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(継続)

代表研究者　　二　見　史　生　　玉川大学　量子情報科学研究所　教授

1 はじめに

通信情報量は増加の一途を辿り,光ファイバ通信システムの大容量化への期待は高まる一方である.現状,100 Gbit/s のトランシーバが実用化され，国内外の商用回線で使用されている．通信情報の中には第三者に見られると困る情報も含まれている．光ファイバでは大容量の通信ができる点は特長であるが，一方で，光ファイバ回線から情報が盗聴されると，膨大な量の情報が漏洩することになる．

光ファイバ回線からの情報盗聴の危険性は，以前から指摘されていたが，実際に光ファイバ回線にアクセスして情報を盗聴されることはないだろうと考えられていた．しかし，2013 年に元 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]．このような事態を予期してか,米国防高等研究計画局(DARPA)は，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 2012 年から開始した．このプロジェクトを契機に，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と考えられるようになってきている.前述の通り，現在商用利用され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・復号化に時間を要するので，通信のレイテンシーが大きくなり，双方向通信などアプリケーションによっては大きな課題となり得る.

暗号は，数式に基づく数理暗号と通信方式を暗号化する物理暗号に大別できる．数理暗号は暗号鍵を用いて 2 値の情報を 2 値の暗号に変換する.従って,暗号文を正しく読み取ることができる.一方,物理暗号は,主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おり[6],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．物理暗号と上位レイヤを守る数理暗号を併用すれば，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，Y-00 暗号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長である．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．昨年度の研究調査で，波長分割多重技術を用いて，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，実際に 100 Gbit/s の光通信量子暗号送受信器を構成し，通信容量 100 Gbit/s の光ファイバ暗号通信を実現した.

本研究調査では，100 Gbit/s の信号光の伝送特性を検討した．はじめに，数値解析用のシミュレータを構築した．このシミュレータを用いて 100 Gbit/s の Y-00 暗号信号光の伝送特性を解析した．群速度分散を有する単一モード光ファイバ(SMF)を伝送路に用いると，群速度分散の影響によりパルス波形が変化し，隣接チャネルとクロストークが発生し，これが伝送距離を 80 km 程度に制限されることを明らかにした．群速度分散が小さな分散シフトファイバ(DSF)伝送路の場合，無中継伝送を行うと，信号対雑音比の制限で，伝送距離は 70 km 程度に制限されることが分かった．最後に，DSF と光増幅中継器を用いた伝送路の場合，波長間の非線形効果が発生して，非線形効果により伝送距離が 520 km 程度に制限されることが分かった．シミュレーション結果に基づき，100 Gbit/s の Y-00 暗号信号光の伝送実験を行い，200 km 伝送時の実験結果からシミュレータの妥当性を検証した．SMF と分散補償ファイバを用いることにより非線形効果を抑圧して，更に伝送距離を延伸することが可能であるが，この伝送路の伝送特性については今後の課題とした.

2 数値解析

2-1 送信機・受信機のシミュレーションモデル

本研究では多値強度変調信号による Y-00 暗号を採用した．この多値信号は，送信機，受信機で共有している暗号鍵（シード鍵と LFSR）を基に生成するが，それらの伝送特性の数値解析のためのモデル化とシミュレータを構築した.以下に,構築したシミュレータのモデルについて概説する.実用化に向けた Y-00 暗号では，より強靭な暗号にするためのランダム化機構が組み込まれている．これらの機構を組み込んだ信号と組み込まない信号を比較すると，多値強度変調という点では違いはない．本研究の主旨は，多値強度変調信号の光ファイバ伝送時の伝送特性を解析することなので，本シミュレータでは，前述のランダム化機構は省いて，多値強度変調信号を生成した．図１に送信機において多値変調用の電気信号を生成するブロック図を示す.

① 擬似乱数発生器として，線形帰還シフトレジスタ(LFSR: Linear Feedback Shift Register)を用い，初期鍵(Seed key)を拡張し，2 値ランニング鍵(Running key)を生成．擬似乱数発生器は安全性の根幹に関わるが，数値計算用に LFSR を代用した.
② 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を生成.
③ 送信データ用信号を擬似乱数により生成.
④ 基底選択信号で送信データ信号をビット毎に変調し多値数 2M の多値信号生成.

以上の手続きで，多値数 2M の多値電気信号を生成する．この電気信号で LD から出力される連続(CW)光を変調し，多値振幅変調の信号光を生成する.
次に，受信端での信号処理について説明する.

① 送信端と共有している暗号鍵を基に送信端と同じ LFSR を用いてランニング鍵を生成.
② M-ary で 2 値ランニング鍵を logM ビット(M:基底数)にブロック化し識別信号を生成.
③ 多値数 2M の受信データを閾値信号を用いて識別し 2 値データに変換

以上の手続きで，送信端で送信した二値信号を受信することができる.

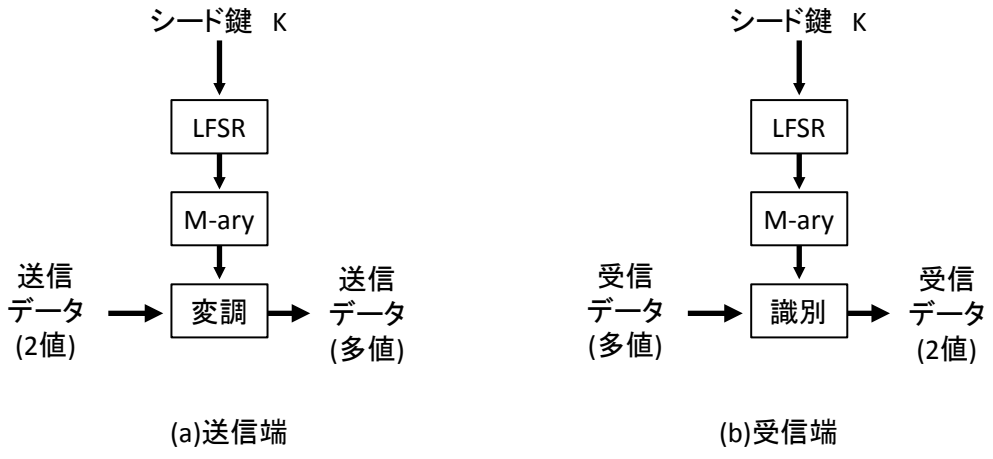

図 1：(a)送信端における 2 値送信データから多値信号生成方法．(b)受信端における多値信号から 2 値信号復号方法.

基底数 M の値により，多値信号の振幅数が異なる．例えば，基底数 M = 32 の時，振幅数は 2M = 64 値になる．安全性を高めるためには，ランダム化機構を組み込むが，ランダム化機構により送信機から出力される波形は変化しない．本研究では光ファイバ伝送路の伝送特性を解析することが目的なので，この機構を送信機に組み込まないで数値解析を行った.

2-2 光ファイバ伝送路設計のためのシミュレーションモデル

光ファイバ内を伝搬する電界は，非線形シュレディンガー方程式で記述できる．ある特定の条件下では，解析解を算出することができるが，一般に，数値解析により電界の挙動を解析することができる．以下に，解析に用いた非線形シュレディンガー方程式を示す．

$$\frac{\partial E}{\partial z} = -\frac{\alpha}{2}E - \frac{i\beta_2}{2}\frac{\partial^2 E}{\partial T^2} + \frac{\beta_3}{6}\frac{\partial^3 E}{\partial T^3} + i\gamma\left|E^2\right|E \quad \cdots\cdots\cdots \text{式(1)}$$

ここで，E は信号光の電界，z は伝搬距離を表している．α は伝送損失，β_2 が光ファイバの群速度分散，β_3 は分散スロープ，γ は非線形係数をそれぞれ表している．T は時間で，次式で表される群速度(v_g)の時間軸で見た時間を表している．

$$T = t - \frac{z}{v_g} \quad \cdots\cdots\cdots \text{式(2)}$$

なお，分散については，分散スロープまでを考慮した．一般に，帯域が広くなるほどより高次の分散効果を取り込む必要がある．本研究では，波長数 10 で波長間隔が 50 GHz なので，通信帯域は 450 GHz(波長に換算すると 4nm 弱)になる．そのため，分散スロープまでを取り込めば分散の効果は正しくシミュレーションできるからである．

信号光パワーが大きくなるにつれて光ファイバは線形伝送路ではなくなり，非線形効果が発生することが知られている．本シミュレーションでは，非線形効果として，信号光の強度に比例して位相が回転する光カー効果の影響のみ取り込んだ．他には，信号光波形の時間変化に起因して発生する非線形効果や信号光と異なる波長の光が発生するラマン効果があるが，これらの効果はいずれも本研究の条件では無視できるほど小さいものとして除外した．

非線形シュレディンガー方程式の右辺は，1～3 項目までの線形項と 4 項目の非線形項に分けられる．これらを時間領域と周波数領域で交互に微小距離分を数値計算するスプリット・ステップ・フーリエ法により数値解を求めた．

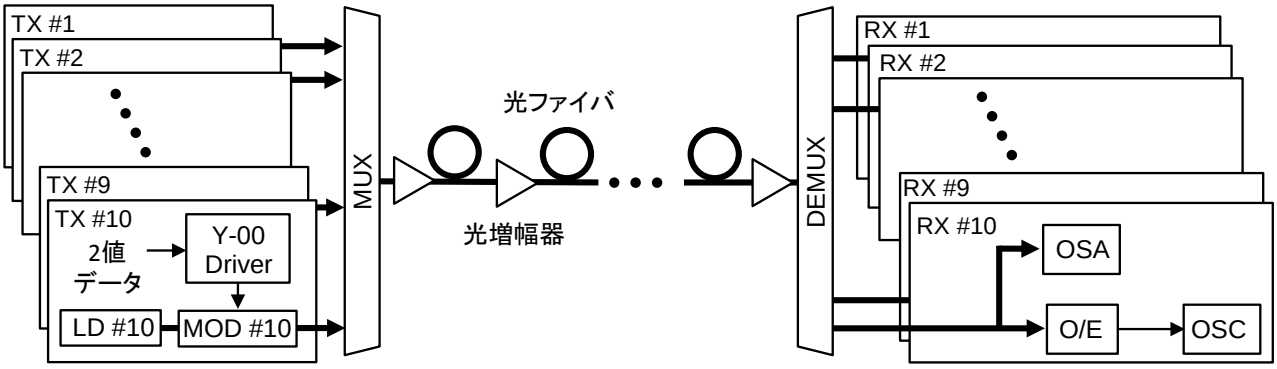

図 2：100 Gbit/s の強度変調 Y-00 信号光伝送シミュレーションのモデルの一例

図 2 に数値解析に用いた波長多重 100 Gbit/s の強度変調 Y-00 信号光伝送シミュレーションのモデルの一例を示す．送信機では，10 Gbit/s の 10 波長分の Y-00 信号光を用意した．それぞれ，レーザ光源(LD)，変調器(MOD)および Y-00 ドライバを用いて生成した．10 Gbit/，10 波長の Y-00 暗号信号光を波長分割多重装置(MUX)で多重して，100 Gbit/s の波長多重 Y-00 暗号信号光を用意した．Y-00 ドライバは図 1(a)に示したものである．伝送路は，光増幅器と光ファイバで構成されている例を示す．後の解析において，光ファイバは SMF もしくは DSF を設定した．また，無中継伝送のシミュレーションでは伝送路で光増幅器を用いていないが，中継伝送のシミュレーションでは図示するように，伝送路で光増幅器を設置した．受信機では，はじめに波長分割多重分離装置(DEMUX)で，10 波長の 100 Gbit/s の Y-00 暗号信号光をそれぞれの波長に多重分離した．光スペクトルアナライザ(OSA)で光スペクトルを解析すると共に，各波長の 10 Gbit/s の Y-00 暗号信号光はフォトディテクタ(O/E)を介してオシロスコープ(OSC)で電気信号に変換し波形を解析した．

2-3 シミュレーション条件

シミュレーションでは波長多重信号の波長は，ITU-T で標準化されている波長グリッド上に設定した．具体的な値を表 1 に波長と対応する周波数を示す．周波数は 193.0 GHz から 50 GHz 間隔とした．

表 1：100 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
周波数 (THz)	193.45	193.40	193.35	193.30	193.25	193.20	193.15	193.10	193.05	193.00
波長 (nm)	1549.71	1550.11	1550.51	1550.91	1551.31	1551.72	1552.12	1552.52	1552.92	1553.32

共通のシミュレーション条件を表 2 に示す．伝送路入力光パワー，伝送距離，中継距離など，その他の条件は，それぞれのシミュレーションの項で示す．

表 2：共通のシミュレーション条件

光ファイバ損失	0.2 dB/km	非線形係数	2.6 $W^{-1}km^{-1}$
群速度分散	20 ps/nm/km	光増幅器雑音指数	6 (7.8dB)
分散スロープ	0.08 $ps/nm^2/km$		

ビット数は 2^{14}(=16,384)とした．従って，計算のビット列は 1.6384 ns である．これは，計算リソースと計算時間に制限された．このビット数で符号誤り率(BER)を計算した場合，BER = 10^{-5}のオーダーになり，BER = 10^{-9}を基準として評価することができない．そのため，本研究では，伝送品質の解析は，光信号対雑音比(OSNR)とした．

2-4 シミュレーション結果

(1) 多値数と波形の関係

まず初めに多値信号の時間波形の例を示す．多値数が多いと波形が分かりづらいので，ここでは一例として 4 値(M = 2)の信号光波形を示す．次の 80 ビットの波形を示す．

{3,1,3,1,1,2,1,1,3,0,3,2,3,2,3,0,0,0,1,2,0,0,3,0,3,3,3,1,2,3,1,1,2,1,1,0,2,0,2,1,2,3,2,0,2,1,3,2,3,2,2,0,0,3,3,0,3,3,0,2,1,1,2,0,3,2,2,0,3,2,0,3,2,2,3,0,3,3,2,2}

図の横軸は 500 ps/div のスケールで示している．

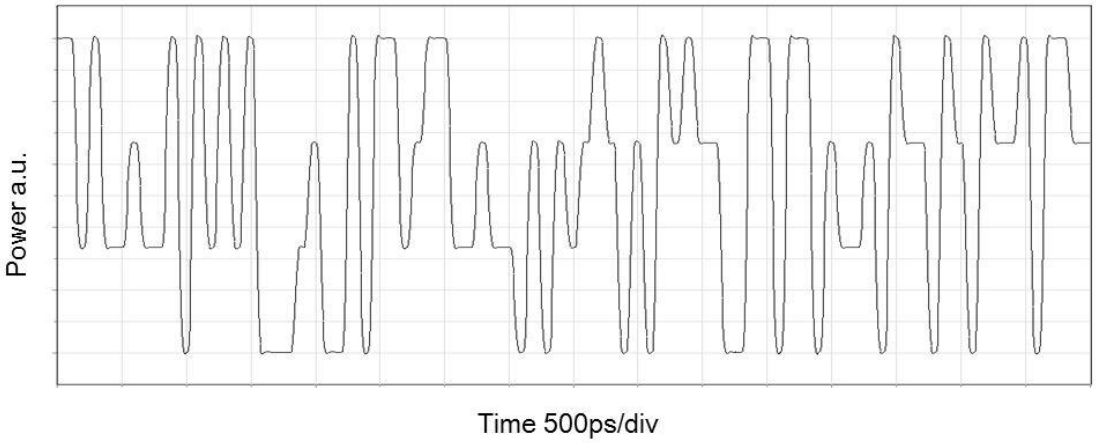

図 3：多値信号光の時間波形の例(M = 2，多値数 = 4)

以下の解析では，時間波形を時系列に表示しても分かりづらいので，2 ビット毎に重ね書きしたアイパターンで表示する．図 4(a)に図 3 のアイパターンを示す．それぞれの信号光レベルが明確に識別できる．これは，暗号の安全性の観点に着目すると，暗号文を正しく識別することができるので，後の暗号解析につながり，解読される可能性があることを意味している．(b)～(f)は，基底数 M の値を増やしていった場合のアイパターンを示している．多値数が 32 になる M = 16 からそれぞれの信号高レベルを正しく識別するのが難しくなっており，64 値ではもは正しいレベルを識別できないことが分かる．このように，雑音により正しい信号光レベルを識別させないこと，つまり第三者に暗号文を正しく読み取らせないことが，Y-00 暗号が安全性を担保する基本原理である．なお，正規受信者は暗号鍵情報により閾値が分かるので，多値信号のレベルを正しく識別する必要はなく,閾値を用いて識別操作することにより,元の 2 値情報を復号することができる．

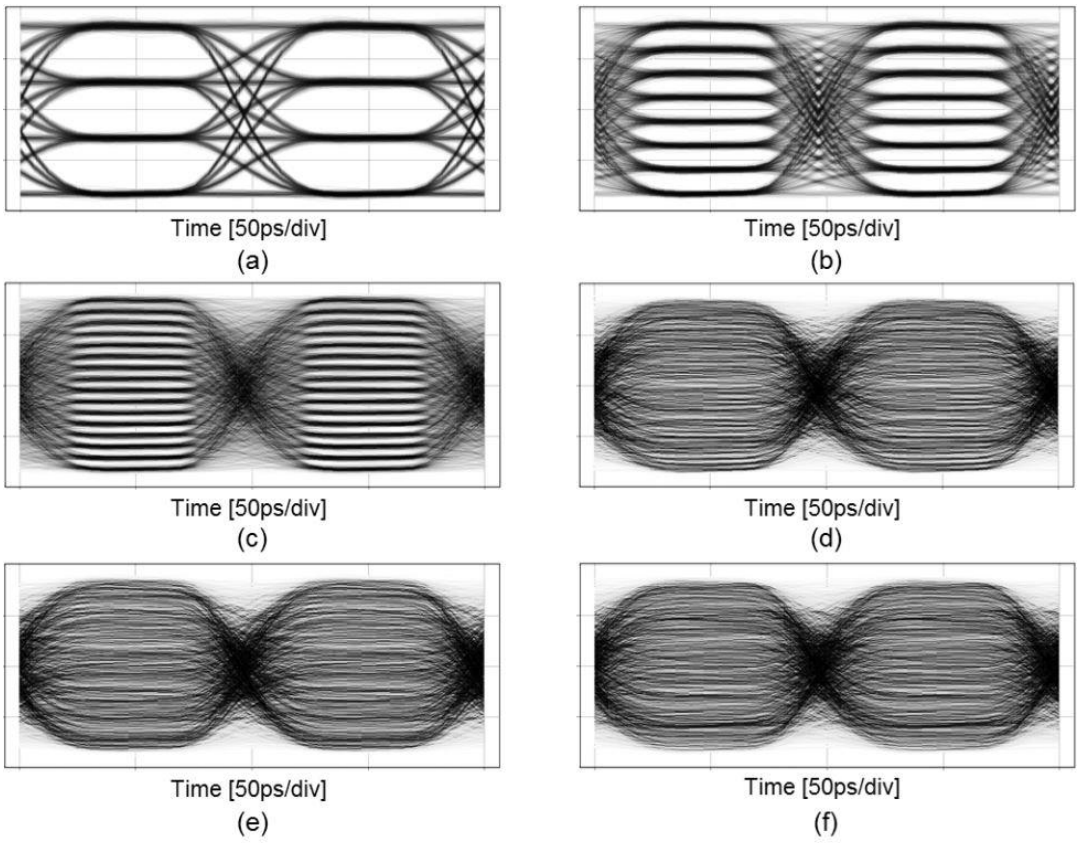

図 4：多値信号光波形．(a)基底数 M = 2（多値数 = 4），(b)M = 4（多値数 = 8），(c)M = 8（多値数 = 16），(d)M = 16（多値数 = 32），(e)M = 32（多値数 = 64），(f)M = 64（多値数 = 128）．

(2) 群速度分散の影響

次に，図 5 に示す SMF を伝送するモデルで群速度分散による波形変化について解析を行った．100 Gbit/s の Y-00 送受信器構成は，図 2 に示したものである．SMF の群速度分散は D = 20 ps/nm/km とした．前述の通り，多値数を大きな値に設定すると波形解析が困難なために，多値数は 4(基底数 M = 2)に設定した．非線形シュレディンガー方程式を数値解析して得られた，SMF を 10 km 毎の波形を図 6 に示す． 図示している波形は，Ch.5(周波数 193.25 THz，波長 1551.31 nm)であるが，他のチャネルも同様の波形特性だった．

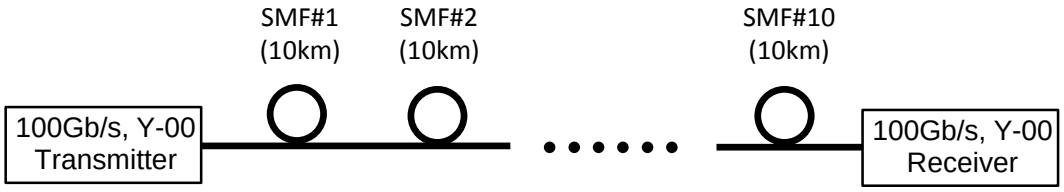

図 5　SMF 伝送路における群速度分散の影響を解析するモデル．

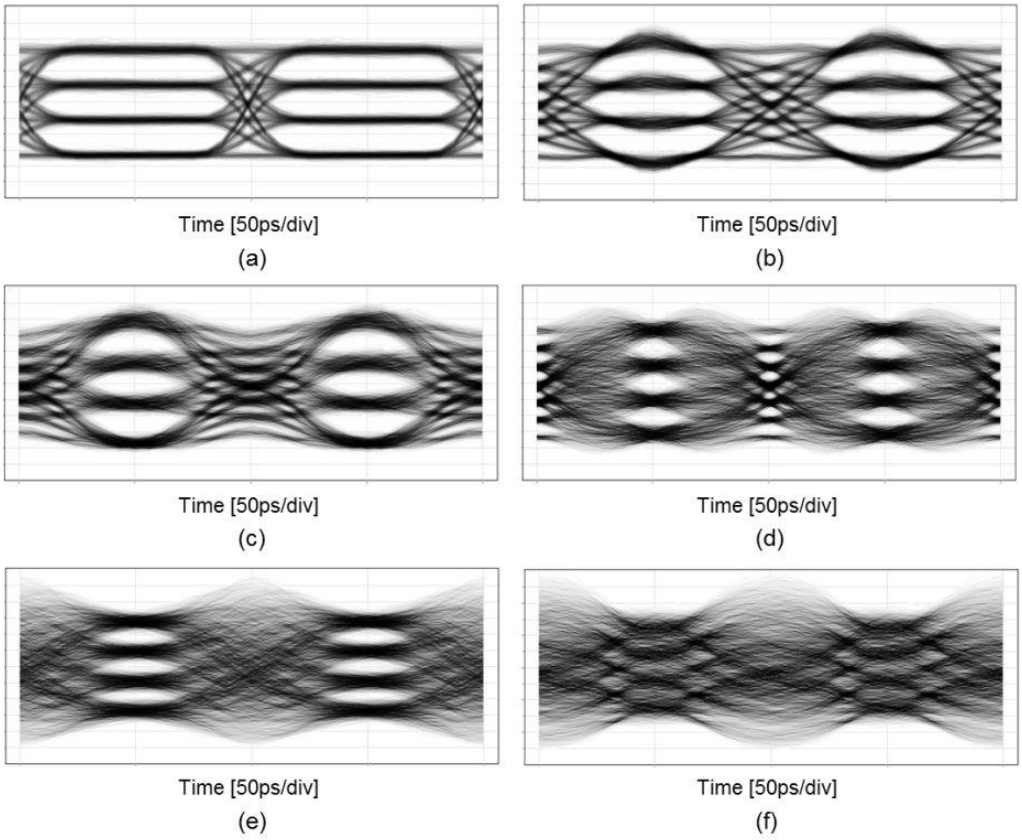

図 6：群速度分散による時間波形変化．(a)L = 0 km，(b) L = 20 km，(c) L = 40 km，(d) L = 60 km，(e) L = 80 km，(f) L = 100 km． 基底数 M = 2（多値数 = 4）．

計算では，波形変化の分析に着目するために，SMF の伝送損失は無視した．図 6 を参照すると，群速度分散の影響で波形が変化しているのが見て取れる．多値信号なので，隣接チャネルに漏れ込んでいく成分が影響して，L = 10 km では，波形が狭くなって見える傾向がある．その後，波形は丸みを帯びてきて，L = 80 km まではアイ開口が見られるが，L = 100 km になると，アイ開口が見られなくなっている．即ち，SMF では，L = 80 km 程度で，群速度分散による隣接チャネルとのクロストークが伝送限界の要因になっていることが分かった．本結果は，次章で後述するが，L = 40 km において実験検証し，シミュレーション結果が正しいことを確認した．

(3) 無中継伝送特性

SMF では群速度分散の影響により伝送距離が制限されることが分かった．群速度分散のない DSF を伝送路に用いた場合の伝送特性を解析した．解析モデルを図 7 に示すが，送信機から出力された 100 Gbit/s の Y-00 暗号信号光を DSF で構成される光ファイバ伝送路を伝搬させ，伝送後の波形と光信号対雑音比(OSNR)を評価した．受信端では光増幅器を用いて DSF 伝送で受けた伝送損失を補償した．

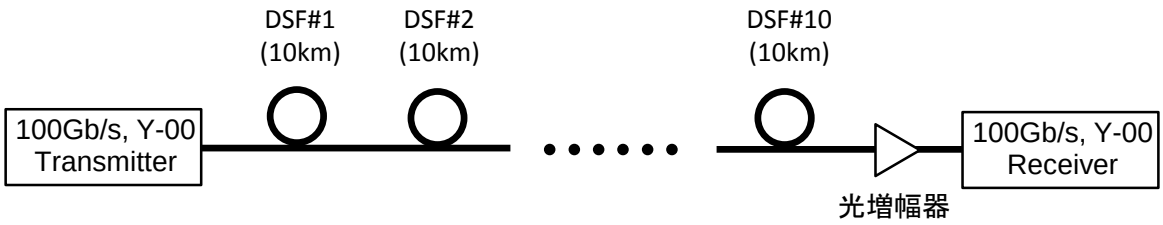

図 7　DSF 伝送路における無中継伝送特性解析モデル

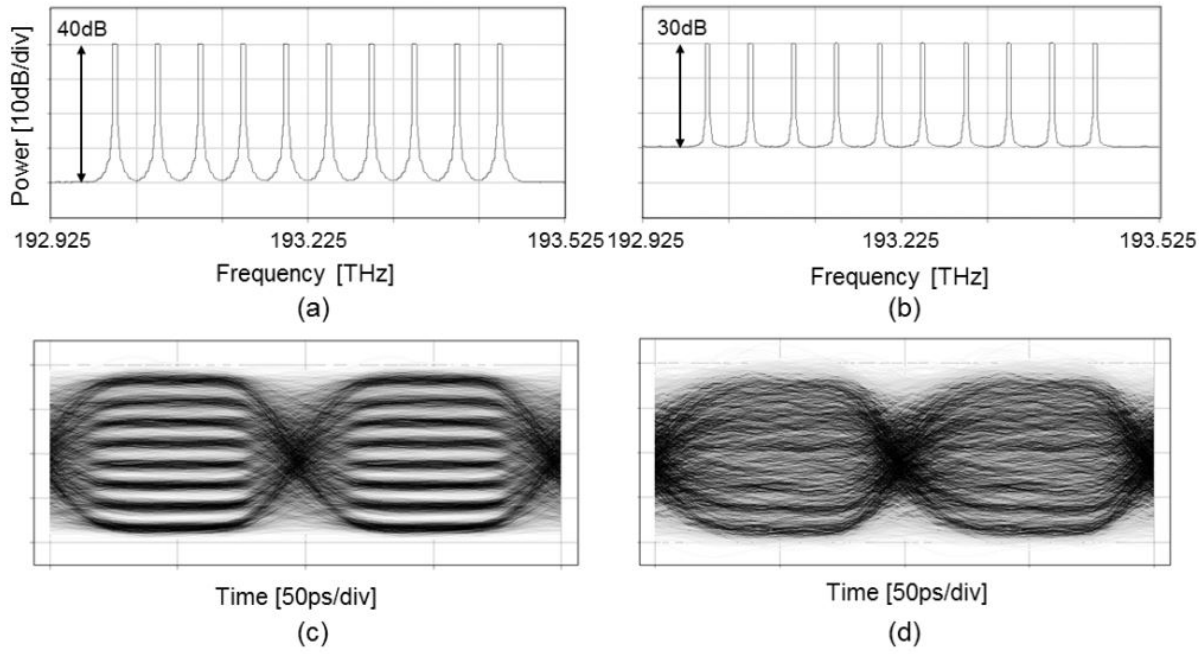

図 8　DSF 伝送路を無中継伝送時の光スペクトルと波形特性．(a)，(c)伝送前，(b)，(d)70km 伝送後．光スペクトルの表示分解能は 10GHz

図 8 に，基底数は M = 4，多値数は 2M = 8 に設定した場合の伝送前の送信端での光スペクトル(a)と波形(c)を示す．光スペクトルの分解能は 10 GHz で表示している．波形は Ch. 5 の特性を示している．伝送後の一例として，L = 70 km 伝送後の光スペクトルを(b)に，Ch. 5 の波形特性を(d)に示す．波形特性は，Ch. 5 以外のチャネルも Ch. 5 と同様の特性だった．OSNR が 30 dB 程度になっているのが分かる．

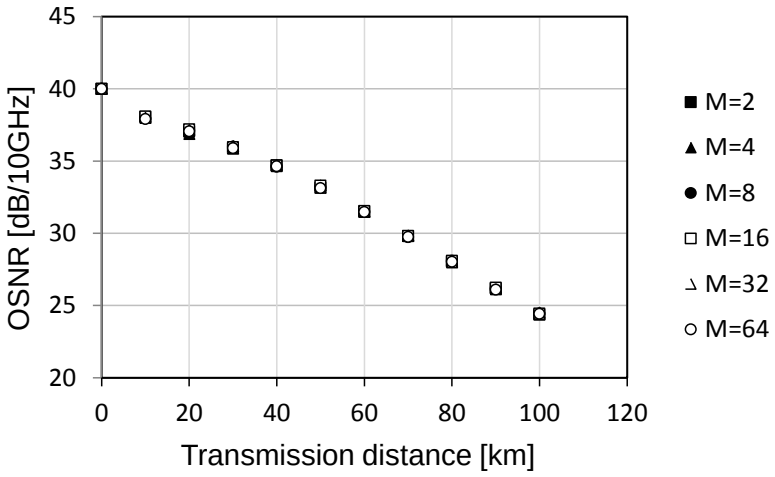

図 9　DSF 伝送路を無中継伝送時の伝送距離と OSNR の関係．
基底数 M = 2，4，8，16，32，64

基底数を変化させて，伝送特性の基底数依存性を解析した．基底数 M = 2，4，8，16，32，64 の場合の OSNR の伝送距離依存性を図 9 にまとめて示す．伝送距離と共に DSF 伝送路の伝送損失が増加するために，伝送距離が長くなるにつれて，受信端での OSNR は劣化している．基底数による OSNR の相違はほとんど見られなかった．前述の通り，計算リソースの制限によりシミュレーションで BER = 10^{-9}を評価することができないが，実験により OSNR = 30 dB あれば BER = 10^{-9}を達成できることは確認しているので，本研究では，OSNR = 30 dB を伝送評価の基準とすることにした．そうすると，群速度分散のない DSF で構成した伝送路においては，伝送距離 L = 70 km 程度が OSNR の制限で伝送限界になる．これは基底数 M によらず同じ結果である．

(4) 光増幅中継伝送特性

SMF 伝送路では群速度分散により伝送距離が制限され，群速度分散のない DSF 伝送路では OSNR 制限で伝送距離が制限されることが分かった．そこで，図 10 に示すように，光増幅器を伝送路中に設置して，DSF 伝送路の損失により弱くなった 100 Gbit/s の Y-00 暗号信号光を光増幅器で増幅して中継伝送する場合の伝送路

モデルにおける伝送特性を解析した．後述する実験条件を考慮し，中継間隔は 40 km に設定し，中継数 15 とし，総長 L = 600 km の伝送特性を解析した．基底数は M = 32(多値数 = 64)に設定した．

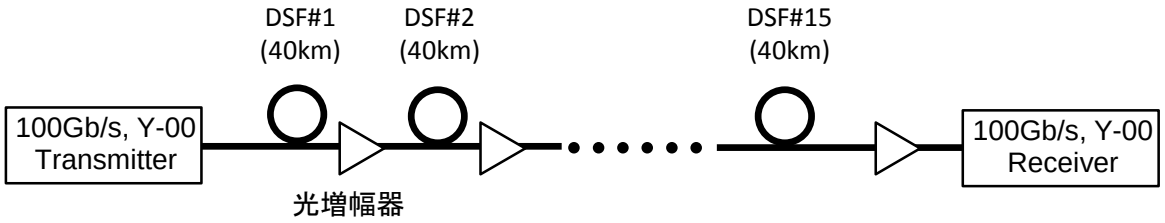

図 10　DSF 伝送路で光増幅器による中継伝送時の伝送解析モデル．

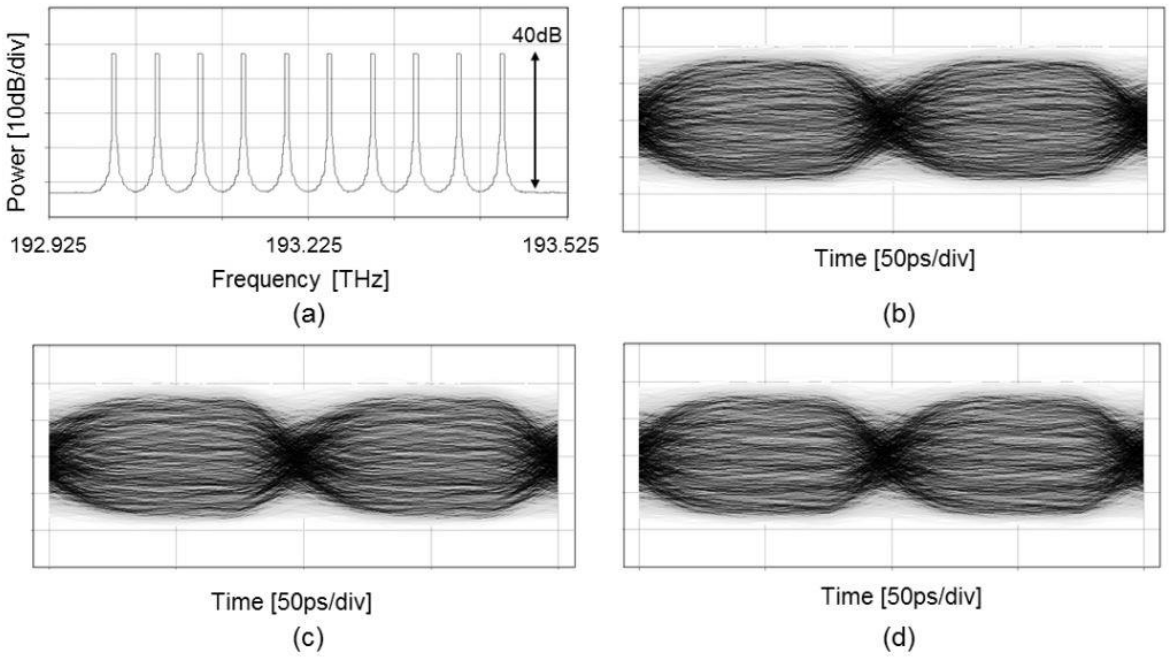

図 11　送信端での(a)光スペクトル，および(b)Ch.1，(c)Ch.5，(d)Ch.10 の波形．

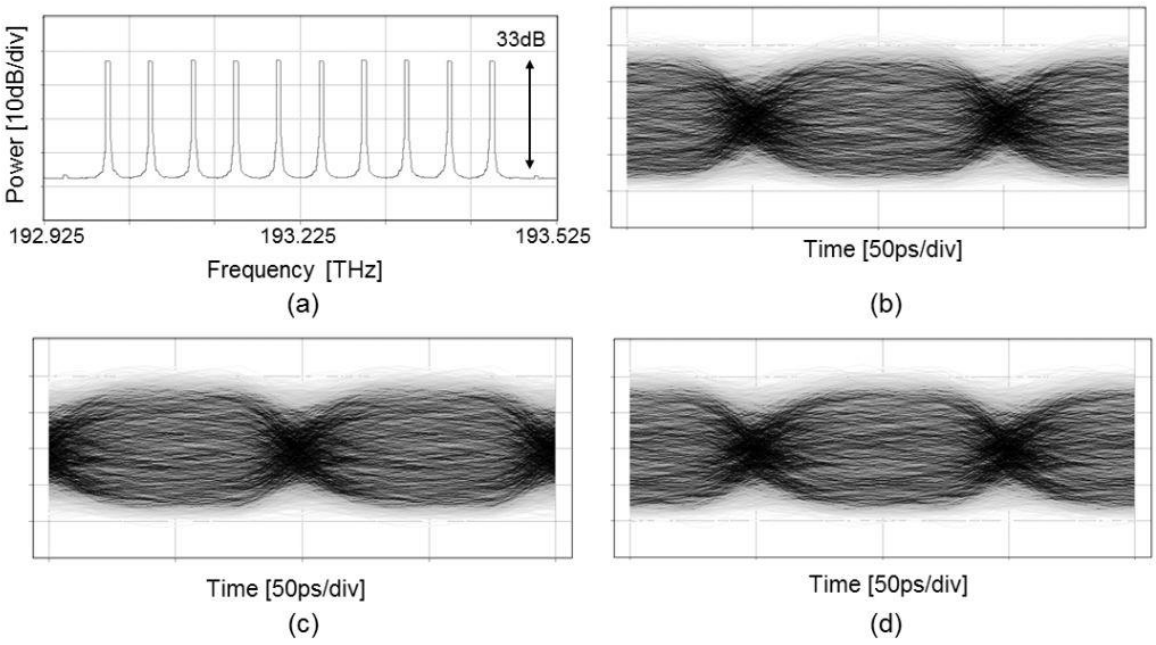

図 12　伝送距離 L = 200 km での(a)光スペクトル，および(b)Ch.1，(c)Ch.5，(d)Ch.10 の波形．

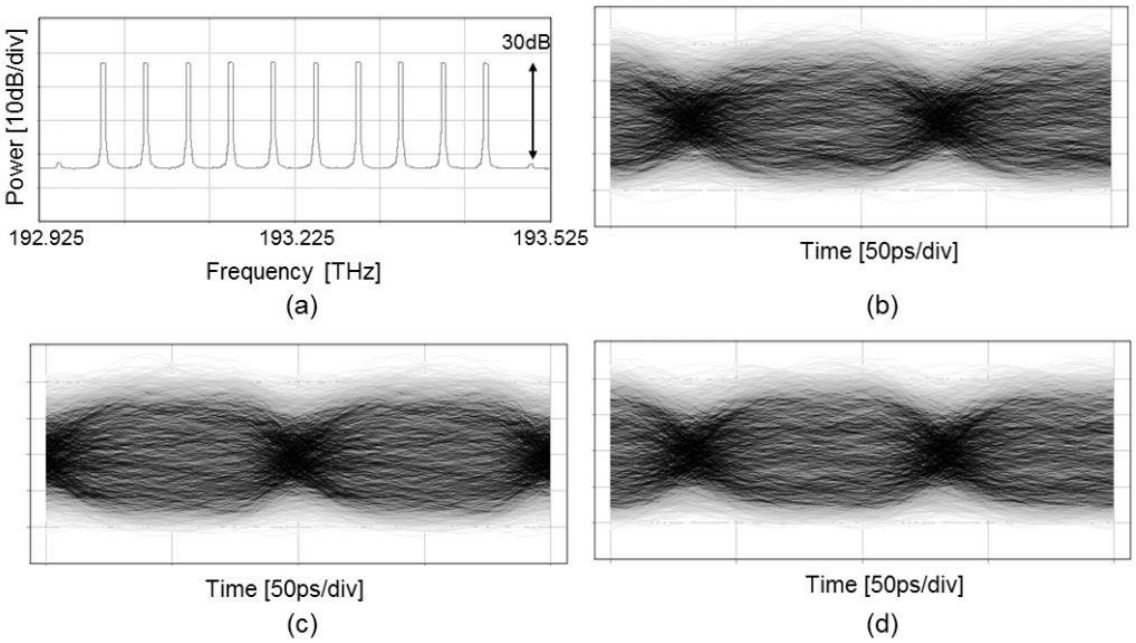

図 13　伝送距離 L = 520 km での(a)光スペクトル，および(b)Ch.1，(c)Ch.5，(d)Ch.10 の波形.

DSF 伝送路への入力光パワーは，波長当たり-3 dBm/ch，合計+7 dBm に設定した．長さ 40 km の DSF の伝送損失は 8 dB なので，光増幅器の利得は 8 dB に設定した.

図 11 に送信端での光スペクトル(表示分解能 10 GHz)と最短波長チャネル Ch.1(波長 1549.71 nm)，Ch.5(波長 1551.31 nm)および最長波長チャネル Ch.10(波長 1553.32 nm)の波形を示す．同様に，伝送距離 L = 200 km，520 km だけ伝送後の光スペクトルと波形を図 12，13 に示す．伝送距離 L = 200 km の光スペクトル(図 12(a))を参照すると，周波数が 192.95 THz 付近と 193.50 THz 付近に僅かであるが，突起が生じている．最短周波数，最高周波数から波長間隔とほぼ等しい 50 GHz 離れた周波数付近である．これは，光ファイバ中で波長チャネル間での相互作用により発生する非線形現象の一つである四光波混合により発生したものと考えられる．試しに，Ch.3(周波数 193.35 THz)の 10 Gbit/s の Y-00 暗号信号光を無しにして伝送特性を解析したところ，このチャネルにも同様の突起が見られた．伝送距離 L = 520 km の光スペクトル(図 13(a))に着目すると，雑音レベルが 3 dB 程度大きくなっているから分かりづらいが，四光波混合による突起はさらに大きくなっている．伝送限界の評価として OSNR 特性を算出した．OSNR の伝送距離依存性を図 14 に示す．光増幅器が発生する雑音の影響で，伝送距離と共に OSNR が劣化している．伝送距離が L = 200 km の時，OSNR は 33.5 dB 程度だった．OSNR = 30 dB になるのは，伝送距離が L = 520 km と時だったことが図 14 から分かる．L = 520 km 伝送時の波形は，OSNR が劣化している分，雑音が追加されているが，分散スロープによる隣接チャネルへの波形広がりは見られなかった．このように，DSF を用いた伝送路で光増幅器による中継伝送した場合，波長分散によるパルス広がりはほとんど観測されなかったが，OSNR 制限により伝送距離が L = 520 km 程度に制限されることが分かった.

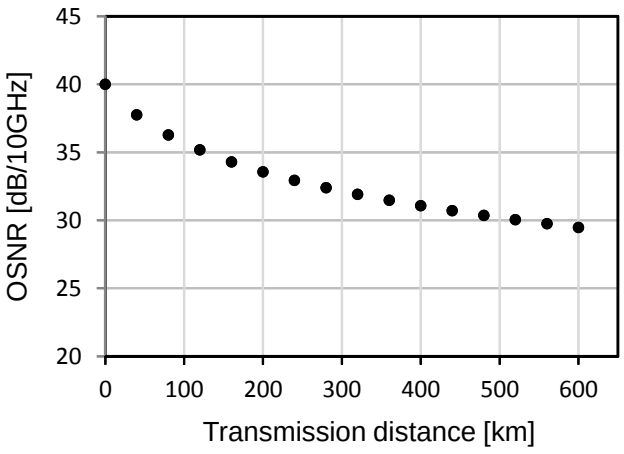

図 14　DSF 伝送路で光増幅器による中継伝送時の OSNR の伝送距離依存性

3 実験検証

前章の 100 Gbit/s の Y-00 暗号通信光の光ファイバ伝送路伝送特性のシミュレーションにより SMF や DSF 伝送路での伝送特性を解析した．本章では，実際に 100 Gbit/s の Y-00 暗号通信光の伝送実験を行った．以下に，実験構成と実験結果を示す．

3-1 実験構成

図 15(a)，(b)に伝送実験用に構築した波長分割多重の 100 Gbit/s(10 波長 x 10 Gbit/s) Y-00 暗号信号光の送信機と受信機の構成を示す．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， 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．シミュレーションでは各波長の光をそれぞれ個別の Y-00 ドライバで変調して Y-00 暗号信号光を生成したが，波長分割多重実験で一般的に行われている手法と同様に，10 波長を多重後に 10 波長を一括して Y-00 ドライバで変調した．

受信機では，10 波長の Y-00 暗号信号光を透過中心波長間隔 50 GHz の AWG で各波長に多重分離した．その後，フォトディテクタで光電変換しサンプリングオシロスコープで波形を測定した．オシロスコープのトリガーは受信した信号光から抽出した 10GHz のクロックを用いた．

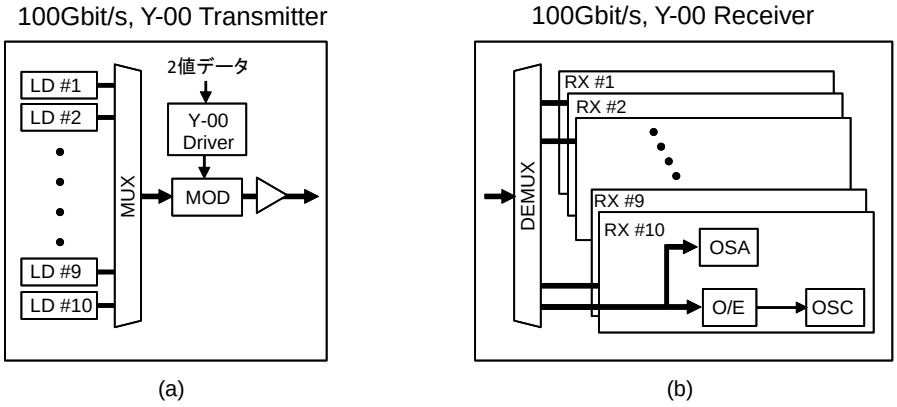

図 15　100 Gbit/s の Y-00 暗号信号光の送受信器構成

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	1550.1	1550.5	1550.9	1551.3	1551.7	1552.1	1552.5	1552.9	1553.3

3-2 実験結果

SMF 伝送時の群速度分散の影響について評価実験を行った．実験系を図 16 に示す．波形変化を観測する目的で，基底数は M = 2 (多値数 = 4)に設定した．100 Gbit/s の Y-00 暗号信号光の送受信器は図 15 に示したもので，伝送路は 40 km の SMF で TAMA net#1 の一部を利用した．TAMA net#1 は，図 17 に示すように，本学キャンパス内の地中に敷設してある光ファイバ通信特性評価用の屋外敷設光ファイバ通信回線である．伝送路 SMF 入力パワーは，非線形効果が発生しない低い値に設定した．

図 18(a)，(b)に伝送前後の Ch.5 の波形を示す．対応するシミュレーション結果は図 6(a)，(c)である．この波形変化を観測するためには広帯域のフォトディテクタが必要だったので，帯域 20 GHz のフォトディテクタを用いて波形を観測した．信号光パワーを低い値に設定したため，および広帯域のフォトディテクタを使用したために，信号帯域外に含まれる雑音成分が観測波形に含まれてしまっている．伝送前の波形は，シミュレーション結果と同様に位相余裕の大きな波形になっていることが分かる．伝送後は，波形が狭くなって

いる傾向が見て取れる．これはシミュレーションで予測された結果と合致しており，前章で構築したシミュレータが正しく機能していることを示している．

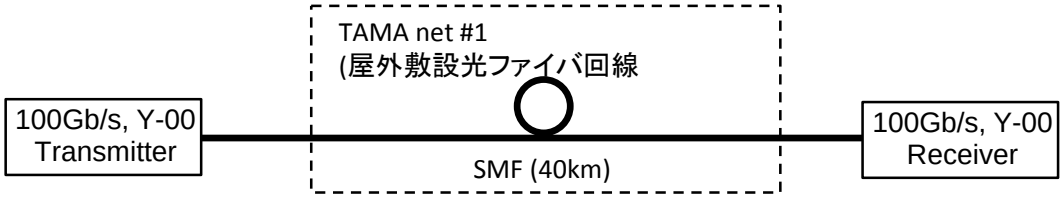

図 16　100 Gbit/s の Y-00 暗号信号光の SMF 伝送路伝送実験構成

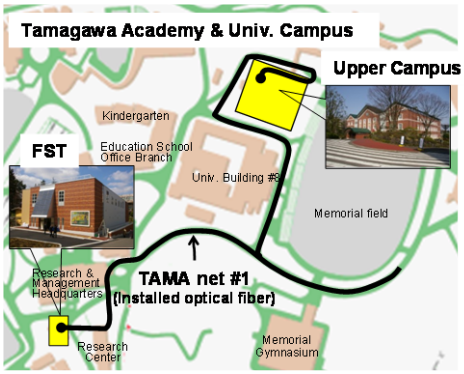

図 17　屋外敷設光ファイバ通信回線「TAMA net #1」

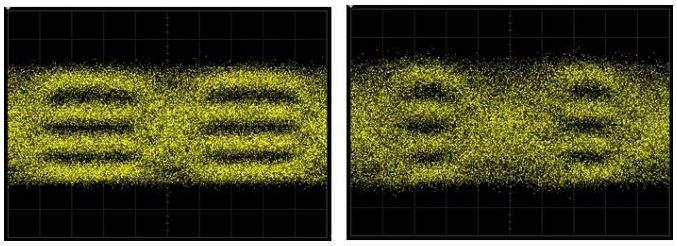

図 18　TAMA net#1 の SMF 伝送時の波形．(a)伝送前，(b)40 km 伝送後．受信帯域は 20 GHz．

次に，図 19 に示す DSF 伝送路で光増幅中継する伝送路を構築し，OSNR の評価実験を行った．長さ 40 km の DSF を用い，中継距離は 40 km に設定し，総長 200 km に設定した．この距離は，手持ちの DSF に制限された．各 DSF に入力するパワーは，一波長当たり－3 dBm/ch，全波長で＋7 dBm になるように，各光増幅器の出力パワーを調整した．暗号信号光の基底数は M = 32（多値数 = 64)に設定した．

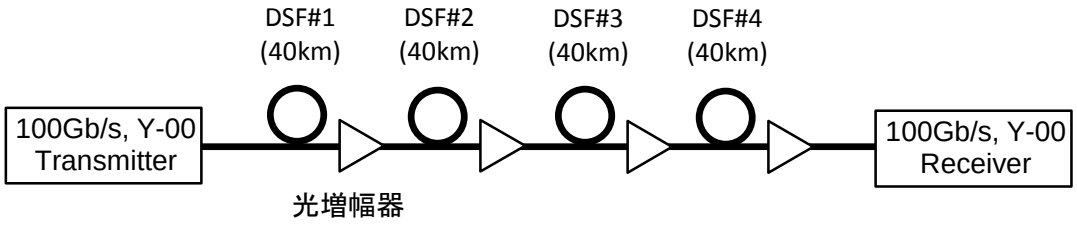

図 19　100 Gbit/s の Y-00 暗号信号光の DSF 中継伝送実験構成．

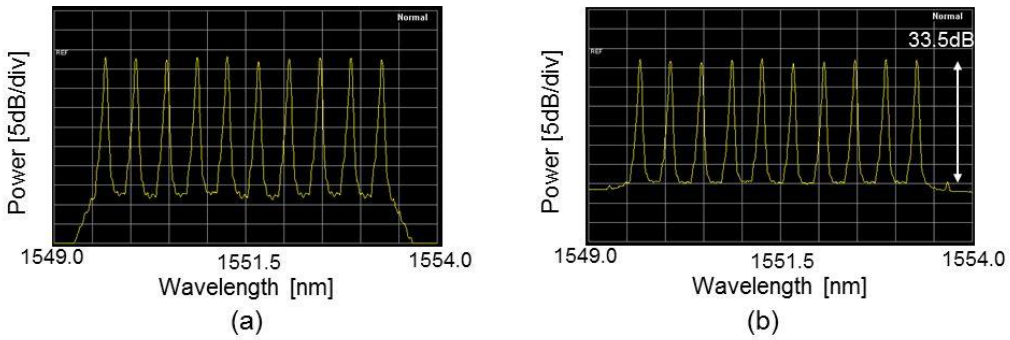

図 20　100 Gbit/s の Y-00 暗号信号光の DSF 中継伝送前後の光スペクトル．(a)送信端，(b)200 km 伝送後．

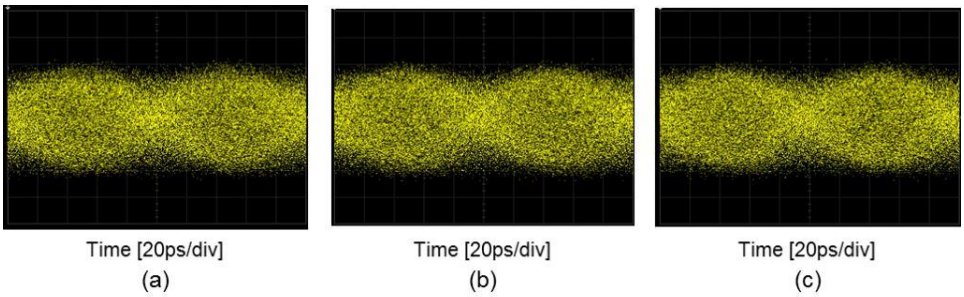

図 21　送信端での 10 Gbit/s の Y-00 暗号信号光波形.
(a)Ch.1(波長 1549.7 nm), Ch.5(波長 1551.3 nm) Ch.10(波長 1553.3 nm). 受信帯域は約 10 GHz.

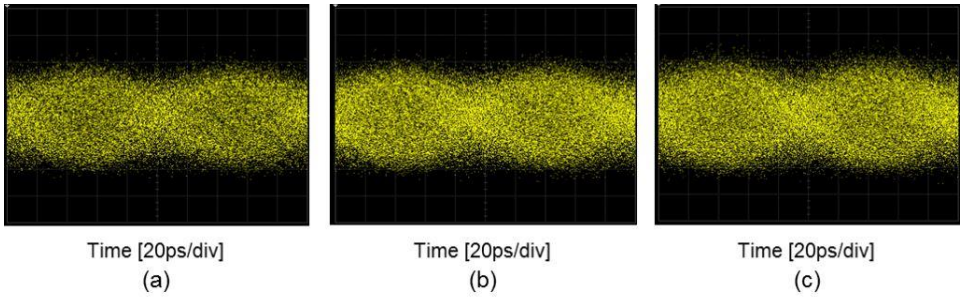

図 22　200 km 伝送後に波長多重分離した 10 Gbit/s の Y-00 暗号信号光波形.
(a)Ch.1(波長 1549.7 nm), Ch.5(波長 1551.3 nm) Ch.10(波長 1553.3 nm). 受信帯域は約 10 GHz.

200 km 伝送前後の光スペクトルを図 20(a), (b)にそれぞれ示す. シミュレーションで対応する光スペクトルは, それぞれ, 図 11(a)と図 12(a)である. 伝送後の光スペクトルでは, Ch.1 の短波長側, および, Ch.10 の長波長側, それぞれ 0.4 nm 程度だけ離れたところに, スペクトルの突起が観測された. これはシミュレーションで予期された現象で, 非線形効果に起因する. 信号光に対する比を測ってみると 33.5dB 程度で, 図 14 に示したシミュレーション結果に良く一致する. SMF 伝送結果に加え, シミュレーションの妥当性が検証できた. 図 21 と図 22 に, 伝送前後の波形を示す. それぞれ, (a), (b), (c)は, Ch.1(波長 1549.7 nm), Ch.5(波長 1551.3 nm) Ch.10(波長 1553.3 nm)の波形である. SMF 伝送時に使用したフォトディテクタと異なり, 信号帯域外の雑音を除去する目的で, 帯域 10GHz 程度のフォトディテクタを用いて観測した. しかしながら, 多値数が 64 値と多いために, 雑音に埋もれてしまいアイ開口を観測できない. 正しい暗号信号レベルを, 第三者が正しく識別できないことが, Y-00 暗号の安全性の根拠である. 暗号鍵を持っている正規受信者は, 識別信号情報があるために, 正しく 2 値の情報に復号できる.

4 まとめ

本研究調査では,通信容量 100 Gbit/s の Y-00 光通信量子暗号の光ファイバ伝送技術の研究開発を行った. シミュレーションと実験の両側面から研究を実施した. シミュレーションでは, 100 Gbit/s の Y-00 暗号信号光の伝送特性を解析するシミュレータを構築した. 実験検証では, まず, 群速度分散による波形のクロストークによる影響を調査するために, 単一モード光ファイバ(SMF)伝送路で 100 Gbit/s の Y-00 暗号信号光を伝送させた. 本学内に敷設してある通信特性評価用の屋外敷設光ファイバ通信回線「TAMA net#1」の一部の SMF を使用した. 40 km 伝送後の波形を解析し, シミュレータで数値計算した波形と同様の結果であることを検証した. シミュレーション結果と合わせると, SMF だと群速度分散による隣接チャネルのクロストークが原因で, 伝送距離が 80 km 程度に制限されることが分かった. SMF だと群速度分散により伝送距離が制限されることが分かったので,群速度分散の影響が小さい分散シフトファイバ(DSF)を伝送路に用いる場合の伝送特性を調査した. シミュレーション結果から, 伝送路に光増幅器を用いない無中継伝送では, SN 制限で伝送距離が 70 km 程度に制限されてしまうことが分かったので, 伝送路に光増幅器を設置する中継伝送路について解析した. 波長分散の影響は受けにくいが, 波形が崩れないために, 高いパワーが保たれる結果, 非線形

効果が DSF 伝送路中で発生することがシミュレーションで判明した．伝送距離と共に非線形成分は大きくなった．DSF で光中継する伝送路では，非線形効果の影響により伝送距離は 520 km 程度に制限されることが分かった．DSF 中継伝送路を構築して検証実験を行った．手持ちの DSF が 200 km だったので，200 km 伝送時の実験結果とシミュレーション結果を比較したところ，ほぼ同様の結果が得られた．この結果から，DSF 中継伝送路では，実際に伝送距離は 520 km 程度になると考えられる．

SMF 伝送路では群速度分散が伝送距離制限になり,DSF 中継伝送路では非線形効果が伝送距離を制限することが分かった．更に伝送距離を延伸する手法として，SMF 伝送路で伝送させて波形を崩し非線形効果を抑圧して，SMF の群速度分散を分散補償ファイバで補償する伝送路が考えられる．この伝送路を用いると，更に伝送できると考えられるが，伝送特性評価は今後の課題とした．

【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.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
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
波長分割多重を用いた 100 Gb/s Y-00 光通信量子暗号の伝送実験	電子情報通信学会技術報告 OCS2014-85	2014 年 11 月
Y-00 光通信量子暗号とその 100 Gb/s 伝送特性	第 13 回 量子情報ミニワークショップ	2015 年 3 月