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

平成　２９　年　　６　月　２３　日現在

機関番号：　３２６３９
研究種目：　挑戦的萌芽研究
研究期間：　2015～2016
課題番号：　１５Ｋ１３９９１

研究課題名（和文）シャノン限界を超える物理暗号の光ファイバ通信

研究課題名（英文）Study on optical fiber communication of the physical cipher beyond the Shannon limit

研究代表者

二見　史生（Futami, Fumio）

玉川大学・量子情報科学研究所・教授

研究者番号：２０４１７６９５

交付決定額（研究期間全体）：（直接経費）　　2,500,000円

研究成果の概要（和文）：暗号学の基本的な限界であるシャノン限界を超越可能な物理暗号は，暗号鍵の利用効率を高められるので，情報通信量が飛躍的に増大している今日，その実現が期待されている。本研究では，その実現を目指し周波数分解して位相変調する方式の物理暗号の原理検証実験を実施した。波長1.5μm帯，データ10Gb/sの信号光の暗号・復号実験に成功し，更に，暗号信号光の光ファイバ120km伝送にも成功した。本成果により，暗号学のシャノン限界を超越する物理暗号の実現に向け大きく前進した。

研究成果の概要（英文）：Today, the data traffic including the sensitive data is rapidly increasing. An encryption key is required for secure communication and an efficient use of the key is an issue for huge amount of data. The physical cipher has a possibility to realize an efficient use of the key which provides the security beyond the Shannon limit of the cryptography. For realizing such physical cipher, we have proposed a novel scheme employing phase modulation in the frequency domain. An experimental demonstration of encryption and decryption using shared keys have been successfully conducted using 10-Gb/s optical signal at the wavelength of 1.5 micron. In addition, we have successfully applied the novel scheme to an optical fiber transmission over 120 km. This result will give a great advance to realize a physical cipher beyond the Shannon limit of the cryptography.

研究分野：　工学

キーワード：　暗号のシャノン限界　物理暗号　光ファイバ通信

１．研究開始当初の背景

光ファイバ通信回線から通信情報を傍受したというニュースがTVや一般紙で報道され，光ファイバ回線から盗聴を防ぐ技術の研究開発が急務になっており，通信情報を暗号化することにより盗聴を防御することが有効である。暗号化では，送信者が暗号鍵で送信する情報をスクランブルし，受信者は同じ暗号鍵を用いて復号する。大量の情報が通信されている今日，効率的な暗号化方式，即ち，なるべく少ない暗号鍵で多くの情報を暗号化する方式が求められている。

２．研究の目的

暗号通信の基本構成を図１に示すが，共有している暗号鍵を用いて通信情報を暗号化・復号化する。図2(a)に示すように，暗号学のシャノン限界という限界があり，数理暗号では暗号化する情報と同量の暗号鍵が最低限必要になる。数理暗号を用いる限りこの限界を破ることができない。一方，物理暗号では，同図(b)に示すように，情報よりも少ない暗号鍵で暗号化できる究極的な暗号，即ち，暗号鍵利用効率が１を超える暗号(シャノン限界超越)の実現性が理論的に示されている。暗号鍵よりも多い情報を暗号通信する技術開発は，大容量の情報を短い鍵で効率的に暗号化できる点で意義は大きい。本研究では，暗号学のシャノン限界の超越につながる物理暗号の送信器と受信器の実現と検証，およびその物理暗号の光ファイバ通信への応用実験を目的とした。

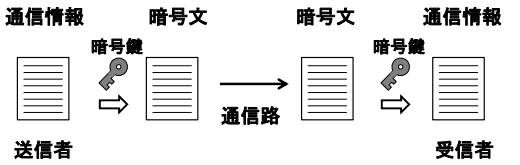


図１：暗号通信の基本構成

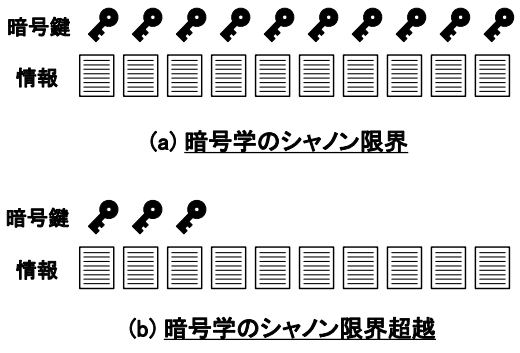


図 2：暗号学におけるシャノン限界。(a)情報と同量の暗号鍵が必要。(b)シャノン限界を超えると情報より少ない量の暗号鍵で暗号化が可能。この場合，暗号鍵の利用効率が上がる

３．研究の方法

盗聴のステップは，一般に，暗号文を正しく傍受するステップと傍受した暗号文を解析するステップの二つに大別できる。シャノン限界超越の暗号を実現するには，暗号文を盗聴者に正しく傍受させない事が有効なので，本研究ではその一つの方式として，信号光の位相をスクランブルする方法を採用した。即ち，送受信者間で暗号鍵を共有し，暗号鍵で信号光の位相を変調し波形をスクランブルする。理想的には，十分な位相変調により，波形を連続(CW)光の様な形状に変化させ，盗聴者に信号光の存在が分からないようにする。加えて，ビット毎に位相変調の変調量を変える。この二つの機構により，暗号鍵を持っていない第三者に通信情報の暗号文を読ませなくする。一方，暗号鍵を共有している正規の受信者は，送信者が変調した位相変調と逆の位相変調を行い，元の位相状態に戻すことにより，暗号信号光を元の情報に復号する。正規受信者もビット毎に位相変調量を変更する。

このような位相マスク型暗号の特徴の一つは，安全性の保証である。先述の通り，数理暗号は数学的構成理論に基づいているので，安全性は計算理論に立脚し，解読法の発見を排除することができない。従って，安全性を保証することができない。一方，位相マスク型暗号は，理論上，解読することができない高い安全性を実現できる。

位相マスクを実現する手法は様々ある。大別すると，時間領域で位相変調する方式と周波数領域で位相変調する方式が挙げられる。図3(a)に時間領域での変調方法例を示す。パルス幅内での一定の位相シフトは強度波形に何ら変化を与えないため，パルスの幅の中で複雑な位相変調を施さないと波形を乱すこ

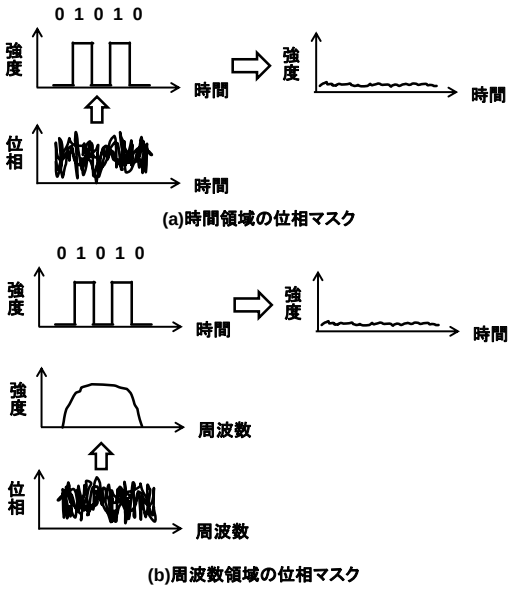


図３：位相マスク技術。(a)時間領域，(b)周波数領域

とができない。そのため，パルス幅より十分短い時間内での変調，即ち，高速の変調が必要になる。例えば Gb/s 級の信号の位相を変調するには，帯域 100 GHz 級の位相変調が必要になる。この高速変調は時間領域での位相マスクを実現する上で，大きな課題になる。一方，周波数領域での変調は，同図(b)に示すように，信号光周波数成分を細かく変調することにより，波形に変化を与えることができる。パルス幅の短い信号光は，パルス幅の広い信号光と比較して，より帯域が広いので，変調しやすくなる特徴がある。また，時間領域における位相変調方式と異なり，信号光のビットレートに対して，桁違いに高速の変調は不要である。位相変調により，高速信号の波形を効率的に乱す観点では，周波数領域で位相を変調する方式の方が有効である。従って，本研究では，周波数領域で位相を変調する方式の検討を行った。

４．研究成果

図 4 に暗号信号光を出力する暗号送信器の構成を示す。連続光(CW 光)を出力する光源(LD)から出力される波長 1550.3 nm の CW 光を強度変調器に入力し，10 Gb/s のデータ(擬似乱数 PN:2^7-1)で強度を変調し，10 Gb/s の NRZ 強度変調光信号を通信情報として用意した。続いて，周波数分解して周波数毎に位相変調した。各周波数での位相変調量は，暗号鍵により設定した。このようにして，10 Gb/s のデータを暗号化し，10 Gb/s の暗号信号光を生成した。

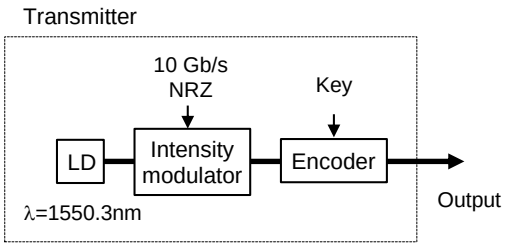


図 4：10 Gb/s の暗号信号光を生成する送信器の構成

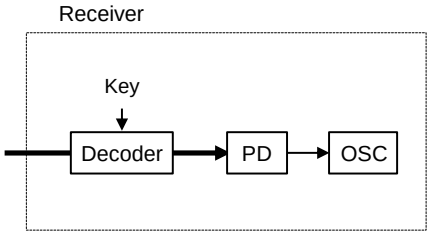
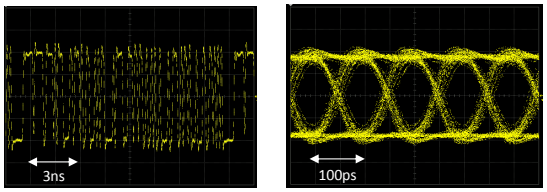


図 5：10 Gb/s の暗号信号光を復号する受信器の構成



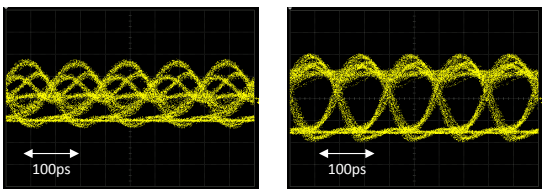
(a) (b)

図 6：送信器での暗号化前の 10 Gb/s 信号光波形。(a)データパターン波形(PN:2^{31}-1)、(b)アイパターン波形。

次に，この暗号信号光を受信する受信器の構成を図 5 に示す。暗号信号を復号するために，10 Gb/s の NRZ 強度変調暗号信号光を送信器と同様の周波数分解位相変調器入力した。位相マスクでは，送信器で用いた暗号鍵と同じ鍵を用いて送信器と逆の位相マスクを周波数領域で施し，10 Gb/s の NRZ 強度変調光信号に復号した。

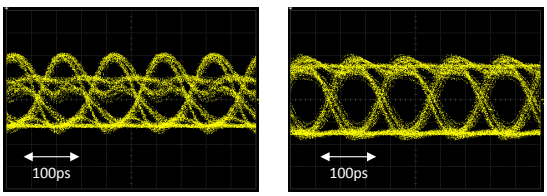
本実験では，復号後の信号光を光検出器で電気信号に変換後サンプリングオシロスコープを用いて波形を観測し，サンプリング波形を評価した。実験で用いた周波数領域での位相変調器の設計周波数分解能は 1 GHz。暗号鍵は 16 ビットとし信号光波長を中心に±8 GHz の帯域で変調を施した。変調器の挿入損失は実測で 4.5 dB と低損失だった。受信器では送信器と同じ暗号鍵を用いて，送信器での変調した位相量と逆の変調を施して暗号を復号した。光検出器の帯域は 12.5 GHz で，帯域 20 GHz のサンプリングオシロスコープで観測した。

初めに 10 Gb/s の信号光波形を図 6 に示す。変調条件は，DC バイアスをπ/2，変調振幅をπとした。(a)は，通信データとしてビット長 127 ビットの信号光パターン波形。スパンは 15 ns なので 1 周期強の波形が見られる。



(a) (b)

図 7：(a)送信器での暗号化後の 10 Gb/s 暗号光のサンプリング波形。(b)受信器での復号化後の 10 Gb/s 信号光のサンプリング波形。



(a) (b)

図 8：(a)送信器での暗号化後の 10 Gb/s 暗号光のサンプリング波形。(b)受信器での復号化後の 10 Gb/s 信号光のサンプリング波形。

波形変化を観測するには波形を重ね書きして表示したアイパターンの方が便利なので，アイパターン波形を同図(b)に示す。横軸のスパンは 500 ps で 5 個のアイ開口が観測されている。
次に，一例として，暗号鍵で暗号化した波形とそれを復号した波形を図 7(a)，(b)に示す。図 7(a)で特筆すべき点は，位相マスクにより波形が変わっていることである。図 6(b)の 10 Gb/s NRZ 信号に対して，理想的には CW 光の様に強度変調のない波形になるのが望ましいが，位相変調器の周波数領域での分解能制限，可変位相量の制約でそこまで波形は変化しないが，明らかに信号光波形の形状が変わり，盗聴者に対して波形は観測されにくくなっている。即ち，暗号文を正しく盗聴しづらくなっていることが分かる。次に，受信器でこの暗号波形を復号した。復号には暗号鍵と逆の位相マスクを設定した。復号後のサンプリング波形を図 7(b)に示す。強度透過特性の周波数依存性が完全に平坦ではないなど位相変調器の不完全性により完全に波形が戻らないものの，送信端での暗号化前の信号光(図 6(b))の形状に近い形の波形を観測できた。
別の暗号鍵をもちいて，暗号化、復号化を検証した。暗号化後の波形を図 8(a)に，受信器での復号化後の波形を(b)に示す。暗号化後は，図 7(b)と同様に位相変調により波形が変わっており，異なる暗号鍵を用いているので，異なる形状に波形が変化している。復号化後の波形(b)は，暗号化前の波形に近い形状に戻っている。
以上の実験評価により，本手法の暗号化・復号化の基本動作を検証することができた。この結果は本方式によりシャノン限界を超える暗号につながることを実験的に検証することができた。
次に本研究のもう一つの課題である，光ファイバ通信応用の研究を実施したので，以下にその結果を示す。光ファイバ通信応用を調査するために，光ファイバと光直接増幅器(EDFA)で構成される光ファイバ伝送路を用いて暗号信号光の伝送実験を行った。その実験系概要を図 9 に示す。本学では，光ファイバ通信研究施設として，本学内の地下に敷設してある光ファイバ通信回線「TAMA Net#1」を所有している。この敷設回線のファイバ種は単一モード光ファイバ(SMF)で，一つのスパンが長さ 40 km の SMF で構成され，合計で 25 スパン，総距離は 1,000 km になる。本研究では，TAMA Net#1 の 3 スパンの SMF を光ファイバ伝送路として利用し，120 km の伝送実験を実施した。
まず初めに SMF の群速度分散について調査した結果，暗号信号光の波長帯では群速度分散が大きいため群速度分散により波形が広がり通信特性に及ぼす影響を取り除くために，群速度分散補償が望ましいとの結論に至った。そのため，各スパンの SMF の出力端の実験室内に群速度分散を補償する分散補償ファイバ(DCF)モジュールを設置した。その後段に，EDFA を接続し，SMF の伝送損失および DCF モジュールの損失を補償した。高次の波長分散の影響、偏波モード分散の影響は無視できるほど小さいとの解析結果だったので、光ファイバ伝送路にこれらの影響を抑圧する機構は設置しなかった。
伝送路 SMF 入力光パワーは-3 dBm(0.5 mW)に設定して 120 km 伝送した後の暗号信号光のサンプリング波形を図 10(a)に示す。サンプリングオシロスコープのトリガーは伝送してきた暗号信号光から抽出した同期クロックを用いた。暗号鍵として図 8 の場合と同じ暗号鍵を用いて暗号化した。図 8 の波形と比較すると，伝送特性は線形伝送で群速度分散も補償したので，光増幅器による自然放出光雑音による光信号対雑音(OSNR)比の劣化により，雑音成分が多くなっている。次に 120km 伝送後の暗号信号光を復号した後のサンプリング波形を図 10(b)に示す。SN 劣化分があるが，波形自体は図 8 の場合と同様に送信器で暗号化する前のサンプリング波形に近い形に戻っている。このように，120 km 伝送後においても暗号信号光は暗号鍵により元の波形に戻ることを実験検証できた。
周波数領域における位相変調を用いた位相マスクデバイスの構成部品の改良により，周

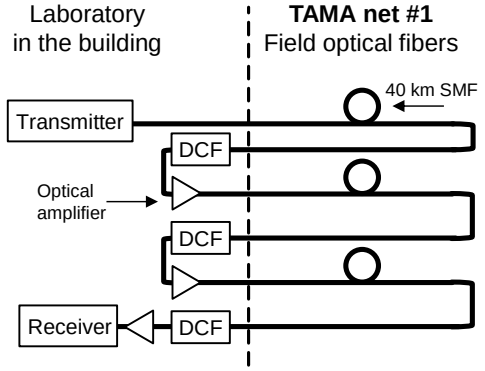


図 9：本学敷設光ファイバ回線「TAMA Net #1」を用いた中継距離 40 km，伝送距離 120 km の光直接増幅中継光ファイバ伝送路の構成。

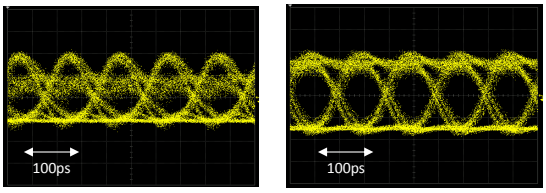


図 10：(a)120 km 伝送後の暗号信号光の 10 Gb/s サンプリング波形。(b)120 km 伝送号に復号した 10 Gb/s 信号光のサンプリング波形。

波数分解能を向上することが可能である。例えば，回折格子の溝本数を多くする，空間に展開する光のビーム経が大きくなるようなコリメータレンズを用いる，液晶変調器のサイズを小さくするなどである。これらの改良は，次のステップの研究課題である。
本成果は，原理実験のため，速度や安全性の性能自身は十分ではないが，この成果をベースとして，開発研究を継続すれば，社会的要請である暗号学のシャノン限界を破る実用的な暗号が実現できる可能性を示唆することができた。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計２件）
① Masaki Sohma, On the relation between Holevo's commutation operator and modular operator, Tamagawa University Quantum ICT Research Insitute bulletin, Vol.6, pp.25-27, 2016.
② Masaki Sohma, Cut-off Rate for ASK signal states, Tamagawa University Quantum ICT Research Institite Bulletin, Vol.5, pp.29-31, 2015.

〔学会発表〕（計４件）
① 二見史生, Y-00 光通信量子暗号の研究開発　～シャノン限界を超える物理暗号通信に向けて～, 第 15 回量子情報ミニワークショップ,2017 年 1 月 23 日,開春楼(静岡県浜松市).
② 相馬正宜, Introduction to Quantum IO Monad, 第 15 回量子情報ミニワークショップ, 2017 年 1 月 22 日, 開春楼(静岡県浜松市).
③ 二見史生, Y-00 光通信量子暗号とその応用　シャノン限界を超える物理暗号通信にむけて, 第 14 回量子情報ミニワークショップ, 2016 年 1 月 10 日, 木もれび(滋賀県大津市).
④ 相馬正宜, Cut-off Rate for Quantum Gaussian Channels, 第 14 回量子情報ミニワークショップ, 2016 年 1 月 9 日, 木もれび(滋賀県大津市).

〔その他〕
ホームページ等
http://www.tamagawa.jp/research/quantum

６．研究組織
(1)研究代表者
二見　史生（FUTAMI, Fumio）
玉川大学・量子情報科学研究所・教授
研究者番号：２０４１７６９５

(2)研究分担者
相馬　正宜（SOHMA, Masaki）
玉川大学・工学部・教授
研究者番号：　７０３８４７１６