連載講座

量子情報処理パラダイム
2. 量子暗号

富田　章久

1. はじめに

インターネットの爆発的普及，電子商取引の実用化を迎え，通信の秘密保持・改竄防止や個人の認証など暗号技術の社会的な必要性が高まっている．現在，DES暗号のような共通鍵方式やRSA暗号をはじめとする公開鍵方式が広く用いられている．しかし，これらは「計算量的安全性」つまり今あるコンピュータでは暗号を解読するのに時間がかかりすぎるということに基盤を置いている．つまり，現行の暗号方式は計算機ハードウェアと暗号解読アルゴリズムの進歩に常に脅かされている．特に銀行間のトランザクションや軍事・外交にかかわる情報などの極めて高い安全性が要求される分野では原理的に安全な暗号方式が実用になればそのインパクトは大きい．量子暗号の安全性は量子力学という物理学の原理に基づいているため，いかなる技術の進歩があっても保証される．Bennettら[1]による具体的な量子暗号鍵配布プロトコルの提案を契機に量子暗号の研究が盛んになっている．

本稿では，量子暗号の中で最も実現性が高いと考えられている量子暗号鍵配布を紹介する．情報理論で無条件安全性が証明されている暗号方式にone time pad法がある[2]．この方法では乱数の列（暗号鍵）を他人に知られないように共有することが必要だが，量子暗号鍵配布はこのための手段を与えるものである．装置が完全な場合には量子暗号鍵配布の安全性は数学的に証明されている[3, 4]．しかしながら，現実には完全な装置を作成するのは不可能である．実際の装置で安全性を保障するには最適なシステムの設計を行う必要がある．以下では，現実のシステム解析に適用できる安全性の解析法を説明する．量子暗号鍵配布の実現法，今後の研究課題についても述べる．

とみた　あきひさ
科学技術振興事業団 今井量子計算機構プロジェクト
NEC基礎研究所
〒305-8501 つくば市御幸が丘34

2. 暗号鍵配布の安全性

今，送信者（Alice）から受信者（Bob）に2進乱数列を送る．得られた生の鍵から図1のような過程で最終鍵が生成される[5]．このとき，乱数について盗聴者（Eve）が持つ情報量よりもBobの情報量が大きければ，情報量の差の分だけの安全な乱数列をAliceとBobが共有することができる．Eveの情報量を減らすために，量子力学の測定の性質を用いるのが量子暗号鍵配布である．量子力学における測定には

① 非直交状態を1回の測定で完全には区別できない（ある確率で間違う）．

② 未知の状態の完全なコピーは作れない．

といった性質がある．Aliceは，いくつかの状態がそれぞれビット値0または1を表すとして，送信する状態がどの固有状態にあるかをあらかじめBobに知らせずに送信する．盗聴を行うためにEveは量子力学的状態を完全に知るには①の性質により多数回の測定を行わなければならないが，1ビット当たり1個しか光子が送られない場合，②により完全なコピーが作れないのでそれは不可能である．Eveの測定結果はこのため必ず誤りを含む．完全な測定ができないのはBobも同様であるが，彼は別の通信路でAliceと通信することができ（この通信路は古典的で誤りはないものとする），送られてきた乱数列のうち自分がどのビットで正しい測定をしたかを知ることができる．Aliceとの古典的な交信によって正しい測定をしたビットだけを鍵として採用すると，鍵のビットについてのBobの誤り率は理想的には0になる．このように，古典的な通信によってBobは鍵についての情報量を高めることができ，安全な鍵の共有ができる．Eveが自分の情報量を増やすために途中で測定を行うとBobの誤り率が異常に増大するため盗聴が検出される．

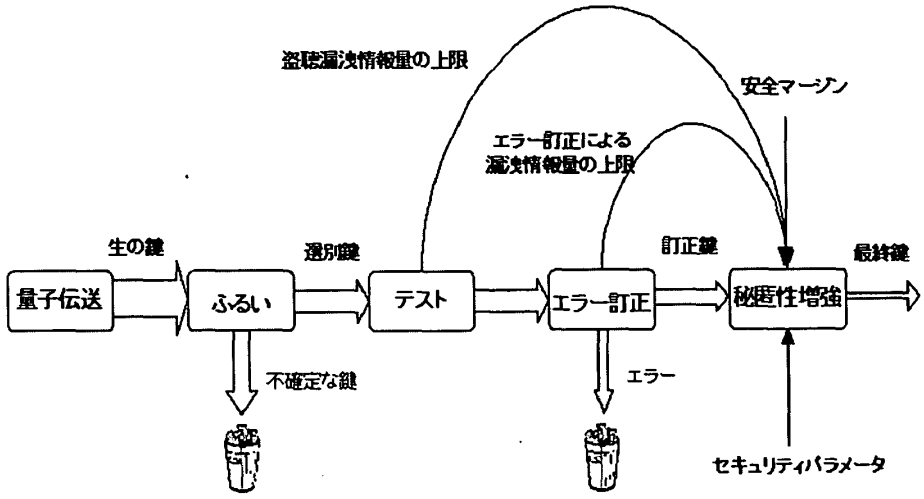

図1　暗号鍵生成の過程

以上のことをより定量的に検討する[6]．Bobの測定結果における誤りは装置が完全な場合は盗聴者の存在を示すが，実際には装置の不完全性からも誤りが生じ，これらは区別できない．現実の装置で誤りを全て盗聴と判断すると暗号鍵の共有が不可能になるので，どの程度誤りがあっても安全な暗号鍵が生成できるかを解析する必要がある．Bobの誤り率をe_BとするとAliceとBobの間のシャノン情報量はアプリオリに等確率な2値信号に対しては

$$I_{AB}=1+e_B\log_2 e_B+(1-e_B)\log_2(1-e_B) \tag{1}$$

で与えられる．Bobは判別できたn_{sift}ビット（sifted bits）のうち$n_{sift}I_{AB}$ビットの情報しか持たない．2方向通信による，知られている最もよい誤り訂正プロトコル[7]では誤り率は0.15以下でなければならないとされている．ここで得られた誤りのない長さn_{rec}のビット列（reconciled bits）からさらに秘匿性増強（Privacy Amplification）アルゴリズムによって安全な暗号鍵を得る．Eveの得る情報量の上限をτとすると，ビット列の長さの$\tau(<1)$倍をハッシングに用い，さらにn_Sビットを安全パラメータとして犠牲にすることで，生成された長さ$(1-\tau)n_{rec}-n_S$の暗号鍵に対するEveのシャノン情報量を

$$I_E^{final}\leq\log_2(2^{-n_S}+1)\approx\frac{2^{-n_S}}{\ln 2} \tag{2}$$

に抑えることができる[8]．ここでn_Sは定数だから十分長い乱数列を送れば無視できるようになり，任意の安全性を持つ長さがほぼ$(1-\tau)n_{rec}$の暗号鍵が得られる．

Eveの得る情報量はRenyiのエントロピーの減少で測る[5]．これは盗聴という行為が，Eveが自分の測定結果からもとの量子状態を推定することに当たるためである．測定結果がμのとき量子状態がiである条件付確率$q_{i\mu}$は，もとの量子状態がとる確率p_i，量子状態がiのときμなる測定結果を得る確率$P(\mu|i)$と測定した結果がμになる確率P_μとを用いてBayesの定理により

$$q_{i\mu}=\frac{P(\mu|i)p_i}{P_\mu} \tag{3}$$

で与えられる．確率p_iと$P(\mu|i)$は測定する系によってあらかじめ決まる．また，確率P_μは測定の結果として得られる．EveのRenyiエントロピーは測定（盗聴）前の値$R_0=-\log_2\sum p_i^2$から測定した結果μによる値$R_\mu=-\log_2\sum q_{i\mu}^2$に減少する．盗聴によって得られるEveのRenyi情報量I^Rは

$$I^R=\sum_\mu P_\mu\left(-\log_2\sum_i p_i^2+\log_2\sum_i q_{i\mu}^2\right) \tag{4}$$

となる．特にアプリオリに等確率な2値信号（$p_1=p_2=1/2$）に対しては

$$I^R=\sum_\mu P_\mu\left(1+\log_2\sum_i q_{i\mu}^2\right) \tag{5}$$

である．I^Rの上限τはCollision Rateの期待値$\langle p_c(y)\rangle$を用いて

$$\tau=1+\frac{1}{n_{rec}}\log_2\langle p_c(y)\rangle \tag{6}$$

で表される．ただし，Collision Rateは以下のように定義される．Aliceの送るビット列をX，Eveが盗聴の結果得たビット列をYとする．測定結果が$y=\{\mu_j\}$のとき，送られたビット列が$x=\{i_j\}$である条件付確率は個々のビットについての条件付確率の直積$P_{Alphabet}(x|y)=\prod_j q_{i_j\mu_j}$になる．Collision Rateは全ての可能なビット列Xについて$P_{Alphabet}$の2乗の和と

して定義される：

$$p_c(y)=\sum_x P^2_{Alphabet}(x|y)=\sum_x\left(\prod_j q^2_{ij\mu_j}\right) \tag{7}$$

これより，Collision Rate の期待値は

$$\langle p_c(y)\rangle=\sum_y p(y)p_c(y)=\left(\sum_{i,\mu} P_\mu q^2_{i\mu}\right)^{n_{rec}} \tag{8}$$

となる．これと式(6)を用いると τ は

$$\tau=1+\log_2\sum_{i\mu} P_\mu q^2_{i\mu} \tag{9}$$

と表される．Jensen の不等式

$$\sum_\mu P_\mu \log_2\sum_\mu q^2_{i\mu}\leq\log_2\sum_{i,\mu} P_\mu q^2_{i\mu} \tag{10}$$

により，$\tau\geq I^R$，すなわち τ が Renyi 情報量の上限であることが示された．

以上で述べた誤り訂正と秘匿性増強の過程で失われるビットを考えると暗号鍵の鍵生成レートは次のように書ける：

$$R=1+\chi[e_B\log_2 e_B+(1-e_B)\log_2(1-e_B)]-\tau \tag{11}$$

ただし，χ は誤り訂正の効率である．安全な暗号鍵配布にはこの鍵生成レートが正の値になることが必要である．実際の暗号鍵の生成レートは上の R に信号検出レートと，検出された信号から判別されたビットが得られる確率をかけたものになる．量子暗号では盗聴によって得られる情報量 τ が大きくなると誤り率 e_B も大きくなる．言い換えれば，誤り率が与えられると Eve の得られる情報量は量子情報理論に基づいて決められる最適な盗聴法における $\tau_{opt}(e_B)$ で上限が抑えられる．これによって所望の安全性を実現するために必要な秘匿性増強のためのビット数や誤り率の許容範囲が決められる．最適な盗聴法は信号の伝送方法と盗聴方法によって変わるため，実際に行われる量子暗号鍵配布の方法に基づいた解析が必要である．

3. 量子暗号鍵配布の実際

3.1 実現法

上に述べた不完全な測定と古典的通信による受信者の情報量増大を量子力学的状態の測定によって実現する具体的な方法として BB 84[1]とよばれる偏光または位相で表された光子の 4 状態を用いる方法，非直交 2 状態を用いる B 92[9]，エンタングル状態を用いる 2 粒子干渉 E 91[10]やこれらの変形が提案されている．ここでは，最も解析が進んでいる BB 84 について説明する．具体的には，光子の偏光状態をビット値に対応させる（符号化）．例えば水平（0°）方向と垂直（90°）方向の直線偏光状態をそれぞれ 0 と 1 とする組と，斜めの 45° 方向と 135° 方向の直線偏光状態をそれぞれ 0 と 1 にする組を用いる．暗号鍵配布の手順は以下のようである．

1. Alice は 1 ビットごとにどちらかの組を使うかを決めて乱数を送る．この段階では Alice は自分の選択を Bob に連絡しない．
2. Bob は送られてきた光子の偏光状態を測定するが，検光子を 0° 方向と 90° 方向の偏光を正しく判別できる基底か 45° 方向と 135° 方向の偏光を正しく判別できる基底のいずれかをランダムに選択して測定する．検光子の向きが送られてきた偏光とあっているときは正しいビット値が得られるが，向きが違っているときは正しい値は得られない．正しい測定が行える確率は 1/2 である．
3. Alice は Bob が全ての光子を受け取った後にそれぞれの光子について自分の選択を Bob に連絡し，Bob は正しい測定をしたビットの位置を Alice に連絡する．これで Alice と Bob はビット列を共有できる．偏光状態の組や検光子の向きについての連絡はビット値そのものを知らせているわけではないので普通の通信路を使えばよい．
4. Bob は送られてきたビットをいくつか選んで Alice に確認し，誤り率を測定する．誤り率が大きければ Alice と Bob は盗聴者がいたと結論し，その回送られた乱数列は全て捨てる．誤り率が小さいとき，誤り訂正と秘匿性増強を経て安全性が確認できた乱数列を最終的な暗号鍵とする．

暗号鍵配布システムの構成はおおよそ図 2 に示すようなものである．送信者は乱数発生器からの出力で光源からの光を変調する．このとき，符号化の基底をランダムに選定するためもう一つ乱数発生器が必要である．生成された光子は伝送路（光ファイバまたは自由空間）を通って受信器に入る．受信者は光子の状態を測定するための基底を受信者の乱数発生器によって定め，光子検出器で光子を検出する．以上で量子通信路が構成される．これに加えて暗号鍵を生成するための古典通信路が必要になる．実際のシステムではさらにクロック分配，送受信者の基底の較正，その他のシステム管理情報の交換が必要だが，これは古典情報路と共用できる．また，量子通信と古典通信で用いる光の波長を変えることで物理的には同一の光ファイバを用いることができる．

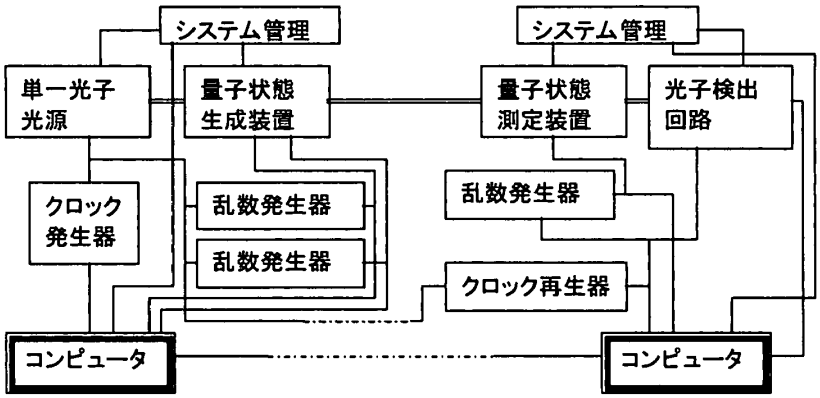

図2　量子暗号鍵配布システムの構成（二重線で結ばれた部分が量子通信路に当たる）

3.2　装置が不完全な場合の安全性[6]

送信側の光源が完全（必ず1光子を放出する）で受信側の装置も誤りがない場合，量子暗号鍵配布は無条件に安全である．盗聴がビットごとに行われる場合(Individual Attack)，送信側の光源が完全で1ビット当たり1光子のみを送る（単一光子光源）場合，BB 84プロトコルでは

$$\tau(e_B)\leq\begin{cases}\log_2(1+4e_B-4e_B^2) & (e_B\leq 1/2)\\ 1 & (e_B\geq 1/2)\end{cases} \tag{12}$$

でτの上限が与えられる[11]．近似的に単一光子を発生する光源としてよく行われているように半導体レーザからのパルス光を0.1光子/パルス程度に弱めたものを使うと，光子数nの分布は平均光子数Nのポワソン分布$P(n,N)=\exp[-N]N^n/n!$になる．1ビット当たり2個以上の光子が送られていると，光を分岐して受信する光子の状態に影響を与えずに測定できるので，検出されることなく盗聴が可能になる．すなわちCollision Rateは1になりうる．今，誤り訂正して得たn_{rec}ビットのうち，mビットが2個以上の光子で送られたとする．盗聴によって状態が変化して誤りが起きるのは光子数が1個のときだから，τの評価式(12)で用いるべき誤り率e_rは測定された誤り率e_Bを$n_{rec}/(n_{rec}-m)$倍したものになる．また，ビット列についてのCollision RateはmビットのCollision Rateが1であることから(8)でn_{rec}を$n_{rec}-m$に置き換えたものになる．Aliceの送るビット列が十分長い（長さn_{tot}）ときmは期待値Mで置き換えてよい[6, 12]ので，

$$e_r=e_B\frac{n_{rec}}{n_{rec}-M} \tag{13}$$

また，M/n_{tot}は送信側で1ビット当たり2個以上の光子が送られる確率$S_M=1-\exp[-N](1+N)$に等しい．また，受信器における検出確率をP_{DET}とすると$n_{rec}=P_{DET}n_{tot}$である．結局，鍵生成レートは

$$R=(1-M/n_{rec})(1-\log_2[1+4e_r-4e_r^2])+\chi[e_B\log_2 e_B+(1-e_B)\log_2(1-e_B)] \tag{14}$$

で与えられる．誤り訂正が完全に行われるとして($\chi=1$)鍵生成レートが正の値を取る誤り率の最大値は光源が完全な場合0.113となる．

一方，伝送路での光子の損失は鍵生成レートを低下させるだけで誤りを生まないので，安全性には直接影響しない．ただし，受信器が光子を誤検出する（ダークカウント）確率が高いときには伝送された光子より誤検出が支配的になるため誤りが増加する．光子検出には一般に光通信用のアバランシェフォトダイオード(APD)が光子計数モードで用いられる[13, 15]が，1ビットスロット当たりのダークカウント確率は10^{-6}から10^{-3}程度になる．伝送路での損失をα(dB/km)，光子の偏光状態が一部ランダムになる割合をvとする．受信器が光子を検出する確率（量子効率）をη，ダークカウント確率をP_d，受信器における損失βとする．L kmの伝送後に受信器が光子を検出する確率は1ビットスロット当たり検出器に1個以上の光子が到達する確率をSとして$P_{DET}=S\eta+P_d-S\eta P_d$で与えられるから受信器における誤り率は

$$QBER=\frac{Sv\eta+P_d}{2P_{DET}} \tag{15}$$

となる．1ビットの乱数を送るのに平均光子数Nのレーザパルスが使われたとすると，Sは

$$S=1-\exp[-10^{-(\alpha L+\beta)/10}N] \tag{16}$$

で与えられる．最終的に鍵が生成されるレートはビット列が送出されるクロック周波数fとを使って以下のように表せる：

$$R_{Final}[\text{bit/sec}]=(1/2)f[\text{Hz}]\cdot P_{DET}R \tag{17}$$

ここで，最初の1/2はBB 84プロトコルでBobが正しい測定をする確率である．観測される誤りが全て受信器に起因すると仮定すると伝送可能な距離を求めることができる．伝送路として光通信に広く用いられる波長である1550 nm帯で得られる$\alpha=0.2$ dB/km，$v=0.01$のファイバを考える．図3は単一光子光源を用いた場合の鍵生成レートでクロック周波数により規格化したものを示す．これから，100 km以上の伝送を行うには光子検出器のダークカウント確率を10^{-4}以下にしなければならないことがわかる．ここで，受信器の損失を1 dB，量子効率を0.18と仮定した．図4は光源としてレーザ光を用いた場合の鍵生成レートを示す．単一光子光源を用いたときに比べ伝送可能な距離が大幅に狭まっている．

3.3 実験の現状

British Telecom[16]，ジュネーブ大[17]，IBM[18]，Los Alamos国立研[19]などいくつかのグループで暗号鍵配布の実験が行われている．ファイバでは

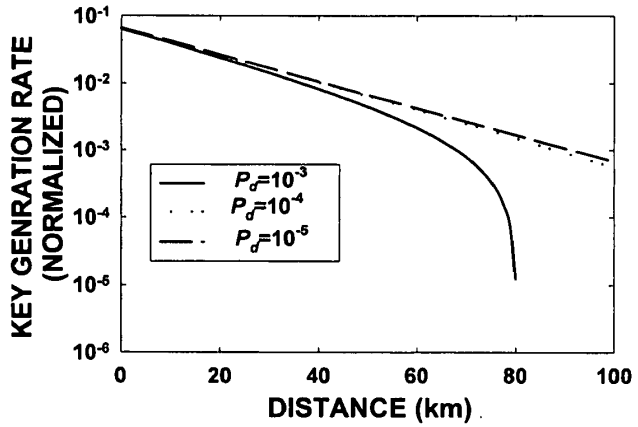

図3　単一光子光源による暗号鍵生成レートと伝送距離（P_dはダークカウント確率）

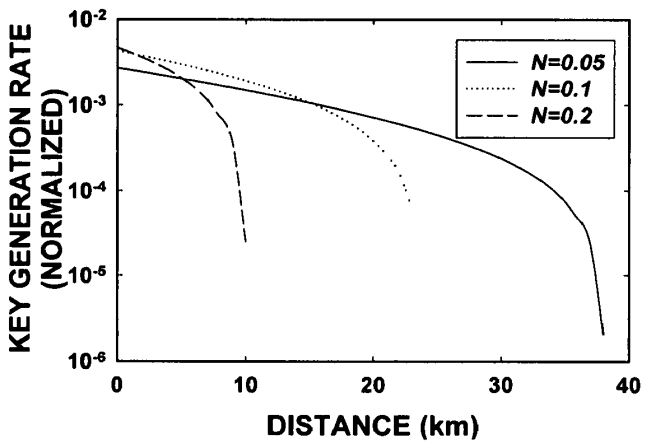

図4　レーザ光による暗号鍵生成レートと伝送距離（Nは1パルスの平均光子数）

偏光は必ずしも保存されないため，ビームスプリッタで分割した光子の位相差をビット値に対応させることがよく行われている．現在得られている最長の量子暗号鍵配布の実験は48 kmのファイバを用いている[19]．また，ファイバを通るときの偏光状態のゆらぎを自動的に補償する方法も提案されている[17]．この方法を用い，誤り訂正や秘匿性の増強も含めたシステム実験も行われ，10 kmのファイバを伝送させて最終的な鍵生成レート200 bit/sが得られている[18]．これらの実験についての詳細は文献を参照されたい．

4. 今後の研究課題

最後に今後研究の進展が期待される課題をいくつかあげる．

前節で見たように安全に伝送できる距離を増すには単一光子光源が必要である．より単一光子に近い光源としては非線形光学結晶から2光子の対が発生する現象（パラメトリックダウンコンバージョン，PDC）を用いることも提案されている[6]．PDCが同時に同じエネルギーの光子を発生することは極めてまれにしか起きないため，ほぼ単一光子を発生する光源とみなすことができる．光子が発生したことは2光子対の片方を検出すれば知ることができる．既にいくつかの研究機関から実験の報告があるが装置の大きさや光子の発生効率の低さを克服する必要がある．

理論的にも，光源が完全でない場合の本稿で述べた解析はindividualな盗聴法しか扱えず，全ての盗聴に対する安全性の証明や効率の良いプロトコル等の研究が必要である．

また，暗号鍵を生成するためのソフトウェアも重要である．誤り訂正や秘匿性の増強，相手の認証などが必要となる．情報理論はビット数の下限を与えるだけであり，アルゴリズムや実装によってどれだけのビットを犠牲にすることが必要になるかが異なってくる．できるだけビットの損失の少ないプログラムを作ることが必要である．これらは実際に量子暗号鍵配布が可能な誤り率の限界をきめるため，実用上の性能-伝送距離・伝送レートなどに大きな影響を与える．

種々の実証実験が示しているように量子暗号鍵配布は既存の光通信デバイスを用いることによって実現できる．理論，実験とソフトウェア開発をさらに進めていくことにより，実用的な量子暗号システムの実現は比較的早いものと期待される．さらに，長距離伝送や交換，多対多の暗号鍵配布，量子暗号鍵配布以外の暗

号プロトコルなどにより高度な安全の保障された量子暗号ネットワークが社会の根幹を支えることを期待している．量子暗号の研究は情報の基礎理論からプロトコル，物理的実装，デバイス開発と広い分野にまたがっている．この中でも実際の設計に必ず現れる最適化の問題を扱うことが今後より重要になっていくものと考えている．

参考文献

[1] Bennett, C. H., and Brassard, G., "Quantum cryptography: Public key distribution and coin tossing", *Proc. IEEE Int. Conf. On Computers, Systems, and Signal Processing, Bangalore, India*, (1984), 175.

[2] 岡本達明, 山本博資,『現代暗号』(1997), 産業図書, 第4章.

[3] Mayers, D., "Unconditionl security in quantum cryptography", (1998), *arXive e-print quant-ph/9802025*.

[4] Nielsen, M. A., and Chuang, I. L., *Quantum computation and quantum information*, Sec. 12.6(2000), Cambridge Univ. Press, Cambridge, UK.

[5] Slutsky, B., Rao, R., Sun, P.-C., Tancevski, L., and Fainman, S., "Defense frontier analysis of quantum cryptographic systems", *Appl. Optics*, 37(1998), 2869-2878.

[6] Lütkenhaus, N., "Security against individual attacks for realistic quantum key distribution", *Phys. Rev., A* 61(2000), 052304.

[7] Bassard, G., and Salvail, L., "Secret-key reconcilation by public discussion", *Proc. Eurocrypt* '93 (Lofthus, Norway, 1993).

[8] Bennett, C. H., Brassard, G., Crépeau, C., and Maurer, U. M., "Generalized privacy amplification", *IEEE Trans. Inf. Theory*, 41(1995), 1915-1923.

[9] Bennett, C. H., "Quantum cryptography using any two non-orthogonal states", *Phys. Rev. Lett.*, 68(1992), 3121-3124.

[10] Ekert, A. K., "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.*, 67(1991), 661-663.

[11] Lütkenhaus, N., "Security against eavesdropping in quantum cryptography", *Phys. Rev., A* 54(1996), 97-111.

[12] Hoeffding, W., *J. Am. Stat. Assoc.*, 58(1963), 13.

[13] Hiskett, P. A., Bonfrate, C., Bujjer, G. S., and Townsend, P. D., "Eighty kilometer transmission experiment using an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55 μm", *J. Mod. Optics*, 48(2001), 1957-1966.

[14] Stuck, D., Ribordy, G., Stefanov, A., Zbinden, H., Rarity, J. G., Wall, T., "Photon counting for quantum key distributiom with Peltier cooled InGaAs/InP APDs", *J. Mod. Optics*, 48(2001), 1967-1981.

[15] Bourennane, M., Karlson, A., Ciscar, J. P., and Mathes, M., "Single-photon counters in the telecom wavelength region of 1550 nm for quantum information processing", *J. Mod. Optics*, 48(2001), 1983-1995.

[16] Marand, C. and Townsend, P. D., "Quantum key distribution over distances as long as 30 km", *Optics Lett.*, 20(1995), 1695-1697.

[17] Zbinden, H., Bechman-Pasquinucci, H., Gisin, N., and Ribordy, G., "Quantum cryptography", *Appl. Phys., B* 67(1998), 743-748.

[18] Bethune, D. S., and Risk, W. P., "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light", *IEEE J. Quantum Electron.*, 36(2000), 340-347.

[19] Hughes, R. J., Morgan, G. L., and Peterson, C. G., "Quantum key distribution over a 48 km optical fibre network", *J. Mod. Optics*, 47(2000), 533-547.