玉川大学学術研究所紀要　第19号：1–4（2013）
Tamagawa University Research Review, 19, 1–4 (2013).

位相マスク型光通信量子暗号の実験評価に向けた基礎研究

二見史生[1]　相馬正宜[2]　加藤研太郎[1]　政田元太[1]
1：玉川大学　量子情報科学研究所，2：玉川大学　工学部
〒194-8610 東京都町田市玉川学園 6-1-1
E-mail: futami@lab.tamagawa.ac.jp

あらまし　暗号学のシャノン限界を超越する暗号の実現を目指し，位相マスク型の光通信量子暗号について研究を行った．回折格子による分光と液晶素子がアレイ状に並んだアレイ型液晶空間光変調器を使うことにより，信号の周波数成分別に位相を変調できることを利用し，実際の光部品で実現可能な周波数分解能を算出し，高速信号に対してどの程度の自由度で位相変調可能か明らかにした．

キーワード　波長分割多重方式，光通信量子暗号，Y-00

Basic research for experimental demonstration of quantum stream cipher by phase mask modulation

Fumio Futami[1)], Masaki Sohma[2)], Kentaro Kato[1)] and Genta Masada[1)]
[1)]Quantum Communication Research Center, Quantum ICT Research Institute, [2)]Department of Intelligent Mechanical Systems, College of Engineering, Tamagawa University,
6-1-1 Tamagawa-gakuen, Machida, Tokyo, 194-8610 Japan

Tamagawa University Research Review, 19, 1-4 (2013).

Abstract

For realizing the cipher exceeding the Shannon limit, basic research on quantum cipher by phase modulation is carried out. Frequency components of optical signal are modulated in the frequency domain independently by use of an arrayed spatial light modulator composed of liquid-crystal modulators. Employing the technique, the achievable frequency resolution for high-speed signals is calculated assuming the use of optical components practically available, and the number of the liquid-crystal modulator is estimated for the experimental demonstrations.

1. はじめに

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，個人情報や秘密情報など当事者以外に盗み見られると問題になる情報もネットワークを流通している．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課題がある．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．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[1,2]は，位相変調[3]，強度変調[4,5]，直交振幅変調[6]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，量子情報科学研究所で開発中の Y-00 暗号は基本 Y-00 で，数理暗号よりも強

1)玉川大学量子情報科学研究所超高速量子通信研究センター
2)玉川大学工学部機械情報システム学科

力な暗号として実利用を目指し，試作した 2.5 Gb/s Y-00 トランシーバで実運用ネットワーク接続試験[7]や屋外敷設光ファイバ回線で 2 ヶ月間にわたる運用試験[8]を行ったり，40 Gb/s 通信実験[9]が可能なまでになっている．また，安全性の基礎実験検証[10,11]も実施済みである．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．

暗号学の観点から，いかに安全に多くの情報を，少ない鍵により通信できるかが重要な側面である．暗号学でシャノン限界と言われる限界があり，これは，通信する情報量と同量の乱数を用いて暗号化し，安全性を実現することである.シャノン限界を超えることは，通信情報量よりも少ない乱数を用いて安全な通信を行うことで，乱数の利用効率を高めることができ，効率的な安全通信を実現できる．数理暗号で，シャノン限界を超越することができないことは明らかになっているので，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，量子情報科学研究所では，無条件でシャノン限界を破る変調・復調の構成法の理論研究を行っており，これまで，シャノン限界を超える手法として，コヒーレント・パルス位置変調(CPPM: Coherent Pulse Position Modulation)[12]や位相マスク型光通信量子暗号[13]を提案している．更に，これらの基礎実験検証を目指した実験研究に取り組んでいる．

本稿では，位相マスク型光通信量子暗号の実験検証に向け，アレイ型液晶空間光変調器を用いた周波数領域における位相変調方式について検討した結果を示す．特に，実信号に適用するための周波数領域での分解能を算出し，アレイ型液晶空間光変調器でどの程度の自由度で位相変調可能か見通しを得られた．

2. 暗号通信の基本構成

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．

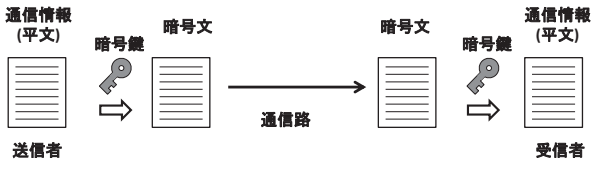

図 1：暗号通信の基本構成

通信路で暗号文が傍受された場合，一般に，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．これは，数理暗号にはない概念で，コヒーレント・パルス位置変調や位相マスク型光通信量子暗号は，この概念に基づき，暗号文を盗聴者に正しく傍受させないことで，高い安全性を有する暗号を実現し，更に，シャノン限界超越を目指すものである．

3. 位相マスク型光通信量子暗号

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．詳細は文献[13]に記述されているが，図 2 に示すように，理想的には，信号光の強度を一定にする．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文傍受阻止

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．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するので，解読法の発見を排除することができず，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，詳細な安全性理論は文献[13]に記述してあるが，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．

4. 位相マスクの実現方法

4.1. 位相マスク技術

位相マスクを実現する手法は様々ある．大別すると，時間領域で変調する方式と周波数領域で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，高速の変調が必要になる．現実の要求に見合った Gb/s 級の信号を想定すると，高速変調は課題になる．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．

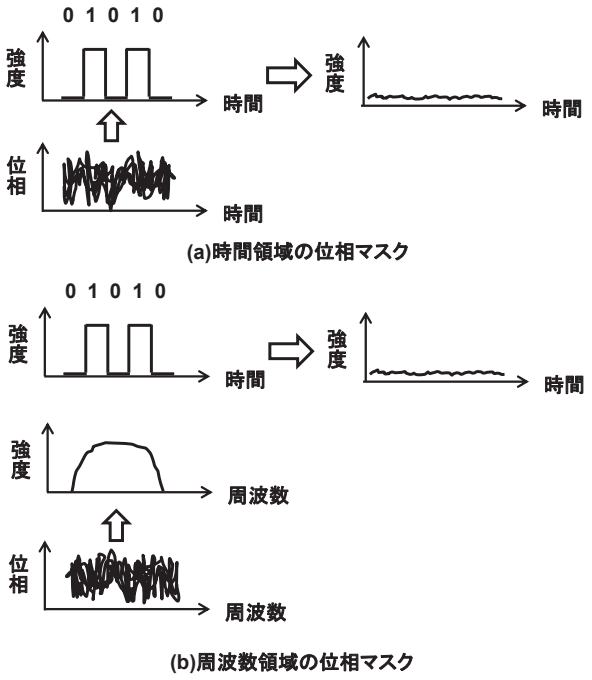

図 3：位相マスク技術．(a)時間領域，(b)周波数領域

4.2. 周波数成分の位相マスクの原理

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．

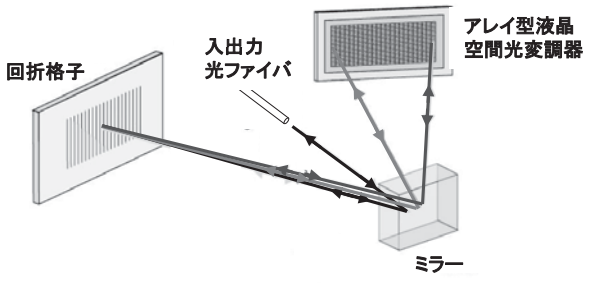

図 4：周波数領域での位相マスク概念

概念図を図 4 に示すが，まず，光ファイバから光を空間に出力し，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．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．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．

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なっている．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．本図面の例では，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．

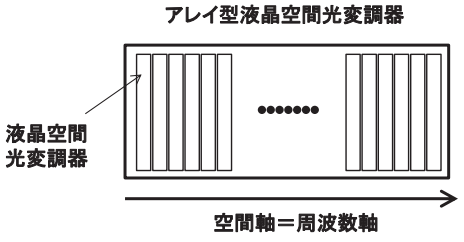

図 5：アレイ型液晶空間光変調器の構成

4.3. 周波数成分位相マスクの分解能と実現性

実際の部品の仕様をもとに，文献[14]を参照して周波数分解能を算出した結果，波長 1.5μm 帯の信号光の周波数成分を，分解能 1GHz 程度で，位相変調できる知見を得られた．この分解能は，図 5 の各ピクセルの幅に対応する．この分解能を前提に，高速信号に対して，どの程度の自由度で位相変調可能か検討した．

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説明する．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と考えられる．

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[15]されている．

5. 今後の計画

位相変調量および液晶空間光変調器数による波形変化は，NRZ，RZ 共に，数値解析シミュレーションにより計算できる．今後，シミュレータを構築し，数値解析を進める．また，得られた波形により，どの程度，盗聴者が暗号文を入手しにくいか理論検討を行う．更に，実験検証に向け，実験系を完成させ，シャノン限界超越の実証実験を行う．位相変調後の波形の光ファイバ伝送についても，数値解析や実験検証をすすめる．

コヒーレント・パルス位置変調と位相マスク型光通信量子暗号を併用すると，更に強靭な暗号を実現できるので，理論研究および実験研究を推進する．

6. まとめ

本稿では，暗号学のシャノン限界を超越可能な位相マスク型光通信量子暗号の実験検証に向けた検討を行った．アレイ型液晶空間光変調器を用いた周波数領域における位相変調方式で，実際の信号に適用するための周波数領域での分解能を算出した．その分解能をもとに，高速信号光に対して，アレイ型液晶空間光変調器でどの程度の自由度で位相変調可能か検討した．これまで理論研究が中心だった位相マスク型光通信量子暗号の実験検証にむけ，研究が大きく前進した．

謝辞

本研究の一部は，玉川大学学術研究所共同研究助成および富士通研究所委託研究により実施した．

文　献

[1] H. P. Yuen, “A new quantum cryptography,” Report in Northwestern University, 2000.

[2] H. P. Yuen, R. Nair, E. Corndorf, G. S. Kanter, and P. Kumar, The security of alpha-eta: response to some attacks on qauantum-based cryptographic protocols, Quantum Information and Computing, vol.6, p.561, 2006

[3] G. A. Barbosa, E. Corndorf, P. Kumar, H. P. Yuen, Secure communication using mesoscopic coherent states, Phys. Rev. Lett., vol.22, 227901, 2003.

[4] 広田修，光通信ネットワークと量子暗号，電子情報通信学会論文誌 B, J-87-B, No.4, p.478, 2004.

[5] 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, 022335, 2005.

[6] K.Kato and O.Hirota, Quantum quadrature amplitude modulation system and its applicability to coherent state quantum cryptography, SPIE conference on quantum communication and imaging III. SPIE Proc. vol-5893, 2005.

[7] 二見史生，広田修，本田真，圷重人，原澤克嘉，” 光通信量子暗号(Y-00)試作器の本学 LAN の GbE 通信への適用実験”，電子情報通信学会，OCS2010-57, pp-25-30, (2010-10), 2010.

[8] F. Futami and O. Hirota, “Field transmission test of 2.5 Gb/s Y-00 cipher in 160-km (40 km × 4 spans) installed optical fiber for secure optical fiber communications,” 11th International Conference on Quantum Communication Measurement and Computing (QCMC2012), P1-38, 2012.

[9] F. Futami and O. Hirota, “40 Gbit/s (4 × 10 Gbit/s) Y-00 protocol for secure optical communication and its transmission over 120 km,” OFC, OTu1H.6, 2012.

[10] F. Futami and O. Hirota, “Masking of 4096-level Intensity Modulation Signals by Noises for Secure Communication Employing Y-00 Cipher Protocol,” 37th European Conference on Optical Communication (ECOC 2011), Tu.6.C.4, Geneva, Switzerland, 2011.

[11] 二見史生，広田修，Y-00(光通信量子暗号)のランダム暗号としての性能評価実験，信学技法，OCS2010-105, pp.37-42, (2011-01), 2011.

[12] 相馬正宜，広田修，光通信量子暗号としての Y-00 と CPPM の特徴比較 ~ 暗号文をランダム化する暗号 ~, 信学技法, ISEC2010-4, pp.17-24, (2010-05), 2010.

[13] M. Sohma, O. Hirota, “Quantum Random Cipher with Phase Mask Encryption,” Tamagawa University Quantum ICT Research Institute Bulletin, vol.2 no.1, pp.5-9, 2012

[14] A. M. Weiner, D. E. Leaird, J. S. Patel, and J. R. Wullert, “Programmable femtosecond pulse shaping by use of a multielement liquid-crystal phase modulator,” Optics Letters, vol. 15, no. 6, pp. 326 - 328, 1990.

[15] M. Nakazawa, E. Yoshida, and Y. Kimura, “Ultrastable harmonically and regeneratively modelocked polarization-maintaining erbium fiber ring laser,” Electron. Lett., vol. 30, no. 19, pp. 1603 – 1605, 1994.