INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2005 情財第 0689 号

量子暗号通信システムに関する
世界的な動向調査報告書

2007 年 4 月

独立行政法人 情報処理推進機構

はじめに

近年になり，相次ぐフィールド試験の報告，試作機の販売等，量子暗号通信システムの実用化がすぐそこまで来ている．量子暗号は物理学の基礎法則に基づき安全性が保証されるため無条件安全性を提供できるはずなのだが，具体的な通信システムにおいては，装置の不完全さにより安全性が低下する可能性が指摘されている．また，従来の量子暗号プロトコルにおける性能限界を凌駕するために提案された新プロトコルの中には，当初の理論解析で期待されたほどの安全性を実現しない，と指摘されているものもある．このため理論的解析のみにとどまらず，実験結果や実装例に着目して安全性を調査・分析することが，今後の量子暗号の普及推進のためにも重要となる．

本調査では，量子暗号通信システムの安全性を，理論および実装の両面から調査する．また 2006 年になって米国や英国で量子暗号システムの標準化の動きが出始めたが，これについても概要を調査する．そしてそれらの結果を反映して，安全な量子暗号システムを選定する際に役立つ明確な判断基準を示す．

量子暗号通信システムに関する文献を入手し，その内容を精査し整理する．また，当社所有の量子暗号実験設備を用いて測定を行える部分に関しては，その測定結果も加えて内容を補足する．そしてそれらを体系化し，調査結果としてまとめる．

目次

１． 量子暗号の概要

量子暗号システムの最終的な目標は，従来型の暗号方式(公開鍵暗号など)と同様で，秘密通信(secret communication)を安全に行うことである．一方で従来型の暗号との最大の違いは，「無条件安全性」(unconditional security)が実現できることである．既存の暗号であれば，PC とインターネットがあればほぼ何でも出来るのに対して，量子暗号においては，レーザや光ファイバなど大掛かりな装置が必要となる理由はここにある．そこでこの節ではまず，量子暗号と従来型暗号の機能上の差異は何か，無条件安全性とは何か，また量子暗号ではそれをいかにして実現しているかについて，概要を説明する．

なお一般に暗号というと，広義では秘密通信以外にもデジタル署名(digital signature)や認証(authentication)も含む．しかし現状の量子暗号研究において，実現可能性が見えている暗号機能は量子鍵配送(quantum key distribution, QKD)のみであり，署名や認証用の量子暗号プロトコルの研究は発展途上である．そこで本報告書では専ら，量子鍵配送についてのみ記述する．

１.１ 量子暗号の機能

量子鍵配送の目的は, 送信者 Alice と受信者 Bob の間で, 秘密のビット列 $k=(k_1,\mathrm{K},k_n)$, $k_i\in\{0,1\}$ を共有することである．なおかつこの k が，いかなる盗聴者 Eve にも盗み見られていないことを，証明つきで保証できる．ただし“盗み見られない”の意味が通常の暗号とはやや異なる．

- まず, 秘密のビット列 $k=(k_1,\mathrm{K},k_n)$ を送信者または受信者が自由に選ぶことはできない．もし k を自由に選べるとすれば，初めからメッセージ m を k として選べば，直接に暗号通信ができる．しかし実際のところ k の具体的な値は，このプロトコルが終わるまで判明しない（これはプロトコルの構造に起因する）．
- 次に，送ったビット列を途中で誰かに盗み見られた場合，事後の検証でそのことをほぼ１の確率で検出できるが，k が盗み見られた事実は覆すことができない．従ってこの場合は，その乱数列 k は捨て去って，このプロトコルを再び実行する．そして，乱数列 k が盗聴されていないことが検証できるまで繰り返す（この場合もちろん，k の値は毎回異なる）．ここでもし攻撃者 Eve がいつまでも盗聴を続けるとした場合には，Alice と Bob は永遠に秘密通信ができないことになる．
- ただし古典暗号通信の場合でも，攻撃者が通信線を遮断すると同じ状況になるので，このことは決して量子暗号の方が弱いことを意味するものではない．なおここでいう「古典暗号」(classical cryptography)とは，量子力学的性質を利用せずとも実装できる従来型の暗号，たとえば AES や RSA 暗号方式をさす．物理の分野において，量子力学を用いなくても記述できる系や現象を「古典的」(classical) と呼ぶのが慣例となっているため，一般にこのような用語が用いられる．

まとめると量子暗号の機能は, Alice－Bob 間で(毎回異なる)ビット列 k を共有することであり, 事後の検証に成功した場合には, それが途中で盗聴されていないことを確信できる, というものである．特定のメッセージ m を秘密に送るには，まず乱数列 k を m と同じ長さだけ共有し，それを秘密鍵として，ワンタイムパッド（one-time pad）で通信する．つまり $C = m \oplus k$ を暗号文として送ればいい.

1.2 無条件安全性

冒頭で触れたとおり，量子暗号の最大の売りは無条件安全性(unconditional security)である。

従来型の暗号はほぼすべて, 何らかの計算量的仮定(computational assumption)をおいた上で始めて安全性が保証される．たとえば現在広く用いられている RSA 暗号方式は，素因数分解問題を解く効率的アルゴリズムが現状では知られていない，ということを安全性の根拠としている．しかし一方で，素因数分解問題が困難であるという数学的な証明が得られているわけでもなく，将来そのようなアルゴリズムが見つかって RSA 暗号が破られる，という可能性が残っている．別の言い方をすれば，RSA 暗号の安全性は数学的に無条件に保証されたものではなく，つきつめると，ある経験則に基づいて保証されているにすぎないといえる.

一方で量子暗号においては安全性の根拠として，量子力学のみを仮定して数学的に厳密に安全性証明を行う．したがって量子暗号を破る方法を見つけた場合には，量子力学に反する現象を見つけたことを意味する．しかし量子力学はいわば物理学における大原則であり，実際にその成立以降 80 年近くにわたって矛盾する現象は一切見つかっていない．この意味で，量子暗号は無条件安全性を達成しているといえる.

1.3 量子暗号の実現方法の概要　－BB84 方式を例として－

このように無条件安全性は重要な概念であるが，その数学的な詳細に立ち入ると内容が専門的になりすぎる上に，紙数も膨大になる．そこで本報告書においては，本節で安全性に関して直感的な説明を行うにとどめる．そして第 2 節以降で，無条件安全性の証明の進展状況について，結果を中心に述べることにする.

以下本節では「どのような原理によって量子鍵配送の安全性が保たれているのか」という疑問に対する直感的な説明をするために，代表的な量子暗号方式である BB84 方式[BB84]を例に挙げて概略を説明する．量子鍵配送方式としては BB84 方式以外にも，B92 方式，DPSQKD 方式ほか数多くの方式が提案されているが，これらの方式もすべて，多かれ少なかれ BB84 方式の改良版であるので, BB84 方式に集中して説明することによって一般性は失われない.

1.3.1 通信に用いる媒体

量子鍵配送の安全性のよりどころとなるのは，1.1 節で説明したとおり，「手が加えられた場合には，高い確率で変化が起こる」媒体である．このような媒体が存在すれば鍵配送が可能となるのだが，それが一般に量子（quantum）である．正確な数学的な議論は教科書[Dirac, Sakurai]にゆずるが，概略を述べると，まず，世の中を構成する物質および全ての力(相互作用)は，電子，核子，光などの微小な粒子を構成要素としているが，これらは全て量子としての性質を示す．つまり物質を微小に分割して精密測定を行うと，上記の“手を加えられた場合”の性質が現れてくる．

一般に光でも物質でも，そのエネルギーには最小単位があるという意味で粒子性を示す．しかしそれと同時に干渉等の波動特有の現象も起こす．量子とはこのように粒子性と波動性の両方を兼ね備えた特定の性質のことである．日常生活では必ずしも意識されないが，どのような物質でも場（field）でも，十分な精密測定を行うとその性質を表す．

従って原理的には，どんなものでも充分微小に分割すれば量子暗号に用いることができるのだが，現状では，雑音への耐性や制御の容易さから，もっぱら光のみを用いて実験が行われている．光の場合には，微小に分割すること＝光の強度を弱めることであり，レーザ光を減衰器で弱めた微弱コヒーレント光 （weak coherent light）を用いることが多い．光強度が十分弱い領域では上記で述べた粒子性が顕著となるが，この光の粒子を特に光子（photon）と呼ぶ．量子暗号通信では，この光子ひとつあたりに１ビットずつ乱数列 k の情報を乗せていく．

1.3.2 符号化

BB84 方式の基本となるのは，複素２成分のベクトルで記述される量子状態であり，これをしばしばキュービット(qubit)と呼ぶ．光を媒体として用いる場合は以下のように考える：光には電磁場としての空間ベクトル成分，つまり偏光（polarization）があって，波長やモードを決め打ちして考えると，これは２次元のベクトル(状態ベクトル)で表現できる．つまりキュービットの分の情報量を記述する物理的な自由度として，光の偏光状態を用いる．例えば乱数 $k=0,1$ をそれぞれ縦偏光，横偏光で表す場合には，それらが

$$|0\rangle_+ = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle_+ = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

という状態ベクトルに対応する．つまり状態 $|0\rangle_+, |1\rangle_+$ に，乱数 k の情報を符号化して送るということになる．この２状態は直行基底をなしているので「＋基底」と呼ぶことにする．

- 量子力学の公理

  少し話は前後するが，ここで量子力学の基本的な考え方について説明する．敢えて誤解を恐れずに，単純化して説明すると以下のとおりになる：

- 物理的な系の状態は全て複素成分のベクトルで表される．古典力学では座標や速度で状態を記述していたが，量子論ではその代わりに，ベクトルの各成分の値を指定することによって状態を記述する．
- ある系が状態$|\psi\rangle$にあるとする．人間がこの状態を測定すると，以下のような不連続な変化が起こる．

  1. 測定に際して測定者は，ベクトルの基底$M = \{|\varphi_1\rangle, \mathrm{K}, |\varphi_m\rangle\}$を指定する．
  2. 実際に測定が行われると，状態$|\psi\rangle$は，$M = \{|\varphi_1\rangle, \mathrm{K}, |\varphi_m\rangle\}$のいずれかに遷移する．測定者はこのとき，どの状態に遷移したかを知ることができる．または同じことだが，測定値として値$x \in \{1, \mathrm{K}, m\}$が得られる．ただしここでどの状態に遷移するかは決定論的ではなく，確率的にしか予測できない．つまり同じ状態$|\psi\rangle$に対して同じ基底Mで測定を複数回行っても，得られる測定結果は毎回異なる．ただし測定を多数回行ったときの確率分布を，理論的に予測することはできる：測定の結果として$|\varphi_a\rangle$へ遷移する確率$P_a = |\langle\varphi_a|\psi\rangle|^2$である．ここで$\langle\varphi_a|\psi\rangle$はベクトル$|\varphi_a\rangle$，$|\psi\rangle$の内積の意味である．

つまり測定値が「位置」であろうとも「光の強さ」であろうとも，測定値をそのまま数として扱うのは不適切で，それらの値を添え字とする複素ベクトルに置き換える必要がある（ちなみにこのために，位置や速度のような連続量を扱う場合には，ベクトル空間の次元は無限次元になる）．そして一般には，どの測定値が得られるかは実際に測定を終えるまで確定しない．なおかつここで，測定によって一旦遷移してしまった状態を元に戻すことは不可能である．量子力学においては，測定をするということは系の状態をかき乱すことと表裏一体である．量子力学のより正確な定式化については，教科書[Dirac, Sakurai, NC00]を参照していただきたい．

量子力学のにおける測定は確率論的であり，同一の状態$|\psi\rangle$に対して測定を行ったとしても，毎回同じ測定結果が得られるとは限らない．しかし一方で，常に測定値が曖昧になるというわけではなく，状態ベクトル$|\psi\rangle$と測定に用いる基底Mの組合せによっては，測定結果が確定的になる．たとえば Alice が選んだ乱数$k = 0,1$に応じて，$|\psi\rangle$ として上記

$|0\rangle_+, |1\rangle_+$ のいずれかを送りだし，測定者 Bob がこれを基底 $M = \{|0\rangle_+, |1\rangle_+\}$ で測定するという場合，常に Bob は k の値を確定的に決定できる．というのはこのとき確率 $P_k = |\langle \varphi_k | \psi \rangle|^2$ が常に 0 か 1 という値しかとりえないからである．しかしこれでは盗聴者 Eve も同様のことができるので，この方式は暗号には使えない．

そこで符号化法をランダム化する．上記の＋基底に加えて，もうひと組「×基底」を導入し，

$$|0\rangle_\times = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad |1\rangle_\times = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

これを＋基底と 1/2 ずつの確率で併用する．

物理的にはこれは，光の進む方向を軸として装置を 45 度回転した状況に対応している．なおかつこれらの状態は＋基底の状態と独立ではなく，例えば状態 $|0\rangle_\times$ は，＋基底の状態の重ね合わせとして $|0\rangle_\times = (|0\rangle_+ + |1\rangle_+)/\sqrt{2}$ と書くことができる．状態を測定値そのものではなくて複素ベクトルを用いた結果として，この「状態の重ね合わせ」のように，古典物理では起こりえない状況が発生している．

基底を 2 種類導入した結果として，$k=0$ に対しては $\{|0\rangle_+, |1\rangle_+\}$ のどちらか，$k=1$ に対しては $\{|0\rangle_\times, |1\rangle_\times\}$ のどちらかの偏光に属する基底をランダムに選んで送る, というプロトコルになる．なおかつ Alice は，Bob が全ての光子の観測を終えるまで，用いた基底を秘密にしておく．Alice が送信に用いた基底と，Bob が受信に用いた基底とが一致した場合には，Bob は k を正しく知ることができるが，一致しなかった場合には Bob の観測する値は全くの乱数となる．なぜならば，上記の規則 2 にしたがってこのときの測定確率を計算すると $P = |{}_+\langle 0|0\rangle_\times|^2 = |{}_+\langle 0|1\rangle_\times|^2 = |{}_+\langle 1|0\rangle_\times|^2 = |{}_+\langle 1|1\rangle_\times|^2 = 1/2$ となるからである．

なおかつ上で述べたとおり，このときの状態はすでにそのランダムな状態に変化していて，正しい基底をもちいて観測を再挑戦したとしても，やはりランダムな値しかえられない．ただし元々送信しているのは乱数なので，Bob が測定できなかった分は捨ててしまえばよくて，Alice-Bob 間の鍵共有としては害が無い．

1.3.3 盗聴の検出

一方で「測定に再挑戦しても情報量が増えない」ということは，盗聴者 Eve にとっても同様である．まず Eve の目的は：Alice の送信した光を途中で傍受して b の情報を得て，な

おかつ Bob の受信機にはうまく偽装した状態の光を送りこんで，盗聴の痕跡を消す，ということである．例えば盗聴戦略のうちもっとも簡単なものは：Eve が＋，×のいずれかの基底を予測し，それを用いて Alice が送信した状態を観測する，というものである．しかしこのとき必ず 1/2 の確率で誤った基底を選ぶので，偏光を 45 度か 135 度変えてしまう．もちろんここでも，観測によって一度変化した状態は元に戻すことができない．この結果 Bob の側としては，正しい基底を用いた場合でも，測定する k の値には確率 1/4 で誤りがおこることになる．もし仮に何らかの理由で，Eve はこの方法しか用いていない，ということを Alice と Bob が知っているとする．そのとき Alice, Bob は，誤り率が 1/4 未満であることさえ検証すれば，秘密通信ができていると結論付けられる．

もちろん本当は，このような粗い攻撃方法よりももっと賢い戦略があるが，とにかくここで強調したいことは，Bob の測定する誤り率と，Eve が秘密鍵 b に関して得る情報量との間にトレードオフがあるということである．実際に多くの場合，量子暗号の安全性証明はこの考え方に沿ってなされている．より詳細については２.２節以降を参照願いたい．

１.３.４　　BB84 方式

以下に，BB84 方式の手続きを具体的に書く．最初に光を用いた量子通信がある．そしてその後は上記のトレードオフを活用すべく，誤り率を検証するフェーズと，ひきつづいて秘密鍵を抽出するフェーズとに分かれている．

1　量子通信フェーズ

1.1 Alice は，乱数列 $a=(a_1,\mathrm{K},a_n)$，$a_i\in\{0,1\}$ と，ランダムな基底の列 $x=(x_1,\mathrm{K},x_n)$，$x_i\in\{+,\times\}$ を選ぶ.

1.2 Bob はランダムな基底の列 $y=(y_1,\mathrm{K},y_n)$，$y_i\in\{+,\times\}$ を選ぶ.

1.3 Alice は Bob に，n 個の光子をそれぞれ $|a_i\rangle_{x_i}$ の状態にして送る.

1.4 Bob は Alice から受け取った光子を，それぞれ基底 y_i で観測し，結果を $b=(b_1,\mathrm{K},b_n)$，$b_i\in\{0,1\}$ として記録する.

2　誤り率検証フェーズ

2.1 Alice は Bob に，基底 x を公開通信路で伝える.

2.2 Bob は基底 x と基底 y とを比較し，基底の一致した光子の番号を $I=\{i\,|\,1\le i\le n,\ x_i=y_i\}$ とし，公開通信路で Alice に伝える.

2.3 I のうち一部を誤り率検証用としてランダムに選び $J(\subset I)$ とする．J に対応するビット列 $a_J=\{a_i\,|\,i\in J\}$，$b_J=\{b_i\,|\,i\in J\}$ を公開通信路で教えあい，それらの間のビット誤り率を求める. 以下はこれらのビットを“ チェックビット ”と呼ぶ.

3　秘密鍵抽出フェーズ

3.1 検証用に使わなかった分のビット列を，Alice，Bob が鍵としてそれぞれ保存する. つまり $I'=I-J$ として，ビット列 $a_{I'}=\{a_i\,|\,i\in I'\}$，$b_{I'}=\{b_i\,|\,i\in I'\}$ を Alice,

Bob がそれぞれ保存する．これを篩にかけられた鍵ということで“ふるい鍵”（sifted key）と呼ぶ.

すなわち，Alice がまず基底をランダムに振って乱数を送り，Bob も独立に基底をランダムに振ってそれを観測する．そして両者は，基底が一致した分だけを秘密鍵の候補として残す．通信路が完全で盗聴者もいないとすると a_I と b_I は全て一致するはずだが，実際には b_I にはある確率で誤りがのっている．

このビット誤り率を見積もるために，両者で示し合わせてチェックビット a_J，b_J をランダム抽出する．ただしチェックビットは Eve に全てもれてしまうので，残りの $a_{I'}$，$b_{I'}$ をふるい鍵として残し，これに古典的なデータ処理をして秘密鍵を算出する．

ビット長を充分長く取った場合は，チェックビットの誤り率によって，ふるい鍵 $a_{I'}$，$b_{I'}$ に誤り率に乗ったビット誤り率 ε を確率的に上から抑えることができる. 別の言い方をすると，チェックビット a_J，b_J の誤り率とふるい鍵の誤り率 ε は本来別の量だが，チェックビットを十分ランダムに選べばほぼ等しいとみなしてよい．以下では簡単のためこれらを同一視して話を進める．

参考文献

[BB84] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in Proceedings of International Conference on Computers, Systems & Signal Processing, Bangalore, India, (1984).

[Dirac] P. A. M. Dirac, “Principles of Quantum Mechanics, 4th Ed.,” (Claredon Press, 1981)；邦訳は「量子力學」朝永振一郎ほか訳，岩波書店，1968 年.

[NC00] M. A. Nielsen and I. L. Chuang, “Quantum Computation and Quantum Information,” (Cambridge University Press, 2000)；邦訳は「量子コンピュータと量子計算 I, II, III」木村達也訳，オーム社，2005 年.

[Sakurai] J. J. Sakurai, “Modern Quantum Mechanics,” (Addison-Wesley, 1994)；邦訳は「現代の量子力学（上，下）」桜井純訳，吉岡書店，1989 年.

２．量子暗号の理論的安全性

第 1 節で述べたとおり，量子暗号の最大の目的は無条件安全性を達成することであり，そのためには，理論的な安全性証明が与えられていることが必須である．

２.１ 理想的な装置における量子暗号の安全性証明

送信者・受信者ともに理想的な性能を持つ装置を持っている場合については，BB84 方式の安全性は比較的容易に示せる．

まず直感的には以下の様に説明できる．

- 目標は「盗聴が行われているかどうか」を検出することである．
- 通信路は全て Eve にのっとられていると仮定する．つまり，Alice が発した信号は全て Eve が一旦受け取り，量子力学的に許される限り最良の攻撃をした後に Bob に渡すとする．
- 盗聴が行われていれば正規の受信者が得るチェックビットに誤りが乗り，行われていなければ誤り率がゼロであるはず，と考える．そして誤り率 ε がゼロの場合には，A 攻撃者 Eve が行った量子操作は非常に弱いとみなせる． ふるい鍵に関して Eve が得る情報はほぼゼロだと結論でき，ふるい鍵をそのまま秘密鍵として採用することができる．
- チェックビットにエラーが乗っていた場合には盗聴があったと結論付けて，プロトコルを最初から（乱数生成も含めて）やり直す．

なお上記の「Eve が行った量子操作が非常に弱い」という言い方は曖昧であるが，正確に記述するには通常，忠実度(Fidelity)と呼ばれる数学的尺度をもちいる必要がある．この議論の詳細については Nielsen-Chuang の教科書[NC00]の 12.6.3 節を参照願いたい．概略を示すと，以下のとおりである：

- 忠実度(Fidelity)

  忠実度(Fidelity)とは，一般の二つの量子状態（一般には混合状態）がどの程度類似しているかを定量的に示す量である．上記でいうところの「Eve の行った量子操作が弱い」というのは，Alice が送り出した量子状態と，（Eve の手を経て）Bob の手に渡った量子状態との忠実度が 1 に限りなく近いという状況を意味する．

２.２ 現実的な装置を用いた場合の安全性

しかし現実の装置には必ず不完全性があり，盗聴者がいない場合でも，装置の不完全性によって誤りが発生する．

特に量子暗号においては，通常の光通信に比べて光強度が 7 桁程度小さいため，装置としては雑音の巣窟となる．これまで多くの研究機関によって 100km 前後の長距離実装の報告がなされてきたが，そこでの典型的なビット誤り率は 10%弱である．また Alice の量子信号の元となる光源としては，厳密な単一光子源を用いるのが理想だが，技術的な制約から

微弱コヒーレント光で代用することが殆どである.

これらの不完全性を取り入れた安全性の理論的研究が2000年ころから活発になされている．現状の殆どの安全性証明の基本的な考え方は以下のとおりである.

- 安全性に影響を与えるパラメタは以下の２つである（２.２.１節）
  - 複数光子率 P_{multi}　　小さいほど安全
  - Bob 側のビット誤り率 ε　　小さいほど安全
- $P_{\mathrm{multi}}, \varepsilon$ の大きさと, 盗聴者 Eve が読み取れる情報量との間にはトレードオフがある．例えば１.３.３節の攻撃例のように，Eve は，各パルスに対する盗聴操作を強めれば強めるほどより多くのビットの値を得られるが，同時にパルスに加わる変化も増えるので，Bob が測定する ε の値も大きくなる.
- 逆に $P_{\mathrm{multi}}, \varepsilon$ がともにある値以下であれば，Eve が盗んだ情報量もある値以下であると定量的に見積もることができる．そしてさらに，もれた情報量を打ち消す秘匿性増強(3.1.1.2 節)と呼ばれる方法が存在する. これによって安全な秘密鍵を得る.

２.２.１ 装置の不完全性の定量化

BB84 方式の安全性に影響するパラメタは，以下の２種類である.

- 複数光子生成率 P_{multi}

  Alice の用いる光子源から出たパルスに，複数の光子が含まれている確率を p_{multi} とおく. 量子暗号では光子数分割攻撃(２.４節参照)と呼ばれる強力な攻撃があり，p_{multi} が高いと Eve に情報が漏洩する．ただし以下では p_{multi} の代わりに便宜的に,

  $$P_{\mathrm{multi}} = p_{\mathrm{multi}} / p_{\mathrm{click}}$$

  という規格化したパラメタを用いる．ここで p_{click} は Bob 側で光子検出が起こる確率である．理想的な単一光子源では $P_{\mathrm{multi}} = 0$ だが，現実の装置では一般にゼロより大きい(２.４節参照).

- ビット誤り率 ε

  しばしば QBER(quantum bit error rate)とも呼ばれる．安全性証明においては通常，ビット誤り率 ε は全て，盗聴者 Eve の盗聴に起因するとみなす.

  - 本来なら誤り率 ε のうち，装置内の雑音に起因するものと，攻撃者 Eve の攻撃によるものを区別できるようにしたい．しかしその区別を行うためには検出器装置性能の詳細を知る必要があり，一般的な解析は困難である．そのため殆どの論文の安全性証明ではこれらを区別せずに上記の仮定をおいている．ただしこれは攻撃者の能力を多めにみつもる「安全サイドに倒す」仮定であり，安全性証明の妥当性を損なうものではない.

  現実の装置における誤り率の原因については３節冒頭を参照願いたい.

２.２.２ 敵の攻撃能力の分類

量子暗号の最大の目標は無条件安全性であり（１.２節），そのためには攻撃者 Eve が量

子力学で許されたあらゆる操作を行えると仮定して安全性を証明する必要がある．なお，この“あらゆる操作”の攻撃をしばしばコヒーレント攻撃(coherent attack)と呼び，無条件安全性のことを“コヒーレント攻撃に対する安全性”と呼ぶことがある．

しかし２.２.１節で述べたような装置の不完全性を正しく考慮した無条件安全性の証明が初めて与えられたのは 2002 年であった(２.４.２節参照). これに対し量子暗号装置の実装はそれ以前にかなり進展しており，その解析には何らかの楽観的な仮定をおいていた．その仮定の代表的なものとしては以下のものがある：

- コヒーレント光を単一光子とみなす
  平均光子数 $\mu = 0.1$のコヒーレント光（３.１.１節参照）を，単一光子と仮定する．後述する解析によって，誤り率 $\varepsilon = 10\%$ 以下であればよいとするもの．現状の長距離量子暗号の殆ど全ての実装において用いられている．コヒーレント光を単一光子であるとみなし，個別攻撃のみを想定した場合に相当する．
- 個別攻撃を仮定する（２.３.１節，２.４.１節参照）
  攻撃者 Eve が，ある特定の種類の量子操作しか行えないと仮定する．

なおかつ今日においても，殆どの実装報告ではこれらの仮定を置いて通信距離や通信速度を評価している．その場合はもちろん無条件安全性は達成されていないが，この種の評価法が今日でも事実上の標準となっている．

一方で今日においてはこれらの仮定を置かない，厳密な意味の無条件安全性を達成する量子暗号実装が報告され始めている([STHS+07]ほか)．このため今後は，より簡易な装置で効率的に無条件安全性を達成することが重要な研究課題となると考えられ，安全性解析の理論の重要性はさらに高まると予想される．

２.３ 単一光子源を仮定した場合

この節では単一光子源を仮定した場合，つまり複数光子生成率 P_{multi} が厳密に $P_{\mathrm{multi}} = 0$ の場合を考える．この場合，ビット誤り率 ε のみで BB84 方式の安全性が議論できる．この節では誤り率 ε と，Eve の得る情報量の上限とのトレードオフを具体的に見てみる．

２.３.１ 個別攻撃

個別攻撃とは攻撃者の能力に対する仮定であり，攻撃者 Eve が各パルスに個別に量子操作を行うとするものである．実際の量子暗号では一度に複数のパルスを送り出すので，Eve もそれらをまたがるような量子操作（コヒーレント攻撃）を行うことができる．しかし数学的な解析を容易にするために，あえて個別攻撃の仮定を置くことがしばしばある．

3.1.1.1 誤り率と，盗聴される情報量のトレードオフ

個別攻撃の場合には，各ビットについてそのトレードオフを独立に考えることができ，トレードオフは以下のようになる．Eve の得る情報量の数学的指標として，相互情報量

$I(A;E)$を用いる場合と Renyi エントロピー $R_\alpha(A)$を用いる場合の両方がある．

- 相互情報量での評価

Eve の情報量を相互情報量で評価した場合，各ビットにつき，

$$I(A;E) \le 1 - H_2\left(\frac{1}{2} + \sqrt{\varepsilon(1-\varepsilon)}\right) \qquad (2.1)$$

のように上から抑えることができる[FGGNP97].

- Renyi エントロピーでの評価

一方で秘匿性増強(後述)を考慮すると, Eve の情報量の尺度として Renyi エントロピーを用いた方が便利である．まず衝突確率および（オーダ $\alpha = 2$ の）Renyi エントロピーの定義は以下のとおりである．

$$P_C(A) = \sum_{a \in A} (P_A(a))^2,$$
$$R(A) = -\log_2 P_C(A)$$

$R_\alpha(A)$は Shannon エントロピー $H(A)$の一般化で， $H(A)$と同様に情報の曖昧さをあらわす．そこでふるい鍵 a の各ビットを Eve から見たときの曖昧さを，以下の条件つきエントロピーであらわすことができる

$$R(A \mid E) = \sum_{e \in E} P_E(e) R(A \mid E = e).$$

この場合にも，誤り率と $R(A \mid E)$にはトレードオフがあり，各ビットに対して

$$R(A \mid E) \ge -\log_2\left(\frac{1}{2} + 2\varepsilon - 2\varepsilon^2\right) \qquad (2.2)$$

が成立する[Lut99]．ただしここで誤り率 $\varepsilon \le 1/2$ であるとした．

3.1.1.2 秘密鍵抽出

ふるい鍵ができた段階では，問題は完全に古典情報理論的になっている．まず Alice は偏りの無いビット列 a を, 誤り率 ε の通信路を通じて Bob に送り, Bob はふるい鍵 b を得る．

同時に Eve は情報 e を得ているが，それと a との相関は，たとえば(2.1)式や(2.2)式で与えられる．この状態から，Alice と Bob は（誤りの無い）公開通信路を活用して，秘密鍵 k の抽出を行う．つまり Alice と Bob は古典通信 c_1, K, c_r を行って $k_A = F_A(a, c_1, \mathrm{K}, c_r)$, $k_B = F_B(b, c_1, \mathrm{K}, c_r)$を求め，高い確率で $k_A = k_B (= k)$が満たされているようにする．それと同時に, Eve には k に関する情報が殆ど分からないようにする．すなわち以下が成立するとする．

$$I(K; C_1, \mathrm{K}, C_r) \ll |K|.$$

この問題は Advantage Distillation などと呼ばれているが，ある程度一般的な結果が知られていて[CK73]，秘密鍵 k の生成速度を $S(A, B \| E)$とかくと，

$$S(A,B\|E)\geq \max\{I(A;B)-I(A;E),\ I(A;B)-I(B;E)\}$$

となる．また Alice-Bob の古典通信が一方向である場合には等号がなりたつ．今の場合ビットあたりでは $I(A;B)\geq H_2(\varepsilon)$ なので，(2.1)式と対比すると，誤り率 ε が 15%程度かそれ以下であれば，理論的には鍵生成が可能である．

3.1.1.3 効率的な秘密鍵抽出方式

一方で実際問題として，ソフトウェアや FPGA で実装するためには計算量的に効率的なプロトコルを用いなければならない．しかし現状では，そのようなプロトコルの具体形としては，以下の様に誤り訂正と秘匿性増強を組み合わせたものしか知られていない．

以下の方式では, まず Bob のふるい鍵 b に誤り訂正を施して Alice のふるい鍵 a と一致させる．次に秘匿性増強と呼ばれる方式によって Eve に漏洩した情報を消去する．

- 誤り訂正

  あらかじめ符号の具体形を Alice-Bob 間で共有しておき，ふるい鍵ビット列のシンドロームを Alice から Bob に公開通信路で送って誤りを訂正する．ただしこのシンドロームは公開通信路上を流れるので，ふるい鍵に関する情報が(2.1)，(2.2)式で与えられているのとは別個に）Eve に漏洩することになる．これを防ぐために，予め Alice と Bob で秘密鍵を共有しておき，それを用いてシンドロームをワンタイムパッドで暗号化して送ることにする．実際には，漏れた分を後から秘匿性増強で消去してもいいのだが，そうすると，除去すべき情報量の計算（衝突確率の計算）が複雑になるという問題がある．また漏れる情報を差し引くのが，先か後かの違いだけで，鍵生成率としてもメリットは無いので，議論を簡単にすべく予め暗号化しておく（つまり先に差し引いておく）ことにする[Lut99]．ここで消費される秘密鍵長の方が，最後に生成される秘密鍵長よりも短ければ，鍵共有プロトコルとして成立するという考えである．

- 秘匿性増強

  以上で Alice と Bob のふるい鍵が一致して，両者とも a を共有できた．

  しかし依然として Eve も a の情報を一部もっているので，次に秘匿性増強（Privacy Amplification，プライバシ増幅と呼ぶこともある）と呼ばれる方式をもちいてこれを消去する[BBBSS92, BBR88]．“ 消去する ” というのは具体的に言うと；Alice と Bob が公開通信 c_1,K,c_r をして，ある値 $k=f(a,c_1,\mathrm{K},c_r)$ を計算し，そのとき k に関する情報量を Eve が殆ど持っていないようにする，ということである．

  このための効率的なプロトコルとしては Bennett, Maurer ほかによって提案された Generalized Privacy Amplification と呼ばれる方式がある[BBCM95]．この方式では Alice と Bob は universal$_2$ と呼ばれる関数の集合 G から[CW79]，関数 $g\in G$ をランダムに選び，ハッシュ値 $k=g(a)$ を求める．そのとき G の入出力のビット長を適切に選ぶと，$I(K;G,E)$ を任意に小さくすることができる．具体的には：各 $g\in G$ は $g:\{0,1\}^n\to\{0,1\}^r$ であるとする．また A が $\{0,1\}^n$ 上の一様分布で，なおかつ

$R(A|E)=n-t$ であれば，“ Eve の A に関する Renyi 情報量は t である ”ということにする．このとき以下が成り立つ

$$I(K;G,E)\le 2^{n-t-r}/\ln 2$$

つまり n が充分大きいところで考えると，ほぼ $R(A|E)$ ビット分の秘密鍵が共有できるということになる．

- 秘密鍵生成レート

  まず，n ビットの b を修正して a と一致させるために，a のシンドロームをワンタイムパッドで暗号化して送る必要がある．ここで Shannon 限界に達した誤り訂正符号を用いる場合には，シンドローム長は誤り率 ε に対して $nH_2(\varepsilon)$ ビットであり，それと同じ長さの秘密鍵が消費される．次にそうやって一致した n ビットのうち，Eve に漏洩している分（(4) 式で与えられる）を秘匿性増強で取り除く．結果として，生成される鍵長から消費する鍵長を差し引いた，正味の鍵生成速度 G（＝生成される秘密鍵長／ふるい鍵長）は以下で与えられる[Lut00].

$$G=-\log\left(\frac{1}{2}+2\varepsilon-2\varepsilon^2\right)-H_2(\varepsilon). \qquad (2.3)$$

  したがって鍵共有が可能となるためには，誤り率が $\varepsilon\le 11\%$ 程度でなければならない．つまり効率的なプロトコルに限定したことによって，理論的な限界である 15%（本節の始め参照）との間に差が生じている．

2.3.2 無条件安全性

無条件安全性も理論的に証明されている．はじめの証明は Mayers [Mayers01]によって 1996 年に与えられたが難解であり，証明の正しさが受け入れられるまで数年を要した．その後 1998 年に Lo-Chau[LC98]が，量子もつれあい純化(entanglement purification, または entanglement distillation)と呼ばれるプロトコルに関する理論的結果[BDSW96]を利用して，より簡単な安全性証明を与えた．ただし彼らが対象とした鍵共有方式は BB84 方式とは異なり，もつれ合い光源，量子メモリ，多キュービットにわたる量子ゲートなどを必要とするもので, 現状の技術では実装不可能である. また 1999 年には Biham らによって，BB84 の安全性に対する別証明が与えられえている[BBBMR99]．つづいて 2000 年に Shor-Preskill は Lo-Chau のアイデアをさらに一歩進め，BB84 方式に対する簡単な安全性証明を与えた(計４頁のレター論文[SP00]). 量子もつれあい純化から出発する点は Lo-Chau と全く同じだが，Shor-Preskill の場合は量子誤り訂正符号，とりわけ Calderbank-Steane-Shor(CSS)符号の性質を積極的に用いることで必要となる量子操作を可換なもののみに整理し，証明を単純化している．

Lo-Chau の方式[LC98]は鍵共有方式というよりもむしろ，Alice と Bob が敵の攻撃の影響を避けつつ，正しく量子もつれあい状態を共有するための方式である．そして一旦もつれ合い状態が正しく共有されれば鍵共有ができることはほぼ自明であるので，その性質を

利用して量子鍵共有の安全性を証明している．一方で Shor-Preskill [SP00]は CSS 符号の性質を利用してその方式をさらに改良し，量子もつれあい純化と鍵共有の順序を部分的に入れ替え，もつれ合い光源や量子メモリの必要としない，したがって実装可能な方式に変換することに成功した，という形になる．このようにして得られた方式が結果として，よく知られている BB84 方式になっている点が彼らの証明の巧妙なところである．

ただしそのように巧妙な証明を用いた結果として，古典的データ処理の方法に関して若干の制約がついている．具体的には，個別攻撃(２.３.１節)の場合と違って誤り訂正とプライバシ増幅を別個に行うことは許されず，CSS 符号と呼ばれる古典的誤り訂正符号を用いて一度にまとめて行う必要がある，ということである．

- Calderbank-Shor-Steane(CSS)符号

  CSS 符号とは本来は量子誤り訂正符号(quantum error-correcting code, QECC)の一方式のことで，Calderbank-Shor[CS96]および Steane[Ste96]により 1996 年に独立に考案されたものである．彼らの方式では，以下に示す性質を持つ古典的誤り訂正符号(error-correcting code, ECC)が存在すれば, それに対応して量子誤り訂正符号を構成できる．ただし元となる古典的誤り訂正符号のことも CSS 符号と呼ぶので注意が必要である．古典的な CSS 符号とは体 F_2 上の符号長 n ビットの線形符号の組 C_1, C_2 で，以下の性質を満たすものである：

  - $C_2 \subset C_1$ である．
  - $C_1, C_2^{\perp}$ はそれぞれ t ビットの誤りを訂正できる．

  いわば $C_1, C_2^{\perp}$ の両方の性能を保ちつつ，それらを入れ子に構成するもので，そこが従来型の誤り訂正符号と比較した場合の難しさである．実例の一つとしては Steane 符号と呼ばれるものがあり，$C_1, C_2^{\perp}$ がそれぞれ[7,4]符号で 1 ビット誤りを訂正できる(文献[NC00], 10.4 節).

- CSS 符号を用いた秘密鍵抽出

  Shor-Preskill の証明に基づいて無条件安全性を達成したい場合には，CSS 符号を用いてふるい鍵を以下のとおり処理する：

  1. Bob は C_1 を用いてふるい鍵のビット誤りを訂正する．この段階で Alice，Bob のふるい鍵とも C_1 の符号語になる．
  2. 修正したふるい鍵を, 商ベクトル空間 C_1 / C_2 に射影したものを秘密鍵とする．

  たとえば Steane 符号の場合には，7 ビットのふるい鍵をステップ 1 で誤り訂正すると 4 ビットとなる．さらにステップ 2 の射影を行うと 1 ビットの秘密鍵として残る(C_1 / C_2 の次元は 1 次元).

前節の個別攻撃の場合と比較すると，ステップ 1 が誤り訂正，ステップ 2 が秘匿性増強という解釈ができる．実際，ステップ 1 の段階で Alice と Bob のふるい鍵は一致しており，Alice と Bob の情報量の差はなくなるので, ステップ 2 は秘匿性増強として解釈するのが自然である．

Shor-Preskill の秘密鍵生成レートは CSS 符号の誤り訂正能力 t/n と符号化率 R との兼ね合いできまる．ステップ 1 で誤り訂正できるためには，ふるい鍵のビット誤り率 ε に対して $\varepsilon \le t/n$ となることが必要であるので，$\varepsilon = t/n$ の場合を考える．CSS 符号ではランダム誤りに対して

$$R = 1 - 2H_2(\varepsilon) \qquad (2.4)$$

が達成できることが知られていて，これがそのまま Shor-Preskill における鍵生成レート G となる[SP00]．しかし符号の存在は示されている一方で，効率的に復号可能な符号を実際に構成することは一般に簡単ではない．これに関しては現在も研究が進行中である．

２.４ 光子源の不完全性を考慮した安全性解析

これまでは複数光子生成率 P_{multi} が厳密にゼロである場合の安全性解析を述べた．

P_{multi} の盗聴に対する影響が深刻に考えられるようになったのは，2000 年に Lutkenhaus ら [BLSM00, Lut00]によって光子数分割攻撃(Photon-Number Splitting Attack, PNS 攻撃)の詳細な解析が行われるようになってからである．それ以前には一種の予想として「平均光子数が 0.1 のコヒーレント光を用いる場合は，厳密な単一光子源を用いた場合と比較しても，安全性に大きな差はない」とされていたが，Lutkenhaus はこの誤りを正した．その結果，それ以前になされていた通信距離 100km 程度での実験は安全ではなく，実際には 25km 程度未満でしか安全性を保てていないことが示された[Lut00]．

- 光子数分割攻撃

  光子数分割攻撃の概要は以下のとおりである．光子源が不完全な場合には，Alice が発するパルスの中に複数光子を含むものが確率的に含まれている．そこで Eve は以下の手順で攻撃を行う．

  - 1 光子のみを含むパルスは全てブロックして，Bob には送らない．
  - 複数の光子を含むパルスからは，1 光子のみを分離して手元に残し，残りの 1 光子を Bob に送る．

  結果として Eve の手元には，Bob と同じ偏光状態を持った量子状態が残ることになる．Eve がこれを，Alice と Bob が基底交換をした後に観測すれば，Bob のふるい鍵を全て正しく読み取れることになる．なおかつ Bob のふるい鍵のビット誤り率は $\varepsilon = 0$ となる．問題となるのは，果たして Eve が十分な数の複数光子を見つけられるかということだが，これが実は多くの場合可能である：例えば Alice が平均光子数 $\mu = 0.1$ のコヒーレント光（３.１.１節参照）をもちいていて，通信距離が 50km の場合を考える．このとき典型的な装置では，Alice の発したパルスのうち Bob に到達するのは約 1/1000 であるのに対し，複数光子の発生頻度は 1/200 程度である．

２.４.１ 個別攻撃

Lutkenhaus は PNS 攻撃を提案すると同時に，それを考慮に入れた場合の，個別攻撃に

おける秘密鍵生成レート G を求めた[Lut00]. 基本的な考え方は単一光子の場合(２.３.１節)と同様である．複数光子パルスの情報は全て Eve に漏れているとし，単一光子パルスから漏れる情報量は(2.3)式のときと同様に見積もる．結果としてレート G は

$$G=\left(1-P_{\text{multi}}\right)\left(1-\log_2\left[1+4\frac{\varepsilon}{1-P_{\text{multi}}}-4\left(\frac{\varepsilon}{1-P_{\text{multi}}}\right)^2\right]\right)-H_2\left(\varepsilon\right) \qquad (2.5)$$

で与えられている．これは複数光子がゼロのとき，つまり $P_{\text{multi}}=0$ の場合にはたしかかに(2.3)式に一致している．

２.４.２ 無条件安全性

さらに無条件安全性も証明されている．始めの証明は Inamori-Lukenhaus-Mayers らによって与えられ[ILM01]，その後別証明が Gottesman-Lo-Lukenhaus-Preskill ([GLLP02], 以下 GLLP 論文と呼ぶ)らによって与えられた．それぞれ，量子暗号装置を記述するための理論的模型が若干異なっている([GLLP02], IV 節参照)が，秘密鍵生成レート G が高いのは GLLP 論文の方で，それによれば,

$$G=1-P_{\text{multi}}-H_2\left(\varepsilon\right)-\left(1-P_{\text{multi}}\right)H_2\left(\frac{\varepsilon}{1-P_{\text{multi}}}\right) \qquad (2.6)$$

である([GLLP02], XII 節)．GLLP 論文は，２.３.２節で紹介した単一光子の場合における Shor-Preskill の証明の一般化であり，$P_{\text{multi}}=0$ の場合には(2.3)式のレートと一致する．

なお GLLP 方式に基づく評価で，厳密な意味での無条件安全性を達成した量子暗号システムの例として，三菱電機と北海道大学の共同研究によるものがある[STHS+07]．この実装例では伝令つき単一光子源(３.１.２節参照)を用いることによって P_{multi} を低く抑え，通信距離 40km における鍵共有に成功している．

２.５ 新方式の提案動向に関する調査

前節まではおもに BB84 方式の安全性解析の動向に関して報告した．安全性解析が複雑になる最大の理由は，もともと BB84 方式が，理想的な光子源を想定して考え出されたことである．一方ここ数年で，BB84 を改良し，微弱コヒーレント光を用いても，長距離での安全性が確保できると主張するプロトコルが複数提案されている．

それらの方式のうち，主なものは以下のとおりである．

- SARG 方式（ジュネーブ大学)
- デコイ方式（トロント大学)
- DPSQKD 方式（NTT, スタンフォード大学)
- Y00 方式（ノースウェスタン大学)

2.5.1 SARG 方式

2002 年に Gisin らによって提案された方法であり[SARG02]，しばしば SARG04 方式とも呼ばれる（論文出版が 2004 年であるため）．この方式は，光源や受信機といったハードウェア面では BB84 方式と全く同様であり，実装が比較的容易である．ただし基底の公表手順が異なり，このために光子数分割攻撃に対しても安全性が高く，長距離実装が容易であるとされていた．しかしながら 2005 年に玉木ら[FTL05]によって SARG 方式の無条件安全性が詳細に議論された結果，この方式は（デコイ方式に基づく）BB84 方式と比較して有利な点はない，という結論が出されている．

2.5.2 デコイ方式

デコイ方式（decoy method）は BB84 方式の改良版で，2002 年に Hwang によって提案されたものである[Hwang02]．単一光子源を用いない，微弱コヒーレント光による実装でも長距離かつ高速な鍵配送ができるとされている．この節で述べた 4 種類の新方式の中でも，現在のところこの方式が最も関連論文が多く，本命の方式であると考えられる．

この方式は基本的には BB84 方式と全く同様だが，Alice が本来の信号(signal)パルスの中に，強度の強いおとり(decoy)パルスを，ある確率でランダムに混ぜ込んで送る．一方で攻撃者 Eve は，どれがおとりパルスでどれが信号かが分からない状況で攻撃を行うので，光子数分割攻撃を行うと光子数分布を乱してしまい，攻撃が発覚する．

具体的なプロトコルは以下のとおりである．典型的な光強度としては，信号パルスを平均光子数 0.3 の微弱コヒーレント光とし，おとり状態を平均光子数 1.0 とする[Hwang02]．

1. Alice は通常の BB84 プロトコルと同様の，4 状態の量子信号を送る．ただし上の段落で述べたとおり，おとりパルスと信号パルスとで光強度をランダムに振る．
2. 通信が終わった段階で Alice と Bob は公開通信路をつかって，どのパルスが信号でどのパルスがおとりであったかを教えあう．
3. Alice と Bob は，信号パルス・おとりパルスのそれぞれについて，検出効率およびビット誤り率を算出する．これらの値が，敵がいないときの平均と大きく外れている場合には鍵共有を中止してやり直す．
4. おとりパルスのふるい鍵は捨て去り，信号パルスのみについてふるい鍵を算出する．そして通常の BB84 と同様の誤り訂正と秘匿性増強を行って秘密鍵を算出する．

安全性としては，Hwang の最初の論文[Hwang02]では光子数分割攻撃に対する耐性のみが議論され，無条件安全性は議論されていなかった．その後 Lo らが，デコイ方式の考え方と GLLP の安全性証明とを組み合わせることによって，無条件安全性をたもちつつ通信距離を大幅に改善できることを示した[LMC05]．それによれば，微弱コヒーレント光を用いる場合，デコイなしでは通信距離は 40km 未満であるのに対し，デコイ方式では（理論的な見積もりとして）140km を達成できる見積もられている．

これを受けて，実際に長距離(光ファイバで 100km 前後，大気中で 140km 前後)での実験

結果の報告が複数なされている[RHRH+07, SWFU+07, PZYG+07]. これらの実装においては無条件安全性が達成されていることをここで強調したい.

現在でもデコイ方式に関する論文は数多く発表され続けているが，主だったものとしては以下のものがある．まず伝令つき単一光子源とデコイ方式を組み合わせてさらに通信距離を伸ばす方式が提案されており，これによって 170km から 200km 程度が達成可能と見積もられている[WWG07, AYKN06, MS06]．また一方で，有限ビット長における光子数や誤り率の統計的な揺らぎを考慮に入れた，詳細な安全性解析も報告されている[Ha06].

2.5.3 DPSQKD 方式

DPSQKD 方式(Differential-Phase-Shift Quantum Key Distribution Protocol)は 2002 年に井上ら[IWY02]によって提案された方式である．デコイ方式と同様に，コヒーレント状態で実装を行った場合でも，光子数分割攻撃に対する耐性をもつとされている.

基本的な考え方は BB84 方式と類似していて，Alice が乱数を選び，それを Bob が受信して秘密鍵を算出するというものであるが，乱数の符号化方式がかなり異なっている．具体的なプロトコルは以下のとおりである.

1. Alice は乱数 $x=\left(x_{0,}\mathrm{K}\,,x_N\right)\in\{0,1\}^{N+1}$ を選び，対応して位相 πx_i，強度 α をもったコヒーレント光パルスを送る．状態で書くと以下のとおりである.

$$\left|\Psi\right\rangle=\left|\alpha\exp\left(i\pi x_0\right)\right\rangle\otimes\Lambda\otimes\left|\alpha\exp\left(i\pi x_N\right)\right\rangle$$

2. Bob は Mach-Zehnder 干渉計を用いて，位相差 $y_i=x_i\oplus x_{i-1}$ を測定する．そして光子の検出があった部分を集めてふるい鍵 $b=\left(y_{i_1},\mathrm{K}\,,y_{i_m}\right)$ とする.

3. ふるい鍵 b に対し，BB84 方式と同様に誤り訂正および秘匿性増強を行って秘密鍵を算出する.

最大の特徴は乱数情報が，異なったパルス間にまたがって送られていることである．これによって，盗聴者が一部の光パルスに対して攻撃を行った場合に，その影響が多数の光パルスに及ぶため，BB84 と比較して安全性が高まるとされている[IWY02].

しかし厳密な意味での安全性解析は未だ発展途上であり，個別攻撃の特殊な場合[WTY06]，および連続攻撃(sequential attack)[WTY06, CZLN06, Tsu06]と呼ばれるものが議論されているのみである．提案者らのグループによって最近，通信距離 100km による実装報告[DTLFY06]がなされたが，その後の連続攻撃の改良によってそのシステムは安全でないということが示されている[Tsu06]．また同文献[Tsu06]では，現在の典型的性能な実験装置(光ファイバ，干渉計，光子検出器)を用いた場合，DPSQKD 方式で達成可能な通信距離は 95km 未満であることも示されている．ただし距離の上限が与えられたとはいえ依然としてコヒーレント光の BB84 方式(2.4 節によれば 25km 程度未満)よりもはるかに長距

離であるうえ, 今後 DPSQKD 方式の改良によって距離性能が向上する可能性も考えられる.

2.5.4 Y00 方式

H. P. Yuen により 2000 年に提案された量子暗号プロトコルの 1 つである. 文献[BCKY03]により実質的に公開された. その特徴は, 単一光子状態の代わりにメゾスコピックコヒーレント状態を伝送キャリアとして用いるものである. このため, 通信路上での伝送キャリアの損失を無視できるため, 単一光子レベルの光子状態を用いる標準的な量子暗号方式に比べてはるかに高速な(ほぼ 3 桁以上の)性能が期待できる.

安全性に関していうと, 伝送キャリアに単一光子状態を用いないため, 不確定性原理に基づく安全性は期待できない. このため量子揺らぎを安全性の根拠にしている. メゾスコピック状態を伝送キャリアに用いているため, 量子揺らぎが古典状態のように無視できるほど小さくないことを利用している. このため, 伝送情報の符号化には 1 ビットあたりに多値状態を用いている. この多値状態の全体ではなく数状態が量子揺らぎによって識別不能になることを利用して, 量子揺らぎの中に"0"に対応づけられる量子状態と"1"に対応づけられる量子状態を混在させることで安全性を保証している. このような状況で正当な受信者が古典情報を正しく復号できるのは, 予め擬似乱数によって正当な送信者と受信者が手がかりを共有しており, この手がかりを用いて正当な受信者は, 多値状態のうち量子揺らぎの大きさよりもはるかに離れた多値状態の 2 つの状態を識別すればよいことによっている.

正当な受信者が擬似乱数のみを手がかりにして正しく古典情報を復号できることに着目して, Y-00 プロトコルの安全性がストリーム暗号の安全性と等価であることを主張する論文が 2 件独立に発表された[NHIII04, YS05]. これによると, Y-00 プロトコルの安全性は, これに用いられる擬似乱数生成アルゴリズムの計算量的複雑さに依存し, その鍵長の古典ストリーム暗号と同等になる.

文献[NHIII04]によると, 量子揺らぎの分解能を越えて量子状態を識別する必要はなく, 量子揺らぎによりジャミングされて曖昧さは正に擬似乱数生成アルゴリズムの計算量的複雑さに還元させることになっている.

これらの攻撃に対して, 提案者らは文献[YKC04]によって安全性が保たれていること, 多値状態配置の位相的欠陥により文献[NHIII04]記載の攻撃のエラーが大きいことを主張しているが過剰見積もりにみえる.

この文献[YKC04]の反論に対しての回答が今福等により文献[NHIII05]で与えられている. これは文献[NHIII04]でヒューリスティックであった攻撃を, POVM を用いること, 解読アルゴリズムを多値状態の対称性を保ったまま数学的にエレガントに記述した攻撃に改良している. これは提案者らの反論に対して明快な回答を与えているようにみえる.

ここまでの攻撃は暗号化された情報を直接解読する方向であったが, 正当な送信者が多値状態の 1 つを選択したことにより, 送受信者間でのみ共有された擬似乱数ストリームの

情報が一部漏洩することに着目した攻撃が文献[DTBCML06]により発表された．これは一種のサイドチャネル攻撃と呼べるもので，擬似乱数アルゴリズムが線形フィードバックシフトレジスタを用いた場合に，盗聴者がホモダイン検出によりどのような情報が得られるかがシミュレーションにより示されている．

この攻撃に対して，提案者は文献[YN06]で反論をしているが，ここで擬似乱数生成アルゴリズムに関して，これまでその条件について曖昧であったが，AES を用いるべきとの見解をはじめて明確にしている．

この攻撃[DTBCML06]をさらに改良した攻撃が文献[MII07]にて発表され現在に至っている．

参考文献

[AYKN06] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, “Simple and efficient quantum key distribution with parametric down-conversion,” arXiv.org, quant-ph/061011, (2006).

[BB84] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in Proceedings of International Conference on Computers, Systems & Signal Processing, Bangalore, India (1984).

[BBBSS92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental Quantum Cryptography,” J. Cryptography, 5, 3-28 (1992).

[BBCM95] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, “Generalized Privacy Amplification,” IEEE Trans., IT-41, 1915-1923 (1995).

[BBR88] C. H. Bennett, G. Brassard, and J.-M. Robert, “Privacy Amplification by Public Discussions,” SIAM. J. Comput., 17, 210 (1988).

[BBBMR99] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychoudhury, “A Proof of the Security of Quantum Key Distribution,” J. Cryptography, 19, 381-439, (2006); arXiv.org, quant-ph/9912053, (1999); ibid, quant-ph/0511175, (2005).

[BCKY03] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, “Secure Communication Using Mesoscopic Coherent States,” Phys.Rev.Lett., 90, 227901 (2003).

[BLMS00] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, “Limitations on Practical Quantum Cryptography,” Phys.Rev.Lett., 85, 1330 (2000).

[BS93] G. Brassard, and L. Salvail, “Secret-Key Reconciliation by Public Discussion,” in Proceedings of Eurocrypt93 (1993).

[BDSW96] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, “Mixed-state entanglement and quantum error correction,” Phys.Rev.A, 54, 3824 (1996).

[CK73] I. Ciszar and J. Koerner, “Broadcast Channels with Confidential Messages,” IEEE. Trans. IT-24, 339 (1973).

[CS96] A. R. Calderbank and P. W. Shor, “Fault-tolerant error-correction with efficient quantum codes,” Phys.Rev.Lett., 77, 3260 (1996).

[CW79] J. L. Carter and M. N. Wegman, “Universal Classes of Hash Functions,” J. Comput. System Sci., 18, 143-154 (1979).

[CZLN06] M. Curty, L.-L. Zhang, H.-K. Lo, and N. Lutkenhaus, “Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states,” arXiv.org, quant-ph/0609094, (2006).

[DTBCML06] S. Donnet, A. Thangaraj, M. Bloch, J. Cussey, J. M. Merolla, and L. Larger, "Security of Y-00 under heterodyne measurement and fast correlation attack," Physics Letters A, 356, pp406-410 (2006).

[DTLFY06] E. Diamanti, H. Takesue, C. Langlock, M. M. Fejer, and Y. Yamamoto, “100km secure differential phase shift quantum key distribution with low jitter up-conversion detectors,” arXiv.org, quant-ph/0608110, (2006).

[FGGNP97] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, “Optimal Eavesdropping in Quantum Cryptography I. Information Bound and Optimal Strategy,” Phys.Rev.A., 56, 1163-1172 (1997).

[FTL05] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, “On the performance of two protocols: SARG04 and BB84,” Phys.Rev.A, 73, 012337 (2006).

[GLLP02] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” Quant.Inf.Comput. 5, 325-360 (2004); arXiv.org, quant-ph/0212066, (2002).

[Ha06] M. Hayashi, “Practical Evaluation of Security for Quantum Key Distribution,” Phys.Rev.A, 74, 022307 (2006).

[Hwang02] W.-Y. Hwang, “Quantum Key Distribution with High Loss: Toward Global Secure Communication,” Phys.Rev.Lett.,91, 057901 (2003); arXiv.org, quant-ph/0211153 (2002).

[INM01] H. Inamori, N. Lutkenhaus, and D. Mayers, “Unconditional Security of Quanum Key Distribution,” arXiv.org, quant-ph/0107017, (2001).

[IWY02] K. Inoue, E. Waks, and Y. Yamamoto, “Differential Phase Shift Quantum Key Distribution,” Phys.Rev.Lett., 89, 037902 (2002).

[KP02] M. Koashi and J. Preskill, “Secure quantum key distribution with an uncharacterized source,” Phys.Rev.Lett., 90, 057902 (2003); arXiv.org, quant-ph/0208155 (2002).

[LC98] H.-K. Lo and H. F. Chau, “Unconditional Security of Quantum Key Distribution

Over Arbitrary Distances," Science, 283, 2050-2056 (1999); arXiv.org, quant-ph/9803006, (1998).

[LMC05] H.-K. Lo, X-F. Ma, and K. Chen, "Decoy State Quantum Key Distribution," Phys. Rev. Lett., 94, 230504 (2005).

[Lut99] N. Lutkenhaus, "Estimates for practical quantum cryptography," Phys.Rev.A, 59, 3301 (1999).

[Lut00] N. Lutkenhaus, "Security against Individual Attacks for Realistic Quantum Key Distribution," Phys.Rev.A, 61, 052304 (2000).

[Mayers01] D. Mayres, "Unconditional Security in Quantum Cryptography," Journal of ACM, 48, 351-406 (2001).

[MII07] M. J. Mihaljevic, K. Imafuku, and H. Imai, "An Improved Security Evaluation of Y-00 under Heterodyne Measurement and Dedicated Fast Correlation Attacks," SCIS2007 1E2-2 (2007).

[MS06] W. Mauerer and C. Silberhorn, "Passive decoy state quantum key distribution: Closing the gap to perfect sources," arXiv.org, quant-ph/0609195, (2006).

[NC00] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information," (Cambridge University Press, 2000); 邦訳は「量子コンピュータと量子計算 I, II, III」木村達也訳，オーム社，2005 年.

[NHIII04] T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku, and H. Imai, "How much security does Y-00 protocol provide us ?," Phys. Lett. A 237, pp.28-32 (2004).

[NHIII05] T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku, and H. Imai, "Reply to: "Comment on: 'How much security does Y-00 protocol provide us?' "," Phys.Lett.A, 346 pp.7-16 (2005).

[PZYG+07] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma. H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding," Phys.Rev.Lett., 98, 010505 (2007).

[RHRH+07] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. H. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-Distance Decoy State Quantum Key Distribution in Optical Fiber," Phys.Rev.Lett., 98, 010503 (2007).

[SARG02] V. Scarani, A. Acin., G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations," Phys.Rev.Lett., 92, 057901 (2004).

[SWFU+07] T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheildl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key

Distribution over 144km," Phys.Rev.Lett., 98, 010504 (2007).

[Ste96] A. M. Steane, "Multiple particle interference and quantum error correction," Proc. R. Soc. London A, 452, 2551 (1996).

[SP00] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Phys.Rev.Lett., 85, 441-444 (2000).

[STHS+07] A. Soujaeff, T. Nishioka, T. Hasegawa, S. Takeuchi, T. Tsurumaru, K. Sasaki, and M. Matsui, "Quantum key distribution at 1550nm using a pulse heralded single photon source," Optics Express, 15, 726 (2007).

[Tsu06] T. Tsurumaru, "Sequential Attacks with Intensity Modulation on the Differential-Phase-Shift Quantum Key Distribution Protocol," arXiv.org, quant-ph/0612204, (2007).

[WTY06] E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," Phys.Rev.A, 73, 012344 (2006).

[WWG07] Q. Wang, X. -B. Wang, and G. -C. Guo, "Practical decoy-state method in quantum key distribution with a heralded single-photon sources," Phys.Rev.A, 75, 012312 (2007).

[YKC04] H. P. Yuen, P. Kumar, and E. Corndorf, "Comment on `How much security does Y-00 protocol provide us?'," Phys.Lett.A, 346, pp.1-6 (2005).

[YS05] Z. L. Yuan, A. J. Shields, "Comment on Secure communication using mesoscopic coherent state," Phys.Rev.Lett. 94, 048902 (2005).

[YN06] H. P. Yuen and R. Nair, "On the Security of Y-00 under Fast Correlation and Other Attacks on the Key," to appear in Physics Letters A, quant-ph/0608028.

３．構成要素に求められる要件

前節までの結果を踏まえ，量子暗号にもちいる構成要素の性能に関して，調査結果を報告する．とりわけここでは，安全性および装置の速度性能に影響の大きい二大構成要素として，光子生成器および光子検出器に注目する．そしてそれらに求められる性能要件，および現状の研究開発の状況について報告する．

第２.２.１節で述べたとおり，量子暗号装置の安全性を決定するのはビット誤り率とε複数光子生成率P_{multi}の２種類である．始めにこれらのパラメタと構成要素の性能との関係について整理する．

- Alice の発した光パルスが Bob 側で観測される確率p_{click}は，一般に

$$p_{\mathrm{click}} = \mu\eta_{\mathrm{ch}}\eta_{\mathrm{det}} \tag{3.1}$$

で与えられる．ただしここで

μ＝Alice の発するパルスの平均光子数,

η_{ch}＝通信路における減衰,

η_{det}＝Bob の検出器の量子効率,

である．量子効率η_{det}とは入射した単一光子に検出器が反応する確率である．現在広く用いられている検出器(avalanche photodiode，３.２.２節)での典型的な値は$\eta_{\mathrm{det}} = 0.1$程度である．

- ビット誤り率εを式で表すと

$$\varepsilon = \frac{\nu p_{\mathrm{click}} + d/2}{p_{\mathrm{click}}} \tag{3.2}$$

となる．ただしここで

ν＝通信路や光学系に起因する誤りの係数

d＝暗計数率

である．暗計数率dとは，光の入射の有無に関わらず検出器が検出信号を出す確率を指し，いわばdは検出器の雑音である．長距離においてはp_{click}が指数関数的に減少するため，この項の影響が支配的になる．

- 複数光子率P_{multi}は

$$P_{\mathrm{multi}} = p_{\mathrm{multi}} / p_{\mathrm{click}} \tag{3.3}$$

であたえられる(２.２.１節).

３.１ 光子生成器

３.１.１ 光子生成器に求められる性能要件

光子生成器（光源，光子源とも呼ぶ）の性能を表すパラメタで，上記(3.1)～(3.3)式に影響するものは平均光子数 μ と，複数光子生成率 p_{multi} の２つである．量子暗号向けの光子生成器としての優劣はこの２つのパラメタで完全に決定される．

- 微弱コヒーレント光

量子暗号実装むけで最も安価で広く用いられている光源は“微弱コヒーレント光”(weak coherent light)と呼ばれるものであり，これはレーザの光を減衰きで弱めたものである．レーザ光の特性として光子数分布はポアソン分布に従うので, 光子数 n のパルスが発せられる確率 $p(n)$ は以下のとおりである：

$$p(n) = e^{-\mu}\frac{\mu^n}{n!}. \qquad (3.4)$$

このため平均光子数 μ を指定すると, 複数光子生成率 $p_{\mathrm{multi}} = \sum_{n=2}^{\infty} p(n)$ が全て決定する．

多くの実験では $\mu = 0.1$ のコヒーレント光を用いており(２.２.２節参照), 上式からこのとき $p_{\mathrm{multi}} \cong 0.005$ である．しかし２.４節で述べた個別攻撃があるために，このパラメタでは長距離の通信は無理である．そこで p_{multi} を改善するために平均光子数 μ を下げると同時に p_{click} も減少し（(3.1)式），これによってビット誤り率 ε の低下を招く（(3.2)式）．微弱コヒーレント光ではこのトレードオフによって，距離の限界がおのずと定まってしまう(２.４.２節).

この問題を克服するために，平均光子数 μ を保ちつつ p_{multi} を最小化する様々な光子生成器が提案されている．以下ではそれらのうち代表的なものについて報告する．

３.１.２ HSPS (heralded single photon sources, 伝令つき単一光子源)

量子暗号通信に好適な単一光子の生成方法の１つとして，パラメトリック下方変換を用いた方法がある．パラメトリック下方変換は光の波長変換技術の１つであり，２次の非線形光学効果を応用したものである．これは非線形感受率 $\chi^{(2)}$ と呼ばれる特性の高い非線形光学結晶にポンプ光を入射すると，波長の長い ２ つの光，シグナル光とアイドラ光に変換されて出てくる現象である．図 1.

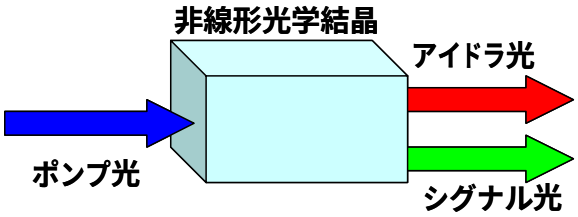


図 1. パラメトリック下方変換

ここで，ポンプ光とシグナル光とアイドラ光の周波数ω_p，ω_s，ω_iの間には，

$$\omega_p = \omega_s + \omega_i$$

の関係が成り立つ．更に高い波長変換効率を得るためには，位相整合条件と呼ばれるそれぞれの光の波数ベクトル$\mathbf{k}_p$，$\mathbf{k}_s$，$\mathbf{k}_i$の間に

$$\mathbf{k}_p = \mathbf{k}_s + \mathbf{k}_i$$

がなりたっていなければならないが，このためには結晶における屈折率の波長分散を考慮しなければならない．

このパラメトリック下方変換を量子レベルでみると，ポンプ光として１つの光子が結晶に入射すると，よりエネルギーの低い 1 組の光子対が生成されたことに対応する．このため，シグナル光の光子を検出するとアイドラ光の光子が射出されたことが認識できる．この仕組みを応用したのが伝令付き単一光子源(HSPS)である．ここで，シグナル光検出信号が伝令信号と呼ばれる．この伝令信号をアイドラ光の単一光子より先行させることにより，単一光子に対する信号変調や光子検出のトリガ信号として利用できる．

ポンプ光として通常 CW ないしパルスレーザー光が入射されるが，これは単一光子ではないので複数の光子対が発生しうる．このため，シグナル光の検出には光子数検出器を用いて複数光子検出時には伝令信号を発信しない光子数識別制御を行うべきであるが，現時点では理論的検討はなされているもの，おおくは on/off 型の光子検出器を用いて伝令信号の発信が行われている．このため，複数光子発生確率，特に P(2)を評価する必要がある．図 2.

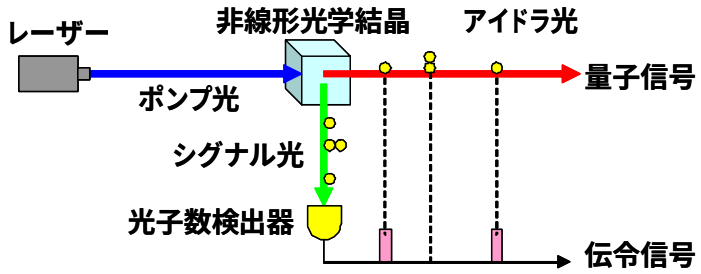


図 2. 伝令付き光子源(HSPS)模式図

さて，この伝令付き単一光子源に用いられる非線形光学結晶であるが，BBO(BaB2O4)結晶，KTP(KTiOPO4)結晶があるほか，最近では PPLN(Periodically Poled Lithium Niobate)結晶が変換効率の高さから注目されている．但し，通信波長帯 1550nm のアイドラ光を得るためには，ポンプ光との波長差が大きいため注目を浴びている．通信波長帯用 HSPS に用いられた非線形光学結晶としては，BBO 結晶[4]，KNbO3 結晶[1]，

PP(Periodically Poled)KTP 結晶[3]が報告されている．

ポンプ光としては，CW レーザー光[1,2]を用いる方式とパルスレーザー光[4]を用いる方式が報告されている．この 2 つの方式の大きな違いは単一光子発生の規則性に現れる．

CW 光の場合は，随時非線形光学結晶にポンプ光が入射されるため，いつでも単一光子が発生しうる．言い換えると，単一光子がランダムに発生する．

一方，パルスレーザー光の場合は，ポンプ光源のクロックに同期してしか発生し得ない．もちろん，全てのタイミングで単一光子が発生しうるわけではなく，確率的に発生するのであるが，発生するときは必ずクロック信号に対して一定の時間差をもって発生する．このため，光子検出，位相変調等の操作に関しては伝令信号による制御によりポンプ光に CW レーザー光とパルスレーザー光のいずれを選択するかは大差が生じないが，将来の量子リピータとの接続を考慮すると，2 光子干渉を行わなければならないので，パルスレーザー光をポンプ光に用いた方式の方がはるかに容易に接続できる．

図 3 は，文献 4 で報告されたパルスレーザー駆動の伝令付き単一光子源の模式図である．ポンプ光源としては，Ti-Sapphire レーザーを SHG で倍波にした波長 390nm，繰り返し周波数 82MHz，ポンプ光出力 240mW を用いている．非線形光学結晶としては，BBO を用い，532nm のシグナル光と 1550nm のアイドラ光からなるパラメトリック下方変換を用いている．このシグナル光とアイドラ光はポンプ光の光軸方向に放射されるので，ダイクロイックミラーを用いてアイドラ光とシグナル光を分離している．シグナル光は on/off 型光子検出器 SPCM(Perkin Elmer 社製)を用いて伝令信号に変換される．SPCM は量子効率 54.7%，暗計数率 90cps である．なお，SPCM は内部ジッタが 500ps 程度あるため，より精密な制御を行うためには伝令信号に加えてクロック信号との併用が提案されている．

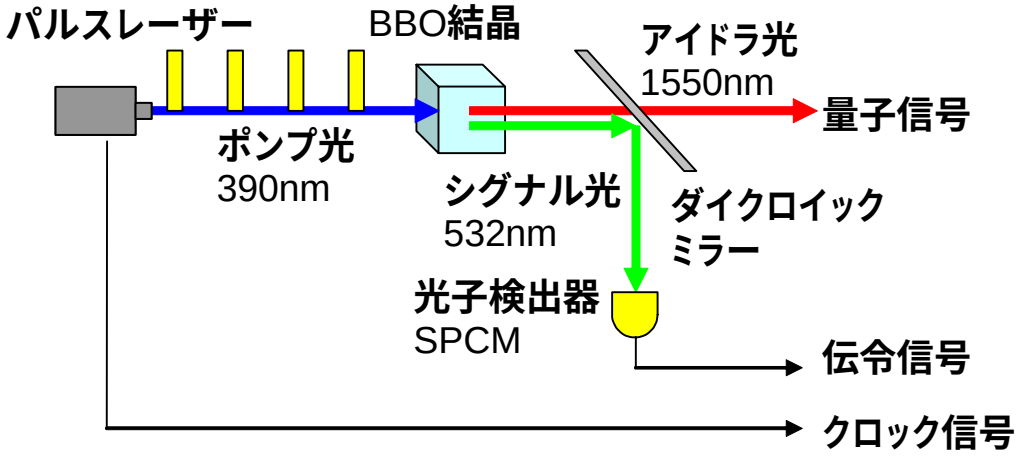


図 3．パルス駆動伝令付き単一光子源

このパルス駆動伝令付き単一光子源の性能は，ポンプ出力 240mW のとき P(1)＝0.1871，

P(2)=2.4E-3 であり，伝令信号レートは 216kHz である．この P(2)は同程度の出力を持つ微弱レーザー光に比して約 1/10 ほどである．

さらに特長的なことは，ポンプ光出力を下げていくと，P(1)はほとんど同じ値を保ったまま，P(2)を任意に低減できる特性をもっている(図 4)．このため，通信距離に応じて許容される P(2)の値をとりつつ単一光子源を動作させることが可能になる．但し，伝令信号レートはポンプ光に比例して小さくなるため，通信速度は遅くなる．

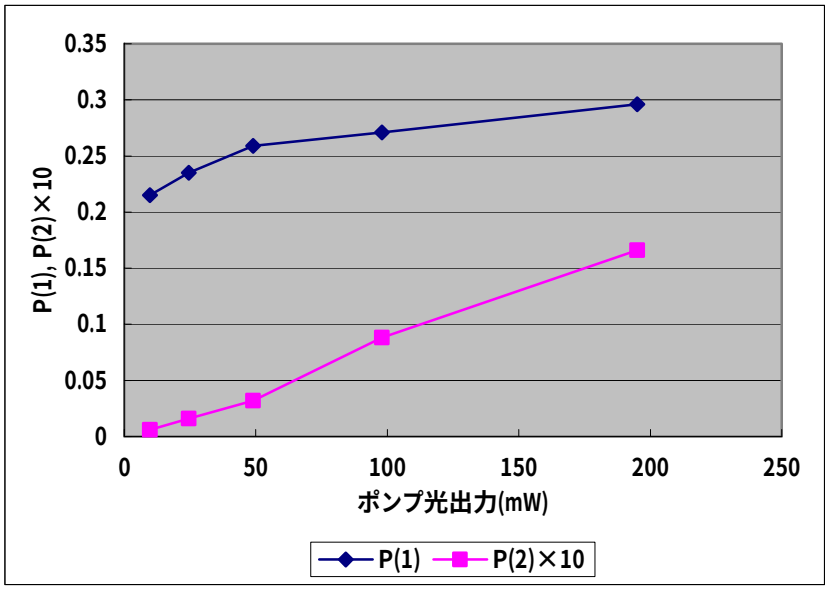


図 4．ポンプ光と P(1)，P(2)の関係

参考文献

[1] S. Fasel, O. Alibart, S. Tanzili, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden, "High-quality asynchronous heralded single-photon source at telecom wavelength," New J. Phys. 6, 163 (2004).

[2] O. Alibart, D. B. Ostrowsky, P. Baldi, and S. Tanzilli, "High-performance guided-wave asynchronous heralded single-photon source," Opt. Lett. 30, 1539-1541 (2005).

[3] M. Pelton, P. Marsden, D. Ljunggren, M. Tengner, A. Karlsson, A. Fragemann, C. Canalias, and F. Laurell, "Bright, single-spatial-mode source of frequency non-degenerate, polarization-entangled photon pairs using periodically poled KTP," Opt. Express 12, 3573 (2004).

[4] A. Soujaeff, S. Takeuchi, K. Sasaki, T. Hasegawa, and M. Matsui, "Heralded single photon source at 1550 nm from pulsed parametric down conversion," to appear in J. Mod. Opt.

３.１.３ ターンスタイル素子

単一電子ターンスタイル素子は，微小トンネル接合における電子間のクーロン反発力を用いて電子を１つずつ規則的に運ぶような素子のことである．この半導体光ターンスタイルを用いる方法では，クーロンブロケード効果をバイポーラ素子（pn 接合）へ適用して，電子と正孔を 1 つずつ活性層に注入し，光子を 1 個ずつ規則的に発生させるものである．

代表的な実験例は，Stanford 大の山本らにより行われたものがある．チャージエネルギーが熱雑音エネルギーを超えるほど微細な 2 重障壁の p-n 結合を利用して，制御されたタイミングで単一の電子と正孔を送りこんで単一光子を生成させるもの．性能としては約 10MHz の繰り返し周波数で，光子を 1 個 1 個ずつ生成することを確認した．

図 1 にある順方向バイアス $V=V_0$ の場合の素子のバンド構造を, また図 1 ある順方向バイアス $V=V_0+\Delta V$ の場合の素子のバンド構造を示す. この図を用いて光子 1 個ずつ発生させることのできる仕組みを具体的に説明しよう．光子が発生される流れは次の通りである．

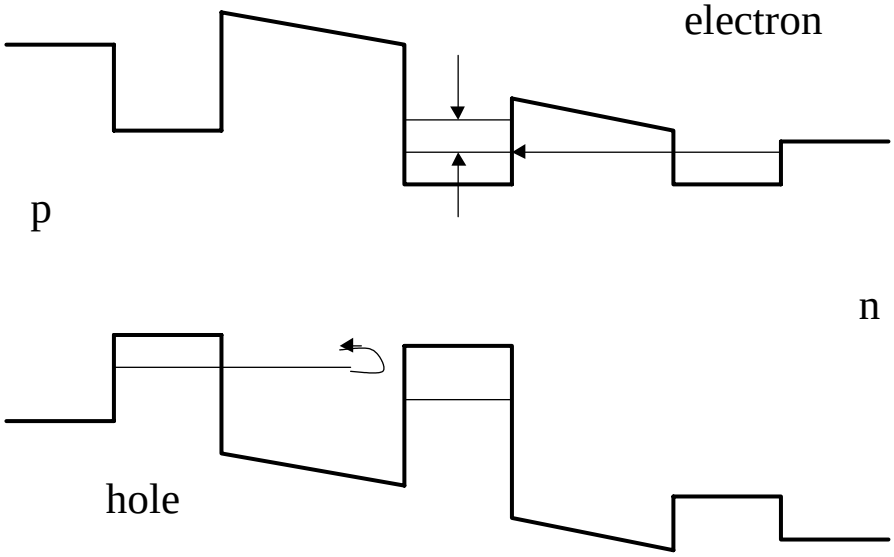
1. ある順方向バイアス V_0 を印加したとき, n 側の AlGaAs 量子井戸から, pn 間の GaAs 量子井戸へ矢印のように電子の共鳴トンネル現象が生じる．（図 1）
2. p と n の間の GaAs 量子井戸に電子が捕獲されると，2 個目の電子はトンネルすることができなくなる（図 1）．これは，電子同士のクーロン反発力があるため，共鳴トンネルのピーク電圧が移動してしまうためである．
3. 印加電圧を $V=V_0+\Delta V$ に上げた場合, p 側の AlGaAs 量子井戸から p と n の間の GaAs 量子井戸へホールの共鳴トンネルが起こる（図 2）.
4. p と n の間の GaAs 量子井戸にホールが捕獲されると，2 個目のホールは同様にトンネルすることができなくなる（図 2）．これは，電子とホールの間のクーロン引力が消えてしまい，共鳴トンネルのピーク電圧が移動してしまうためである．
5. 上記 1～4 までのように電圧 V を V_0 から $V=V_0+\Delta V$ というように変調することにより，電子とホールの発光再結合で光子を１個ずつ発生する．電子とホールを必ず 1 つずつ活性層である中央の量子井戸へ注入して実現する．

ここで，動作するための満たすべき条件をここで考える．ターンスタイル素子を用いたこの方式が正常に単一光子生成動作をするためには，次の条件を満たす必要がある．

条件 1：　電子，ホールのトンネル時間や電子とホールの発光再結合時間が，電圧を変調する周期よりも十分に短い

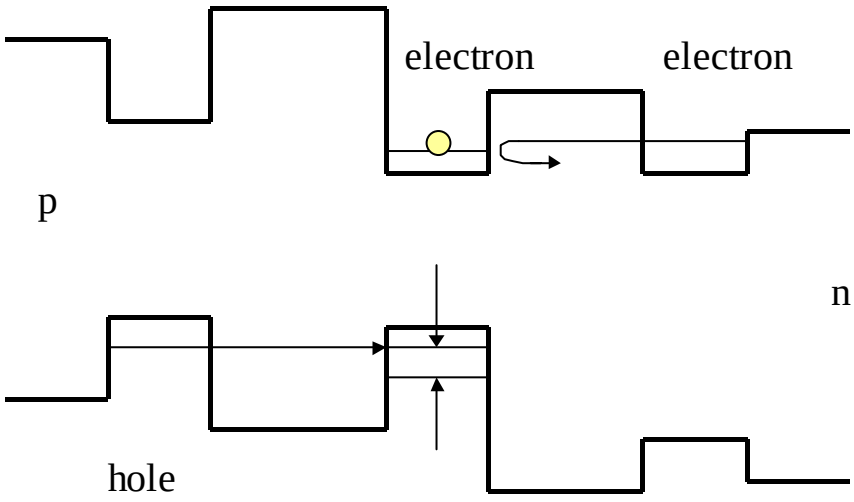
条件 2：　単一電子とホールの帯電エネルギーが，熱揺らぎの大きさ，共鳴トンネル幅よりも十分に大きい

条件 3：　非発光再結合が無視できるほど小さい



$V(t) = V_0$ **の場合**

図 1 単一光子ターンスタイル素子（p-i-n ダブルバリアトンネル接合）のバンド構造 1
（順方向バイアス $V=V_0$ の場合）



$V(t) = V_0 + \Delta V$ **の場合**

図 2 単一光子ターンスタイル素子（p-i-n ダブルバリアトンネル接合）のバンド構造 2
（順方向バイアス $V=V_0+\Delta V$ の場合）

- さらなる特性向上のための方法

マイクロキャビティ構造の導入，量子井戸活性層を単一の量子ドットでの置き換えなどにより，素子を高温動作させることや高速動作につなげることが可能であると考えられている．特に現在の実験では動作温度が 50mK と非常に低いため，動作温度の高温化は使用用途にもよるが，必要である．

3.1.4 量子ドット

半導体中にナノメートルサイズの粒状構造を設けることにより，そこに閉じ込められた電子のポテンシャルが離散化される．このため，閉じ込められた電子を励起することで，単一光子性の高い光源を得ることができる．

一例としてここで、東芝欧州研で行った通信波長の単一光子発生実験に関して紹介する。

発光波長が約 900nm の量子ドットを、低密度（～$10^8 cm^{-2}$）において、形成する方法を開発している。低密度であれば、1 個の量子ドットからの発光を空間的に分離することができて、その単一光子性でも実証されている。これから、発展させて通信波長帯 1300nm で発光する量子ドットの研究開発も行っている。大きな量子ドットを高い密度で成長させるには、InAs 層を厚く積層することで実現できており、従来の光通信用 LED やレーザー応用で開発されているが、この方法では大きなサイズの量子ドットを低密度で成長させること（これが単一光子源では必要であるが）は困難であった。東芝欧州研は、量子ドットの形成プロセスに第二の臨界膜厚が存在して、これ以上の厚さになると量子ドットが選択的に高く成長することをみつけ、大きなサイズの量子ドットを任意の低密度で形成できた。これにより、通信波長帯の単一光子源用にすることができる。

高温で動作させるためには、クラッド層のポテンシャル障壁を高くして、量子ドットからキャリアが熱励起で逃げないようにすれば良い。一つの量子ドットからの発光を分離するためには、柱の頂上にだけ量子ドットが残るように加工すればよい。

量子ドットを用いた単一光子発生は、これまで、アメリカ、フランス、スウェーデン、イギリス、日本の研究グループなどが取り組んでいる。

参考文献

[1]A. J. Bennet, et al., “Electrical control of the uncertainty in the time of single photon emission events,” Phys. Rev. B. 72, 033316 (2005).

[2]M. B. Ward et al., “On-demand single photon source for 1.3um telecom fiber,” Appl. Phys. Lett. 86, 201111 (2005).

[3]P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. Zhang, E. Hu, and A. Imamoglu, “A quantumdot single-photon turnstile device,” Science, 290, 2282 (2000)

[4]E. Moreau, I. Robert, J. M. Geard, I. Abram, L. Manin, and V. Thierry-Mieg, “Single-mode solid-state single photon source based on isolated quantum dots in

pillar microcavities," Appl. Phys. Lett., 79, 2865 (2001).
[5] V. Zwiller, H. Blom, P. Jonsson, N. Panev, S. Jeppesen, T. Tsegaye, E. Goobar, M. Pistol, L. Samuelson and G. Bjork, "Single quantum dots emit single photons at a time: Antibunching experiments," Appl. Phys. Lett., 78, 2476 (2001).
[6] K. Takemoto, Y. Sakuma, S. Hirose, T. Usuki, N. Yokoyama, T. Miyazawa, M. Takatsu, and Y. Arakawa, Jpn. J. Appl. Phys. 43, 7B, L993 (2004)
[7] D. Englund, D. Fattal, E. Waks, G. Solomon, B. Zhang, T. Nakaoka, Y. Arakawa, Y. Yamamoto, and J. Vuckovic, Phys. Rev. Lett. 95, 013904 (2005)

３.１.５ その他の方式

- 同時に 2 つの光子を発生できないような 1 つの 2 準位量子系を用いる方法
  SC.Kitson et al., Brunel et. al., Fleury et. al.,などによって考案・実験がなされているが，ここでは特に Brunel らの実験例である「単一分子の電子励起状態への遷移を利用した単一光子発生方法」を取り上げる．この実験では，単一分子の電子励起状態への遷移を利用して，電気的トリガーにより，期待する時刻に単一分子を励起し，次いで光子を放出させる．結果として，繰り返し周波数 3MHz において 74%の確率で単一光子の発生が可能であることが確認された.
- メゾスコピックな p-n junction の single electron を用いて光子を生成する方法
  Kim et. al.,などによって考案・実験がなされている
- 半導体量子ドットにおけるエレクトロン-ホール対の光子放出を利用する方法
  Gerard et. al., Santori et. al., Michler et. al.,などによって考案・実験がなされている.
- 半導体を使った発光ダイオードによる実現方法

最近の東芝欧州研の Z.Yuan らによって実験がなされ報告された「LD による単一光子発生素子」．最近の報告で東芝欧州研の研究例を取り上げる.

半導体を用いた発光ダイオード(LED)で実現された．従来の装置と異なり，電圧で駆動できるという利点があり外部のレーザー光源が不要となる．まだまだ原理検証実験ではあるが，発光ダイオードで単一光子発生素子が実現できれば大幅に小型化でき実用化につながるため量子情報通信の実用化に向けた明るい材料.

- その他方式に関する課題

単一光子生成技術に関しては，まだまだ克服すべき技術課題が多く中長期的スパンで研究開発を行っていかなければならない課題である．現在のところ，量子暗号のシステム実験では，単一光子源の代わりに微弱レーザー光を用いて擬似的に実現しているのが現状ではあるが，純粋な単一光子生成の研究や実験も着実に進んでいる．その性能に関しても，例えば速度面では，Stanford 大の山本らの方式では，約 10MHz の繰り返し周波数で単一光子を発生させた報告がある．また，パラメトリックダウンコンバージョンを用い

て光子対の片方を制御に片方をソースにするものでは，この実験に必須な高効率光子検出器の開発も進み高性能な実験も近い将来可能と思われる．もちろん動作温度などではまだまだ，物理実験の域を越えず，極低温であったりするが，着実に物理的実現へ進んでいる．またつい最近では，大型のレーザー装置等を必要とせず，電圧で駆動できる発光ダイオードによる単一光子発生素子の原理検証実験の報告もあり，小型化も期待でき実現可能性も高いと考えられる．

３.２ 光子検出器

３.２.１ 光子検出器に求められる安全性要件

光子検出器の性能を表すパラメタで, 上記(3.1)～(3.3)式に影響するものは量子効率η_{det}および暗計数率dである．量子暗号向けの光子検出器としての良し悪しは，この２つのパラメタで左右される．

量子暗号で用いる光パルスは，通常の光通信と比較して強度にして 7 桁程度小さく，通常の光通信向けの検出器では検出できない．そこで特別に敏感な，つまり量子効率η_{det}が高い検出器を特別に構成する必要がある．(3.1)式によれば，素子の調整を行ってη_{det}を上げればp_{click}が増え，(3.2)式のビット誤り率εが改善することになる．しかし同時に，検出器の一般的な傾向としてη_{det}と同時にdも増加するので，中間で必ず最適値が存在する．

３.２.２ APD(avalanche photo-diode)素子

光通信における SN 比の高い受光素子として APD (Avalanche Photo Diode) を量子暗号通信の光子検出器として用いるアイデアは自然であるが，通信波長帯である 1550nm における光子検出性能を満足する素子は中々見出されなかった．これは光子検出性能を有するシリコン APD がより短波長帯域で動作し，通信波長帯では大幅に感度が低下すること．通信波長帯域で動作するインジウム・ガリウム・砒素系 APD においては，光子検出動作としての感度が低かったためである．この状況に転機をもたらしたのが，産総研の吉澤らによる EPITAXX 製 APD を用いた光子検出器開発であった[1,2]. この光子検出器は 1 個の光子が入射したときにどれだけ反応するかを示す量子効率が 20%，ノイズに相当する光子が入射しないときでも反応する暗計数率が 0.005%と以前の通信波長帯 APD に比して極めて高い SN 比を有するため，十分量子暗号通信に耐えられる性能を持っていた．この報告後，EPITAXX 製 APD を用いた量子暗号実験の報告が相次ぎなされてきた上，通信波長帯光子検出器，量子暗号通信装置が市販されるようになった．残念ながら EPITAXX 社は JDSU 社に吸収された後，光子検出用の APD の製造を取りやめたが，その技術ノウハウを活かして PLI 社が光子検出用の APD を販売している．また，国内においては，NEC 社が学会発表等で自社製 APD が光子検出に耐える性能を有することを報告している．

光子検出においては，SN を非常に大きくとるために APD を既存の光通信における動作モードではなく，ガイガーモードと呼ばれる特殊な動作モードで動作させる．このため，最近では光子検出能力を有する APD において，通常の光通信用 APD とは異なるガイガーモードにおける仕様も明記されるようになってきた．参考までに，EPITAXX 製 APD の仕様 (表 1)と，

表 1. EPITAXX 製 APD に添付された仕様表例

型式	EPM239BA SS
シリアル#	0110T1886
Flow #	205234
Idark(@Vb-2.0V)	0.23nA
Vbreak(@10uA)	57.1V
Vmargin(@1uW)	2.3V
Vop(@M=3, 25℃, 10uW)	48.9V
Vop(@M=10, 25℃, 10uW)	55.1V
Vop(@M=20, 25℃, 10uW)	56.5V

最近の光子検出動作を前提にした Princeton Lightwave 製 APD (AGD-25-SE-1-T46)の仕様(表 2), および, Goodrich (Sensors Unlimited)製 APD （SU055-GM-APD-FO）の仕様(表 3)を下記に示す.

表 2. Princeton Lightwave 製 APD の仕様例

Parameter Description	Test Conditions	Specifications			Unit
		Min	Typ.	Max	
Effective Optical Diameter			25		Um
Linear Mode Parameters (295K, all voltages and currents are reverse biased)					
Breakdown voltage Vb	295, Id=10uA	40	50	65	V
Temperature dependence of Vb, γ	Btween 300K and 150K, linear approximation		0.15		%/K
Quantum Efficiency, QE	1550nm, M=1 (linear mode) 1300nm, M=1 (linear mode)		60 70		%
Responsibility, R Total Dark Current, Id	1550nm, M=1 (linear mode) 1300nm, M=1 (linear mode) M=10; primarily non-multiplied Id		0.75 0.75 0.1		A/W nA
Punchthrough Voltage, Vp	V(R=0.1A/W) at 0.1uW illumination		Vb-10		V
Capacitance, C	M=10, 1MHz		0.25		pF
Geiger Mode Parameters (all voltages and currents are reverse biased)					

Dark Count Rate per 1ns, DCR(1ns)	220K, 10kHz (no afterpulsing) 3V overbias 5V overbias 7V overbias 200K, 10kHz (no afterpulsing) 3V overbias 5V overbias 7V overbias		 3E-5 1E-4 4E-4 1.5E-5 5E-5 2E-4		 probability per 1ns gate
Detection Efficiency, DE	3V overbias 5V overbias 7V overbias		13 20 30		%
Jitter, J	3V overbias 5V overbias 7V overbias NOTE: highly circuit dependent		120 50 <50		Ps
Minimum Hold-off to avoid Afterpulsing	Hold-off time for DCR increase <2X DCR at 1ms hold-off (no afterpulsing) 200K		 20		 us

表 3. Goodrich 製 APD の仕様 (Geiger-Mode Specification (-60℃, 1.3um)

Parameter	Test Conditions	Min	Typ	Max	Units
Quantum Efficiency	Single photon input, Excess bias 5%-10%	50			%
Dark Count Rate	Excess bias as required for 50% QE			500,000	Counts/s
Output Pulse Jitter (Leading Edge)	Excess bias as required for 50% QE			100	Ps RMS

このように, 光子検出動作を特徴とした APD には光子検出動作に相当するガイガーモードにおける仕様記載があることが特徴的である.

- APD の光子検出動作における性能指標

上記仕様表からも読み取れるように APD の性能指標としては,

- 量子効率 η_{det}
- 暗計数率 d
- アフターパルス確率

が挙げられる.

量子効率は, 1 個の光子が入射したときにどのくらいの率で検出されるかを示すもので, 光子検出に使用できる APD での典型値は 10%前後である. この値はビットレートに関係し, 大きければ大きいほどよい.

暗計数率は，光子が入射しないときに検出信号が出力される率で，単位時間あたりの発生率もしくは，ゲートあたりの発生率で示される．特に通信波長帯の APD でゲートパルスを印加したときにどれだけ発生するかを示すゲートあたりの発生率は，量子効率との比較が可能になる．この量子効率と暗計数率の比は 1 種の SN 比であり，この値により通信距離の上限が決まってしまう.

アフターパルス確率は，APD のゲーティドガイガー光子検出動作を通信に用いたときに見えてきた現象である．光子検出のためにはゲートパルスを APD に印加するのであるが, ゲートパルスの間隔が短くなると光子が入射していないのに検出信号が出力される現象が発生することが分かってきた.

基本的には, APD に 2 連ゲートパルスを印加し, 初段パルスに同期して光子を入射する. この初段パルスに応じて検出信号が出力されたとき，光子入射のない 2 段パルスに対して検出信号が出力される確率で表現される．但し，この値は 2 連パルスの時間差の関数となるため，アフターパルス確率が暗計数率と同程度になる時間差で表現された方が実用的である．このため表 2 では Hold off 時間のような表記となっている.

参考文献

[1] A. Yoshizawa and H. Tsuchida, "A 1550 nm single-photon detector using a thermoelectrically cooled InGaAs avalanche photodiode," Jpn. Appl. Phys. Pt.1, vol.40, pp.200-201, 2001.

[2] http://staff.aist.go.jp/yoshizawa-akio/を参照.

[3] http://www.princetonlightwave.com/を参照.

[4] http://www.sensorsinc.com/を参照.

3.2.3 パラメトリック上方変換

長距離通信に適した長波長の光を，検出性能に優れた短波長帯向けの光検出器で検出できるように波長変換を行う．それでは，波長変換による高速光子検出に関して説明しよう．

近年，NTT/Stanford 大学において，波長変換を用いた単一光子検出技術が研究されており，これを用いると，通常の InGaAsInP APD を用いる場合より，高速化が目指せるということで研究が進められている．

具体的には，1550nm などの通信波長帯の光子を，非線形結晶を用いて短波長帯の光子に変換して Si-APD で高速高効率に検出する．変換された短波長帯の光は，Si-APD の検出器で，InGaAs/InP APD を用いた通信波長帯での高速化の障害である afterpulse の影響を殆ど考慮せずに高速検出が可能である．

波長変換を利用した光子検出の原理は次の通り．

通信波長帯 1550nm のシグナル光子は，1300nm のポンプ光とともに，PPLN（Periodically Poled Lithium Niobate：周期分極反転ニオブ酸リチウム）に入れられる．PPLN では，結晶の主軸の向きを周期的に反転させており，長い結晶長にわたり擬似的に位相整合して，効率の良い非線形性を得ることが可能である．PPLN 導波路で，光非線形効果である和周波発生過程により，短波長帯（ここでは例えば 700nm）に変換されたシグナル光子が出力される．その後，ポンプ光なその雑音光子をフィルタで取り除き，短波長帯に適した Si-APD で検出する．

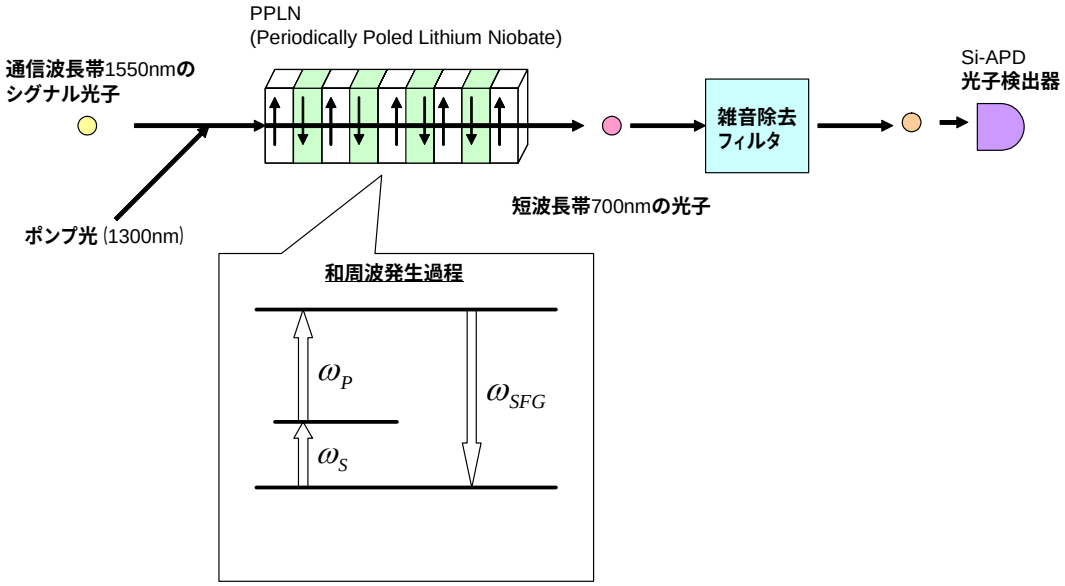
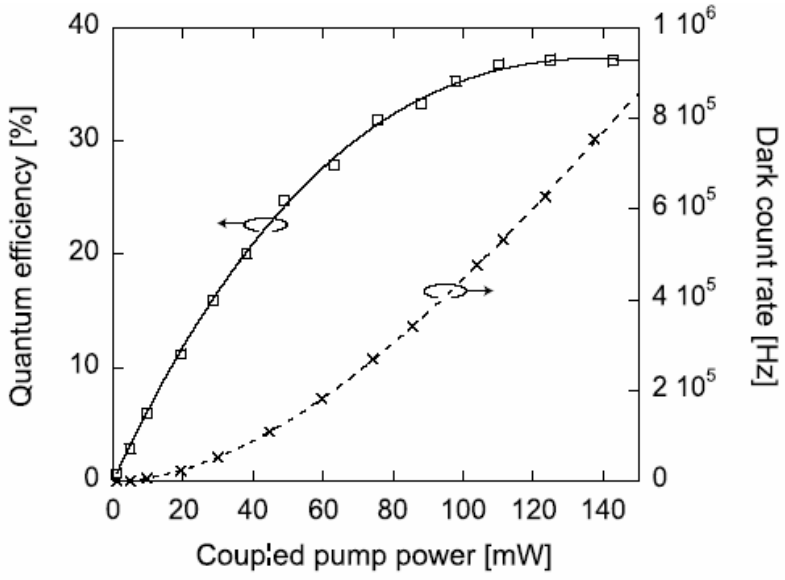


図 1 波長変換を用いた通信波長帯の高速光子検出器のしくみ

実際の NTT/Stanford 大学における実験では，pump 光は 1319nm, signal 光は 1560nm を用いている．また，光子検出系の検出効率と暗計数率のポンプ光のパワー依存性は次の表の通りである．

グラフ 1 光子検出器特性のポンプパワー依存性（NTT/Stanford 大学の実験例）



（quant-ph/0507110 よりグラフを抜粋）

通常の InGaAs/InP APD を用いた方式と波長変換方式の検出器特性比較は，下表の通りである．

表 1. InGaAs/InP APD 方式と波長変換方式の検出器特性比較

	InGaAs/InP APD	波長変換方式	
波長レンジ(nm)	1300-1600	1550	
検出効率(%)	10	37	9
暗計数率(kHz)	20	800	13
Afterpulse 率	大きい	小さい	
動作モード	ゲート動作	非ゲート動作	
動作温度	低温	比較的高温	

参考文献

[1] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, Nature 397, 500 (1999).

[2] C. Brunel, B. Lounis, P. Tamarat, and M. Orrit, Phys. Rev. Lett. 83(14), 2722 (1999).

[3] Z. Yuan, B. E. Kardynal, R. M. Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N. S. Beattie, D. A. Ritchie, and M. Pepper, Science 295, 102 (2002).

[4] S. Takeuchi, J. Kim, Y. Yamamoto, and H. H. Hogue, Appl. Phys. Lett., 74, 1063 (1999); J. Kim, S. Takeuchi, Y. Yamamoto and H. H. Hogue, Appl. Phys. Lett., 74, 902 (1999).

[5] Th. Basche, W. E. Moerner, M. Orrit, and H. Talon, Phys. Rev. Lett., 69, 1516 (1992).

[6] F. De Martini, G.D.Giuseppe, M.Marrocco, Phys. Rev. Lett., 76, 900 (1996).

[7] B. Lounis, W.E.Moerner, Nature 407, 491 (2000).

[8] L. Fluery, J. -M. Segura, G. Zumofen, B. Hecht, U. P. Wild, Phys. Rev. Lett., 84, 1148 (2000).

[9] P. Michler et al., Nature 406, 968(2000).

[10] P. Micher et al., Science 290, 2282(2000).

[11] C. Santori, M. Pelton, G. Solomon, Y. Dale, Y. Yamamoto, Phys. Rev. Lett. 86, 1502 (2001).

[12] V. Zwiller et al., Appl.Phys.Lett. 78, 2476 (2001).

[13] R. M. Thompson et al., Phys.Rev. B 64, 201302R (2001).

[14] C.Kurtsiefer, S.Mayer, P.Zarda, H.Weinfurter, Phys.Rev.Lett. 85, 290 (2000).

[15] R.Brouri, A.Beveratos, J.-P.Poizat, P.Grangier, Opt.Letters 25, 1294 (2000).

[16] 太田，氏原，QIT99-25，第 2 回量子情報技術研究会(1999).

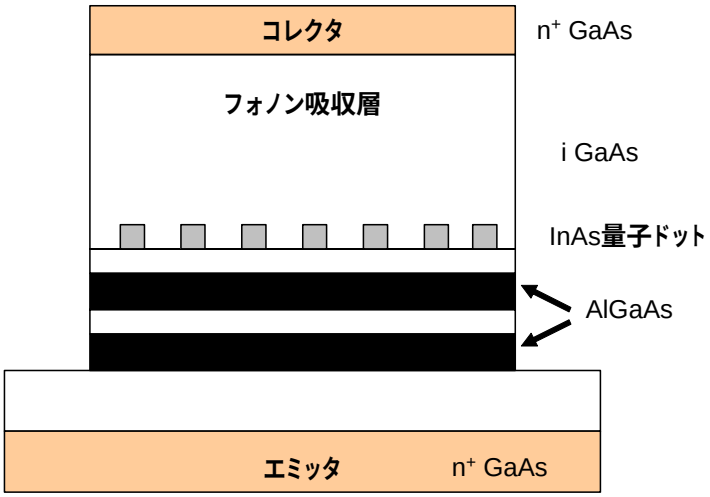
[17] N.Gisin, G.Ribordy, W.Tittel, H.Zbinden, Rev. Mod. Phys.,74, 145 (2002).

[18] H. Takesue, E. Dianmanti, T. Honjo, C. Langrock, M. M. Feyer, K. Inoue, and Y. Yamamoto, New J. Phys., 7, 232 (2005).

３.２.４ 量子ドット

量子ドットを用いた単一光子検出の実験は、例えば東芝欧州研などで行われている。電界効果型トランジスタ(field effect transistor)のゲート電極に量子ドットを配置し、光が量子ドットに入射し、励起された電荷が二次元電子チャネルであるドレイン-ソース間のコンダクタンスに変化を生じさせる。このときの変化量を捉えることにより光子数識別を行うデバイスを開発した。

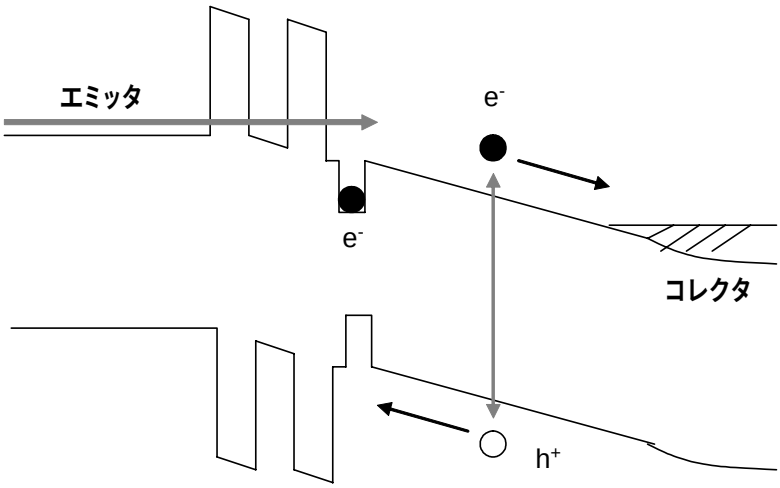
東芝欧州研では、2000 年 5 月に量子ドットを用いた単一光子検出器の開発に成功しており、2005 年には、単一光子の検出効率を 10%以上に高めた。このデバイスの基本構造は、GaAs/AlGaAs 共鳴トンネルダイオードである。図のように二重障壁に接近して InAs 量子ドットを配置していることが特徴である。共鳴トンネルダイオードのエミッタからコレクタに流れる電流は、エミッタのエネルギー準位と二重障壁で挟まれた量子井戸のエネルギー準位との位置関係に非常に敏感である。外部の電圧を、二つのエネルギー準位が等しくなるよう設定すると、デバイスを共鳴状態となり大きな電流が流れる。トンネル電流が二重障壁の両端での電位差に敏感であることを利用して単一光子を検出するというのが基本的な考え方である。



量子ドットの構成図

図 1. 量子ドットの構成図

光励起された正孔が量子ドットに捕獲されると、電子と再結合し、量子ドットでの電位が低下して二重障壁の電位差をかえるので、検出器に流れる電流が鋭く変化する。



光子捕獲時のトンネル電流の変化

図 2. トンネル電流の変化

単一の光子が捕獲されたときのデバイス電流の変化では、電流上昇の応答時間は、計測装置の性能で制限される。このような電流ステップが起こる頻度は、単位時間に入射する光子数に比例し、量子効率は 12%程度であった。バンドパス増幅器を設ければ、電流のステップ的増加をパルス出力に変換できる。単一光子検出での発生するパルスは、雑音レベルと区別でき、通常のパルス計測回路で実時間計測ができる。一般的に、デバイスと電子機器を統合したシステムでは、10^{-8}-10^{-5} カウント/ns 程度の暗電流がある。単一光子検出効率は 1-5%になる。量子ドットを利用した光子検出器は、高い周波数で動作が可能である。

参考文献

[1] A. J. Shields, M. P. O'sulivan, I. Farrer, D. A. Ritchie, R. A. Hogg, M. L. Leadbeater, C. E. Norman, and M. Pepper, "Detection of single photons using a field-effect transistor gated by a layer of quantum dots", Appl. Phys. Lett., 76, 3673 (2000).

[2] J. C. Blakesley, P. See, A. J. Shields, B. E. Kardyna, P. Atkinson, I. Farrer, and D. A. Ritchie, "Efficient single photon detection by quantum dot resonant tunneling diodes", Phys. Rev. Lett., 94, 067401 (2005).

３.２.５ その他の方式

最近になり報告されてきた光子検出器のうち，超伝導素子を用いた光子検出器が応答速度，もしくは，量子効率において，従来の APD を用いた光子検出器に比して格段に優れた性能を挙げていることが注目されている．このためここでは超伝導素子を用いた光子検出器に絞って報告する．

現在，超伝導素子を用いた光子検出器としては２つのものが知られている．１つは超伝導転移端センサ(Transition Edge Sensor, TES)と呼ばれ，もう１つは超伝導ナノワイヤ単一光子検出素子(Superconducting Single Photon Detector, SSPD)と呼ばれるものである．TES は量子効率が高く，SSPD は応答速度が高いという特徴をそれぞれ有する．

- TES

TES は，入射した光子による温度変化を検出する１種のカロリメータである[1]．カロリメータの構成は，光子を吸収する吸収体，吸収体の温度変化を検知する温度計，吸収体に生じた熱を熱浴に逃がすサーマルリンクからなる．

単一光子の吸収による吸収体の温度変化は微々たるものであるが，従来の半導体温度計に比して感度が 300 倍以上になる TES 温度計を使うことにより検出が可能になっている．ここで「温度計」は温度による電気抵抗の変化をみるもので，従来の半導体温度計ではその感度αは３くらいである．ここで感度αは，

$$\alpha = \frac{d \ln R}{d \ln T},$$

R は抵抗，T は温度で定義される．

一方，TES 温度計と呼ばれる温度計では，検体が超伝導転移温度直下に置かれているため，超伝導状態から常伝道状態への遷移がおこる境界に位置し，抵抗の温度変化は急激なものとなる．感度αにして 1000 程度のオーダーとなっている．このため，はるかに高い分解能をもって温度検知ができる．この抵抗の温度変化は電流変化として読み出されるため，微小電流を読み出し可能な SQUID（Superconducting Quantum Interference Device）が高感度低インピーダンス電流計として用いられている．

このような TES はエネルギー分解能を低温であればあるほど高くできるため，当初は X 線用光子検出器として開発されてきたのだが, 通信波長帯である波長 1.55um である赤外線光子検出器も報告されている[2]．　この報告[2]によると，吸収体と温度計はタングステンの薄膜からなる．大きさは 25um 四方厚さ 20nm である．超伝導臨界温度は 100mK となる．光子検出器としては，量子効率 88%，1 秒あたりの暗計数率は 1E-3cps を示す．ゲーティドガイガモードで動作する APD と単純には比較できないが, 仮に 1ns ゲートをかけたとすると，暗計数率は 1E-12cpp と桁違いに小さな暗計数率となる．

さらに，エネルギー分解能が高いため，光子が１,2,3,4 個入射したことを識別できる光子数検出器にもなっている．但し，吸収体が始状態に復帰する時間オーダーは 5us である．応

答速度は 50kHz 程度になっている．

- SSPD

超伝導ナノワイヤ単一光子検出器[3]は．超伝導状態にある素子に光子が入射した際に，クーパー対を破壊されることを利用する．このため，形状はメアンダライン(蛇行)状の超伝導薄膜からなる．この極細線状の薄膜には超伝導状態が破壊される臨界電流 Ic よりわずかに低い電流が流れている．

このとき，クーパー対の束縛エネルギーよりも高い光子が入射すると，クーパー対が破壊される．細線状であることが効いて，この入射スポットは超伝導状態から常伝導状態に移行する．これをホットスポット(hotspot)と呼ぶ．このホットスポットができると電流は抵抗の高いホットスポットを迂回して流れようとするため，その周辺は電流密度が高くなる．但し，既に臨界電流ぎりぎりの電流が流れているため，電流密度の上昇に伴い周辺部も常伝導状態に移行する．こうしてホットスポットが広がっていくことになる．一方で，ホットスポット中での励起電子は周辺にエネルギーを散逸させることで超伝導状態に復帰する．このため，素子において光子が入射するたびにホットスポットが生成，拡大，回復のサイクルを繰り返すことになる[4]．ホットスポットの生成はマクロ的には素子の電気抵抗の変化を引き起こすため，電圧パルスが出力されることになる．

このような超伝導ナノワイヤ単一光子検出器として窒化ニオブを用いた光子検出器が報告されている[3]．この報告のサーベイによると，モスクワ州立教育大学，MIT，NIST により動作温度 4.2K にて量子効率 57%，暗計数率 0.1cps，応答速度 2GHz になるものが実現されている．この方式の特徴は速い応答速度にある．ホットスポットの生成から消滅までの時間オーダーは電子とフォノン間の緩和時間に特徴付けられ，そのオーダーが数 10ps であることから，数 10GHz までの動作周波数が期待できる．

参考文献

[1] 満田和久, “ 熱量計測を応用した光子検出器, ” http://www.astro.isas.jaxa.jp/~mitsuda/r2/index.html

[2] D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam, “Noise-free high efficiency photon-number-resolving detectors,” Phys. Rev. A, 71, 061803 (2005).

[3] 王鎮，三木，藤原，佐々木, “ 窒化ニオブ(NbN)超伝導ナノワイヤ単一光子検出器, ” QIT2006-50 (2006).

[4] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, and A. Dzardanov, C. Williams, and R. Sobolewski, "Picosecond superconducting single-photon optical detector," Appl. Phys. Lett., 79, pp.705-707 (2001).

４．既存の実装報告および既存製品

本節では量子暗号の実装報告および既存製品についての調査結果を報告する．

量子暗号ではすでに，通信距離 100km 超での実装報告が多くの研究機関によってなされている．また複数のベンチャー企業から量子装置が発売されている．本節ではそこで用いられている安全性指標について概観を示した後，各製品の安全性を評価する．

４.１ 装置に求められる性能要件

装置に求められる性能要件としては，安全性を含む以下の五項目を考慮し，ホームページや展示会で公開されている情報を元に調査を行った．

① 価格
② 装置の大きさ
③ 基本性能
④ 安全性
⑤ 使いやすさ

各製品の紹介を行う前に，このうち安全性に関しては２節と３節の調査結果を踏まえ，判定基準を以下で整理し直す．

量子暗号装置の究極目標は無条件安全性を達成することであり，現在では実際にこれが実験室レベルで可能となっている．実装例としては伝令つき単一光子源を用いたもの(２.３.２節)や，デコイ方式によるもの(２.５.２節)がある．しかしこれは主に 2006 年以降の流れであり，それ以前の実装報告では，何らかの仮定を置き，安全性の要件を緩めたうえで安全性評価を行っていた．そのような仮定の代表的なものとしては以下のものがある(２.２.２節参照)．

- 平均光子数 $\mu = 0.1$ のコヒーレント光を単一光子とみなす
  平均光子数 $\mu = 0.1$ のコヒーレント光（３.１.１節参照）を，単一光子と仮定する．
- 個別攻撃を仮定する（２.３.１節，２.４.１節参照）
  攻撃者 Eve が，ある特定の種類の量子操作しか行えないと仮定する．

現在でもこれらの仮定を置いた実装報告が多く，そこでは無条件安全性は達成されていない．これは歴史的な経緯によって，上記の評価基準が一種の標準として学界で長らく受け入れられてきたことによる．

一方で市販の量子暗号装置では，安全性の根拠となるパラメタ(複数光子率 P_{multi}，ビット誤り率 ε など)を明示していないので断言はできないが，以下の理由から無条件安全性が達成されているとは考えづらい．まず市販装置では価格・サイズ・安定性の点から，光子源としては微弱コヒーレント光以外の光源を用いることは事実上不可能である．その場合 BB84 方式で 30km 以上の距離を達成することはできない（２.４節参照）．これに対して現在知られている唯一の解決策は，２.５.２節で紹介したデコイ方式である．しかしデコイ方

式の長距離実装に関しては，2006 年になって始めて実験室レベルの報告がなされたという状況であり，それが 2006 年以前の発売の製品にすでに適用されていたとするのには難がある．したがって無条件安全性は達成されていず，上記２種の仮定を置いていると推測するのが妥当である．

ただし上記はあくまで推論であり，この点を明確にしたい場合には今後更に本格的な調査が必要となる．以下本報告書では，無条件安全性に関して疑いのある場合にはその可能性を指摘するにとどめた．

４.２ 実装報告および既存製品

４.２.１ MagiQ 社

この会社の製品は量子暗号を使った VPN 装置を目指しており，製品名は MAGIQ QPN SECURITY GATEWAY 7505 というものである．

図 1. QPN SECURITY 7505 外観

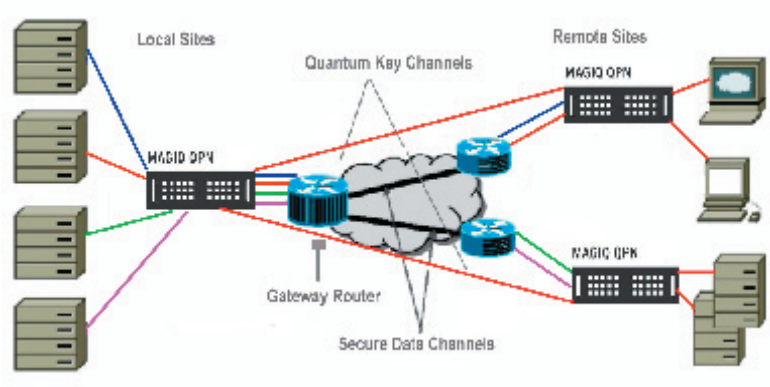


図２Gateway としての利用イメージ

① 価格

公表されていないため，不明である．

② 装置の大きさ

標準的な 19 インチラック, 高さ 175mm, 幅 475mm, 奥行 600mm, 重さ 20Kg

③ 基本性能

量子鍵配送プロトコルとしては BB84 プロトコルを使い, 暗号アルゴリズムとしては 3DES と AES(256bit)を実装. 鍵交換レートは, 最大で毎秒 100 鍵. 最大通信距離は 120Km. Decoy 方式も利用可能とのこと. また乱数も物理乱数生成装置が組み込まれている. IPSEC ベースの VPN 装置としての利用の他, 高度な安全性の要求に対しては, 最上位レイヤーに量子鍵配送とバルク暗号転送モード（おそらく One-Time Pad のこと）が組み込まれている.

④ 量子暗号としての安全性

安全性の要件に関しては詳細な記述がないが, 最大通信距離 120km とあるので無条件安全性を達成しているとは考えづらい. ただしデコイ方式で無条件安全を達成している可能性も, 論理的には否定できない.

⑤ 使いやすさ

次のようなセキュリティモニターを備え, 脅威を監視. また, この製品は FIPs 140.2 レベル 3 の認証を取得する予定であるという.

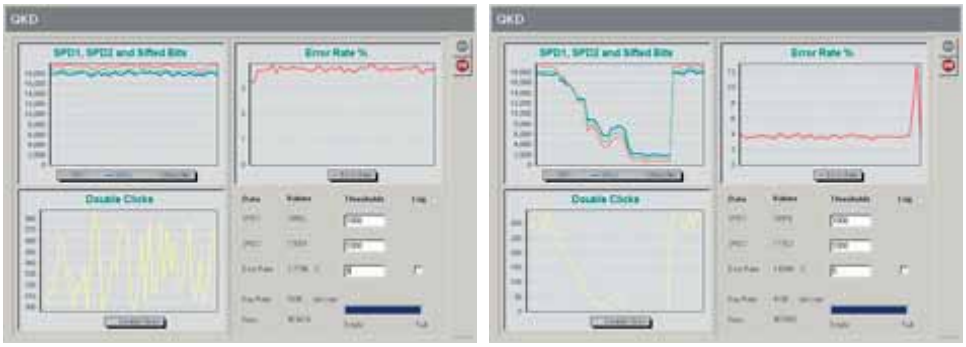


図 3 セキュリティモニター：左, 安全な状態, 右, 盗聴者進入

参考文献

[1] Magiq Technologies 社ホームページ, www.magiqtech.com

[2] “Magiq QPN Security Gateway,” www.magiqtech.com/press/7507_Data_Sheet.pdf

4.2.2 idQuantique 社

量子暗号製品としては VPN 装置的な Vectis というものと, 通常の量子暗号通信装置としての Clavis という 2 つの製品がある。その他にも光子検出器などの製品を幅広く販売しており, 量子暗号製品のパイオニアとして君臨している.

図４　Clavis システム

図５　Vectic システム

まず下記写真右の Vectis の概要は次のとおりである．

① 価格

公表されていないため，不明である．

② 装置の大きさ

高さ 177mm，幅 428mm，奥行 466mm，重さ 16kg

③ 基本性能

量子鍵配送(QKD)の後，AES で暗号通信を行っている．暗号通信等は IEEE802.3u 準拠の高速イーサーネットで実施し，通信距離は最大 100Km である．安全性に影響する鍵交換レートは最大１秒間に 100 回であり，暗号アルゴリズムとしては AES(128, 192, 256bit)が利用できる．

④ 量子暗号としての安全性

平文の暗号化に AES を用いた場合は AES と同等の安全性，すなわち計算量的仮定に基づく安全性が達成されるのみである．デコイ方式を用いない BB84 方式である上に通信距離 100km となっているので，仮にワンタイムパッドを用いた場合でも無条件安全性は達成されないと考えられる．

⑤ 使いやすさ

Vectis の暗号通信は，オフラインで管理している．操作系はタッチパネルによる直感的な方法を採用している．システムのログ情報の表示も行え，Web サーバーとしての利用も可能である．SimpleNetwork Management Protocol（SNMPv3）を使ったオンラインでの単点モニタリング機能もある．これによる中央管理によりネットワーク管理者への負担も軽減される．

写真左の Clavis の概要は次のとおりである．

① 価格

公表されていないため，不明である．

② 装置の大きさ

高さ 160mm，幅 460mm，奥行 420mm，重さ 10kg.

③ 基本性能

特許取得の Plug&Play 方式による量子暗号装置．通信距離は最大 100Km．プロトコルとしては BB84 と SARG プロトコルが実装されている．鍵の精製プロトコル（誤り訂正，秘匿性増強，認証処理）も全て実装されており，通信速度は通信距離 25km で 1.5Kbps 以上．また暗号化通信には，自動鍵管理機能と Triple-DES(ANSI 9.52, 168bit), AES(128, 192, 256bit)が実装されている．

④ 量子暗号としての安全性

平文の暗号化に AES や Triple-Des を用いた場合は，計算量的仮定に基づく安全性が達成されるのみである．デコイ方式でない上に通信距離 100km となっているので，仮にワンタイムパッドを用いた場合でも無条件安全性は達成されないと考えられる．なお BB84 方式以外に SARG 方式にも対応しているとあるが，これによって性能的に有利になるとは考えがたい(２.５.１節参照).

⑤ 使いやすさ

外部の装置との同期を取るための，Sync out 信号などのインタフェースも備えており，拡張性がある．ドキュメントの整備された VC++ベースのライブラリを持ち，ハードウェアパラメータをセットするための低レベルの関数から，鍵配布処理を行う高レベルのライブラリを備えている．

参考文献

[1] idQuantique 社ホームページ，www.idquantique.com

[2] Clavis の仕様，www.idquantique.com/products/files/clavis-specs.pdf

[3] Vectis の仕様，www.idquantique.com/products/files/vectis-specs.pdf

４.２.３ SmartQuantum 社

CEO は Frederic Coste という人物であり，フランスで修士，博士号を取得している．同社の量子暗号に関しては，SQBox という製品がある．ただしホームページ上から取得できる情報は限定されており，製品の詳細は不明である．

装置レベルの暗号化および，プロトコル無依存のユーザデータの転送．ギガイーサーポート，光学的な WAN ポートによる量子暗号通信，音声，映像，データ，画像などを扱うことができ，AES192 ビットの暗号プロセッサを搭載．あらゆる暗号アルゴリズムを搭載する自由度を持つ．

参考文献

[1] SmartQuantum 社ホームページ，www.smartquantum.com

4.2.4 東芝欧州研

製品としては販売されていないが，Telecom World 2006（香港）で装置を出品しており，少なくとも外観の完成度としては高いので，参考としてここに挙げる．価格など製品としてのデータはないが，展示の説明員の説明によれば，光学系の方式は Plug&Play ではなく 1 方向であり，光源の駆動周波数は 8MHz であるとのこと．

図 6　Telecom World 2006 に出展されていた装置

５．量子暗号の安全性評価動向

５.１ 安全性評価動向

前節まで出述べたとおり, これまで量子暗号システムと言えば, BB84 プロトコルを用い, Plug&Play 光学系を構成して実現するのがほとんどであった．BB84 プロトコルは光源が完全な単一光子源であれば，無条件安全性が証明されている．また光源や装置が不完全な場合においても安全性の研究は十分になされている．一方 Plug&Play 光学系は，光子が同じ通信路(ファイバ)を往復することで，その中で生じる偏波ゆらぎや複屈折などの影響を，自動的に補償し，その名の通り，繋ぐだけで簡単に安定動作できる優れた方法である．これまで世界中で行われてきたファイバを用いた量子暗号の実験は，こうした理由により，多くのものが “ BB84 プロトコル＋Plug&Play 方式 ” を用いて行われてきた.

しかし最近，本格的な実用化を目前に，一般の光通信装置の速度に比べ，量子暗号の通信速度の遅さと，通信距離の短さが際立ってきた．一般の光通信では，既に基幹系はテラビットも視野に，また端末周辺でも 160Gbps の通信速度がすぐそこまで来ている．これに対して量子暗号の鍵共有速度は，通信距離にもよるが，最終鍵レートでだいたい 1Kbps 前後であると思われる．基幹系通信の１テラ(10^{12} ビット)に比べると，実に 10^{9} もの開きがある．また通信距離に関しても，単一光子を使った場合でも 100Km 前後しか安全に通信することができない．このことが量子暗号システム導入の最大の障害となっていると感じる.

この速度と通信距離の問題は独立ではなく，単一光子かそれに匹敵する弱い光を用いている以上，トレードオフの関係にある．なぜなら送信側での光強度は光子 1 個（レベル）と決まっているため，通信距離が長くなれば，通信路上での伝送損失により，到達できる光子の数が減り，結果として通信速度は遅くなるからである.

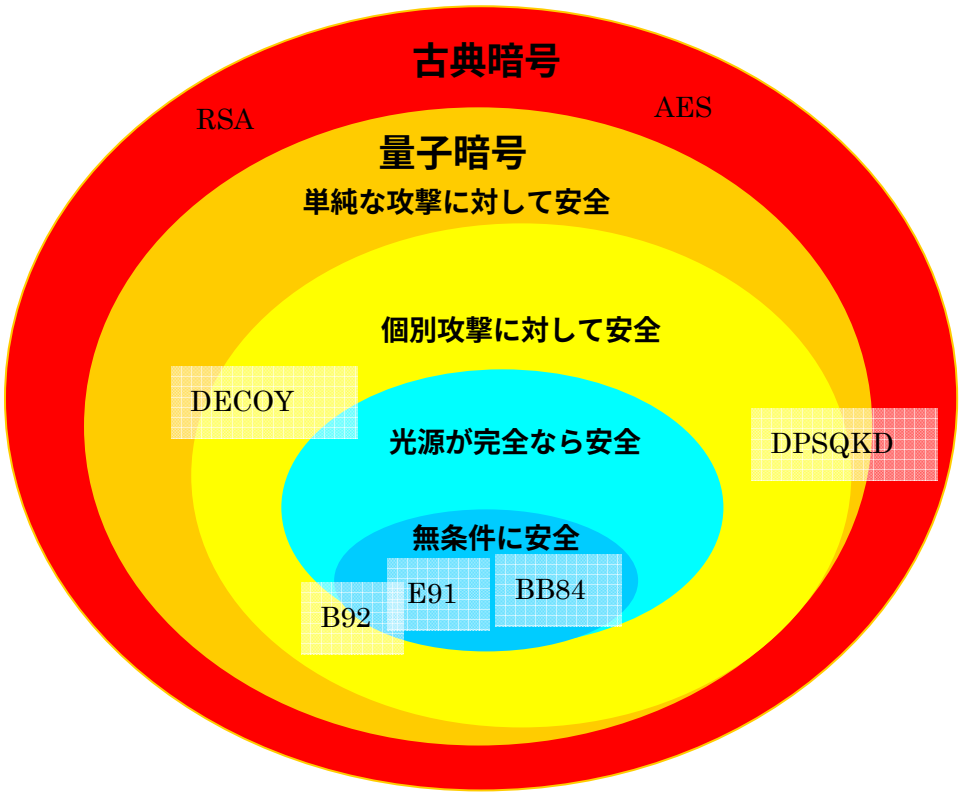
通常のシングルモード光ファイバの場合，通信距離 100 Km で約 20 dB(= 1/100)の損失が生じるため，送信者は 100 個の光子を出しても受信者には 1 個しか到達しない．別の言い方をすれば，受信者が平均 1 bps(ビット/秒)の速度で受信するためには送信者は少なくとも 100 bps 以上の速度で出力しなければならない．しかもこれは光ファイバの損失しか考えていない場合である．実際には検出器の検出効率や変調器の損失，接続端面でのフレネル反射など，様々な損失の要因が加わり，受信者のレートに対して，送信者の正味の送信レートは, 一般的に 1 万倍以上の高速性が要求される. 受信レートが 1 Kbps なら 10 Mbps, 即ち 10 MHz 以上，1 Mbps なら 10 GHz 以上の速度が求められる．つまり，装置としては現在でも，ギガヘルツレベルで動作し，光子を送信しても，受信側のビットレートとしては，この程度のものしか得ることができないのである.

一方，実用化にはさらなる高速化が必要であるというのが大方の見方である．そこで方式自体を根本的に見直し，高速化に対応し，効率も上げようとする研究が盛んに行われている．しかしこうした研究は，多くの場合，情報のキャリアとして，単一光子ではなく，より強い光を用いることを前提としている場合が多い.

BB84 プロトコルという量子暗号方式が提案されて以来，我々はその安全性を単一光子の「存在」に求めてきた．しかし今，その前提に基づかない方式が数多く提案され，本来，同じ土俵で評価できないものが，混ざりあって議論されている．勿論，こうした方式の中から将来の量子暗号の本流となるプロトコルが登場する可能性は大きいとは思うが，BB84 プロトコルを用いた単一光子量子暗号の無条件安全性でさえ，数年前にようやく証明されたことを考えると，これら新たに提案された量子暗号が，現時点で安全であるという保障は残念ながらどこにもない．

従って量子暗号システムの標準化といった場合，単純に高速のものを追求していけばよい訳ではなく，常に安全性の上に立脚したものでなければ受け入れることはできない．このように考えてくると，現時点で量子暗号システムとして標準化のレベルにまで達しているのは，BB84 プロトコル及び Plug&Play 方式，そしてシンプルな単一光子をベースとした一方向の光学系だけであろう．しかしこの場合，デバイスの進歩なくして大幅な高速化は望めず，従って一朝一夕に性能が改善されるものではない．

量子暗号を推進したい者にとって，このことはジレンマであり，何らかのブレークスルーを皆が望んでいることに違いはない．ただ，そこには常に安全性（証明）と言った高い壁が存在する．



５.２ 標準化動向

５.２.１ ワークショップ“Toward Quantum Standard”について

安全性だけに限らないが，量子暗号システム全体に関する標準化の動きとして，下記の会議について報告しておかなければならない．この会議は，Quantum Technology Group, Cambridge-MIT Institute & NIST が主催したもので，量子情報処理技術に関する標準化を先導して行こうとするものである．その意図は，量子情報処理技術の将来を見据えて，これを標準化することで，装置やサービスの流通を促進し，また新規参入者への門戸を広げ，市場が発展するのをサポートするところにある．しかし上述に示したように，実際にはまだ決められることは限られているし，本当に現時点での標準化に意味があるのかは，もう少し慎重に考えてみる必要があるだろう．

3.1.1.4 会議の概要

同会議に国内から唯一参加された NEC の富田章久氏のご好意により，同氏の報告をベースに，会議の内容について紹介する．

- 会議名：Toward Quantum Standards：A Workshop on Quantum Information Technology
- 期間：2006 年 5 月 25～26 日
- 場所：Royal Society, London
- 主催：Quantum Technology Group, Cambridge-MIT Institute & NIST
- 参加者：名簿上 36 名(NIST2，NSA2，NPL3，GCHQ，DTI など米英の政府関係者，
  MagiQ 2，ARC 2，id quantique 1，NEC1，Toshiba 1 等のベンダー，
  Telecordia，AboveNet，Quantum Information Partners，HP2,その他大学)

尚，この会議の運営委員は以下の通りである．

- 組織委員会：Clarles Clark, Chair (NIST); Mattthias Christandl (Cambridge), Artur Ekert (Cambridge/QTG) and Sonia Schirmer (Cambridge/QTG)
- プログラム委員：Nicolas Gisin (Geneva), Andy Hammond (MagiQ), Richard Hughes (Los Alamos); Sir Peter Knight (Imperial/NPL); Mark Heiligman (NSA), Peter Landshoff (CMI); Seth Lloyd (MIT), Peter Smith (GCHQ), Larry Parker (TBC), Nabil Amer (TBC)

また，同会議について，インターネット上で紹介されている HP は次のものである．
http://www.cambridge-mit.org/events/article/default.aspx?objid=1345

会議の要点をまとめると次の通りである．

- ♦ 今回はワークショップを持つことに意義があるという様子で，具体的に決定されたことがあるわけではない．

- 今後継続していくということで，日本でも対応できる体制を作っていくことが必要である（日本の政府関係機関の参加が期待されている）.
- 技術的な標準化だけでなくアプリケーションやビジネスモデルも視野に入っている.
- 量子鍵配送システムの標準化が主目的で開かれたが，物理量の量子標準なども議論された.
- 安全性基準，相互接続性などのワーキンググループと，既存ネットワーク・現代暗号システムとの統合からビジネスモデルまで商業的な検討をするワーキンググループの設置が議論された.
- 各国の標準化機関, 関連分野の専門家に参加を呼びかけるべき, 等の意見があった.
- 今後も NIST の Charles Clark 氏を中心にこうした議論が展開していくものと思われる.

以下では，同会議で紹介された資料の中から，NEC 富田氏のご好意により，幾つかを抜粋して添付する．最初は，米国のベンチャー企業 MagiQ 社の資料から，次のものはヨーロッパの SECOQC プロジェクトから発表された資料，最後に富田氏の発表資料の中から幾つか抜粋して添付する．尚，MagiQ の資料，および SECOQC の資料については，内容を要約して掲載する.

3.1.1.5　MagiQ Technologies 社の資料から

■量子暗号の背景及び市場予測

情報セキュリティ犯罪の増加

情報セキュリティに対する投資額の増加

量子暗号の需要予測（http://www.qipirc.org/documents.php）

悲観的：300,000,000＄@2015

１＄＝１１８円（2006/12/22 現在）で計算すると，日本円で約 350 億円

楽観的？：3,000,000,000＄@2015

同様に円に換算すると，3 兆 5 千億円

■量子暗号が目標とする市場の採択段階

フェーズ１：　政府，軍事関係，研究機関向け

フェーズ２：　巨大金融機関及び外交関係

フェーズ３：　中規模金融機関，航空管制，警察，賭博場

フェーズ４：　公共利用及び地方議会，州政府

フェーズ５：　データ保管庫のような詳細なデータベースを利用する巨大な組織，秘密の顧客情報を守る必要のある会社，たとえば大きな会計事務所や法律事務所.

■一般的な標準化に関するケーススタディ

（1）　１９世紀の北と南の鉄道レールのゲージ闘争

- 1860 年には７個の異なるゲージが使われていた.
- 商業的な圧力と南北戦争により結局は標準化された.
- 学んだこと
  - ✧ 互換性が無いのは，ほとんどの場合偶然から生じ，歳月がそれに固執させる.
  - ✧ ネットワークの市場は，先導者に向かう傾向がある.
  - ✧ 標準化の調整過程から逸脱することは，将来，自分を市場の弱い位置に置くことになる
  - ✧ 巨大な購入者は供給者よりも大きな影響力を持つ.
  - ✧ ポピュラーでない技術を持った，取り残された人たちは，自ら，その損失を排除する方法に気が付くことになるだろう.

（2）エジソンとウェスチングハウスのシステムの争い

- トーマス・エジソンは直流（DC）を推進した.
- ジョージ・ウェスチングハウスは交流（AC）を推進した.
- AC が勝った.
- 学んだこと
  - エジソンは,DC の方が安全であるということを消費者に納得させることに苦心した.
    - 電気椅子を AC で作り,“ウェスチングハウスする”という言葉を普及させた.
  - もし標準化に向かう力が圧倒的なものでなければ,技術は良く適したニッチ市場を探し当てることができるだろう.
  - 最初の発起人のアドバンテージは,優れた技術を持つことで打ち勝つことができる.
  - 改革の継続が標準化戦争において勝利することができる.

（3）RCA と CBS のカラーテレビの争い

- 白黒の支配
- CBS と　RCA が異なる標準を持っていた.
- RCA は 1960 年にキラーアプリ“ウォルトディズニーの不思議な色の世界”を作り，最終的に勝者となった.
- 学んだこと
  - 新しい技術の採用は，もしそれがあまり魅力的ではなく，そしてたくさんの異なる関係者に採用を働きかけたいとき,腰を据えて行った方が良い.
  - 最初の発起人のアドバンテージは決定的である必要はなく,マーケットが強いものに傾いていけばよい.
  - 標準化の勝利のためには，時には同盟が必要.
  - 技術の一時代において支配的な位置にいるものは,次世代の技術において必ずしも主流になるわけではない.

■一般的な発展段階の市場の標準化戦略

- 標準化は，ネットワークの強い影響下の発展段階の市場にとって重要．例えば,
  - Fax
  - Modems
  - VPN
  - PKI
  - Internet

- 標準化戦争の回避事例
  - CD
  - ビデオ
  - 初期の標準が利益をもたらす
- 量子暗号は進化，発展して促進されるべきであり，改革によるものではない.
  - 消費者の切り替えコストを減らす必要がある.
  - 認識された危険性は減らす必要がある.
  - 量子鍵は既存のセキュリティ標準の上位レイヤーに存在できる.
  - 量子鍵は一まとまりのものの外側に存在することができる.

■標準化に対する勧告

- 国際的な視点
- 標準化開発
  - 透明で，開かれており，広く受け入れられている
  - 買い手，売り手，サービスを守る
  - 社会的な利益を生み出す，資本，仕事を含む新しい市場の創出.
- 推奨される結果
  - 測定とプロトコルに関する報告
  - 量子暗号工業コンソーシアムの設立
  - メンバー
    - 政府
    - ベンダー
    - 消費者
- Biometrics.org をお手本に
  - 重要な点は,
    - 研究
    - 開発
    - テスト
    - 評価
    - 応用
- 標準アーキテクチャ
  - 物理レイヤー
  - 量子プロトコル
  - 古典システムとの統合

- MagiQ は量子暗号工業コンソーシアムのスポンサーである

- Qcrypto.org
  - 工業的な標準化の発展は消費者の投資と相互運用性の促進
  - 検出器や光源のような領域において革新的な研究を促進することによりコスト削減を行う戦略の開発，信頼できる供給連鎖の開発，供給者と購買者に関する経済規模の発展.
  - 潜在的な消費者に対して独立した情報を与えることにより，売り手と買い手が直面するマーケット障壁を下げることができる.
  - 層状のネットワークセキュリティ戦略の一部として，安全な量子秘密鍵配布の価値を認めることで量子暗号の購買に対するビジネスケースを構築する.
  - この Workshop はその設立会議.
- Verizon，AT&T，IBM，Toshiba，NEC，id Quantique，Qinetq が QCrypto.org への参加で興味を示した.

■ QCrypto.org 設立会議議題

- コンソーシアムを形成すべきか？
- どういった類の管理構造にするか？
- 委員会
- 役員
- ワーキンググループ
  - 標準化の枠組
    - 何の枠組
    - 標準化の発展過程
    - 外部の標準化法人との契約
  - 市場開拓
    - 量子暗号に関する価値提案
    - 消費者に対する独立及び信頼できる情報源の開拓
  - 政府
    - 資金の優先度調査
    - 政策立案者の立案
      - 行政官の立案
      - 連邦議会の立案
      - 関連する省庁

■MagiQ の QPN は今日，妥協の無い安全性を提供する.

計算量的な仮定や困難さではなく，量子力学の法則に基づく絶対的な安全性.

- 物理の法則をベースとした安全な鍵配布に鍵の運搬が変わる
- 脆弱リンクである人間の介在を取り除く
- いつでも侵入者を検出できる
- 鍵配布の問題を解決できる
- 確率的に安全な鍵配布に基づく（基底）暗号化
- 連続的に鍵を更新（１秒以下）
- 量子鍵及び古典暗号の組み合わせを用いた強度のオーダーによる安全性の増加
- 絶対的なエンドツーエンドネットワーク安全性のみ与える

■ MagiQ の製品ロードマップ

QPN7505 の特徴

- 多重ギガビットデータプレーン
- 遠隔管理
- 警告
- 多重化鍵

QPN7505 フィールドテスト結果

- テスト場所：防衛，OEM， 大規模電話会社
- 最長 100Km
- カスケードシステムでは 160Km
- 24 時間フルに一週間（7 日間）実施
- 安定性と信頼性

■MagiQ のカスタム性能

- 量子暗号システム
  - 一方向システム
  - デコイ状態
  - カスケード型の格子状ネットワーク
  - 低コスト
  - 長距離
  - 小型
- 専門性
  - 量子情報処理
  - 新 QKD アルゴリズム
  - QKD 関連ネットワーク研究
  - 単一光子検出

- 乱数生成源
- 暗号
- 度量学
- コンピュータ科学
- 教育応用
- ネットワークプロトコル及び構造的な特徴
- もつれあい状態

■量子暗号によって古典暗号の弱点を解決する

- 専門家は大きな数の素因数分解にショートカットはないと信じているが，RSA や楕円暗号は数学的に証明されておらず，ある日突然，革新的な方法が見つかるかも知れない．
- 量子計算機が素因数分解を効率的に解けることは知られている．
- 量子暗号では長期に渡る安全性が保証される．
- ロンドンのロイズ銀行は最近，ハッキングに基づく電子財産の損失の排除を行った．銀行やその他の金融機関は今こそ電子的な保存情報に対して厳しく防御しなければならない．

3.1.1.6 SECOQC の資料から

SECOQC プロジェクトは，2004 年 4 月から 2008 年 4 月までの EU の拡大プロジェクトである．目的は，長距離，高秘匿通信のためのネットワーク基盤を構築することであり，任意の遠隔ノード間で共有する秘密の生成と分散を実現することにある．一方科学的，技術的な目標として，

（1） 量子鍵配布（QKD）技術の改良
（2） インタフェース技術の開発（ユーザ，QKD 供給者）
（3） ネットワーク概念の構築

を掲げている．また，ウィーンの ARC Seibersdorf 研究所が製作推進責任者として参加している．11 カ国，41 機関の参加があり，予算は 16.5 百万ユーロである．

■プロジェクトの構成は次の通り．

- 量子関係
  - 量子光学要素技術（COM）
  - 実験的量子鍵配布（QKD）
  - 量子情報理論（QIT）
- 社会基盤関係
  - 安全性及び暗号（SEC）

- ✧ ネットワーク構造（NET）
- ✧ システム構築及び要求分析（SYS）
- ✧ 共通の基準に従った保証（CCC）

➢ 実装関係

- ✧ 量子バックボーン（QBB）
- ✧ 量子アクセスネットワーク（QAN）
- ✧ ネットワーク実装（NI）

SECOQC プロジェクトでは，標準化が必要なネットワーク関連について，既にその方法論として，Quantum Back Bone という方式を提案し，構築している．この方式はメッシュ上のネットワークの各接合部を QBB ノードと呼び，隣とのリンクを持っている．秘密は隣から隣へバケツリレーで送られる．各 QBB ノードは様々な異なる方式と繋がっている．例えばそれは，コヒーレント一方向システムであり，一方向の微弱パルスシステムであり，連続変数システムであり，もつれ合い光子を用いたものであり，Plug&Play システムであったりする．ウィーンで準備中のものは，５つの QKD 技術を使い，５つの QKB ノードと７つの QKB リンクを持ったものである．ノードのモジュールは，組み込みシステムとして実装されており，その中心部分には，

（１） 鍵管理
（２） 公開チャネルモジュール
（３） 対称鍵暗号モジュール
（４） ネットワークモジュール
（５） 管理モジュール

が入っている．また QBB リンクから鍵を集める機能を有している．

■Q3P(Quantum Point to Point Protocol)インタフェース

Q3P インタフェースには Q3P-QEEP, Q3P-CP, Q3P-TR があり，それぞれ以下の通りである．

Q3P-QEEP

- Quantum key Establishment Encapsulation Protocol
  (量子鍵構築カプセル化プロトコル)
- 量子鍵を作るために QBB リンクとやり取りする．
- QBB リンクメッセージのカプセル化は量子鍵精製における異なる段階で（の接続に）必要となる．

➢ 基底のふるい

- 誤り検出および訂正
- 秘匿性増強

・ Q3P エンジンは QBB リンクに関して（通常／認証／暗号化）古典チャネルで提供される.

・ QBB リンクはある一定間隔ごとに QBB ノードの鍵管理モジュールに生成した鍵をプッシュする.

・

Q3P-CP

・ Q3P-CP
  - Configuration Protocol（CP）
  - QBB リンクパラメータをセットする.（ふるい, 誤り訂正及び秘匿性増強パラメータ）
  - QBB リンクのハードウェアをセットする.
  - 通信セッティングを行う
  - 暗号化パラメータ（認証アルゴリズム，認証モード）
  - 鍵データベースパラメータをセットする（鍵１単位の長さ）

・ Q3P-TR
  - Transmission Protocol(TR)
  - 他のノードへ（から）の送（受）信
    - ✧ QBB リンクの張られた Alice から Bob へ，またはその逆.
    - ✧ 鍵管理者から鍵管理者へ：(秘密のネットワーク)
  - 無条件安全な暗号と認証を利用

■ SECOQC Q3P 標準化

CEN ワークショップ合意

・ CEN(Commite Europeen de Normalisation)の指導に基づく新しいアプローチ
・ 作業分科会において標準化文書（CWA）を作成.
・ この文書は CEN によって出版され，管理されている.
・ 興味のあるどんな団体でも参照することができる.
・ 自発性を基本とする.

スケジュール

・ CW ビジネスプラン作成：2006 年 6 月
・ ワークショップ開始：2006 年 8 月

■ 標準化に関するその他のインタフェース

- ハードウェアインタフェース
  - 量子リンクの中の Alice／Bob のコンポーネント
  - ハードウェアで得られるものとプロトコルの処理で得られるもの
- 応用インタフェース
  - QKD 構造と応用の間
  - IPv6

3.1.1.7 NEC 富田氏の資料から

なぜ標準化が必要か？

量子暗号における顧客の信用を得るため.

- 実用上期待できる安全性のレベルを定義する.
- 相互接続性を保証する.
- 様々な応用を提供し，従来のネットワークに安全性を付加する.

量子暗号の研究を加速する

- 共通の定義，共通のテスト環境を与える
- 応用に関して共通のプラットフォームを提供する.

何を標準化するか？

安全性

- 測定（最終鍵に対する盗聴者の情報量）
- 仮定（プロトコル，モデル,・・・）

装置

- 仕様（性能，環境，信頼性,・・・）
- 校正

ネットワーク

- 監視（モニター），経路制御,・・・
- 相互接続性

応用

- 鍵管理
- 既存のネットワークとの統合

最後に QCrypto というコンソーシアムを紹介する.
http://www.qcrypto.org/
これは先ほどのワークショップを開催した MagiQ がスポンサーとなっている団体であり，その中に，Commercial Prospects for Quantum Information Processing という報告書があり，量子暗号に関する市場予測などが示されている.

６．まとめ

本報告書では，量子暗号通信システムの安全性を，理論および実装の両面から調査した．量子暗号の研究が盛んになった 1990 年代後半は，この分野の主眼は安全性の理論的研究，および実験室レベルでの実証実験にあったが，やはて量子暗号装置は徐々に安定性を増し，フィールド実験の報告が複数なされるようになった．そして 2006 年になって，第５節で述べたような量子暗号システムの標準化の動きが出始めるにいたった．

これらの活動は，実態としては標準化活動というよりも量子暗号製品実現に向けたワークショップという色彩が強い．第４節で述べたとおり，現在でもすでに，MagiQ Technologies 社， id Quantique 社，SmartQuantum 社から量子暗号製品が発売されているが，広く利用されているという状況とは言いがたい．このため上記の標準化活動も，すでにある程度の需要が存在している製品に対して標準化を行うものではない．むしろ未だ基礎研究の段階にある製品の需要を，いかにして掘り起こすかという点に主眼がおかれている．

一方で第１節でも述べたとおり，量子暗号と従来型暗号との最大の違いは，「無条件安全性」の達成である．２.２.２節や４.１節でも述べたとおり，現在では実際にこれが実験室レベルで可能となっている．実装例としては伝令つき単一光子源を用いたもの(２.３.２節)や，デコイ方式によるもの(２.５.２節)がある．しかしこれは主に 2006 年以降の流れであり，それ以前の実装報告では，以下の２種類の仮定を置き，安全性の要件を緩めたうえで安全性評価を行っていた：

- 平均光子数 $\mu = 0.1$ のコヒーレント光を単一光子とみなす．
- 個別攻撃を仮定する．

上記 3 社の製品に関しては，安全性のよりどころとなるパラメタ(ビット誤り率 ε や複数光子生成率 P_{multi})が非公開であるため断言は難しいが，実際に無条件安全性が達成されているとは考えがたい状況証拠がある(４節参照)．

これらの例に見られるように，現在は量子暗号実装における評価基準の端境期であり，これまでの仮定つきの安全性から，仮定なしの厳密な無条件安全性へ移行がなされている．今後の量子暗号研究においては無条件安全性が最低条件となることは必至であり，その流れは当然市販製品にも及ぶと予測される．そして標準化活動（もし今後も持続するなら）においてもこの流れの影響を強く受けると考えられる．

ただし無条件安全性への移行はまだ始まったばかりであり，どこまで安価に効率的に実現できるかが今後の重要な研究課題となる．この方向性の一つとして２.５節で紹介した新プロトコルがあり，例えばデコイ方式は実際に，従来型の BB84 よりも安価に無条件安全性を実現することに成功している．現在これ以外にも DPSQKD 方式などの多くの有望な方式が提案されており，最適方式の決定には少なく見積もっても数年を要すると思われる．つまり従来型の暗号研究の歴史と同様に，方式提案と改良の繰り返しの時代が続くと予測される．

このように現在は，標準化を行って方式を固定するにはあまり時期尚早である．むしろ重要なことは，これまでなされてきたように理論と実験のバランスを保ちつつ方式改良を進めていくことである．そしてそのような量子暗号装置の経済性向上へのをたゆまぬ努力が，結果として顧客開拓へと結びついていくと考えられる．