光通信量子暗号(Y-00)による超大容量光ファイバ暗号通信システムに関する研究

研究代表者　　二　見　史　生　　玉川大学　量子情報科学研究所　准教授

1 はじめに

昨年，元 CIA 職員の E. Snowden の証言により，英国の情報共同体の諜報機関である政府通信本部(GHCQ：Government Communications Headquarters)が光ファイバ通信回線から信号光を盗み出し，電子メールなどの通信情報を傍受して，個人情報や国家機密情報を盗み読みしていたことが公になった[1]．一方，米国防高等研究計画局(DARPA)が，目標伝送容量 1～10 Gbit/s，伝送距離 1,000～10,000 km という巨視的量子通信を利用した物理暗号プロジェクト「Quiness」[2]を実施しており，物理層である光ファイバ通信回線に物理暗号を導入することはネットワークでは必須の状況になってきている．光ファイバ通信回線は大量データが流通しているので，情報漏洩がないように，実用的な盗聴防止技術の確立が急務である．

現状，一部の通信情報は数理暗号(SSL, IPsec 等)で暗号化されている．数理暗号は実用的な点が特長だが，その安全性は主に計算量的安全性を拠としているため，解読手法が発見されると計算量が激減する危険性が避けられない．数理暗号解読の歴史[3-5]を振り返ると，数理暗号は盗聴の危険性を排除できない．複雑な数式を用いれば暗号強度を高めることができるが，暗号化・復号化に時間を要し，通信のレイテンシーが課題となる．

暗号には，数理暗号と，通信方式を暗号化する物理暗号がある．物理暗号は，特に，通信回線を守るために用いる暗号で，暗号文を盗ませない点で，数理暗号と異なる．光通信量子暗号(Y-00)は，従来の数理暗号概念にはない新たな暗号で，数理的なアルゴリズムによる解読法を無効にし，理論的に高い安全性が示されている[6]．それ故，数理暗号を凌ぐ高い安全性を確保した高セキュアネットワーク構築に繋がる有望な暗号である．物理暗号を数理暗号と併用すれば，光ファイバ回線の安全性を飛躍的に高められる．

著者等は，実用的な物理暗号として，光通信量子暗号(Y-00)の研究開発を行ってきている．その中で課題の一つに，昨今の通信情報量の飛躍的な増大に対応するため，暗号通信の大容量化が指摘されている．Y-00 暗号は，多値信号を使う方式で過剰な帯域を必要としない点が一つの特徴である．それ故，異なる波長の信号を複数多重して一つの光ファイバで通信する波長分割多重技術により，通信容量を増大することが可能である．

本研究調査では，波長分割多重技術による光ファイバ暗号通信システムの伝送容量の超大容量化に向け，通信容量 100 Gbit/s の超高速・大容量光ファイバ暗号通信システムの基盤技術である送受信機技術の実験検証を実施した．はじめに，Y-00 暗号信号光の波長多重技術，波長分離技術の検討を行い，多重分離方法を明らかにした．次に，波長分割多重時に検討を要する周波数利用効率について評価実験を行った．最後に，実際に多重分離装置を試作し，通信容量 100 Gbit/s の光ファイバ暗号通信を実現した．

2 通信容量 100 Gbit/s の光ファイバ暗号通信システム

2-1 Y-00 暗号の基本構成

Y-00 暗号は，高速データを暗号化するストリーム暗号の一種で，正規通信者同士は古典的通信理論に基づいている．それ故，現在実用化されている光ファイバ通信部品を利用できる．盗聴者は量子効果が避けられず，そこで発生する量子雑音が安全性の拠り所になる．送信端では，送受信間で共有する暗号鍵列(K_S)を基に乱数生成器(PRNG)で生成する擬似乱数により拡張したランニング鍵系列で，ビット毎に基底(2 値データを送信する信号の組み)を切り換え，2 値の平文を変調する．基底数を M とすると，2M のレベル数の信号光が生成される．これが暗号文で，Y-00 信号光と呼ばれる．

一方，受信端では，共有している暗号鍵から送信端と同一の基底情報を用意し，これに合わせ信号識別点をビット毎に移動させ，Y-00 信号光から平文を復号する．暗号鍵を持つ正規受信者は情報を受信することができるが，暗号鍵を持たない盗聴者は，識別点が分からない．また，正しい Y-00 信号光レベルの認識は，基

底数を大きくすれば，受信時に発生する雑音により困難になる．雑音が信号レベルをマスクする現象をマスキング効果と呼ぶが，盗聴者が量子雑音限界の測定ができる受信機を持ったとしても，受信時に発生が避けられない量子雑音がマスクする．

2-2 強度変調方式 Y-00 の原理

2 値信号(平文)を強度変調 Y-00 信号光に暗号化する方法，およびその逆の復号原理の概要を，図 1 を参照して説明する[7].

① 擬似乱数発生器(PRNG：Pseudo-Random Number Generator)で，初期鍵(Seed key)を拡張し，2 値ランニング鍵(Running key)を生成．現状，PRNG として，線形帰還シフトレジスタ(LFSR: Linear Feedback Shift Register)を代用している.

② OSK(Overlap Selection Keying)において，ビット毎に 2 値ランニング鍵と入力信号の排他的論理和(XOR)をとり，”0”,”1”の極性をスクランブル.

③ M-ary で，2 値ランニング鍵を logM ビット(M:基底数)にブロック化し基底選択信号(Y-00 信号の DC バイアスレベルに相当)を生成.

④ Mapper では，基底選択信号と M 値信号を対応付け.

⑤ Key DSR(Deliberate Signal Randomization)で，受信時の雑音が拡散して見えるよう，基底選択信号値の確率分布を補正

⑥ Driver において，OSK でスクランブルした信号を，⑤の基底選択信号でビット毎に変調し，2M 値の電気信号を生成.

上記処理で生成した電気信号でレーザ駆動電流を変調し，強度変調 Y-00 信号光を生成する．受信端では，光検出器で Y-00 信号光を直接検波し電気信号に変換後，送信時の処理と逆の処理を行い，元の平文に復号する．復号時には，送信機と同一の暗号鍵を基に生成した送信端と同一のランニング鍵が必要．ランニング鍵により，正しい閾値判定および識別が可能になる．なお，正規受信者には復号時に Keyed DSR の影響はないので，その復号機能は必要ない.

図 2 に波形の模式図を示す．雑音が十分発生するように設計すると，受信時，Y-00 信号光のレベルが雑音に埋もれるが，暗号鍵により基底選択信

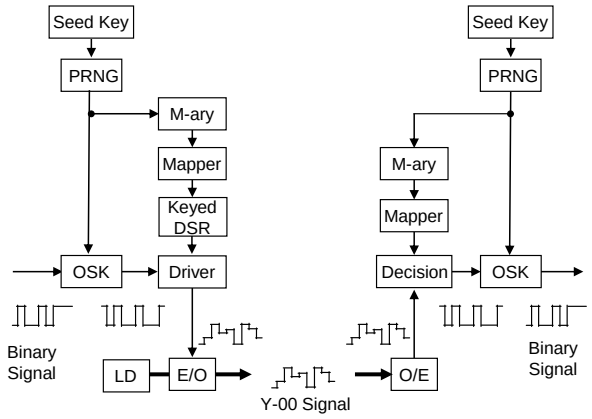


図 1　Y-00 暗号の暗号・復調

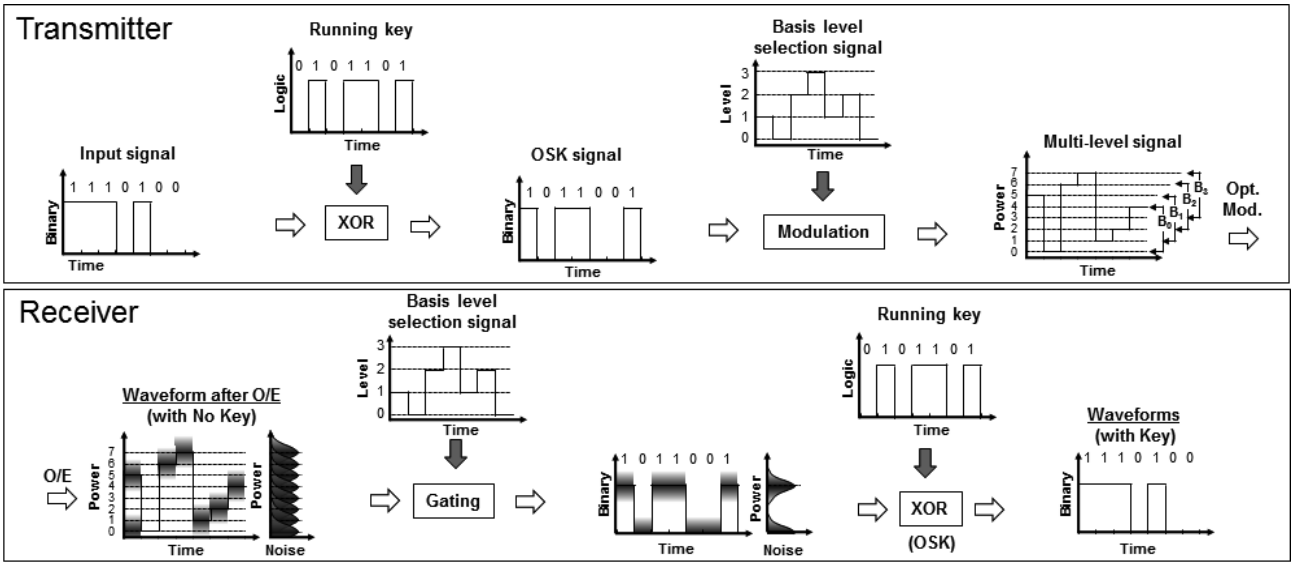


図 2　Y-00 暗号送受信器主要部の波形の模式図

号情報が得られ，適切な信号識別が可能で正しい情報を受信できる．

①で鍵長 256 ビットの暗号鍵から鍵長 2^{256} (~ 10^{77})のランニング鍵を生成する．擬似乱数発生器として，現状は，LFSR を使用している．ランニング鍵は疑似乱数で，その繰り返しは約 10^{77} 毎になる．これは，伝送容量 2.5 Gbit/s の場合，10^{52} 億年の間，繰り返しがないことを意味する．②の OSK は，通信情報で連続した”0”や”1”，また，繰り返される情報をスクランブルし，既知平文攻撃を暗号文単独攻撃に転ずる．④の Mapper で，2 値の情報の閾値を変調するバイアスレベルをビット毎に設定する．Y-00 信号は多値信号になるが，それぞれのビットは 2 値で，バイアス(=基底)が複数のレベルになっている．

2-3 波長多重技術・多重分離技術の理論検討

波長 1.55 μm 帯において，効率的に 100 Gbit/s 暗号信号光を多重する方式に関して，理論検討を行った．Y-00 暗号は超多値変調信号を用いることにより，その強い安全性を実現できる．国内外の国際会議・研究会から関連する情報収集を行い,本検討では,多値数は 6 ビット(64 値)とした.著者等が研究開発している Y-00 暗号光の生成は強度変調方式なので，変調帯域以上にスペクトルが拡散しない．効率的に 100 Gbit/s を収容するために適した変調速度は，64 の多値変調を実現するのに，分解能が 6 ビット以上のデジタル・アナログ変換器(DAC)が必要なので，DAC の動作帯域を最大 10 Gbit/s とし，変調速度 2.5 Gbit/s と 10 Gbit/s について理論比較した．各変調速度で変調時の所要波長は，表１に示すように，それぞれ波長数は 40 波長，10 波長になる．波長数が多くなると，システム運用時の監視や制御が煩雑になる．そこで，システム運用時も考慮に入れ，100 Gbit/s 暗号信号光の収容方式は，波長数が少ない 10 Gbit/s の変調速度で，波長数 10 とし，実験評価することにした．

表１：100 Gbit/s 暗号信号光の変調速度と所要波長数の関係

変調速度 (一波長当たり)	2.5 Gbit/s	10 Gbit/s
波長数	40	10
備考	波長数が多く取り扱い難	波長数は適当

次に，波長多重した暗号信号光の多重分離について，理論検討を行った．一般に，複数の波長を多重した信号光を波長分離するには，光帯域透過フィルタ(OBPF)の使用が有効である．波長数が多数の場合，波長毎に直列に OBPF を挿入すると，光損失が大きくなるために，通信特性が劣化してしまう．例えば，光カプラを用いて 10 波長の信号光を直列に分岐すると，光カプラの理論分岐損失だけで 12 dB を上回り，信号品質の劣化に繋がる．そのため，損失が比較的少なく分岐できる 1 対 N 型に分岐可能な干渉型光フィルタを波長分離に採用することが適切である．次に，干渉型光フィルタの波長間隔に関して理論検討を行った．検討では，変調速度が 10 Gb/s で，帯域は C バンド帯(通常光ファイバ通信で用いられる波長帯で，1530 - 1565 nm)とした．光ファイバ通信では，通常，ITU-T(International Telecommunication Union Telecommunication Standardization Sector：電気通信標準化部門)勧告に準拠する．G.671 では，12.5 GHz，25 GHz，50 GHz,100 GHz および 100 GHz の整数倍が周波数グリッドとして規定されている．暗号通信システムが実際の光ファイバ通信システムと整合するように，本勧告に準拠させることにした．強度変調の 10 Gbit/s を 12.5 GHz 間隔に収容することはできないので，最も狭くても 25 GHz となる．10 Gbit/s の信号光を 10 波長収容する場合の周波数間隔と所要帯域の関係を表 2 に示す．隣接波長信号光とのクロストークを小さくするという観点からは，周波数間隔は大きい方が良い．一方，周波数利用効率も重要である．周波数利用効率とは，単位周波数当たりどれだけの情報の通信ができるかということで，限られた帯域を有効に利用することに繋がる．周波数利用効率を高めるという観点からは，より周波数間隔を狭めた方が良い．このように，隣接チャネルとのクロストークと周波数利用効率向上との間には，トレードオフの関係がある．本研究調査では，周波数間隔を 50 GHz とすることにした．

表 2：周波数間隔と 100 Gb/s 波長分割多重時の所要帯域の関係

周波数間隔	25 GHz	50 GHz	100 GHz	200 GHz
所要帯域	1.9 nm	3.8 nm	7.5 nm	15 nm

2-3 周波数利用効率評価実験

周波数利用効率の実験評価を行った.評価実験では,情報容量 2.5 Gbit/s の Y-00 暗号を 3 波長用意して,波長間隔をどれだけ狭めることができるか評価した.2.5 Gbit/s で評価を行ったが,本評価結果は 10 Gbit/s にもスケーリングが可能である.

図 3 に評価実験の構成を示す.異なる秘密鍵を有する 2 台の Y-00 変調器を用いた.1 台には,波長$\lambda_{\#2}$ = 1548.1 nm(波長固定)の連続光を入力した.もう 1 台には,2 波長($\lambda_{\#1}$, $\lambda_{\#3}$)の連続光を入力した.この 2 波長は可変とした.3 波長は,$\lambda_{\#2}$を中心とし,間隔が常に等しくなるよう設定し,波長間隔を調整した.2 台の Y-00 変調器から出力される Y-00 信号光を光カプラを用いて一つの光ファイバに入力し,3 波長の Y-00 信号光を生成した.

波長分割多重した 3 波長から,中心チャネル(波長$\lambda_{\#2}$)の信号を,光バンドパスフィルタを用いて分離した.光検出器(O/E)を用いて Y-00 信号光の強度を検波し,電気信号に変換した.電気信号を分岐し,一方から同期クロックを抽出し,他方は識別回路を経由して,OSK 回路で元の 2 値情報を復元した.抽出した同期クロックを用いて符号誤り率(BER)を評価した.透過帯域は約 0.1 nm(～12 GHz)の光バンドパスフィルタを波長分離に用いた.

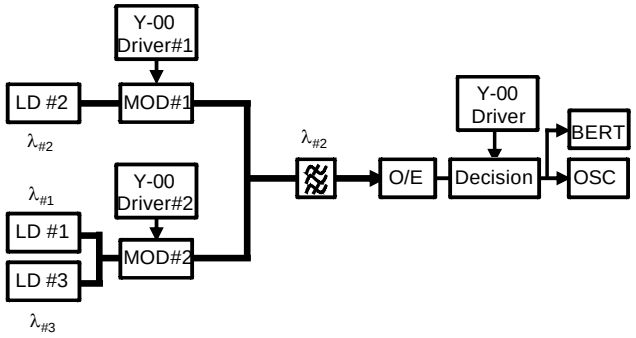


図３　周波数利用効率評価実験系

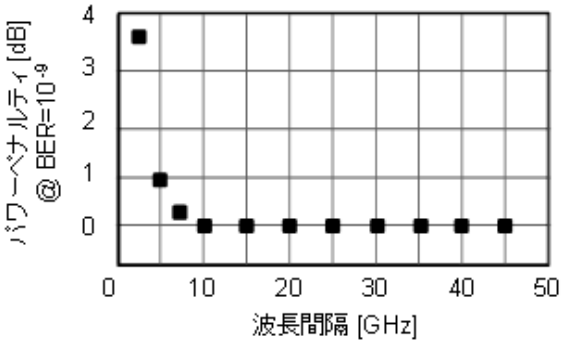


図４　波長間隔に対するパワーペナルティ

BER = 10^{-9} になる受信器入力パワーに対するパワーペナルティを波長間隔の関数として測定した.その結果を図 4 に示す.波長間隔が 10 GHz よりも広い場合は,パワーペナルティは発生しなかった.即ち,異なる波長の信号光を完全に分離できている.一方,波長間隔が 10 GHz よりも狭くなると,徐々にパワーペナルティが発生し,クロストークが生じていることが分かった.

波長間隔が 20 GHz と 5 GHz の場合の Y-00 信号光およびその復号波形を図 5(a), (b)に示す.Y-00 信号光波形は両方共に同様で,大きな相違は見られなかった.Y-00 信号光は多値なので雑音にマスクされ,アイ開口を観測でない.一方,識別判定後の 2 値波形のアイ開口も両方ともに明瞭である.しかしながら,(b)5 GHz の場合,隣接チャネルとのクロストークが原因で誤った値に識別判定されているため,良好なアイ開口が得られているにもかかわらず,符号誤りが生じ,パワーペナルティが発生していた.

現状,1 dB のパワーペナルティを許容すると,周波数利用効率(SE : Spectral Efficiency)は,SE = 0.5 bit/s/Hz 程度である.本実験で使用した光バンドパスフィルタの帯域が 0.1 nm 程度なので,このような結果になったが,より狭帯域の光バンドパスフィルタを使用すれば,パワーペナルティが発生する波長間隔はより狭められ,周波数利用効率の向上が期待できる.ただ,信号光の変調速度が 2.5 Gbit/s の場合,透過帯域 5 GHz の理

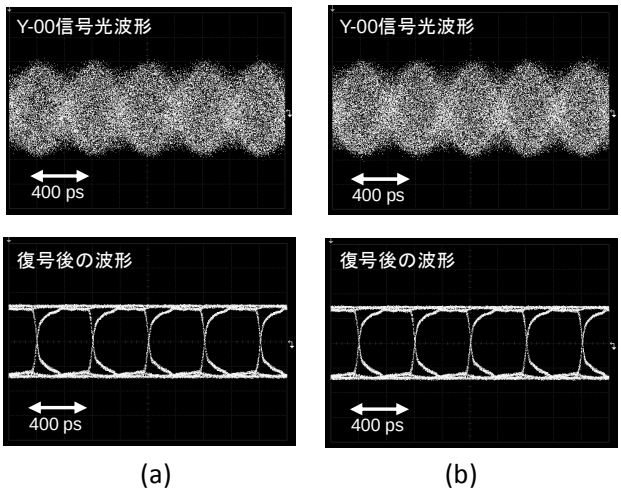


図５　Y-00 信号光波形と復号後の 2 値信号光波形.
波長間隔 : (a) 20 GHz, (b) 5 GHz

想的な光バンドパスフィルタを用いても，周波数利用効率を 1 より大きくすることはできない．

この結果を 10 Gbit/s の場合にスケーリングすると，透過帯域が 0.4 nm の光バンドパスフィルタを使用した場合，波長間隔が 40 GHz を下回ると，隣接チャネルのクロストークによりパワーペナルティが発生することが分かった．

2-4 通信容量 100 Gb/s の光ファイバ暗号伝送実験

まず初めに，図 6 に示す実験系で，単一波長の強度変調 Y-00 信号光(10 Gbit/s)の伝送実験を行った．波長は 1551.7 nm に設定し，信号レベル数 64 とした．設計上，盗聴者が正しい暗号レベルを識別できない程の雑音が発生するよう信号光の SNR は 3 dB 程度に設定した．伝送路は全長 120 km の光ファイバで，40 km 毎に，光ファイバ伝送時に発生する信号光パワー減衰を光ファイバ増幅器(EDFA ： Erbium-doped Fiber Amplifier)で補償した．各光ファイバ入力パワーは Pin = − 3 dBm 程度とした．

図 7(a)，(b)に伝送前後の Y-00 信号光および共通鍵を用いて識別し復号した電気信号波形を示す．Y-00 信号光は，直接検波で測定した．Y-00 信号光は 2048 値の強度レベルなので，伝送前でも，雑音が最小の信号強度レベル差よりも大きく，アイ開口を観測することができない．これは，雑音が信号光レベルをマスクしており，このマスキング効果により盗聴者は正しい信号レベルを識別できない，即ち，暗号文を盗聴できないことを示している．一方，共通鍵を持っている正規受信者は，共通鍵を用いて送信機で使用した基底選択信号と同一の基底選択信号で正しく識別判定できる．図 7 に識別判定後の 2 値信号を示しているが，きれいなアイ開口を観測できる．これらの符号誤り率(BER)を測定し，信号の品質を評価した．送信前，送信後共に BER ＜ 10^{-9} を達成しており，高品質な暗号通信ができることを検証できた．

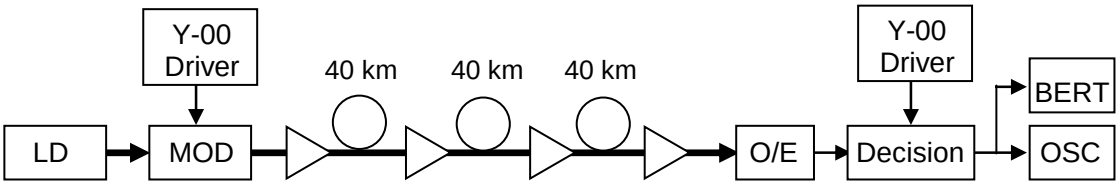
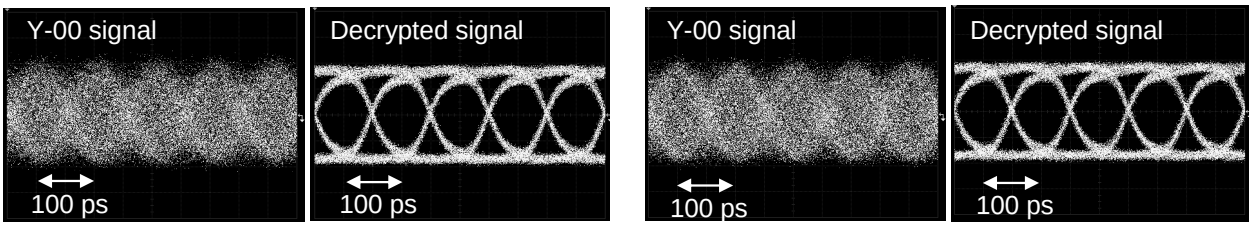


図６　単一波長の強度変調 Y-00 信号光(10 Gbit/s)の伝送実験系構成



(a)伝送前　　(b) 120 km 伝送後

図７　Y-00 信号光波形と復号後の２値波形．(a)伝送前，(b)120km 伝送後

次に，図 8 に示す実験系で 100 Gbit/s(10 波長 x 10 Gbit/s) 波長分割多重信号の伝送実験を行った．波長チャネル数は 10 波長，波長(周波数)間隔は 50 GHz，各波長は表３に示す ITU-T 勧告に準拠した値に設定した．波長分割多重には，低損失で 10 波長の光を波長多重できるよう，干渉型光フィルタであるアレイ導波路グレーティング(AWG ： Arrayed Waveguide Grating)を用いた．次に，$LiNbO_3$ 変調器で 10 波長の連続光を一括して基底選択信号でビット毎に 10 Gbit/s で変調し，レベル数 4096 の 10 波長の強度変調 Y-00 信号光(合計容量 100 Gbit/s)を生成した．伝送路構成は前節の単一波長伝送実験と同じく長さ 40 km の光ファイバを１スパンとして，3 スパンで全長 120 km とした．各スパンの光ファイバへの入力パワーは，単一波長伝送と同じく一波長当たり P_{in} = − 1 dBm 程度とした．

表 3：100 Gbit/s 暗号信号光の設定波長

ﾁｬﾝﾈﾙ	Ch. 1	Ch. 2	Ch. 3	Ch. 4	Ch. 5	Ch. 6	Ch. 7	Ch. 8	Ch. 9	Ch. 10
波長 (nm)	1549.7	1549.7	1549.7	1550.9	1551.3	1551.7	1552.1	1552.5	1552.9	1553.3

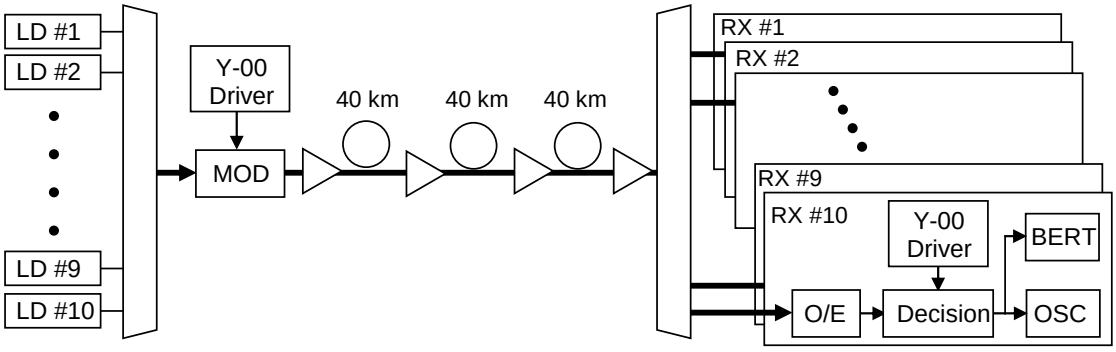


図８　100 Gbit/s の強度変調 Y-00 信号光伝送実験系構成

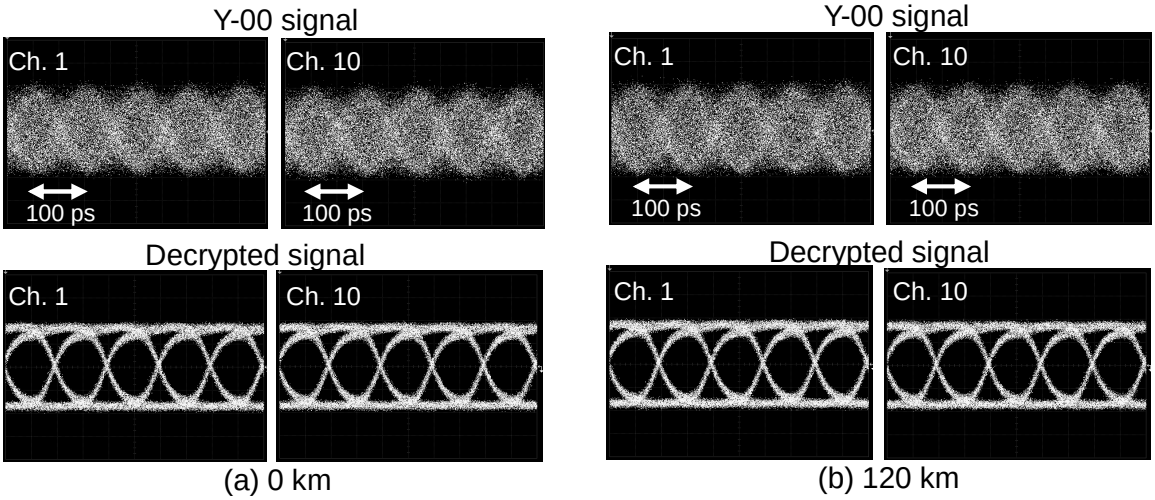


図９　100 Gbit/s 伝送時の Y-00 信号光波形と復号後の２値波形．(a)伝送前，(b)120km 伝送後

受信端では，まず，送信端と同様に，低損失の AWG を用いて 100 Gbit/s(10 波長)の信号光を，波長分離し，10 Gbit/s 毎に分けた．AWG はフラットトップの波長透過特性で，隣接チャネル間のクロストークは 26 dB(1/400)以上の小さな値で，この AWG により高品質の波長分離を実現した．次に，それぞれの波長の 10 Gbit/s 信号光を PD で電気信号に変換後，その電気信号からクロックを抽出した．また，共有鍵を用いて識別判定し，信号レベル 64 の Y-00 信号を 2 値信号に復号した．伝送前後の BER を測定した．

図 9(a)に，送信端(伝送距離 0 km)で，AWG で各波長に分離後に直接検波で観測した Y-00 信号光波形，および平文(2 値信号)への復号後の電気信号を示す．10 チャネルあるが，図中には，Ch. 1 と Ch. 10 を表示した．他のチャネルも同様の波形を観測できた．Y-00 信号光は信号レベル数が 64 なので雑音によりアイ開口をみることはできないが，共有鍵に基づく識別操作により，2 値の平文電気信号に復号すると，良好なアイ開口を観測できる．10 チャネル全ての 2 値信号の BER を測定し，全てのチャネルで 10^{-9} 以下を達成することを確認した．

次に，120 km 伝送後の光スペクトルを図 10 に示す．Y-00 信号光は，CW 光を 64 値の電気信号で強度変調した強度変調信号光なので，他の Y-00 信号光の波長域にスペクトルが拡散していない．それ故，WDM 方式により，他のチャネルに影響無く，多重することができる．本実験では，装置の制約上，波長間隔を 50 GHz としたが，この間隔を狭め，周波数利用効率の向上を図ることができる．120km 伝送後でも，

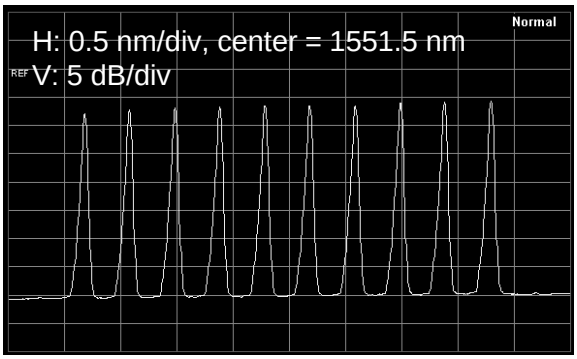


図１０　120km 伝送後の光スペクトル

光信号対雑音比(OSNR)は，30 dB/0.1nm 程度以上を確保できていた．スペクトル解析では，伝送路の光ファイバ中で四光波混合などのチャネル間の非線形相互作用は発生せず，線形伝送特性だった．光スペクトルを見ると，若干信号光強度が異なっている．この原因は,中継に使用した EDFA の利得特性が波長に対して平坦ではなく，波長依存性があるためである．

120 km 伝送後，波長分波，強度検波して測定した Y-00 信号光波形,および平文電気信号を図 9(b)に示す．図内では，Ch.1 と Ch.10 の波形しか示していないが，全チャネルにおいて，前節の単一波長での伝送後の波形と同様の波形が得られた．チャネル間の相互作用無く WDM 伝送できることを示している．

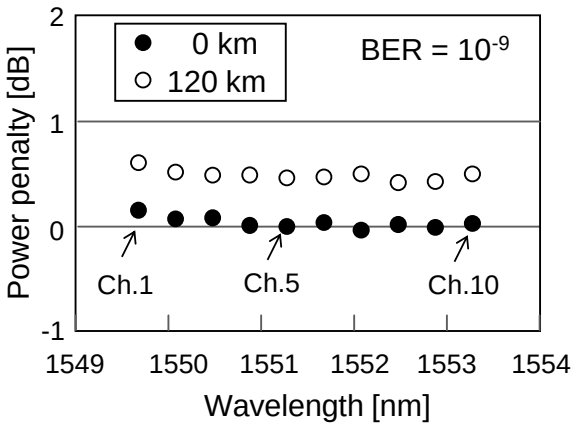


図１１　パワーペナルティ(@BER=10^{-9})

復号後の電気信号の BER を測定した．図 11 に，BER=10^{-9} の時のパワーペナルティを示す．●印が送信端で測定した値で，○印が 120 km 伝送後の値を示す．伝送前，伝送後共に，チャネルにより若干パワーペナルティが異なっているが，これは主に測定誤差に起因していると考えられる．120km 伝送後は，各チャネル共に 0.5 dB 程度のパワーペナルティが発生しているものの，全てのチャネルで BER = 10^{-9} を達成でき，100 Gbit/s の暗号通信ができたことを示している．

以上，Y-00 信号光の波長分割多重および多重分離装置を用いて，レベル数 64 値，一波長当たり 10 Gbit/s の強度変調 Y-00 信号光を 10 波長多重し，合計通信容量 100　Gbit/s の暗号通信を実現し，本研究調査の目標を達成した.本実験結果は,Y-00 信号光を波長領域で多重することにより,適切な波長間隔を設計すれば，チャネル間の相互作用無しで，通信容量を増大できることを示すものであり，波長分割多重方式により，大容量の Y-00 暗号通信が可能なことを明らかにした．多重する波長数を更に増やすことにより，通信容量を更に大きくすることが容易にできる．具体的な見通しについては，次節にまとめて示す．

波長分割多重時に他の波長のチャネルとクロストークがないということは，波長分割多重光ファイバ通信システムの未使用のチャネルに Y-00 信号光を導入したり，もしくは，使用中のチャネルを Y-00 信号光に交換することにより，既存のシステムを暗号通信システムにアップグレードすることも可能である．

100Gbit/s 伝送実験では，伝送距離は 120km に設定した．これは主に実験部材の制限で制約されており，伝送距離の最適化の検討は行っていない．今後，光ファイバ伝送路の仕様の検討を行い，伝送距離の長距離化について研究開発を実施する．

2-5 更なる大容量化に向けた理論検討

波長数を増やすことにより，通信容量を増大できる点が WDM 方式の特徴である．どれだけの波長数を多重できるのかということが，大容量化への鍵になる．高密度で多重させるためには，隣接する波長間隔を狭くすればよい．そして，波長数を増やして通信容量を増大させる．波長間隔が狭すぎると隣接チャネル間でクロストークが発生し通信品質が劣化する．一方，利用できる帯域は，主に，光ファイバ増幅器の帯域で制限される．最後に，光ファイバ通信で一般的に用いられる C バンド帯域(1530-1565 nm)の 35 nm に利得帯域を限定して，更なる大容量化に向けた理論検討を行った．

波長 1.55 μm 帯で帯域 35 nm は，周波数に変換すると 4.4 THz 程度になる．前章で検証したように，周波数利用効率 SE = 0.5 bit/s/Hz は実現できる．この場合，通信容量は 2.2 Tbit/s 程度になる．波長当たりの信号光ビットレートを 10 Gbit/s とすると，220 波長程度を多重することになる．

周波数利用効率は SE = 0.5 bit/s/Hz として計算したが，更に効率が良い場合の所要波長数と周波数利用効率の関係を図 12 に示す．波長当たりのビットレートは，■が 10 Gbit/s，▲が 40 Gbit/s，●が 100 Gbit/s を表している．

図 13 に周波数利用効率と通信容量の関係を示す．利得帯域を 4.4 THz としているので，周波数利用効率に対して伝送容量が一意に決まる．そのため，図 12 と異なり波長当たりのビットレートには無関係になっている．例えば，周波数利用効率を向上し周波数利用効率 SE = 0.7 bit/s/Hz を実現できると，容量は 3 Tbit/s を上回る．

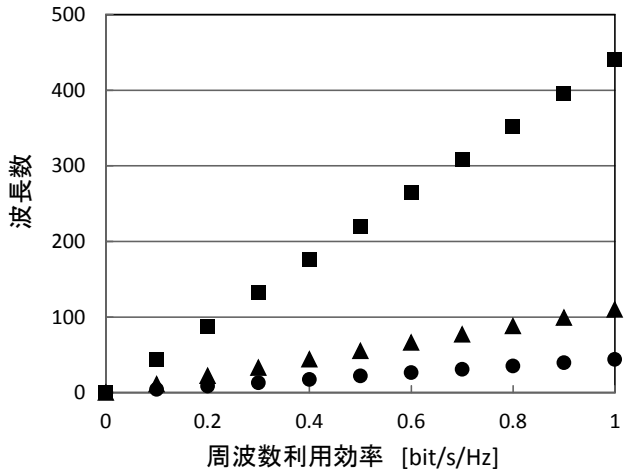


図１２　所要波長数と周波数利用効率の関係

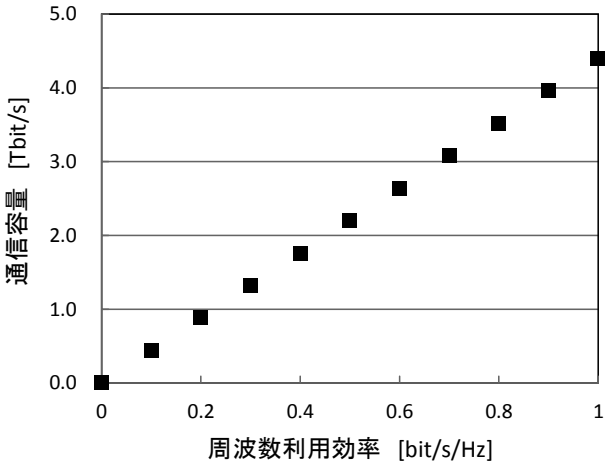


図１３　通信容量と周波数利用効率の関係

以上の検討をまとめると，光ファイバ増幅器の利得帯域を 4.4 THz(35 nm)とすると，周波数利用効率 SE = 0.5 bit/s/Hz の場合，通信容量は 2.2 Tbit/s を実現できる．波長あたりのビットレートが 10 Gbit/s だと波長数 220 波長，40 Gbit/s だと 220 波長程度必要になる．多重分離を改良して，例えば，周波数利用効率 SE = 0.7 bit/s/Hz を実現できれば，C バンド帯域に限定しても 3 Tbit/s を超える大容量通信の実現が可能になる．

3 まとめ

本研究調査では，通信容量 100 Gbit/s の超高速・大容量光ファイバ暗号通信システムの基盤技術である送受信機技術の実験検証を行うことを目標に，Y-00 暗号信号光の波長多重技術，波長分離技術の検討を行った．周波数利用効率が 0.2 bit/s/Hz で，通信容量 100Gbit/s の Y-00(光通信量子暗号)の光ファイバ暗号通信システムを実現した．Y-00 暗号は実用的な暗号で，新規技術や部品の開発が不要で，現在，一般の光ファイバ通信で用いられている部品・装置を使える点が特長で，Y-00 暗号の実用により，安全で安心して利用できる光通信システムの実現が期待される．

本研究では，通信容量 100 Gbit/s を目標に研究調査を実施したが，更なる大容量化が可能である．理論検討の結果，光ファイバ通信で一般に用いられる C バンド帯域(**波長 1530nm～1565nm，帯域 35nm**)において，テラビット毎秒以上の大容量暗号通信が可能であるとの見通しも得られた．通信容量 100Gbit/s の光通信量子暗号通信実験の伝送距離は 120km だったが，これは技術的な伝送距離限界ではなく，実験部材の数に制限された．伝送路の研究開発は今後の課題で，群速度分散など光ファイバのパラメータや光増幅器による中継間隔など設計し最適な光ファイバ伝送路を実現すれば，伝送距離は延伸可能である．

【参考文献】

[1] Gardian, “GCHQ taps fibre-optic cables for secret access to world's communications,” 21 June, 2013. http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[2] DARPA, “Quiness: Macroscopic Quantum Communications,” Solicitation Number: DARPA-BAA-12-42,https://www.fbo.gov/index?s=opportunity&mode=form&id=6a3a61d577305f71d9be268925c4b201&tab=core&tabmode=list&=

[3] E. Tews, R. Weinmann, and A. Pyshkin, Breaking 104 bit WEP in less than 60 seconds,” Cryptology ePrint, 2007

[4] 寺村亮一，曽谷紀史，仲神秀彦，朝倉康生，大東俊博，桑門秀典，森井昌克，“WEP の現実的な鍵導出法(その2)，” CSS2008 (Computer Security Symposium 2008)，(社)情報処理学会コンピュータセキュリティ研究会，vol.2008, no.8, pp.421-426, 2008 年 10 月．

[5] プレスリリース:富士通研究所, 情報通信研究機構, 九州大学, “次世代暗号の解読で世界記録を達成 ペアリング暗号の安全性を確立し、次世代暗号の標準化に貢献,”, http://pr.fujitsu.com/jp/news/2012/06/18.html
[6] O. Hirota, “Practical security analysis of quantum stream cipher by Yuen 2000 protocol,” Physical Review A ,76, 032307, 2007.
[7] 原澤克嘉, 広田修, 山下喜市, 本田真, 圷重人, 細井健司, 土井吉文, 大畠賢一, 片山武彦, 清水哲也, Yuen2000プロトコルによる物理暗号のためのRandomizationの実装回路の考察, 電子情報通信学会論文誌 C Vol.J91-C No.8, p.399, 2008.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
波長分割多重方式による Y-00(光通信量子暗号)の大容量化に関する検討	電子情報通信学会技術報告 OCS2013-71	2013 年 10 月
Y-00(光通信量子暗号)を用いたセキュア光アクセスシステムに関する実験検討	電子情報通信学会技術報告 OCS2013-89	2013 年 11 月
Experimental demonstrations of Y-00 cipher for high capacity and secure optical fiber communications	Quantum Information Processing, Springer	2014 年 6 月
100 Gbit/s (10 × 10 Gbit/s) Y-00 Cipher Transmission over 120 km for Secure Optical Fiber Communication between Data Centers	OptoElectronics and Communication Conference and Australian Conference on Optical Fibre Technology 2014	2014 年 7 月