# 科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　２４　日現在

機関番号：　３２６３９
研究種目：　挑戦的萌芽研究
研究期間：　2012～2013
課題番号：　２４６５６２４５

研究課題名（和文）シャノン限界を超える一般化物理暗号の研究

研究課題名（英文）Study on the general 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・准教授

研究者番号：２０４１７６９５

交付決定額（研究期間全体）：（直接経費）　　2,800,000円、（間接経費）　　840,000円

研究成果の概要（和文）：一般化コヒーレント・パルス位置変調法は，暗号学のシャノン限界を超える物理暗号を実現する理論モデルである一般化盗聴通信モデルにほぼ等価な特性を持つことが期待されている。本研究ではその実現を目指し，位相マスク型光通信量子暗号の実現法を解明することに挑戦し，光ファイバ通信で主に用いられる波長1.5μm帯で動作する液晶空間光変調器など光通信用デバイスを用いて，周波数領域で位相変調する方式で位相マスク型光通信量子暗号を実現する方法の解明に成功した。本成果により，暗号学のシャノン限界を超越する究極の光通信量子暗号の実現に向け大きく前進した。

研究成果の概要（英文）：The scheme of coherent pulse position modulation with phase mask is expected to be a concrete method of realization of the generalized wiretapped channel model (keyed communication in quantum noise) which provides the security beyond the Shannon limit of the cryptography. For realizing such a new idea, we have studied a scheme of Y-00 quantum stream cipher with phase mask and demonstrated a simple model for the phase mask modulation scheme. The phase mask is realized in the frequency domain by using optical devices such as the liquid-crystal spatial light modulators operating in the wavelength range of 1.5 micrometer suitable for the optical fiber communication. This result will give a great progress to realize whole scheme of Y-00 quantum stream cipher beyond the Shannon limit.

研究分野：　工学

科研費の分科・細目：　電気電子工学・通信・ネットワーク工学

キーワード：　暗号のシャノン限界　物理暗号

## １．研究開始当初の背景

情報通信技術が飛躍的に発展し，様々なネットワークサービスが日常的に利用されている今日，個人情報や極秘情報など当事者以外に盗み見られると問題になったり，大きな損害を被る可能性のある情報もネットワークを流通している。通信情報の秘匿性が完全なものでないと，今後のネットワークの発展が妨げられる危険性が指摘されている。現在，数理暗号により必要に応じて通信情報が暗号化され、当事者以外への情報漏洩・盗聴の防止に活用されているが，数理暗号の安全性は，現実的な時間内には鍵を盗むための計算ができないという「計算量的安全性」を拠としている。従って，逆計算のアルゴリズムに近道が発見されると，計算量は激減し，現実的な時間内で鍵を算出することが可能になる。このように，数理暗号では安全性を保証することが難しいという大きな壁がある。対照的に，物理暗号は安全性を物理現象によって定量化でき，究極的な暗号を実現できる可能性がある。特に，光の巨視的量子性に着目した量子暗号である Y-00 暗号は，安全性保証可能な暗号を実現できる有力な候補である。Northwestern 大学の H. P. Yuen が提唱した Y-00 暗号は，位相変調、強度変調などの実現方式があり，特に，強度変調方式は他の方式と比較してシンプルでかつ量子雑音効果を極めて大きく利用できる。更に，現状の光通信システムとの整合性に優れている。現在,著者等が開発中のY-00暗号は基本Y-00で，数理暗号よりも強力な暗号として実利用を目指し，ビットレート 40 Gb/s の伝送が可能なまでになっている。基本 Y-00 の安全性は，盗聴者の受信デバイスの物理制限の下で盗聴不可能（情報理論的安全）が保証されている。将来的には，一切の条件を取り外した究極的な物理暗号の実現が強く求められている。そのためには，無条件で暗号学のシャノン限界を破る変調・復調の構成法が必要となる。

## ２．研究の目的

本研究では，暗号学のシャノン限界を超える物理暗号を実現する理論モデルである一般化盗聴通信モデルにほぼ等価な特性を持つことが期待される一般化コヒーレント・パルス位置変調法等の実現法を解明することに挑戦することを目的としている。

## ３．研究の方法

一般化コヒーレント・パルス位置変調方式を光通信デバイスによって実現する方法の研究を行った。特に，光ファイバ通信で用いられる波長1.5μm帯で動作する光通信デバイスを用いた位相マスク型光通信量子暗号の実現方法に関して，位相マスク技術の実現方法の解明を行った。

図１に暗号通信の基本構成を示す。送信者と受信者が暗号鍵(乱数)を共有している。送信者は，通信する情報を暗号鍵で暗号化し，暗号文を作成する。具体的には, 2 値信号(“０”, “１”)からなる情報を乱数でスクランブルする。暗号文は，通信路を伝搬し，受信者に到達する。受信者は，暗号に使用した同じ暗号鍵で情報を復号する。このようにして，遠隔地の二者間で通信が成立する。

通信路で暗号文が傍受された場合，一般に，

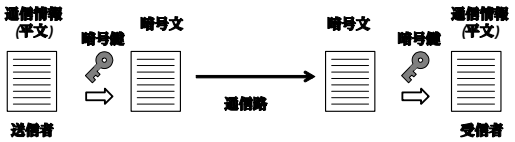


図１：暗号通信の基本構成

暗号鍵がないと情報を盗み読むことができない。ただし，暗号強度が弱いと，情報を盗聴される危険がある。いかにして強い暗号を実現するかが，安全性に直結する。

一般に，盗聴のステップは，次の二つに大別できる。

(1) 暗号文を正しく傍受
(2) 傍受した暗号文を解析

数理暗号では，暗号文も 2 値信号なので，ステップ(1)の暗号文の傍受は容易である。従って，暗号強度が弱いと，(2)の暗号文解析により，通信情報や暗号鍵が盗聴されてしまう。より強い暗号を実現する手法の一つは，ステップ(1)を阻止する方法である。

位相マスク型光通信量子暗号は，通信情報を載せた信号光の位相を，暗号鍵に基づく乱数で変調し，信号光波形を乱すことを特徴とする。即ち，ステップ(1)の暗号文を傍受させない。図 2 に示すように，理想的には，位相マスク(位相変調)により，信号光の強度を一定にし，これにより暗号鍵のない盗聴者に，暗号文を傍受させない。


図２：位相マスク型光通信量子暗号による暗号通信

位相マスク型光通信量子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，位相マスク型光通信量子暗号は，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ある。図 3(a)に時間領域での変調方法例を示す。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

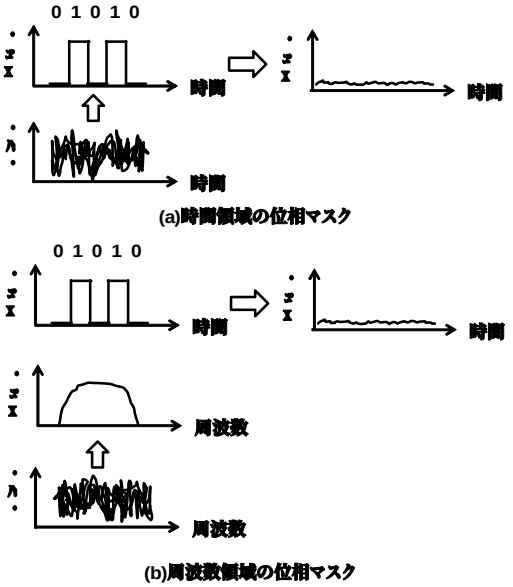


図 3：位相マスク技術。(a)時間領域，(b)周波数領域

変調が必要になる。現実の要求に見合った Gb/s 級の信号の位相を変調する場合，暗号鍵長を 100 ビットとすると，帯域 100 GHz の位相変調が必要になり，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。なお，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。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 に位相マスク型光通信量子暗号を実現する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を示す。構成する各デバイス選定においては部品の低損失性を重視した。光ファイバ通信では，光ファイバの伝送損失が最も小さくなる波長 1.5μm 帯の光が主に用いられている。光通信に応用する場合，光信号対雑音比が通信特性を本質的に

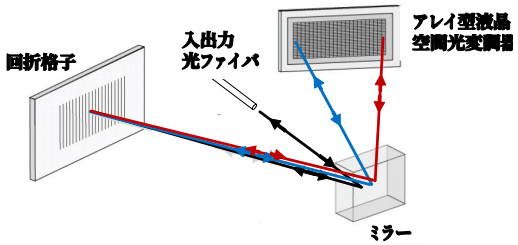


図 4：周波数領域における位相変調を用いた位相マスクデバイスの構成

制限してしまうため，光パワーを高い値にたもつことが可能な低損失の部品選定が重要になる。各部品の動作原理と機能を以下に示す。まず，光ファイバからコリメータレンズを用いて平行光の光を空間に展開する。次に，回折格子で周波数毎に回折角が異なることを用い，信号光を各周波数成分に分光する。回折格子での分解能が主に位相変調の周波数分解能を決める。光の位相を変調できる液晶変調器をアレイ状に配置したアレイ型液晶空間光変調器で，それぞれの液晶変調器を透過する各光周波数成分の位相を独立に変調する。図面では，反射型の構成になっている。液晶素子に印加する電圧の大きさにより，各液晶変調器で位相を 0～2π まで変調できるようになっているので，任意の位相変調を与えることができる。位相変調後，回折格子を介し，周波数別だった光を再び平行光に変換し，コリメータレンズを介して，光ファイバに集光する。図面では反射型回折格子を示しているが，アレイ型導波路回折格子を用いると高い分解能を実現できる。

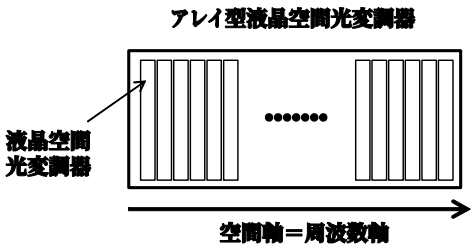


図 5：アレイ型液晶空間光変調器の構成

次に，アレイ型液晶空間光変調器の構成について説明する。図 5 に示すように，水平方向に複数の液晶光変調器が配置している。回折格子で分光されているので，水平方向が周波数軸に対応する。液晶は印加する電圧に応じて，透過する光の位相を変調することができる。本図面では，各液晶変調器に独立に透明電極が設置され，反射して戻ってくる間に，電極に印加した電圧に応じた位相シフトを与えられる。個々の液晶に独立に電圧を印し，各周波数成分の位相を独立に変調できる。
波長 1.5μm 帯で動作する光通信デバイスを用いて，位相変調できる周波数成分の分解能を算出した。回折格子の溝本数は 2400 本/mm，

液晶変調器のサイズは100μmのものを用いた．その結果，波長1.5μm帯の信号光の周波数成分を，分解能 1GHz 程度で，位相変調できることが分かった。帯域はピクセル数で決まり，100個の液晶変調器を用いれば，100GHzの帯域の信号の位相を変調することができる。
次に，光ファイバ通信で用いられる高速信号に対して，この分解能でどの程度の自由度で位相変調可能か検証した。ここで，予備知識として，信号光のデータ強度変調について示す。主に，NRZ（Non Return to Zero）およびRZ(Return to Zero)と呼ばれる強度変調方式がある。NRZは，”1”が続いた場合，光がない状態に戻らない。そのため，ビットレートがBとすると，信号光が占有する周波数帯域もBとなる。一方，RZは，”1”が続いても，光がない状態に戻る。ビットレートをBとすると，信号光のタイムスロットは 1/B になる。”1”の場合，光がある時間幅(パルス幅)とタイムスロットの割合をデューティー比と呼ぶ。例えば，デューティー比が 1:10 だとすると，光が占有する周波数帯域は 20×Bと，ビットレートの20倍になる。NRZの場合，ビットレート B = 10 Gb/s を想定すると，信号帯域は 10 GHz になるので，位相変調できるのは液晶空間光変調器の数は 10 程度になる。この程度では，大きく波形を乱すことは困難だと考えられる。一方，RZの場合，ピクセル数はデューティー比により大きく変えられる。例えば，ビットレートがB = 10 Gb/sでデューティー比が 1:10 とすると，帯域は200 GHz になり，液晶空間光変調器数は 200程度になる。更に，デューティー比が高く，1:100だとすると，帯域は10倍になり，ピクセル数は 2000 程度になる。これだけ多くのピクセルを使用できると，波形を大きく乱し，盗聴者には波形を認識させなくすることが可能になる。 ビットレート B = 10 Gb/s の場合，パルス幅を 1 ps にすると，デューティー比1:100を実現できる。なお，10 GHzと高速でも，1 ps程度の光パルスを安定に生成する技術は既に確立されている。
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, Osamu Hirota, Masking property of quantum random cipher with phase mask encryption, Quantum Information Processing, springer, 査読有, Vol.13, 2014, 印刷中, DOI 10.1007/s11128-014-0748-4.
② Masaki Sohma, Osamu Hirota, Quantum random cipher with phase mask encryption, Tamagawa University Quantum ICT Research Insitute bulletin, 査読有, Vol.1, 2013, 5-9, http://www.tamagawa.jp/research/quantum/bulletin/pdf/Tamagawa.Vol.2-2.pdf


〔学会発表〕（計 4 件）


① 二見史生, Y-00実験評価進捗状況とシャノン限界を超える物理暗号について，第12回量子情報ミニワークショップ，2014年1月21日，花乃丸(愛知県知多郡).
② 相馬正宜, Quantum random cipher with phase mask encryption, 第11回量子情報ミニワークショップ，2013年2月21日，鳥羽シーサイドホテル(三重県).
③ 二見史生, Y-00暗号通信システム研究開発状況と展望, 第11回量子情報ミニワークショップ，2013年2月20日，鳥羽シーサイドホテル(三重県).
④ Masaki Sohma, Osamu Hirota, Coherent pulse position modulation quantum cipher, 11th International Conference on Quantum Communication, Measurement and Computing, 査読有, 2012年8月2日. ウィーン(オーストリア).


〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）
○取得状況（計 0 件）

〔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・准教授
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

広田　修（HIROTA, Osamu）

玉川大学・量子情報科学研究所・教授
研究者番号：４０１１４８８９

(3)連携研究者
なし