量子雑音によるランダムストリーム暗号 Y-00

広田　修・相馬　正宜・川西　悟基

Quantum Noise Randomized Stream Cipher

Osamu HIROTA, Masaki SOHMA and Satoki KAWANISHI

It is well known that there is the Shannon limit for information theoretic security of the conventional symmetric key cipher. However, it is pointed out that the Shannon limit is not an absolute limitation. Hence it should be denoted that the conventional ciphers belong to the Shannon theoretical frame. Yuen protocol so called Y-00 is an example of the ciphers which get out of the Shannon frame. Y-00 consists of Gauss private randomization and quantum measurement theory. We explain that Y-00 cannot be described by Shannon theory showing an explicit example, and introduce the realization methods of the ultimate security based on Y-00 protocol.

Key words: random cipher, Y-00, quantum stream cipher, quantum optimum receiver

これまで，量子暗号は Shannon（シャノン）[1] の暗号理論体系において最も安全性が高い one time pad を実現する補助技術として，安全な鍵配送の実現を目的に発展してきた．しかし，鍵配送に加えて，物理現象を用いて直接データを暗号化する量子共通鍵暗号を研究考察の対象とする時期にきている．特にストリーム暗号は高速性，時間遅延特性にすぐれており，その量子版を開発対象とすることは自然である．固定の短い共通鍵で究極的に安全性がどこまで保証できるかを研究することは挑戦的な課題であるが，数理的な暗号ではシャノン限界がある．この限界を超越しようとする試みはこれまで挑戦されたが，成功した事例はない．シャノン限界を超越する暗号構成理論の一例が 2000 年の DARPA のプロジェクトにおいて Yuen（ユーエン）によって提案された [2]．それは KCQ 原理（“keyed communication in quantum noise”）とよばれる従来にはない概念を基礎としている．これは現在ユーエン-2000（Y-00）プロトコルとよばれているランダムストリーム暗号 [3,4] の原型である．Y-00 はこれまでのいかなる暗号とも異なる新しいランダム暗号を実現する技術である．すなわち，変調方式と暗号理論を融合させることによって，正規受信者と盗聴者の情報収集能力に決定的な差を作り出し，従来の暗号では実現できない安全性を実現する [5–7]．加えて，原則的に現在使用されている普通の光通信装置を変形して実現できることは特質のひとつである．一方，正規受信者の二値量子最適受信器が開発されれば，情報理論的安全性をもつ共通鍵暗号通信が実現可能である [8]．本稿では，KCQ 原理から派生的に開発された新しいランダム暗号である Y-00 プロトコルが既存の暗号理論とどのように異なるかを詳細に解説し，現時点で知られている，この魅力ある究極的な暗号を実現するための方法論を紹介する．

1. シャノン暗号理論

Shannon の 1949 年に出版された暗号理論に関する論文は，共通鍵暗号の情報理論的解析の基盤を与えるものである [1]．ここでは，その概要を記述する．まず，平文を X_n，暗号文を Y_n，共通鍵を K_s とする．このとき，暗号文単独攻撃に対する平文の情報理論的安全性は以下のように定義される．

〈定義 1〉

$H(X_n|Y_n)>0$ であれば，暗号文単独攻撃に対し，この平文は情報理論的安全であると定義する．

次に，共通鍵暗号の情報理論的安全性の限界として，以

玉川大学量子情報科学研究センター（〒 194–8610 町田市玉川学園 6–1–1）　E-mail: hirota@lab.tamagawa.ac.jp

下のような定理が示された．

〈定理１　シャノン限界〉

共通鍵暗号の情報理論的安全性の限界は，以下のように暗号文の条件付きエントロピーが共通鍵 Ks のエントロピーより小さいという関係式で表現される．

$$H(X_{\mathrm{n}}|Y_{\mathrm{n}}) \leq H(K_{\mathrm{s}}) \qquad (1)$$

上記定義のもとで，以下の結論が得られる．

〈定理 2〉

完全秘匿を達成する必要条件は，定理１より以下のようになる：$H(X_{\mathrm{n}}) = H(K_{\mathrm{s}})$．

上記の結果は，完全秘匿を実現するには平文と同じ長さの鍵系列を共通鍵として共有する必要があることを示唆する．すなわち，one time pad が必要である．

2.　シャノン理論枠の超越

2.1　ガウス・ユーエンランダム暗号

前章で述べたように，共通鍵暗号の情報理論的安全性にはシャノン限界とよばれる限界がある．しかし，その限界が暗号の理論において絶対的なものであるという証明は存在しない．したがって，ここでは，それをシャノン理論枠ということにする．以上より，シャノン限界を破る具体的な暗号が発見されれば，それはシャノン理論枠を超えたといえる．ユーエンは，ガウスによって提唱された“私的ランダム化”を用いてシャノン理論枠を超える暗号が構成可能か否かに挑戦した．その結果，以下のようなランダム暗号を定義し，その構成原理の研究を行った．

〈定理 3（Yuen, 2006 [5]）〉

ランダム暗号によってシャノン限界を超える，すなわち $H(X_{\mathrm{n}}|Y_{\mathrm{n}}) > H(K_{\mathrm{s}})$ の必要条件は，正規受信者（Bob）の取得する暗号文と盗聴者（Eve）の暗号文が異なることである．

$$\boldsymbol{Y}^{\mathrm{B}}(\mathrm{n}) \neq \boldsymbol{Y}^{\mathrm{E}}(\mathrm{n}) \qquad (2)$$

〈定理 4（Hirota, 2009 [8]）〉

シャノン限界を超える必要条件を実現するには，量子力学的効果（量子重ね合わせの崩壊）が必要である．

〈定義 2〉

正規受信者と盗聴者の暗号文が異なり，かつ正規受信者の受信信号の誤り確率が盗聴者のそれより小さいランダム暗号をガウス・ユーエンランダム暗号と定義する．

以上のように，シャノン限界を超越することが可能であれば，共通鍵暗号の情報理論的安全性の理論体系を再整備する必要がある．

2.2　暗号の安全性概念の拡張

ここでは，正規受信者の暗号文取得の誤り確率が十分小さくできると仮定して議論する．

2.2.1　平文に対する暗号文単独攻撃

シャノン限界を破る必要条件は簡単に実現することが可能であるが，十分条件は現時点で明確に解明されていない．ガウス・ユーエンランダム暗号において，正規受信者の暗号文が誤りなしで，かつ盗聴者の取得する暗号文の誤りが大きく，その暗号文から復号される平文の復号誤りが2分の1に漸近すれば，数学的な証明は別途必要であるが，シャノン限界を大きく超えて，以下が期待できる．

$$H(X_{\mathrm{n}}|Y_{\mathrm{n}}^{\mathrm{E}}) \sim H(X_{\mathrm{n}}) \qquad (3)$$

これを準完全秘匿という．

無条件安全鍵配送が可能となる以下の条件式（4）[2,9] が成立するときは明らかにシャノン限界を超え，準完全秘匿となりうる．

$$H(X_{\mathrm{n}}|Y_{\mathrm{n}}^{\mathrm{E}}, K_{\mathrm{s}}) > H(X_{\mathrm{n}}|Y_{\mathrm{n}}^{\mathrm{B}}, K_{\mathrm{s}}) \sim 0 \qquad (4)$$

しかし，これは非常に強い条件であり，盗聴者が信号測定の後で真の鍵を得たとしても，正確な平文を解読することができないことを意味する．

2.2.2　既知平文攻撃

盗聴者は暗号文と伝送されている平文が与えられる．このとき，数理暗号では情報理論的安全性を実現することは不可能である．したがって，既知平文攻撃に対する情報理論的安全性は議論されなかった．ここでは，定義と評価法を与える．

〈定義 3〉

以下を満足するとき，既知平文攻撃に対して強情報理論的安全と定義する．

$$\inf_{\mathrm{n}} H(K_{\mathrm{s}}|Y_{\mathrm{n}}^{\mathrm{E}}, X_{\mathrm{n}}) > 0 \qquad (5)$$

上式の inf は n に対する最小化を意味する．

具体的な評価法として以下が提案されている[10]．

$$S(\mathrm{n}) = \max_{\boldsymbol{Y}^{\mathrm{E}}} \max_{K_{\mathrm{s}} \in \boldsymbol{K}_{\boldsymbol{Y}^{\mathrm{E}}}} P(K_{\mathrm{s}}|\boldsymbol{Y}^{\mathrm{E}}(\mathrm{n})) \qquad (6)$$

ただし，$0 \leq S(\mathrm{n}) \leq 1$．既知平文攻撃に対する情報理論的安全性の一般理論は，現時点ではまだ確立されていない．しかし，先の条件式（4）が成立すれば，従来の暗号には存在しない情報理論的安全性の存在が保証される．なぜなら，真の鍵でも真の平文を特定できないことは，真の平文を知っていても，真の鍵を特定できないことを意味するからである．

3. ユーエンプロトコル：基本 Y-00

ガウス・ユーエンランダム暗号を実現する具体的なプロトコルの一例はユーエン-2000（Y-00）である．Y-00 は基本的に共通鍵暗号であるストリーム暗号の一般化である．したがって，送信者（Alice）と受信者（Bob）は最初に短い共通鍵 K_s を共有する．その鍵の知識で本来，盗聴者の盗聴環境が優位である通信路に有意性を作り出す．その基本概念を以下に説明する．

基本的なプロトコルを以下に示す．

(a) Alice は光送信器において，$2M$ 個の古典的な位相信号に対応する非直交量子状態（一般にコヒーレント状態：$|\alpha\rangle$, α は光信号の複素振幅）を用意し，それぞれ 2 つを組としてデータ 1 と 0 を送る基底状態の対とする．したがって，用いられる位相のセットは M 個となり，データ 1 と 0 を送信する位相は順番に交互にセットされる．すなわち，(1：0 度，0：180 度)，(1：190 度，0：10 度)，(1：20 度，0：200 度)，…．

(b) 共通鍵 K を擬似乱数生成器（線形フィードバックシフトレジスター，あるいは非線形）で長い擬似乱数 K^* に伸長し，その列の $\log M$ ビットのブロックの十進数に対応する基底を M 個の基底集合から選ぶ．選ばれた基底でデータである 1 か 0 を伝送する．スロットごとに基底が異なるので，各スロットにおけるデータ 1 と 0 に対応する光信号（コヒーレント状態）は疑似乱数に従って不規則となる．

(c) Bob は Alice と同じ擬似乱数をもつので，どの基底が用いられているか既知のため，常に 1 と 0 の二値位相シフトキーイング（PSK）の受信が可能である．ただし，その受信時の誤りは十分小さい条件で使用する．

(d) 盗聴者はシード鍵（さらに擬似乱数列）を知らないので，送信直後の光信号をモニターする際，盗聴者は $2M$ 個の量子状態を識別しない限り暗号通信に関するいかなる情報も得ることができない．ここで，$2M$ 個の量子状態は密に並んでいるので，誤り確率や S/N 比は Bob のそれよりきわめて悪い状況となる．

このような状況において，正規受信者は信号間距離の大きな二値の信号の判定を採用でき，盗聴者は信号間距離の小さな多値信号の判定を採用することになる．

このように，基本的な構造は従来の光通信の概念を用いて構成されるため，これは“光通信量子暗号”とよばれる．暗号学的な名前としては，量子雑音によるランダム化ストリーム暗号や単に量子ストリーム暗号が用いられる．

4. 量子重ね合わせ崩壊の制御

光通信量子暗号によって究極的な暗号を実現するためには，定理 4 より光信号の量子状態の重ね合わせが測定によって崩壊する現象を利用する必要がある．量子測定を数理的に公式化する試みはすでに長い歴史がある．量子測定理論の数学的な一般化から発見された量子最適受信理論は，Y-00 の安全性理論には必要不可欠である．ここでは，その理論体系を簡単に紹介する．

4.1 一般化量子測定理論

量子物理学における確率現象には，教科書で解説されているような量子測定に関する理論のみでは完全に記述することができないものがある．光信号の測定過程の厳密な解析においても，従来の量子確率論を拡張する必要がある．それらは，一般化量子測定理論として 1970 年代に議論された．その拡張は，単位分解の一般化である確率作用素測度（POVM）の導入によって実施された．この確率作用素測度は，次のような条件を満足するエルミート作用素 $\boldsymbol{X}$(B) として定義される．(1) $\boldsymbol{X}(B)\geq 0$，$B\in\mathcal{B}$（非負性），(2) $\boldsymbol{X}(B)=\Sigma_j\boldsymbol{X}(B_j)$（加法性），(3) $\boldsymbol{X}(\phi)=0, \boldsymbol{X}(\Omega)=I$．ヒルベルト空間 $\mathcal{H}_s$ は量子状態 $\{\rho\}$ によって構成されるものとする．量子測定に伴う確率分布は同様に

$$T_r\rho\boldsymbol{X}(B)\equiv P(x\leq B),\quad B\in\mathcal{B} \qquad (7)$$

上式は確率としての条件をすべて満足する．以上より，量子測定による量子重ね合わせの崩壊は信号の量子状態と量子測定を表す確率作用素測度によって制御できることがわかる．

4.2 最適条件

量子重ね合わせの崩壊によって発生する量子雑音の効果を最小にするための最適理論は，量子信号検出理論とよばれる．その最適問題の結実は以下の定理である[11]．

〈定理 5（Holevo, Yuen-Kennedy-Lax, 1973)〉

最小誤り確率を与える測定過程の必要十分条件は：

$$\begin{aligned}&(\boldsymbol{W}_j-\gamma)\boldsymbol{X}_j=\boldsymbol{X}_j(\boldsymbol{W}_j-\gamma)=0,\quad\forall j\\&\boldsymbol{X}_j(\boldsymbol{W}_i-\boldsymbol{W}_j)\boldsymbol{X}_i=0,\quad\forall i,j\\&\boldsymbol{W}_j-\gamma\geq 0,\quad\forall j,\quad \boldsymbol{W}_j\equiv\sum_{j=1}^{M}=\xi_iC_{ji}\rho_i\end{aligned} \qquad (8)$$

このとき，平均誤り確率は以下の最小値となる．

$$\overline{P_e}=T_r\gamma,\quad \gamma=\sum_{j=1}^{M}\boldsymbol{X}_j\boldsymbol{W}_j=\sum_{j=1}^{M}\boldsymbol{W}_j\boldsymbol{X}_j \qquad (9)$$

5. Y-00 のための量子最適受信の理論

基本 Y-00 による光通信量子暗号は鍵を知っている正規受信者と鍵を知らない盗聴者の信号測定の精度の違いに

よって，共通鍵暗号のシャノン限界を破るプロトコルである．すなわち，ガウス・ユーエンランダム暗号を具現化する．ここでは，鍵を知っている場合の量子測定と知らない場合の量子測定に関する最適化を解説する．

5. 1　正規受信者：二値量子最適受信器

正規受信者は鍵をもっているので，常に二値の純粋コヒーレント状態を受信する．そのときの量子最適解は，以下のヘルストロム限界になる．

$$\overline{P_{\mathrm{e}}}=\frac{1}{2}\left[1-\sqrt{1-|\langle\alpha_0|\alpha_1\rangle|^2}\right] \tag{10}$$

これは，現存するいかなる受信器よりすぐれた特性である．これを達成する量子最適受信器を表す作用素 $\{\boldsymbol{X}_0=|\mu_0\rangle\langle\mu_0|, \boldsymbol{X}_1=|\mu_1\rangle\langle\mu_1|\}$ は，以下のように求められる．

$$\begin{aligned}|\mu_0\rangle&=A|\alpha_0\rangle-\mathrm{e}^{-\mathrm{i}\phi}B|\alpha_1\rangle\\ |\mu_1\rangle&=B|\alpha_0\rangle-\mathrm{e}^{\mathrm{i}\phi}A|\alpha_1\rangle\end{aligned} \tag{11}$$

ここで

$$\begin{aligned}&A=\left(\frac{1-\sqrt{1-\kappa^2}}{1-\kappa^2}\right)^{1/2},\quad B=\left(\frac{1+\sqrt{1-\kappa^2}}{1-\kappa^2}\right)^{1/2}\\ &\kappa=\exp\left[-1/2\left(|\alpha_0|^2+|\alpha_1|^2\right)+\mathrm{Re}\left(\alpha_0^*\alpha_1\right)\right]\\ &\phi=\mathrm{Im}\left(\alpha_0^*\alpha_1\right)\end{aligned} \tag{12}$$

これらの実現法については後に解説する．

5. 2　盗聴者：二値から多値受信へ

5. 2. 1　暗号文単独攻撃

鍵をもたないで受信するとき，信号系は混合状態となる．平文と鍵に対する暗号文単独攻撃の場合，盗聴者に対する統計作用素は，それぞれ

$$\rho_x^{\mathrm{COAonD}}=\frac{1}{M}\sum_{k=1}^{M}|\alpha(k,x)\rangle\langle\alpha(k,x)|\qquad x=0,1 \tag{13}$$

$$\rho_k^{\mathrm{COAonK}}=\frac{1}{2}\sum_{x=0}^{1}|\alpha(k,x)\rangle\langle\alpha(k,x)|\qquad 1\le k\le M \tag{14}$$

このような混合状態の量子最適受信器を求めるのは困難であるが，幸いにもヘテロダイン受信が数値解析から最適であることがわかっている．

5. 2. 2　既知平文攻撃

この場合，既知の平文をどのように活用するかによって受信方法を変える必要がある．(i) 鍵なしの受信器で暗号文から平文を復号して，その復号された平文と既知の平文を比較する．(ii) 既知平文を考慮した多値のランニング鍵を受信して鍵の推定を実施する．前者では，受信器はアナログ光信号を受信する必要がある．すなわち，測定後の信号を二値の判定機構で決定する（post measurement process）．しかし，Y-00 は次のような機能をもっている．

〈定理 6（Hirota, 2009 [8]）〉

盗聴者が正規受信者と同じ機構の二値識別受信器を用いて，すべてのシード鍵の可能性を試したとき，Y-00 プロトコルでは雑音がない場合でも，1 つの平文系列に対して多数のシード鍵が候補として残る．

上記性質は，通信方式によって発生する key redundancy という．これによって，二値として信号を判定することは最適な盗聴ではなくなり，必然的に多値信号を識別する受信方式を考察の主題にする必要に迫られる．

後者の場合，Y-00 に用いられる量子状態は多値の非直交状態をもつ光信号であり，それらの原理的な識別限界は多値信号に対する量子信号検出理論（定理 5）によって評価される．このとき，盗聴者に対する統計作用素は

$$\rho_k^{\mathrm{KPA}}=|\alpha(k,0)\rangle\langle\alpha(k,0)|\qquad 1\le k\le M \tag{15}$$

ここで，システムの量子雑音の効果が小さいときは，定理 6 より，多値の量子最適受信器によって直接，ランニング鍵系列を受信するほうが暗号解析を実施するうえで最適となる．一方，量子雑音の効果が大きくなるように設計されていれば，多値の受信は機能しなくなり，最終的に，二値の受信による全数探索以外，暗号解析は不可能となる．そのとき，多値として伝送されてくる信号系の二値信号に対する全数探索用最適受信器は，前述のようにヘテロダインのような光アナログ受信器となる．このような特徴から以下の結論が導かれる．

〈定理 7（Hirota, 2009 [8]）〉

基本 Y-00 による暗号が強情報理論的安全性をもつためには，正規受信者の二値量子最適受信器が必要である．

6.　量子最適受信器の実現技術

前述のように，基本 Y-00 によって究極的な安全性をもつ光通信量子暗号を実現するための最も確実な方法は，正規受信者用の二値量子最適受信器を実現することである．これまで，フィードバックを用いるドリナー受信器と，従来の受信器の前に量子状態を制御する受信量子状態制御受信器が広田によって提案されている[12]．カリフォルニア工科大はドリナー型と受信量子状態制御型を比較検討し，フィードバックを用いるドリナー受信器の実験を推奨した[13]．それに基づきニューメキシコ大グループは，その実験に成功したことを Nature で報告している[14]．一方，受信量子状態制御に基づく量子受信器の実験がマックス・プランク研究所チームによって行われ，原理実験に成功した[15]．

6.1 臼田・佐々木・広田受信器

量子最適受信器は量子信号検出理論の最適解として理論的に予言された．前述のように，1970年代にKennedy, Dolinarは発見的な手法でその予言を実現する研究に着手し，最終的には数学的予言は達成可能であることを示唆した．しかし，その物理学的な分析は行われなかった．その数学的な予言の中に，どのような物理現象が存在するかに関する研究は，1994年から筆者のグループによって開始された．以下にその概要と実験への道程を示す．

6.1.1 標準量子限界

既存の光受信器は直接検出（エネルギー直接検出，光子計数を含む），ホモダイン受信器，ヘテロダイン受信器がある．これらの受信法と量子最適受信法の本質的な違いを解明するために，標準量子限界が以下のように定義された．

〈定義4（Hirota, 1993[16]）〉

信号物理量のスペクトル分解によって表現される量子測定の最小誤り確率を，光信号検出に対する標準量子限界と定義する．

この意味は，フォンノイマンの観測理論の数学的記述として表現される受信器のクラスを標準とすることに等しい．前述の既存の受信器群はこれに属する．これらの標準受信器では達成できない受信特性を実現するためには，受信過程で新しい現象が必要である．そこで，発見的なケネディ受信器を含めて，伝送されてきた量子状態の制御と標準の受信法を組み合わせた一般方式として受信量子状態制御受信法が提案された[12]．その標準量子限界を破るための必要条件が，以下のように与えられている．

〈定理8（Hirota, 1993[16]）〉

標準量子限界を破るためには，受信量子状態変換過程を担うユニタリー作用素が信号物理量と非可換な作用素で生成される必要がある．

6.1.2 臼田・広田受信器[17]

ケネディ受信器は，コヒーレント振幅に対するシフト・ユニタリー作用素と光子計数受信器による受信量子状態制御受信の特殊例であり，上記を満たしている．一方，二値位相変調信号の標準量子限界を破るために，受信量子状態制御受信法のさらに一般性をもつ具体例が臼田らによって提案された．まず，信号物理量は$X_c=\frac{1}{2}(a^{\dagger}+a)$となる．量子状態変換として光カー効果デバイスを採用し，その出力をホモダイン受信器で受信する．そのユニタリー作用素は以下のように記述される．

$$U=\exp[\frac{\mathrm{i}}{2}\chi\hat{n}(\hat{n}-1)] \qquad |\Phi\rangle=U|\alpha\rangle \qquad (16)$$

ここで$\hat{n}$は光子数作用素，χはカー媒質の非線形パラメーターである．上式は，必要条件である定理8を満足している．しかし，十分条件ではないので，数値的に検証する必要がある．その結果，ホモダイン受信器の局発位相のある範囲で標準量子限界を破ることが示された．この結果は，古典光学におけるカー効果は単に位相回転であるが，カー効果がもつ量子的特性は上式からわかるように，量子状態を歪ませる効果があるために生じている．量子状態の歪みとホモダイン受信器による誤り確率の改善の物理的解釈が，佐々木ら[18]，と百瀬ら[19]によって試みられ，上記システムの量子測定過程に量子干渉が発生していることが証明された．

6.1.3 佐々木・広田受信器とDolinar受信器

上記受信器はヘルストロム限界まで達成できない．そこで，その改良として，量子状態制御のユニタリー作用素の非線形性を高くする方法が佐々木・広田によって提案された[20]．近年，Geremiaによって，この提案を含めた種々の提案受信器について詳細な特性の比較分析が実施された[13]．その結果，この受信器は，性能はすぐれているが高次の強い非線形光学効果を実現する必要があるため，実験的に実現することが困難であると指摘している．ヘルストロム限界を達成するためにはDolinar受信器が最良であるとし，実際にそれの世界初の実証実験に成功した[14]．

6.2 新しい受信量子状態制御受信器の提案に向けて

Dolinar受信器は量子状態制御を含むが，測定結果をその制御にフィードバックさせる能動的機構をもつので，われわれの受信量子状態制御受信器とは異なる．Dolinar受信器は，そのフィードバック機能のために受信器の帯域特性が通信速度の数万倍必要になる．これは，将来，高速通信に対応するためには致命的な欠点となるので，可能であれば受動的制御で実現することが望ましい．マックス・プランク研究所チームは，光子数を正確に計数できる光子受信器とケネディ受信器の概念を融合させる受信量子状態制御受信器を提案し，実験に成功した[15]．このような試みは，大変重要な進展である．

本稿で，光通信を用いて究極の安全性をもつ共通鍵暗号を実現する光通信量子暗号の最近の成果を紹介した．これまで，おもに量子暗号は物理学的な興味に基づく研究が優先されてきたが，ここで紹介した量子暗号は高速性と安全性性能のバランスにすぐれており，工学的観点からもきわめて期待がもてる．完全な指数関数的計算量の保証のもとでの光通信量子暗号は，すでに10 Gbit/sの試験器が完成している．情報理論的安全性を保証するためには，ここで紹介した量子最適受信器の開発が必要であるが，いずれの場

合も，当該暗号は従来の暗号では達成できない素晴らしい能力があり，それが近い将来に実用化されると確信する．

文　　献

1) C. E. Shannon: “Communication theory of secret systems,” Bell Syst. Tech. J., **28** (1949) 656–715.
2) H. P. Yuen: Los Alamos, arXiv, quant-ph/0311061v6, 2003.
3) G. A. Barbosa, E. Corndorf, P. Kumar and H. P. Yuen: “Secure communication using microscopic coherent states,” Phys. Rev. Lett., **90** (2003) 227901.
4) 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** (2005) 022335.
5) H. P. Yuen, R. Nair, E. Corndorf, G. S. Kanter and P. Kumar: “On the security of $\alpha\eta$: Response to some attack on quantum based cryptographic protocol,” Quantum Inform. Comput., **6** (2006) 561–582.
6) R. Nair, H. P. Yuen, E. Corndorf, T. Eguchi and P. Kumar: “Quantum noise randomized cipher,” Phys. Rev. A, **74** (2006) 052309.
7) O. Hirota: “Practical security analysis of quantum stream cipher by Yuen 2000 protocol,” Phys. Rev. A, **76** (2007) 032307.
8) O. Hirota, K. Ohhata, M. Honda, S. Akutsu, Y. Doi, K. Harasawa and K. Yamashita: “Experiments of 10 Gbit/sec quantum stream cipher applicable to optical Ethernet and satellite link,” SPIE Proc., **7465** (2009) 1–12.
9) H. P. Yuen: “Key generation: Foundation and a new quantum approach,” IEEE J. Sel. Top. Quantum Electron., **15** (2009) 1630–1645.
10) R. Nair and H. P. Yuen: “Comment on exposed-key weakness of $\alpha\eta$,” Phys. Lett. A, **372** (2008) 7091–7096.
11) 広田　修：光通信理論―量子論的基礎―(森北出版，1985)．
12) O. Hirota: “Properties of quantum communication with received quantum state control,” Opt. Commun., **67** (1988) 204–208.
13) J. M. Geremia: “Distinguishing between optical coherent states with inperfect detection,” Phys. Rev. A, **70** (2004) 062303.
14) R. L. Cook, P. J. Martin and J. M. Geremia: “Optical coherent state discrimination using a closed-loop quantum measurement,” Nature, **446** (2007) 774–777.
15) C. Wittmann, U. Andersen and G. Leuchs: “Discrimination of optical coherent state using a photon number resolving detector,” Los Alamos, arXiv, quant-ph/0905.2496V3, 2009.
16) 広田　修：“量子確率論に基づく信号検出に関する一考察”，電子情報通信学会技術研究報告，**93** (1994) 25–30.
17) T. S. Usuda and O. Hirota: “An example of a received quantum state controller by optical Kerr effect,” *Proceedeings of QCM-94* (Plenum Press, 1995) pp. 419–428.
18) M. Sasaki, T. Usuda and O. Hirota: “Physical aspect of improvement of quantum noise characteristics caused by unitary transformation with non-linear optical medium,” Phys. Rev. A, **51** (1995) 1702–1705.
19) R. Momose: “On a relation between quantum interference and standard quantum limit,” *Proc. of 4th Squeezed State and Uncertainty Relation* (1995) 307–312.
20) M. Sasaki and O. Hirota: “An optimum decision scheme with unitary control process for binary qantum state signals,” Phys. Rev. A, **54** (1996) 2728–2736.

(2009 年 9 月 9 日受理)