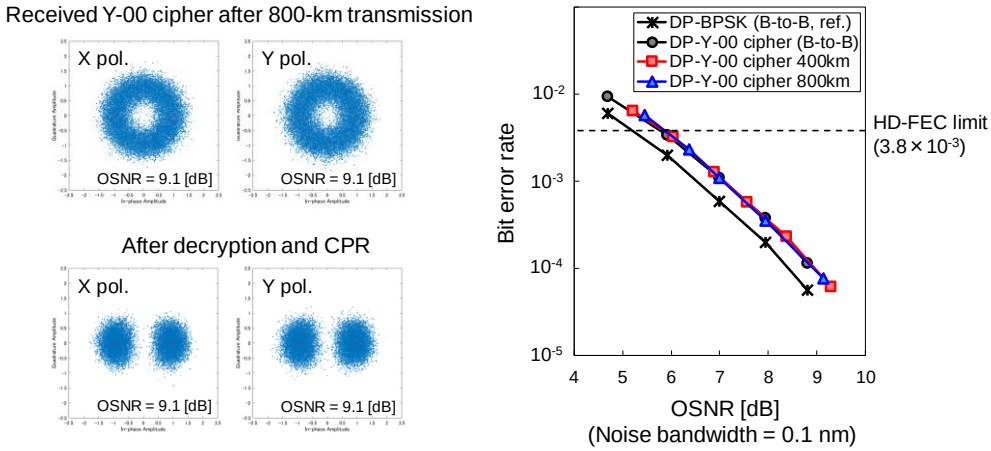


図 5: 20-Gbit/s PSK Y-00 暗号の 400&800km 伝送実験系

図 6 に実験の結果を示す．(a)の上段は波長分散補償と偏波分離後，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である．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のような形状であることがわかる．(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 BPSK のコンスタレーションが回復している様子が確認できる．(b)には，バック・トゥー・バック構成と 400km および 800km 伝送後の BER の測定結果を示している．偏波分離を含むデジタル信号処理が正しく動作し，鍵をもつ正規の受信者が FEC リミット以下の BER を達成できるということが実証できた．また，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 BPSK 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 OSNR のペナルティは，1dB 以下と小さいということが確認できた．図 7 に 400km および 800km 伝送における，光ファイバ伝送路への入力光パワーを変化させたときの受信 Q 値（赤青実線）とショット雑音によるマスク数（黒実線）を示す．このマスク数は，光信号パワーで決まるショット雑音により隣接する信号がマスクされる（覆われる）数を示している．Y-00 暗号の安全性の評価指標であり，大きいほど高い安全性を実現できる．この測定結果より，光パワーが大きくなるにつれ，受信 Q 値は改善するが，マスク数は低下することがわかる．つまり，信号品質を確保できる範囲で光パワーを小さくすることが，伝送性能と安全性を両立するうえで重要である．800km 伝送において，硬判定の誤り訂正符号（HD-FEC）閾値を達成できるときのマスク数は，約 150 程度である．マスク数 150 とは，鍵をもたない盗聴者の受信のシンボル誤り率が>0.99 であり，実用上きわめて高い安全性といえる．



(a) (b)

図 6: 20-Gbit/s PSK Y-00 暗号伝送の実験結果（a）コンスタレーション，(b)BER 特性

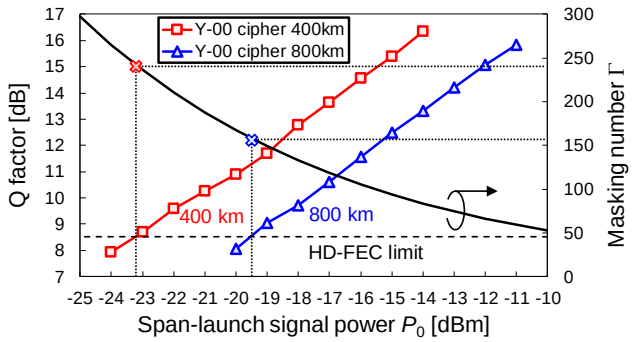


図 7: 入力光信号パワーを変化させたときの受信 Q 値とショット雑音による信号マスク数

4- 2 偏波多重 48-Gbit/s PSK Y-00 暗号の伝送実験

次に，チャネル当たりの容量をさらに拡大するために QPSK データ変調を採用し，48Gbit/s の PSK Y-00 暗号の伝送実験を行った．図 8 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 データと鍵を入力して暗号化を行った．これを DA 変換として用いる 12Gsample/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，粗密位相ランダマイズ法のための 3 つの変調器を駆動した．可変波長レーザから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をランダム化する．こうして発生した 2^{18} の光位相をもつ Y-00 暗号は，可変アッテネータでパワーを調整されたのちに光ファイバリンクを伝送する．光ファイバリンクは 100km のシングルモード光ファイバとエルビウム添加光ファイバアンプ(EDFA)により構成され，100km の伝送と増幅が繰り返されるようなリンクとなっている．今回は，伝送距離として 400km と 800km の場合の実験を行った．受信では，フリーランの可変波長レーザを局発光として用いて，90 度光ハイブリッド回路とバランスディテクタにより，イントラダイン受信を行った．リアルタイムオシロスコープにて波形を取り込み，オフラインにて 2.3.にて示したデジタル信号処理を行った．

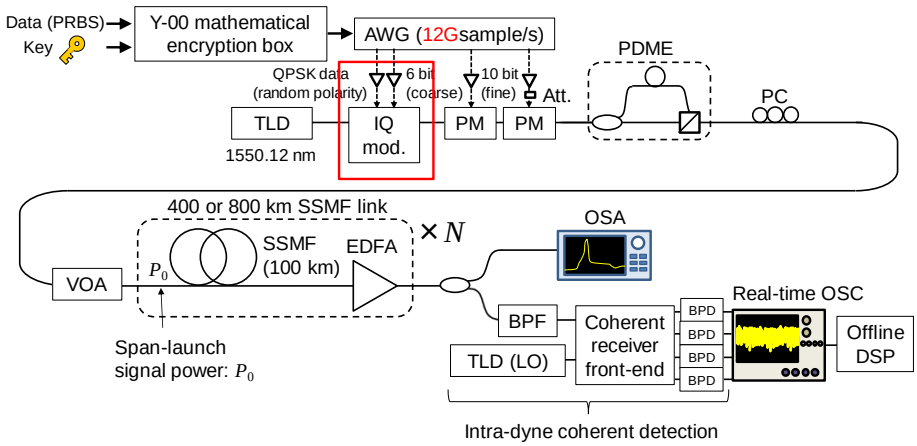
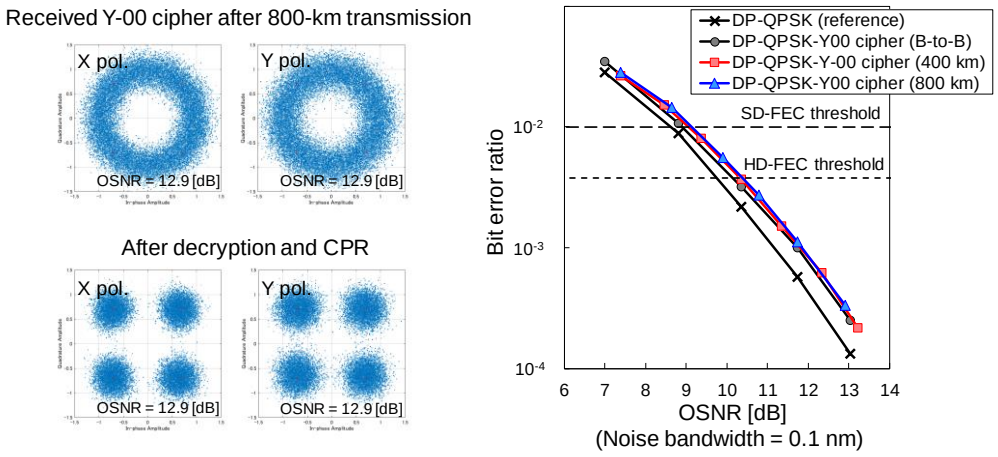


図 8: 48-Gbit/s PSK Y-00 暗号の 400&800km 伝送実験系



(a) (b)

図 9: 48-Gbit/s PSK Y-00 暗号伝送の実験結果 (a) コンスタレーション，(b)BER 特性

図 8 に実験の結果を示す.(a)の上段は 800km の伝送後に波長分散補償と偏波分離とを行った後のコンスタレーションである．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のような形状であることがわかる．(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.データ変調を QPSK とした場合においてもデジタル信号処理が正しく動作してデータ変調を復元できることを確認した.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．先の実験結果と同様に，1dB 以下の小さな OSNR ペナルティで暗号化・伝送・復号が実現できることを実証した．図 10 には，400km および 800km 伝送における，光ファイバ伝送路への入力光パワーを変化させたときの受信 Q 値（赤青実線）とショット雑音によるマスク数（黒実線）を示す．800km 伝送において

軟判定の誤り訂正符号(SD-FEC)閾値を達成できるときのマスク数は，約 200 程度である．先の実験の考察で示した通り，盗聴者が鍵情報なしで受信するときのシンボルエラーレートは極めて 1 に近い値となり，高い安全性と信号品質の両立が実現できるということがわかる．このように，BPSK から QPSK へデータ変調をアップグレードしても Y-00 暗号は高い性能を発揮することができる．

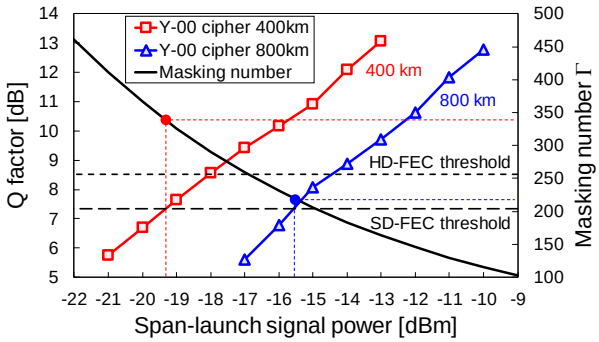


図 10：入力光信号パワーを変化させたときの受信 Q 値とショット雑音による信号マスク数

4- 3 偏波多重 48-Gbit/s Y-00 暗号の 4 チャネル波長多重実験

典型的な光ファイバ伝送システムにおいては，大容量化を実現するために波長多重が行われる．先の実験で実証した 48-Gbit/s の Y-00 暗号の波長多重実験を行った．まず予備検討として，Y-00 暗号と QPSK 信号（暗号化前）の光スペクトルの比較を行った．波長分解能 0.01nm の光スペクトルアナライザで測定した結果を図 11 に示す．Y-00 暗号は，位相変調により光位相のランダム化を行っていることから，光スペクトルが拡がることが懸念されていた．しかしながら，QPSK 信号と比較したときのスペクトルはほぼ同等であった．暗号化のための位相変調量が小さいことから，スペクトルの拡がりが非ナイキストの QPSK 信号との比較では無視できるほど小さいと考えられる．この結果は，Y-00 暗号が非ナイキストの QPSK 信号と同等の占有帯域幅で波長多重できることを示唆している．次に，ナイキストフィルタリングによる帯域削減について検討した．ナイキストフィルタリングを用いる波長多重伝送システムでは，通常，送信側でルートレイズドコサインのフィルタリングを占有帯域削減のために施し，受信側では帯域外の雑音除去のために同じくルートレイズドコサインのフィルタリングを行う．実験による実証を計画していたが，実験装置の都合で送信側でのフィルタリングの実施ができないことがわかった．そこで，原理検証として受信側で送信側のフィルタリングもあわせたレイズドコサインのフィルタリングを行った場合の信号品質について実験にて調べた．その結果，ナイキストフィルタリングによる Q 値へのペナルティは，OSNR=13dB において約 0.6dB と小さいということがわかった．よって，Y-00 暗号は小さなペナルティを許容すればナイキスト波長多重伝送が可能である．

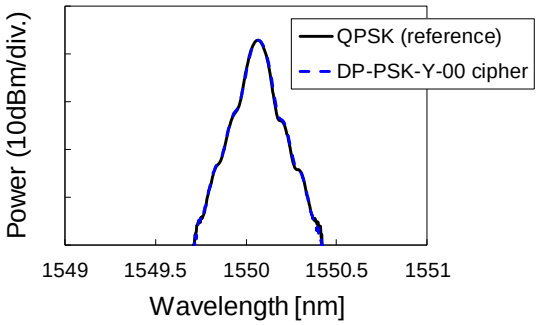


図 11：48-Gbit/s の Y-00 暗号と非暗号の QPSK 信号の光スペクトルの比較

次に，非ナイキストの 48-Gbit/s の Y-00 暗号の 4 チャネル高密度波長多重実験を行った．図 12 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 データと鍵を入力して暗号化を行った．これを DA 変換として用いる 12Gsample/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，粗密位相ランダマイズ法のための 3 つの変調器を駆動した．4 つの可変波長レーザを用意し，それらを 37.5GH 間隔に設定した．4 つの異なる波長の

コヒーレント光は，まず IQ 変調器により一括で QPSK 変調される．IQ 変調器によるデータ変調は本来異なる変調器を用いるが，ここでは実験装置の都合のため一括で行った．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をランダム化する．この位相ランダム化は，異なる波長間で QPSK 変調が時間的に同期していれば，一括して行うことができる．この一括の暗号化は，当初研究計画にはなかったが，本テーマを進めるうえで得られた新たな提案である．こうして発生した 2^{18} の光位相をもつ 4 波の Y-00 暗号は，可変アッテネータとエルビウム添加光ファイバアンプ(EDFA)を用いて受信 OSNR が調整足される．その後，フリーランの可変波長レーザを局発光として用いて，90 度光ハイブリッド回路とバランスディテクタにより，波長分離を兼ねたイントラダイン受信を行った．リアルタイムオシロスコープにて波形を取り込み，オフラインにて 2.3.にて示したデジタル信号処理を行った．

図 13 に実験結果を示す．(a)に示された光スペクトルから 4 波長が多重されていることがわかる．(b)は 1 波長を分離して受信した後のコンスタレーションである．上段は波長分散補償と偏波分離を行った後であり，後段は共有鍵による暗号の復号化とキャリア位相推定を行った後である．ドーナツ形状の暗号化されたコンスタレーションが，暗号化前のデータ変調に戻るということが確認できる．次に，受信 OSNR が 13dB のときの Q 値を測定した結果を(c)に示す．リファレンスとして暗号化を行わない偏波多重 QPSK で実験を行った結果もプロットした．これらの比較により，約 0.5dB の Q ペナルティで波長多重した QPSK 信号の暗号化・復号化が実施できることがわかった．同様のペナルティは波長多重を行わないシングルチャネルの結果でも観測されているため，ペナルティの原因は波長多重によるものではないと推察される．

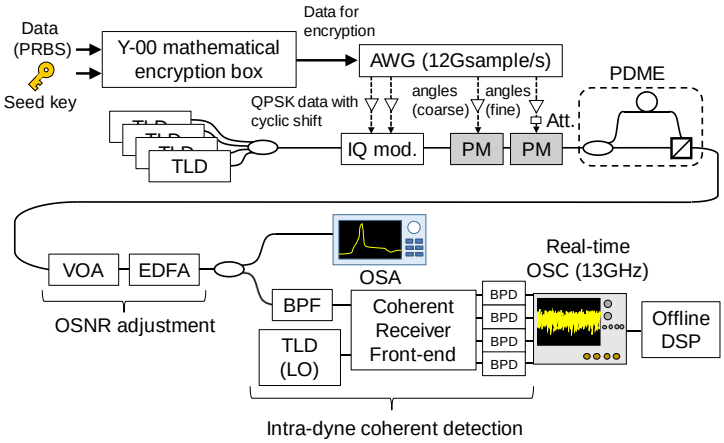
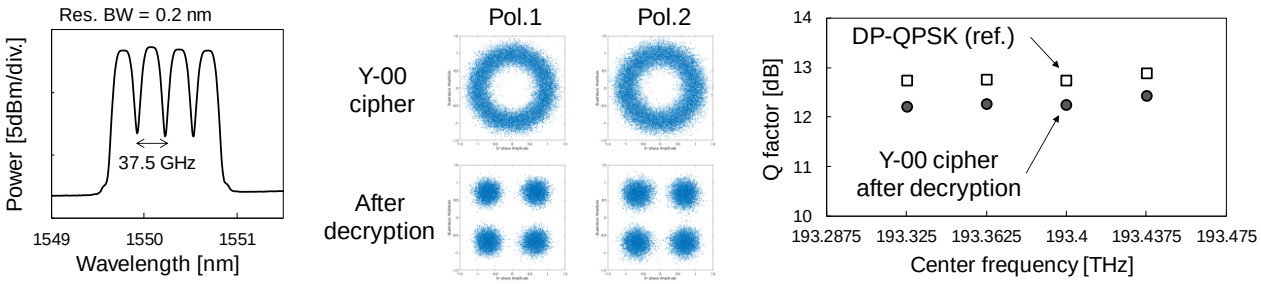


図 12: 4 波長×48-Gbit/s PSK Y-00 暗号の暗号化・復号化の実験系



(a) (b) (c)

図 13: 4×48-Gbit/s PSK Y-00 暗号の実験結果 (a) 光スペクトラム，(b)コンスタレーション，(c)Q 値

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距離の関係

量子雑音によるマスキングの効果を定量的に扱うために，マスキング量を定義する．データ変調を BPSK として基底のビット数を m としたとき，マスク量は，図 2 における量子雑音による信号の不確定性を表す角度と隣接する信号のなす角度の比として，

$$\Gamma = \frac{\Delta\phi_{\text{shot}}}{\Delta\theta_{\text{basis}}} = \frac{2^{(m-1)}}{\pi}\sqrt{\frac{R\cdot h\nu_0}{P_0}} \tag{3}$$

と表される．ここで，R, h, ν_0, P_0 は信号のシンボルレート，プランク定数，信号の周波数，光パワーである．この値は，量子雑音が覆う暗号化後の信号の数であり，大きいほど信号受信時の不確定性が大きくなる（エラーの確率が上がる）ため，暗号として安全になる．

次に伝送路のモデルを定義する．ここでは，最もシンプルな均一な伝送路を仮定する．図 14 に示すように，光ファイバ伝搬による損失が光増幅器により完全に補償されるとする．スパン長 L は共通とする．このような伝送路で非線形効果の影響が無視できるほど小さい線形伝送が行われた場合，受信端での OSNR は，

$$\begin{aligned} OSNR_{\text{out}} &= \frac{P_0}{N\cdot 2n_{sp}h\nu_0\Delta\nu_{\text{noise}}(G-1)} \\ &\approx \frac{P_0}{N\cdot 2n_{sp}h\nu_0\Delta\nu_{\text{noise}}G} \end{aligned} \tag{4}$$

と見積もられる．$N, n_{\text{sp}}, \Delta\nu_{\text{noise}}, G$ は，スパン数，光増幅器の反転分布係数，OSNR を規定するノイズ帯域幅（通常 0.1nm），光増幅器のゲインである．ここで，受信端で十分な信号品質を確保するために必要とされる OSNR を $OSNR_{\text{req}}$ としたき，式(3)と(4)から，伝送可能な最大スパン数 $N_{\text{Y00\_max}}$ は，

$$N_{\text{Y00\_max}} = \left\lfloor \frac{2^{2(m-1)}R}{2n_{sp}\pi^2\Delta\nu_{\text{noise}}G\cdot OSNR_{\text{req}}}\cdot\frac{1}{\Gamma^2} \right\rfloor \tag{5}$$

となる．BPSK のデータ変調のとき OSNR はビット当たりの信号対雑音比 E_b/N_0 と以下の関係となる．

$$OSNR = \frac{E_b}{N_0}\cdot\frac{R}{2\Delta\nu_{\text{noise}}} \tag{6}$$

よって，(5) 式は，

$$N_{\text{Y00\_max}} = \left\lfloor \frac{2^{2(m-1)}}{n_{sp}\pi^2 G\cdot\left(\frac{E_b}{N_0}\right)_{\text{req}}}\cdot\frac{1}{\Gamma^2} \right\rfloor \tag{7}$$

と表すことができる．受信端で必要とされるビット当たりの信号対雑音比$(E_b/N_0)_{\text{req}}$ は，ターゲットとする BER から，シンボルレートなどによらず一意に決まる．式(7)より，受信端での必要 BER（例えば FEC 閾値）と目標のマスク数を決めると，伝送可能なスパン数，つまり，伝送可能距離が決まる．このとき，この関係はシンボルレートに依存しないということがわかる．これはこの暗号をさらに高速化するうえで極めて好ましい特性である．

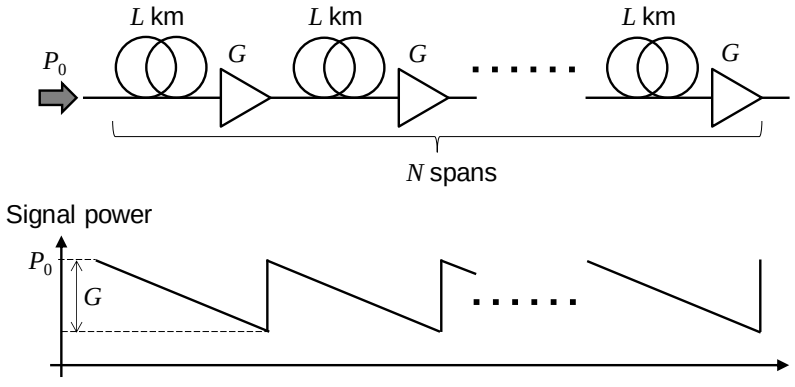


図 14：光ファイバ伝送路のモデル

3-2 数値計算結果

Y-00 暗号の長距離伝送について式(7)を用いて具体的に考察する．まず日米海底間などの超長距離伝送について考える．表 1 に数値計算の条件を示す．スパン長 L は 60km とし，極低ロスの光ファイバを用いる場合とする．図 15 に基底ビット数 m を変化させたときのマスキング量と伝送距離の関係を示す．m=16 としたとき，10,000km の伝送において 100 以上のマスク量を達成できることがわかる．次に，陸上系の長距離伝送について考える．表 2 に数値計算の条件を示す．スパン長 L は 100km とし，典型的なロスの光ファイバを用いる場合とする．図 16 に基底ビット数 m を変化させたときのマスキング量と伝送距離の関係を示す．m=16 としたとき，2,500km の伝送で 100 以上のマスク量を達成できることがわかる．このように，Y-00 暗号では基底数を十分大きくとることでセキュアな長距離伝送を実現できる．

TABLE I

SIMULATION PARAMETERS IN ULTRA-LONG-HAUL TRANSMISSION

Item	Value
Fiber span length: L	60 km
Fiber loss	0.155 dB
Amplifier gain: G	9.3 dB
Noise figure of amplifier: $2n_{sp}$	5.0 dB
Target BER (HD-FEC threshold)	3.8×10^{-3}

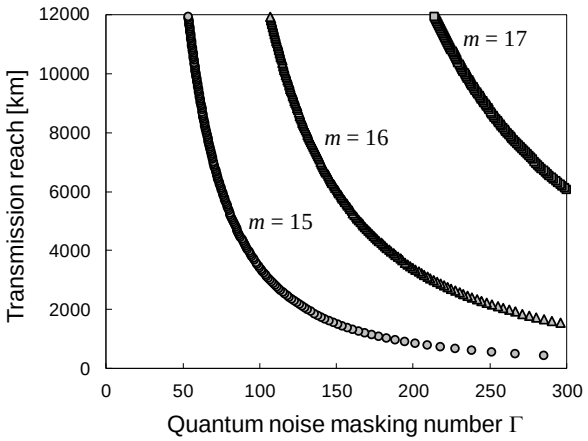


図 15：超長距離伝送における伝送距離とマスキング量の関係のシミュレーション結果

TABLE II

SIMULATION PARAMETERS IN LONG-HAUL TRANSMISSION

Item	Value
Fiber span length: L	100 km
Fiber loss	0.18 dB
Amplifier gain: G	18.0 dB
Noise figure of amplifier: $2n_{sp}$	5.5 dB
Target BER (HD-FEC threshold)	3.8×10^{-3}

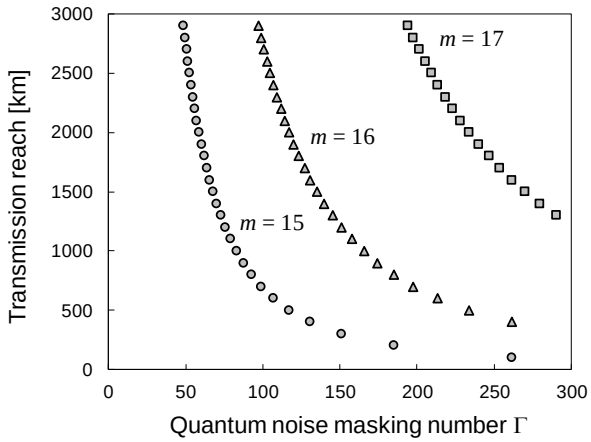


図 16：長距離伝送における伝送距離とマスキング量の関係のシミュレーション結果

5 まとめと今後の展望

本助成による研究により，偏波多重と波長多重技術を導入することでデジタルコヒーレント方式の PSK Y-00 暗号の大容量化を達成した．チャネル当たり 48Gbit/s の Y-00 暗号の 800km 光ファイバ伝送を実証した，また，安全性と通信性能に関する理論的な検討を行い，そのトレードオフを明らかにした．数値計算により，16 ビット程度の大きな基底数とすることで 10,000km 級の長距離の光ファイバ伝送においても，高い安全性と信号品質を両立できることを示した．理論検討では，安全性と信号品質のトレードオフは暗号のシンボルレートに依存しないことが明らかになった．よって，現状 12Gbaud のシンボルレートを高速化することにより現状の光ファイバ通信システムで用いられるチャネル当たり 100Gbit/s 級のセキュアな光ファイバ伝送が期待できる．

【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 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.
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. M. Yoshida, T. Hirooka, K. Kasai, and M. Nakazawa, "Single-channel 40 Gbit/s digital coherent QAM quantum noise stream cipher transmission over 480 km," Opt. Express 24, 652-661 (2016).
12. 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).
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. Seb J. Savory, "Digital filters for coherent optical receivers," Opt. Express 16, 804-817 (2008).
15. B. Szafraniec, B. Nebendahl, and T. Marshall, "Polarization demultiplexing in Stokes space," Opt. Express 18, 17928-17939 (2010).
16. 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).

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Single channel 48-Gbit/s DP-PSK Y-00 quantum stream cipher transmission over 400- and 800-km SSMF	*Optics Express*	2019年　9月
Multi-Channel Simultaneous Encryption in WDM Systems of PSK Y-00 Quantum Stream Cipher	*25th Opto-Electronics and Communications Conference (OECC 2020)*	2020年　10月（発表予定）
Digital coherent PSK Y-00 quantum stream cipher for secure and high-capacity optical transmission systems	*Asia Communications and Photonics Conference 2019 (ACP2019)*	2019年　11月
48-Gbit/s Dual-Polarization PSK Y-00 Quantum Stream Cipher Based on QPSK Data Modulation	*24th Opto-Electronics and Communications Conference (OECC 2019)*	2019年　7月
48-Gbit/s PSK Y-00 光通信量子暗号の800-km光ファイバ伝送	電子情報通信学会 2020 年総合大会	2020年　3月