量子情報セキュリティ技術の動向と電子政府における利用に向けた課題調査

平成 19 年 5 月 17 日

目 次

第1章　業務名および概要

1.1　業務名

量子情報セキュリティ技術の動向と電子政府における利用に向けた課題調査

1.2　業務の概要

平成18年度の暗号技術検討委員会（CRYPTREC）における量子暗号技術の動向調査及び電子政府における利用可能性検討等の活動を円滑に実施するための業務について、本仕様書の通り委託する。暗号技術検討会における量子暗号技術に対する検討の必要性について、概要を以下に示す。

総務省と経済産業省により設置された暗号技術検討会は、電子政府等において利用すべき暗号について、電子政府推奨暗号リストとして平成15年2月に公表した。電子政府推奨暗号選定作業当時は、量子暗号技術は実用化段階に至っていなかったが、昨今では、さまざまな研究や実証実験が活発に行われるのみならず一部製品化も進んでいる。電子政府等において、量子暗号技術を利用する場合には、一定水準以上の安全性及び信頼性について客観的な評価を得たものであることが必要である。このため同検討会において量子暗号技術の評価の必要性、や技術動向及び電子政府利用の可能性等に関する検討を実施すべきとの指摘がなされた。

上記指摘を踏まえ、暗号技術検討会及び同検討会活動の技術的側面を担当する暗号技術監視委員会（NICT及びIPA主催）の活動を実施するにあたり、量子暗号技術に関する専門知識を基とした広範囲に渡る調査・検討作業が必要となる。詳細部分に至るまで技術動向や製品化動向を把握し、利用可能性等の検討を実施するためには、量

子暗号技術に関わる情報収集作業、及び収集した情報に基づく実利用の方向性を検討する作業が必要である。本仕様書では「量子情報セキュリティ技術の動向調査」作業および「電子政府における利用に向けた課題検討作業」を委託する。また上記の専門知識を持って詳細な調査作業を実施できることが本業務を遂行する上で肝要である。

量子暗号技術の技術動向等に関する調査作業及び電子政府利用の可能性検討作業報告業務として具体的には以下の作業を行う。

1. 学会等必要と判断される会議への参加、もしくは資料取り寄せなどして、量子暗号に関する技術動向に関わる情報を収集する。

2. インターネット等を通じて、量子暗号技術に関する技術動向及び製品化動向に関わる情報を収集する。

3. 量子暗号に関する技術動向などをテーマとして研究会などを開催し、それに関わる情報を収集する。

4. 上に示した作業で収集した情報をもとに、国内外の量子暗号に関する技術動向及び標準化動向に関して整理・分析を行う。また、電子政府利用の可能性について検討を行う。

1.3　注目すべき動向と本報告書の内容

本報告書では、上述の目的を達成するために、量子暗号技術のうち、特に実用に近いＢＢ８４鍵配送プロトコルを中心に、理論解析技術のトレンドとしての安全性証明技術のここ数年の発展と、実用化に向けた技術開発のトレンドとしてのデコイ方式に焦点を当て概説を行う。また、電子政府利用の可能性についても動向調査に基づき、そこに至るために必要な課題の整理を行うものとする。

第2章　安全性証明に関するトレンド —情報攪乱定理からの視点—

2.1　量子暗号とは

量子暗号プロトコルは、計算量的安全性ではなく、情報論的安全性をもつ暗号方式である。典型的な例である（またほぼ唯一のうまくいっている例である）鍵分配プロトコルでは、盗聴者は物理法則（量子論）に従う限り何をおこなってもよい。現在までに効率的な方法で解くことができていない問題であっても、効率的に解けるような計算機をもっていると仮定してもよい。そのような条件下においてもなお、Alice と Bob は Eve に全く推測不可能な乱数列を共有することができる。この量子鍵分配プロトコルと呼ばれる方式は、1984 年に Benneett と Brassard によってまず最も簡単なものが提案された [5]。これは今日 BB84 プロトコルと呼ばれるものである。その後、1991 年に Ekert が（一見）異なる方式 (E91 プロトコル）を提案した [11]。（後にこれらの同等性は示された。）また、1992 年には Bennett が B92 プロトコルと呼ばれる方式を提案している [12]。これらの方式はかなりシンプルではあるが、その無条件安全性が示されたのは 1996 年に Mayers によってであった [17]。この証明は非常に複雑であったため、その後もいくつかの別証明が現れた。この状況は現在に至るまで続いている。これら別証明のうちまずあげられるのが、2000 年の Lo と Chau によるものである [22]。この方法は、Entanglement Distillation と呼ばれる方法を用いている。これは、Alice と Bob が不完全なエンタングルド状態から量子的な操作（LOCC=Local Operations and Classical Communications) をほどこすことにより、いくつかの完全なエンタングルド状態（EPR 対）を抽出する方法である。この証明は非常にシンプルなものであったが、実際のプロトコルを考えると、Alice と Bob に量子的な操作を課すということであまり

現実的なものではなかった。この難点をカバーした、なおかつシンプルな証明方法として Shor と Preskill が 2000 年に提案したもの [19] があげられる。これは量子符号の一種である CSS 符号 (Calderbank-Shor-Steane) と呼ばれるものを用いた方法である。これは One-way な通信のみに制限した Entanglement Distillation に対応している。本質的に同じ符号を用いた別証明が Boyer、Boykin、Mor と Roychowdhury [8] によっても提出されている。彼らの証明の特徴は Information-Disturbance 定理と呼ばれる示唆に富む定理を介していることである。これは、量子論の最も本質である不確定性関係の情報理論版とでも言うべき定理であり、その後も多くの研究者によりとりあげられてきた。この章では、まずこの証明方法を紹介し、後に最近の大きな発展である Hash fuction を用いた方法を紹介する。

2.2 BB84 プロトコル

まず、BB84 プロトコルについてふりかえってみよう。登場人物は正規ユーザであるAlice と Bob、そして盗聴者である Eve である。Alice は、量子ビット (二次元ヒルベルト空間である $\mathbf{C}^2$ によって記述される）を何個も用意し、それを Bob に送る。この $\mathbf{C}^2$ に 2 つの基底を導入しよう。１つの基底 $G_z = \{e_1, e_2\}$ は、縦と横の偏光を記述する。もう一つの基底 $G_x = \{h_1, h_2\}$ は、対角と反対角の偏光を記述する。これらは mutually unbiased な関係、

$$|(e_i, h_j)| = \frac{1}{\sqrt{2}}, \quad i, j = 1, 2 \tag{2.1}$$

にある。基底 G_z からのベクトル e_1, e_2 と基底 G_x からのベクトル h_1, h_2 は、それぞれ、パウリ行列 σ_z と σ_x の固有ベクトルである。

Bob は、光子検出器 (2 つの基底の一つに単一光子を検出する装置) を持っている。Alice は光子エミッタで放出される光子を Bob に送ることができ、Bob は光子検出器で光子を検出する。

プロトコル

1. Alice は、ランダムな偏光基底を選び、選んだ基底に属しているランダムな偏光を持つ光子を用意する。彼女は、その光子を Bob に送る。

2. 各光子に対して、Bob は、どの偏光基底を使用するかをランダムに選び、光子の偏光を測定する。（もし、Bob が Alice と同じ基底を選べば、彼は確実に光子の偏光を識別することができる。）

3. Alice と Bob は、彼らが使用した偏光基底を比較するために、公開された通信路を使用する。（但し、この通信は改変されてはならない。＝あらかじめ共有された短い秘密鍵によってこれは保証される。）彼らは、偏光基底が同じであるデータをだけを保存する。誤りと盗聴がない場合、これらのデータは、両者で同じものである。このように得られたデータ（必ずしも Alice と Bob で一致しているわけではない）を、原鍵 (sifted key) と呼ぶ。

4.Alice と Bob はランダムに半分の原鍵を公開し、エラー率を検討する。このエラー率がある閾値よりも大きければ、このプロトコルは失敗とみなし、破棄する。

5. 最後に、Alice と Bob はこの原鍵にたいして、エラー訂正と秘匿性増強を古典通信路により対話を行うことにより行う。

上記、プロトコルの結果として、Alice と Bob は、同じランダムなデータを共有する。このデータは、その後、対称暗号法の秘密鍵として使用することができる。

偏光された光子の代わりに、任意の 2 準位量子系を使用することができる。また、k 個の基底を持つ d-次元ヒルベルト空間を使用して、一般化された量子鍵配送プロトコルを考えることもできる。

上記、エラー訂正と秘匿性増強部分には大きくわけて二つのやり方がある。一つは、前述の CSS 符号を用いた方法であり、もう一つはごく最近になって提案されたものであるが、古典情報理論の概念である Hash function を用いた方法である。前者は、秘匿性増強の方法を盗聴者も知っていてよい、という点において古典論とは著しく異なるプロトコルである。この場合、ランダムに何かを選んだりする必要は全くない。しかしながら、実際に CSS 符号を構成することは非常に難しい。この点をカバーするのが後者の方法である。これは、古典論においてよく知られた Hash function の知識を用いることができるという点で優れている。

まず次節以降しばらく、このプロトコルの最も量子らしい部分、「Eve の情報搾取が Bob の結果に誤りを生じさせてしまう」という事情を最近出版された Biham らの論文にそってみていく。

2.3　コピー不可能性定理

量子鍵分配の安全性の説明として、よく引き合いに出されるのがコピー不可能性定理である。もちろん、このコピー不可能性定理だけでは、全く安全性は保証されないが、これをより精緻化した Information-Disturbance 定理を理解するうえではこの定理を理解しておくことは意義深いと思われる。通信傍受者である Eve は Alice のおくったデータの完全なコピーを手に入れたい。(Eve は Alice から送られてきたものをただ奪ってしまったままではいけない。なぜなら、Bob は Alice からの通信が途絶えたことにより、Eve の存在を気づいてしまう。そこで、Eve は手元にコピーをのこしつつ、その形を変えずに Bob へとものを送らなければならない。) ところが、Wootters と Zurek [21] によると、量子論の世界では完全な量子状態のコピーは不可能である。

まず簡単な版から始めよう。

Proposition 1 $\mathcal{H}$ はヒルベルト空間、ϕ_0 は $\mathcal{H}$ 上のベクトルとする。すると、全てのベクトル ψ について $M(\psi\otimes\phi_0)=\psi\otimes\psi$ をみたすような線形写像 $M:\mathcal{H}\otimes\mathcal{H}\to\mathcal{H}\otimes\mathcal{H}$ は存在しない。

proof 実際、もしそのような写像が存在したとすると、

$$M(2\psi\otimes\phi_0)=2\psi\otimes 2\psi=4\psi\otimes\psi$$

が成り立つ。しかし、写像の線形性により

$$M(2\psi\otimes\phi_0)=2M(\psi\otimes\phi_0)=2\psi\otimes\psi$$

も成り立たなければならない。よって矛盾する。　Q.E.D.

次に完全なコピー不可能定理を証明しよう。

定理 2 今、 $\mathcal{H}$ と $\mathcal{K}$ を各々ヒルベルト空間とする。$\dim\mathcal{H}\geq 2$ とせよ。 M を線形写像 *(コピーマシン)*

$$M:\mathcal{H}\otimes\mathcal{H}\otimes\mathcal{K}\to\mathcal{H}\otimes\mathcal{H}\otimes\mathcal{K}$$

で、以下の性質をもつものとする。

$$M(\psi \otimes \phi_0 \otimes \xi_0) = \psi \otimes \psi \otimes \eta_\psi$$

が任意の $\psi \in \mathcal{H}$ に対して成り立つ。但し、$\psi_0 \in \mathcal{H}$、と $\xi_0 \in \mathcal{K}$ は何かゼロでないあるベクトル、$\eta_\psi \in \mathcal{K}$ は $o\psi$ に依存して構わない。すると、 M は自明な写像 $M = 0$ であることが示される。（すなわち、$\eta_\psi = 0$ が ψ に依らずに成り立つ。）

proof $\{e_i\}$ を $\mathcal{H}$ の正規直交基底としよう。すると、

$$M(e_i \otimes \phi_0 \otimes \xi_0) = e_i \otimes e_i \otimes \eta_i$$

が成り立つ。 但し、η_i は $\mathcal{K}$ 上のベクトルである。今、$\eta_i = 0$ を証明すれば定理は示されたことになる。さて、もし $i \neq j$ であれば $(e_i + e_j)/\sqrt{2}$ は単位ベクトルである。（ここで $\dim \mathcal{H} \geq 2$ を 用いている。）これに対して、等式

$$\frac{1}{\sqrt{2}}(e_i + e_j) \otimes \phi_0 \otimes \xi_0 = \frac{1}{\sqrt{2}} e_i \otimes \phi_0 \otimes \xi_0 + \frac{1}{\sqrt{2}} e_j \otimes \phi_0 \otimes \xi_0$$

が成り立つ。 写像 M をこの両辺に適用すると

$$\frac{1}{\sqrt{2}}(e_i + e_j) \otimes \frac{1}{\sqrt{2}}(e_i + e_j) \otimes \eta_{ij} = \frac{1}{\sqrt{2}} e_i \otimes \frac{1}{\sqrt{2}} e_i \otimes \eta_i + \frac{1}{\sqrt{2}} e_j \otimes \frac{1}{\sqrt{2}} e_j \otimes \eta_j \tag{2.2}$$

を得る。但し、η_{ij} は $\mathcal{K}$ 上のベクトルである。(2.2) は

$$e_i \otimes e_i \otimes (\eta_{ij} - \eta_i) + e_i \otimes e_j \otimes \eta_{ij} + e_j \otimes e_i \otimes \eta_{ij} + e_j \otimes e_j \otimes (\eta_{ij} - \eta_j) = 0$$

と書ける。 今、e_i と e_j が $\mathcal{H}$ の基底の一部であることを考慮にいれると、

$$\eta_{ij} - \eta_i = 0, \quad \eta_{ij} = 0, \quad \eta_{ij} - \eta_j = 0$$

が成り立つ。 よって $\eta_i = 0$ が全ての i について成り立つ。　　Q.E.D.

Remark 3 もし $\dim \mathcal{H} = 1$、すなわち $\mathcal{H} = \mathbf{C}$ であれば、この定理は成り立たない。$\phi_0 = 1$ と $\psi \in \mathbf{C}$ について、$\psi \neq 0$ に対し $M(\psi \xi_0) = \psi \xi_0 = \psi^2 \eta_\psi$ （但し $\eta_\psi = \xi_0/\psi$）とおくことができる。

本節では、Eve は完全な量子状態のコピーを行うことができないということを示した。すなわち、量子状態のコピー不可能性定理は Eve による完全な傍受の可能性を排除するものである。

完全なコピーはできないが、この定理とは矛盾せず、最適なコピーを行うという機械は存在しうる。[13]

2.4 Information-Disturbance 定理–Biham らによる証明の核心–

上記のコピー不可能定理の情報理論版とも言える Information-Disturbance 定理を用いた証明が Biham らにより提出されている。この原型は 2000 年に彼らにより提出されたが、出版されたのはごく最近 2006 年になってからである。ここでは、この骨子を紹介しよう。

ここで、まずプロトコルを正確に書いてみよう。

i) Alice は $b \in \{0,1\}^N$ をランダムに選ぶ。すなわち長さ N のビット列を適当に選択する。また、$i \in \{0,1\}^N$ もランダムに選ぶ。

ii) Alice は $b = b_1 b_2 b_3 \cdots b_N$ と $i = i_1 i_2 \cdots i_N$ を用いて、$b_l = 0$ ならば σ_z の固有状態に i_l をエンコードする。すなわち、σ_z の固有状態で固有値が i_l のほうを用意する。また、$b_l = 1$ ならば σ_x の固有状態を用意する。

iii) Alice は上記のように用意した N 個の量子ビット列を Bob に送る。

iv) Bob は N 個の量子ビット列を受け取ったと報告する。

v) Alice は b を公開する。

vi) Bob は公開された b に従った観測量で（つまり、$b_l = 0$ なら l 番目の量子ビットは σ_z で、$b_l = 1$ なら l 番目の量子ビットは σ_x で）測定する。この測定結果を j_{Bob} と書こう。

vii) Alice は N 個の中からランダムにテスト量子ビットを選択し、どれを選んだかを公開し、またそれらにエンコードした値（i_T と書こう）を公開する。

viii) Bob は対応する測定値 $j_{Bob,T}$ を公開する。もしこの中で誤ったものの割合が一定値を越えていれば Alice と Bob はこの試行を破棄する。

ix) Alice と Bob は秘密にしてある残りのビット列（i_S 及び j_S と書こう）についてあるエラー訂正符号に関するシンドロームを公開することによりお互いに一致した情報を得る。(エラー訂正)

x) Alice と Bob はプライバシー増幅を行い（これもあるエラー訂正符号を用いる)、短い完全秘匿な情報を共有する。これが、鍵となる。

但し、これらのプロトコルのうち、古典的通信路を用いて行われるものは傍受されてもよいが、書き換えられてはならない。Eve は量子通信路、すなわち過程 iii) も傍受できるとする。ここでは Eve は通信内容を書き換えても良い。いや、これから示すことは書き換えることなくしては Eve は有意な情報を得ることができない、ということである。すなわち、Eve が有意な情報を得たかどうかが、vii) 及び viii) の過程で Alice と Bob はチェックすることができるのである。これが以下に述べる情報ー攪乱定理である。

2.4.1 Biham らによる Information-Disturbance 定理

さて、上のプロトコルがうまくいくか否かのポイントは Eve の傍受を Alice と Bob が感知できるか否かというところである。Eve にとっては Alice と Bob にはうまくいっていると見せかけておいて、情報は得ているのが理想的である。ところが、この BB84 ではこのようなことは不可能である。

今、簡単のため上のプロトコルの vii) 以降は無視して vi) までの段階で Eve の得る情報量と、Bob の得る結果の誤りがどう関係するかを見ていく。

Eve の攻撃

まず Eve は過程 iii) において何もしなければ、何も得られないので iii) でこのプロトコルに加わることになる。Eve は何ができるだろうか。Eve は Alice から送られてくる量子系を途中で奪ってはみるものの、そのまま持っているわけにはいかない。受け取った分と同じ数だけ Bob に送らないと Bob は中間に邪魔が入ったことに気がついてしまうからである。そこで、Eve は量子論に従って、一般に以下のようなことをすることになる。Eve は送られてきた N 個の量子系を自分のもつ「測定器」と相互作用させ、でき

るだけ情報を吸い取りつつ、なおかつ元の量子系の状態は壊さないようにして、その元の量子系 N 個を Bob におくる。その後、Alice から公表される基底の情報 b を聞き、その情報を用いて手持ちの「測定器」をなるべくうまく測定して情報を取り出す。無論、量子系が送られてくるたびに一個一個と相互作用させて Bob に送ることもできるが、それは上の攻撃方法に含まれる（個別攻撃と呼ばれる）。また、Alice の基底の情報が公表される前に「測定器」を測定してしまうことも考えられるが、これも上の攻撃に含まれる。そこで、この攻撃方法はもっとも一般的なものと考えられるだろう。（本当はエラー訂正と秘匿性増強の段階を考えなければならないが。）最も理想的な攻撃は、Alice から送られてくる量子状態を Eve はそのままコピーして片方を手元に残し、片方を Bob に送ることであるが、これはコピー不可能性定理により許されない。ではこの Eve にとって「理想的な」状況以外を考えればどうだろうか。もっと、一般的に、あらゆる攻撃にかんして、Eve は Bob の状態を乱さずには情報を吸い出せないということが以下に示される。

具体的に数式を用いて Biham らの行ったことを見ていこう。まず、Alice から Bob に送られる N 個の量子系と、Eve のもつ「測定器」の相互作用は一般に合成系のユニタリー発展で表される（ユニタリーでない発展（CP 写像）を考えることもできるが、それは Eve のもつ空間を拡張することにより、ユニタリー化することができる）。今、基底 b を一つ固定して、その基底に応じた表示をする。つまり、例えば $b = 010\cdots$ なら $|000\cdots\rangle$ は $|\sigma_z = 0\rangle \otimes |\sigma_x = 0\rangle \otimes |\sigma_z = 0\rangle \otimes \cdots$ のことである。さて、一つ b を固定してこの表示に関してユニタリー変換 U は一般に

$$U|0\rangle \otimes |i\rangle = \sum_j |E_{ij}\rangle \otimes |j\rangle$$

とあらわされる。ただし、ここで $|0\rangle$ と $|E_{ij}\rangle$ は「測定器」の状態であり、ユニタリー性のために $\langle E_{ij}|E_{kj}\rangle = \delta_{jk}$ を満たす。

Eve の攻撃の対称化

ところで、ここで、以下の証明のために、今採用している基底に関する対称化された

変換 U^s を導入する。

$$U^s|0\rangle \otimes |i\rangle = \sum_j |E^s_{ij}\rangle \otimes |j\rangle$$

ただし、Eve のもつ「測定器」は N 個の量子ビットを追加され、

$$|E^s_{ij}\rangle := \frac{1}{\sqrt{2^N}} \sum_m (-1)^{m\cdot(i\oplus j)} |m\rangle \otimes |E_{i\oplus m\ j\oplus m}\rangle$$

と書かれる。ここで m は 2^N 個の状態を走る。この対称化された変換は、Eve が U の前後に controlled-not を行ったものであり、物理的に実現可能なユニタリー変換である。さて、今から、元の U ではなく、この対称化された変換 U^s による影響について見ていく。何故それでよいか、についてまず説明しよう。まず、Eve が得る情報量について、であるが Eve は追加された量子ビットを測定することによって、状態 $\sum_j |E_{i\oplus m\ j\oplus m}\rangle\langle E_{i\oplus m\ j\oplus m}|$ と情報 m を得る。これで、元の攻撃方法と同じだけの情報を得たことになる。Eve は追加された量子ビットを測定するのではなく別の戦略も考えられるが、少なくとも元の U による攻撃よりは多くの情報を Eve はこの対称化された攻撃によって得ることができる、ということがわかる。さて、次に Bob の受け取る情報に生じるエラーについてであるが、まず対称化されていない攻撃の場合は、b と i を固定したとき、$P(B=j|A=i,b) = \langle E_{ij}|E_{ij}\rangle$ となり、c だけ誤る確率は、b を固定したとき

$$P(B = A \oplus c|b) = \sum_i P(B = i \oplus c|A = i, b)P(i)$$

となり (ここで $P(i)$ は Alice が i を選ぶ確率)、$P(i) = 1/2^N$ を考慮すると、

$$P(B = A \oplus c|b) = \frac{1}{2^N} \sum_i \langle E_{i\ i\oplus c}|E_{i\ j\oplus c}\rangle$$

となる。さて、対称化された攻撃については同様の量は、

$$P^s(B = A \oplus c|A = i, b) = \frac{1}{2^N} \sum_i \langle E_{i\ i\oplus c}|E_{i\ i\oplus c}\rangle$$

となり、i に依らなくなり、結局

$$P^s(B = A \oplus c|b) = \frac{1}{2^N} \sum_i \langle E_{i\ i\oplus c}|E_{i\ i\oplus c}\rangle = P(B = A \oplus c|b)$$

となる。つまり、Alice から Bob への通信にかかわるエラー確率はまったく同じである。（ここで、全ての入力値 i が等確率で選ばれることは本質的であった。）
さて、この対称化が今固定した b に依るものであることは強調したが、他の基底については対称化されていないのだろうか。これは一般には対称化されてはいない、が特殊な基底については対称化されている。それは b と全く逆の基底、すなわち $b = 01011\cdots$ なら $\bar{b} := 10100\cdots$ である。これを共役な基底と呼ぼう。今、$\bar{b}$ に基づいた基底を $|k^0\rangle$ と書くことにすると、b に対応した表示を用いてそれらは

$$|k^0\rangle = \frac{1}{\sqrt{2^N}}\sum_i (-1)^{i\cdot k}|i\rangle$$

と書かれる。これを用いると、b で対称化された U^s は $\bar{b}$ で対称化された変換と一致することが示される。
われわれの導く定理は「Eve が b に関して得る情報」「Bob が $\bar{b}$ に関して得るエラー」との関係式になる。（言葉のはっきりした定義は後ほどわかるだろう。）実際、同じ b についてであれば、Eve は完全に情報を得ながら Bob は誤りを感知しないこと、はありうる。例えば、

$$U|0\rangle \otimes |i\rangle = |i\otimes\rangle \otimes |i\rangle$$

はそのような変換である。繰り返しになるが、ここで示したいのは、しかし、そのようなアタックにおいては、もし Alice が $\bar{b}$ を選んだのなら Bob はエラーを感知してしまうということである。

Eve の得る状態

さて、Eve が引き出せる情報を考えるためにこの対称化されたアタックにおいて、Eve の手にする状態を考えよう。またしばらく Alice の選ぶ基底 b は固定する。さて、もし Alice が i を送信したとしたら、Eve の得る状態は

$$\rho^i := \sum_j |E^s_{ij}\rangle\langle E^s_{ij}|$$

となる。今、これは一般に混合状態であるが仮想的な N 量子ビット系を考えて合成系

の純粋状態としてあらわそう。

$$|\phi_i\rangle := \sum_j |E^s_{ij}\rangle \otimes |i \oplus j\rangle$$

もちろん、この合成状態から引き出せる情報は元の ρ^i から引き出せる情報より大きい。そこで、ここからどれだけ情報が引き出せるかを以下に考えていこう。今、$|\mu_i\rangle := \frac{1}{2^N}\sum_l (-1)^{i\cdot l}|\phi_l\rangle$ で $|\mu_i\rangle$ を定義すると、これは逆に

$$|\phi_i\rangle = \sum_l (-1)^{i\cdot l}|\mu_l\rangle$$

と解け、

$$\langle\mu_k|\mu_l\rangle = 0 \ (k \neq l) \tag{2.3}$$

が示される。今、$d_l^2 := \langle\mu_l|\mu_l\rangle$ $(d_l > 0)$ とおき、$|\hat{\mu}_l\rangle := \frac{1}{d_l}|\mu_l\rangle$ を導入する。
さて、この d_l^2 には物理的意味があることを次に説明しよう。今、Eve の攻撃は同じとして、この状況下で Alice の選んだ基底が b と共役であった場合の Bob の誤り確率を考えよう。共役な基底に関して対称化を行うことは、もとの基底に関して対称化を行うことと同じであり、計算を進めると

$$P(B = A \oplus c|\bar{b}) = P^s(B = A \oplus c|\bar{b}) = d_c^2$$

となることがわかる。

Eve の得る情報

さて、以上で Bob の受け取るデータの誤り確率を計算したので、次に Eve の得る情報量を計算しよう。求めたいものは、$\sum_b I(A:E|b)P(b)$(但し、$P(b)$ は基底 b が選ばれる確率) である。さて、A は N ビット列なので、$A = A_1A_2\cdots A_N$ と分けて考えられる。すると、古典情報理論の関係式より

$$\begin{aligned} I(A:E|b) &= I(A_1A_2\cdots A_N : E|b) \\ &\leq \sum_{j=1}^{N} I(A_j : E|A_1A_2\cdots A_{j-1}A_{j+1}\cdots A_N) \\ &\leq \sum_{j=1}^{N} max_{i_1\cdots i_N} I(A_j : E|A_1 = i_1\cdots A_{j-1} = i_{j-1}A_{j+1} = i_{j+1}\cdots A_N = i_N) \end{aligned}$$

が成り立つ。さて、今 $I(A_j : E|A_1 = i_1 \cdots A_{j-1} = i_{j-1} A_{j+1} = i_{j+1} \cdots A_N = i_N)$ は何か Eve の測定を決めた後の値であるが、Eve はこれを最も大きくするように選びたい。そこで、以下のシャノンの識別可能性指標を導入する。

$$SD(\rho^{i_1 i_2 \cdots \quad i_j=0 \cdots i_N}, \rho^{i_1 i_2 \cdots i_j=1 \cdots i_N}) = sup_{\text{Eve の測定}} I(A_j : E|A_1 = i_1 \cdots A_N = i_N, b)$$

但し、$\rho^{i_1 i_2 \cdots \quad i_j=0 \cdots i_N}$ は Alice が基底 b を選び、$i_1 \cdots i_j = 0 \cdots i_N$ を送ったときに Eve が手にしている状態である。この一つ一つの j に関して sup で選ばれる Eve の測定は、必ずしも全体の情報量に関しては sup であるとはいえないが、以下の不等式が当然成り立つ。

$$I(A_j : E|A_1 = i_1 \cdots A_{j-1} = i_{j-1} A_{j+1} = i_{j+1} \cdots A_N = i_N) \leq SD(\rho^{i_1 i_2 \cdots \quad i_j=0 \cdots i_N}, \rho^{i_1 i_2 \cdots i_j=1 \cdots i_N})$$

そこで、これからこの識別可能性指標を見積もることになる。

今、$j = 1$ とする。つまり、Bob は Alice の送った $i_2, \cdots i_N$ は知っており、i_1 が 0 か 1 かをうまい測定を行って推定したい。ここで区別すべき量は $\rho^{0 i_2 \cdots i_N}$ と $\rho^{1 i_2 \cdots i_N}$ である。無論、これらよりは、純粋化した状態 $|\phi_{0 i_2 \cdots i_N}\rangle\langle\phi_{0 i_2 \cdots i_N}|$ と $|\phi_{0 i_2 \cdots i_N}\rangle\langle\phi_{0 i_2 \cdots i_N}|$ のほうが区別しやすい。そこで、これら二つの状態があったときに、うまい測定をおこなってこれらを区別するということを考える。今、$i_F := 0 i_2 \cdots \quad i_N$、$\mathcal{C} := \{00 \cdots 0, 10 \cdots 0\}$ と $\mathcal{D} := \{0 j_2 \cdots j_N\}_{j_2 \cdots j_N}$ とおき、$m \in \mathcal{C}$ について

$$|\mu'_m\rangle := \sum_{j \in \mathcal{D}} (-1)^{i_F \cdot n} |\mu_{m \oplus n}\rangle$$

とおくと、

$$|\phi_{i_1 i_2 \cdots i_N}\rangle = |\mu'_0\rangle + (-1)^{i_0} |\mu'_1\rangle$$

が成り立つ。これらは内積、

$$\langle\mu'_m|\mu'_n\rangle = \delta_{mn} (d'_m)^2$$

を満たす。但し、

$$(d'_m)^2 := \sum_{n \in \mathcal{D}} d^2_{m \oplus n}$$

である。ここで、シャノンの識別可能性指標に関する定理

$$SD(\rho, \sigma) \leq \frac{1}{2} tr\left(|\rho - \sigma|\right)$$

を用いると、長い計算により、

$$SD(|\phi_{i_1=0 i_2 \cdots i_N}\rangle\langle\phi_{i_1=0 i_2 \cdots i_N}|, |\phi_{i_1=1 i_2 \cdots i_N}\rangle\langle\phi_{i_1=1 i_2 \cdots i_N}|) \leq 2 d'_0 d'_1$$

が得られる。詳細は論文を見よ。これは任意の α について

$$\begin{aligned} 2d'_0 d'_1 &= \frac{2}{\alpha} \alpha d'_0 d'_1 \\ &\leq \alpha (d'_0)^2 + \frac{1}{\alpha} (d'_1)^2 \\ &\leq \alpha + \frac{1}{\alpha} \sum_{|c| \geq 1} d_c^2 \end{aligned}$$

となる。

情報攪乱定理

さて、上の式に現れる d_c^2 には物理的な意味があった。そこで、

$$SD(|\phi_{i_1=0 i_2 \cdots i_N}\rangle\langle\phi_{i_1=0 i_2 \cdots i_N}|, |\phi_{i_1=1 i_2 \cdots i_N}\rangle\langle\phi_{i_1=1 i_2 \cdots i_N}|) \leq \alpha + \frac{1}{\alpha} \sum_{|c| \geq 1} P(B = A \oplus c | \bar{b})$$

となる。今、$j = 2, \cdots N$ とあわせると、

$$I(A : E|b) \leq N \left(\alpha + \frac{1}{\alpha} \sum_{|c| \geq 1} P(B = A \oplus c | \bar{b}) \right) \tag{2.4}$$

を得る。α として $\sqrt{\sum_{|c| \geq 1} P(B = A \oplus c | \bar{b})}$ を選ぶと、これは

$$I(A : E|b) \leq 2N \sqrt{\sum_{|c| \geq 1} P(B = A \oplus c | \bar{b})}$$

を導く。この式の意味は b の基底に関する試行で情報を得られるような Eve の攻撃は、Alice が $\bar{b}$ を選んだならば Bob の状態は不可避的に乱す、ということである。これは不

確定性原理の情報理論的表現ともいえるだろう。さて、式 (2.4) に戻って、これを b について平均をとると、

$$\sum_b I(A:E|b)P(b) \leq N\left(\alpha + \frac{1}{\alpha}\sum_{|c|\geq 1} P(B=A\oplus c)\right)$$

を得る。ここで、$P(Error) := \sum_{|c|\geq 1} P(B=A\oplus c)$ とおいて、$\alpha := \sqrt{P(Error)}$ とおくと、

$$\sum_b I(A:E|b)P(b) \leq 2N\sqrt{P(Error)}$$

を得る。これが情報ー撹乱定理である。これは、Eve が有意な情報を得たとすれば、Bob の得る状態は必ず乱れてしまうということを意味している。

以下にこれを一般化した定理を紹介する。これは量子論の基本原理である不確定性関係から直接導かれるという点で興味深い。まず不確定性関係について概説する。

2.5 不確定性関係

不確定性関係とは、量子論の性質を最もよくあらわす重要な関係式である。その代表的なものは以下の Robertson 型の不確定性関係と呼ばれるものである。

Robertson 型不確定性関係 [4] 二つの観測量 A と B を考える。ある状態 $\langle\cdot\rangle$ を一つ固定したときに、その状態に関する A の観測結果の分散を ΔA、B の観測結果を ΔB と書く。すると、以下が成り立つ。

$$\Delta A \Delta B \geq \frac{1}{2} \left| \langle [A, B] \rangle \right| .$$

不確定性関係には、上記の広く知られた Robertson 型のもの以外にもいくつかの形が存在している。これらはひとくくりにすると、二つ（以上）の観測量 A, B を考えたときに、ある状態について **「A と B の観測結果の確率分布の相容れなさ」** と **「A と B の非可換性」** を結びつけるものであるといえる。具体的には以下の二つのものが本論文に関係するものである。

エントロピー型 [30] 二つの観測量 A と B を考える。ある状態 $\langle\cdot\rangle$ を一つ固定したときに、その状態における A の観測結果の確率分布についての Shannon エントロピーを $H(A)$、B については $H(B)$ と書くと、以下が成立する。

$$H(A) + H(B) \geq -2 \log \left(\max_{a,b} \| E_a P_b \| \right) ,$$

但し、$A = \sum_a a E_a$、$B = \sum_b b P_b$ をそれぞれの観測量のスペクトル分解とする。

確率型 [34] N-qubit 系とこの上の任意の状態を考える。今、各 qubit について z 軸に沿った観測を行ったときに得られる測定値の（$\{0,1\}^N$ 上の）確率分布を $Q^{+}(\cdot)$、x 軸に沿った観測を行ったときに得られる測定値の確率分布を $Q^{\times}(\cdot)$ と書く。すると、任意の $L^{+} \subset \{0,1\}^N$、$L^{\times} \subset \{0,1\}^N$ について、

$$Q^{+}(L^{+}) + Q^{\times}(L^{\times}) \leq \left(1 + \sqrt{2^{-N} |L^{+}| |L^{\times}|} \right)^2$$

が成り立つ。

2.5.1　一般化された Information-Disturbance 定理

本節においては、BB84 量子鍵分配プロトコルにおける Information-Disturbance 定理の一般化をエントロピー型不確定性関係を用いて導く。まず、状況設定について述べる。これは、BB84 プロトコルから誤り訂正と秘匿性増強のプロセスを除いた簡略版と考えられるが、以下の解析は完全な BB84 プロトコルにも適用可能である。登場人物は Alice と Bob と Eve の三者である。Alice と Bob は秘密鍵（乱数）を共有するために以下の手続きを行う。1 つの量子ビット $\mathbf{C}^2$ において、基底 $b := \{|0\rangle, |1\rangle\}$ とその「共役な」基底 $\bar{b} := \{|\bar{0}\rangle, |\bar{1}\rangle\}$ を導入する。これらは理想的な場合には、mutually unbiased な関係を満たしているが、今、その必要はない。Alice はまず、乱数をエンコードするために基底のうちのどちらか、b あるいは $\bar{b}$、を選択する。次に、Alice は N ビットの乱数 $i \in \{0,1\}^N$ を等確率 $p(i) = \frac{1}{2^N}$ で生成する。この N ビットの乱数を表す確率変数を A とおこう。Alice はこの情報を、先に選んだ基底を用いた状態にエンコードして Bob に送る。たとえば今、Alice が基底 b を選び、数列 $i = i_1 i_2 \cdots i_N$ を生成した場合を考える。すると、彼女は対応した状態 $|i\rangle = |i_1\rangle \otimes |i_2 \otimes \cdots \otimes |i_N\rangle \in \mathbf{C}^2 \otimes \cdots \otimes \mathbf{C}^2 =: \mathcal{H}_A \simeq \mathcal{H}_B$ を Bob に送る。また、もし共役な基底 $\bar{b}$ と数列 $i = i_1 i_2 \cdots i_N$ を Alice が選んだ際には、$|\bar{i}\rangle = |\overline{i_1}\rangle \otimes |\overline{i_2}\rangle \otimes \cdots \otimes |\overline{i_N}\rangle \in \mathcal{H}_A$ を Bob に送ることになる。Alice は、Bob が実際に N 個の量子ビットを受け取ったということを確認した後、どちらの基底を用いたか、を古典通信路で知らせる。（この情報は盗聴されても良いが、改変されてはならない。）この基底に沿った測定を Bob は受け取った量子ビットについて行い、結果を得る。この測定結果を表す確率変数を B と書こう。もし盗聴者が誰もいなければ、Alice の送ったデータそのものを Bob は受け取ることになる。すなわち、$A = B$ である。盗聴者 Eve は確率変数 A の情報を得ることを目的として、Alice から Bob に送られてくる長さ N の量子ビットを途中で手に入れて、手持ちに準備した系（測定器）と相互作用させて何とか情報を吸い出そうと試みる。無論、その後 Eve は Bob へと N 個の量子ビットを送らなければならない。Eve の用意する測定器をあらわす Hilbert 空間を $\mathcal{H}_E$ と書くと、

一般に Eve の操作は合成系のユニタリー発展 U で書き表される：

$$
\begin{aligned}
U : \mathcal{H}_E \otimes \mathcal{H}_A &\to \mathcal{H}_E \otimes \mathcal{H}_B \\
|0\rangle \otimes |i\rangle &\mapsto \sum_j |E_{ij}\rangle \otimes |j\rangle,
\end{aligned} \tag{2.5}
$$

但し、$|0\rangle$ は測定器における正規化された状態ベクトルであり、$\{|E_{ij}\rangle\} \subset \mathcal{H}_E$ はユニタリー性を保証するための条件 $\sum_{j\in\{0,1\}^N} \langle E_{ij}|E_{kj}\rangle = \delta_{ik}$ を満たすベクトルの族である。Eve はその後 Alice から Bob に伝えられる基底の情報を聞いた後で、手持ちの測定器を工夫して測定し、古典情報を得ることになる。ここで興味があるのは、ここで、Eve がどれだけ A の情報を得ることができるか、である。この量を $I(A:E|b)$ と書こう。すると、以下が成り立つ。

定理 4 以下の不等式が成り立つ。

$$
I(A:E|b) - N\log(2p) \le H(A \oplus B|\bar{b}), \tag{2.6}
$$

但し、p は基底 b と $\bar{b}$ の *biasedness* をあらわす量であり、

$$
p := \max_{i,j=0,1} |\langle i|\bar{j}\rangle|^2
$$

で定義され、これは $\frac{1}{2} \le p \le 1$ の範囲をとる。($p = \frac{1}{2}$ のときが *unbiased* な場合である。) また、$H(\cdot)$ は *Shannon* エントロピーを表す。すなわち、*Eve* の操作が、*Alice* が基底 b を選んだときに大きな情報を得るものであれば、その操作は *Alice* が共役な基底 $\bar{b}$ を選んだときに *Bob* の得る結果を不可避的にランダムにするものである。

Proof: この証明には、BB84 プロトコルと E91 プロトコルの同等性を用いる。すなわち、上記のプロトコルは Alice が EPR 対を生成し、そのうち片方を Bob に送り、後で Alice と Bob が対応した測定を行うというプロトコルと同等である。Alice と Bob と Eve の三者間における以下の状態 $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_E \otimes \mathcal{H}_B$ を取り扱う。

$$
|\Psi\rangle = \sqrt{\frac{1}{2^N}} \sum_i |i\rangle \otimes U\left(|0\rangle \otimes |i\rangle\right)
$$

但し、ここで基底 b に対応する Alice と Bob の測定は観測量 $A := \sum_i i|i\rangle\langle i|$ と $B := \sum_j j|j\rangle\langle j|$ とあらわされ、基底 $\bar{b}$ に対応する Alice と Bob の測定は $\underline{A} := \sum_i i|\underline{i}\rangle\langle\underline{i}|$ と $\overline{B} := \sum_j j|\overline{j}\rangle\langle\overline{j}|$ とあらわされる。ここで正規直交基底 $\{|\underline{i}\rangle\}$ は $|\underline{i}\rangle := \sum_j |j\rangle\langle\overline{i}|j\rangle$ で定義されるものである。

今、Eve は適当な POVM$\{E_\alpha\}$ を行ったものとし、何か値 α を得たとしよう。このときの Alice と Bob の a-posteriori 状態を ρ_α と書くことにする。ここで、この状態についてエントロピー型不確定性関係を適用する。考える観測量は $\underline{A} \oplus \overline{B} = \sum_l lE_l$ と $A \otimes \mathbf{1} = \sum_j jP_j$ である。すると、以下が成り立つ。

$$H(\underline{A} \oplus \overline{B}|\rho_\alpha) + H(A|\rho_\alpha) \geq -2\log\left(\max_{l,j} \|E_l P_j\|\right) \tag{2.7}$$

そこで、$\|E_k P_j\|$ を見積もることになる。今、

$$\underline{A} \oplus \overline{B} = \sum_{l,i} l|\underline{i}\rangle\langle\underline{i}| \otimes |\overline{i \oplus l}\rangle\langle\overline{i \oplus l}|$$

より、$E_l = \sum_i |\underline{i}\rangle\langle\underline{i}| \otimes |\overline{i \oplus l}\rangle\langle\overline{i \oplus l}|$ となる。よって、

$$E_l P_j = \sum_i |\underline{i}\rangle\langle\underline{i}|j\rangle\langle j| \otimes |\overline{i \oplus l}\rangle\langle\overline{i \oplus l}|$$

となる。このノルムを求めるために、正規化されたベクトル $|\Phi\rangle := \sum_{ku} \alpha_{ku}|k\rangle \otimes |\overline{u}\rangle$ を導入すると、

$$E_l P_j|\Phi\rangle = \sum_i \alpha_{ji\oplus l}|\underline{i}\rangle \otimes |\overline{i \oplus l}\rangle\langle\underline{i}|j\rangle$$

となり、

$$\begin{aligned}
\|E_l P_j|\Phi\rangle\|^2 &= \sum_i |\alpha_{ji\oplus l}|^2 |\langle\underline{i}|j\rangle|^2 \\
&\leq \max_i |\langle\underline{i}|j\rangle|^2 \sum_i |\alpha_{ji\oplus l}|^2 \\
&\leq \max_i |\langle\underline{i}|j\rangle|^2
\end{aligned}$$

となる。ここで $|\langle\underline{i}|j\rangle| = |\langle\overline{i}|j\rangle|$ を用いると、結局、

$$\max_{lj} \|E_l P_j\| \leq p^{N/2}$$

となる。これを式 (2.7) に適用すると、

$$H(\underline{A} \oplus \overline{B}|\rho_\alpha) + H(A|\rho_\alpha) \geq -N \log p$$

を得る。ここで、Eve が結果 α を得る確率 $p(\alpha)$ をかけて全ての α について足し合わせ、両辺に N を加えて整理すると、

$$I(A:E) - N \log(2p) \leq H(\underline{A} \oplus \overline{B})$$

を得る。これを Eve の測定について sup をとり、BB84 における元の変数で書くと

$$I(A:E|b) - N \log(2p) \leq H(A \oplus B|\bar{b})$$

となる。 **Q.E.D.**

2004 年に、Boykin と Roychowdhury はこの Information-Disturbance 定理の、純粋化とトレースノルム不等式の方法を用いた簡単な証明方法 [26] を発表したが、彼らの定理は Eve の得る情報量と、共役な基底（unbiased な場合に限られる）を用いたときにおける Bob の結果に含まれる誤り確率との関係式であった。[27] において、彼らの証明方法と類似の方法を用いることにより、彼らの結果を改良した定理が報告されている。この定理によれば、Eve の情報搾取は Bob の得る結果に誤りをもたらすだけではなく、結果を**ランダムにする**ということがわかる。

2.6 秘匿性増強

情報理論的安全性をもつ古典暗号系では秘匿性増強プロトコルは、盗聴者の鍵に対する部分的な情報を無効にする過程としてよく知られている。そこでは、簡単な情報理論的考察により、Renyi エントロピーで決まる鍵生成の限界が求められている。しかしながら、量子論においてはこの限界式を直接用いることはできない。なぜならば、盗聴者は秘匿性増強プロトコルが行われている間にも、量子メモリに量子状態を蓄えておき、正規ユーザ間の（公開された）通信が終了後にそこで聞いた情報を元に最適な測定をメモリに対して行うことができるからである。ところが、ごく最近、量子暗号系においても古典論におけるものと類似した限界式が存在することがわかった。以下、これを説明する。

2.6.1 古典論における秘匿性増強

まず古典論における秘匿性増強プロトコルについて簡単に説明する。ここで取り扱うのは Alice からの通信のみ行われるもっとも簡単な一方向プロトコルである。

Alice、Bob はエラー訂正を終えており一致した情報を得ている。この確率変数を X と書く。これは $\mathcal{X}$ に値を持つ。盗聴者の得ている情報をあらわす確率変数を Z と書こう。これは $\mathcal{Z}$ にあたいを持つ。これは X とは一般に相関をもち、$I(X:Z)\neq 0$ である。（但し、$I(X:Z)$ は X と Z の間の相互情報量。）目標は、何か関数 f で $f(X)$ に対してはEve の情報は全く役に立たない、というようなものを構成しようということである。ここで、重要になるのが two-universal Hash function と呼ばれる概念である。

Definition 5 二つの（可算）集合 $\mathcal{X}$ と $\mathcal{Y}$ を考える。今、$\mathcal{F}\subset\{f:\mathcal{X}\to\mathcal{Y}\}$（$\mathcal{X}$ から $\mathcal{Y}$ への写像の族）が *two-universal Hash function* の族であるとは、任意の $x_1,x_2\in\mathcal{X}$ について、$x_1\neq x_2$ であれば、以下が成り立つことである。

$$\frac{|\{f\in\mathcal{F}|\ f(x_1)=f(x_2)\}|}{|\mathcal{F}|}\leq\frac{1}{|\mathcal{Y}|}$$

また、$f\in\mathcal{F}$ を *Hash function* と呼ぶ。

このような Hash function の簡単な例は $\mathcal{X}$ から $\mathcal{Y}$ の写像全体であるが、暗号通信に使われるためにはもっと効率的なものでなければならない。（すなわち、Hash function の指定に情報量がなるべく少なくすむもの（セキュリティパラメータの範囲）でなければならない。）そのようなものも、Wegman と Carter [1] などによって構成されている。（集合の分割と簡単な Hash function の繰り返しによってシステマティックに構成される。）Alice と Bob、Eve は一つ Hash function の族を事前に共有している。エラー訂正後、Alice は Hash function を一つランダムに選び公開する。この Hash function による写像の値が Eve にとって全く不可知であることが目標である。すなわち、

$$I(F(X)|F, Z = z) \text{ は指数的に小さい}$$

となっていれば良い。以下が成り立つ。

定理 6 $\mathcal{Y} := \{0, 1\}^r$ とする。

$$I(F(G) : Z|F) \leq \frac{2^{-R(X|Z)+r}}{\log 2}$$

但し、R は *Renyi* エントロピーと呼ばれる量であり、

$$R(X) : -\log \sum_x P_X(x)^2$$

で定義される。

証明はきわめて簡単であり、Renyi エントロピーと Shannon エントロピー間の不等式、$R(X) \leq H(X)$ と凸関数に対する Jensen の不等式が用いられる。

2.6.2　量子論における秘匿性増強

　次に量子論における秘匿性増強について説明を行う。先に説明したように、古典論と異なりあらかじめ Eve のもつ確率変数 Z を設定することはできない。（すなわち量子メモリに状態を保存しておいて「後だし測定」が可能である。）ここではこの量子メモリがどれほど強力なのか、について考える。

問題設定は以下のとおりである。今、$\mathcal{X} := \{0,1\}^N$ とし、X はそこに値を持つ確率変数、その分布は $P_X(x)$ とする。この確率変数が量子状態 $\{\rho_x\}_{x\in\mathcal{X}}$ にエンコードされているとしよう。すなわち、$X = x$ となる確率は $P_X(x)$ であり、そのとき状態 ρ_x が準備される。今、この量子系は q 量子ビット系であるとする。さて、Hash function $f : \{0,1\}^N \to \{0,1\}^M$ を一つ公開したときに、この量子系をもっている者（Eve) は $f(X)$ についてどの程度推測可能であろうか。この問題は R.Konig,U.Maurer, R.Renner によってはじめに考えられた [2]。以下ではまず彼らの手法を紹介する。今、単純に $M = 1$ としよう。すなわち、Eve は量子メモリをもとに、$f(X) = 0$ か $f(X) = 1$ を推測することになる。今、f を一つ固定すると、識別すべき状態は

$$
\begin{aligned}
\rho_0(f) &:= \frac{\sum_x^{f(x)=0} P_X(x)\rho_x}{\sum_x^{f(x)=0} P_X(x)} \\
\rho_1(f) &:= \frac{\sum_x^{f(x)=1} P_X(x)\rho_x}{\sum_x^{f(x)=1} P_X(x)}
\end{aligned}
$$

である。これらはそれぞれ、確率 $P_0(f) := \sum_x^{f(x)=0} P_X(x)$ と $P_1(f) := \sum_x^{f(x)=1} P_X(x)$ で渡されている。これらを区別する最小エラー推定問題は 1970 年代に Helstrom [3] により Lagrange 未定乗数法を用いて解かれており、また 90 年代に Fuchs [24] により簡単な解法も得られている。今、$P(Guess|f)$ を正しい推定確率とすると、その最大値は

$$
P(Guess|f) = \frac{1}{2} + \frac{1}{2}\mathrm{tr}(|\Lambda_f|)
$$

で与えられる。但し、Λ_f は Hash function f にたいして、

$$
\Lambda_f := P_0(f)\rho_0(f) - P_1(f)\rho_1(f)
$$

で定義されており、$|\Lambda_f| := (\Lambda_f^*\Lambda_f)^{1/2}$ で定義されている。今、Hilbert-Schmidt 内積に対する Cauchy-Schwarz の不等式により、$\mathrm{tr}(|\Lambda_f|) = \mathrm{tr}(\mathbf{1}|\Lambda_f|) \le 2^{q/2}\mathrm{tr}(\Lambda_f^2)^{1/2}$ が導かれる。そこで、

$$
P(Guess|f) \le \frac{1}{2} + 2^{q/2-1}\mathrm{tr}(\Lambda_f^2)^{1/2}
$$

を Hash function$f$ について平均化したものを上から押さえていけばよい。

$$
\begin{aligned}
P(Guess) &:= \sum_f P(Guess|f)P(f) \\
&\leq \frac{1}{2} + 2^{q/2-1} \sum_f P(f)\mathrm{tr}(\Lambda_f^2)^{1/2}
\end{aligned}
$$

Jensen の不等式を用いると、

$$
\begin{aligned}
P(Guess) &\leq \frac{1}{2} + 2^{q/2-1}\mathrm{tr}(\sum_f P(f)\Lambda_f^2)^{1/2} \\
&= \frac{1}{2} + 2^{q/2-1}(\sum_{x,x'} \lambda_{x,x'} P_X(x)P_X(x')\mathrm{tr}(\rho_x \rho'_x))^{1/2}
\end{aligned}
$$

となる。但し、$\lambda_{x,x'} := 2Prob(f(x) = f(x')) - 1$ である。これは two-universal Hash function の定義により、$x \neq x'$ に対しては $\lambda_{x,x'} \leq 0$ である。そこで、以下が成り立つ。

$$
\begin{aligned}
P(Guess) &\leq \frac{1}{2} + 2^{q/2-1}\sqrt{\sum_x P_X(x)^2} \\
&= \frac{1}{2} + 2^{-\frac{R(X)-q}{2}+1}
\end{aligned}
$$

但し、$R(X) := -\log \sum_x P_X(x)^2$ は Renyi エントロピーである。

すなわち、$R(X) \gg q$ であれば、$P(Guess) \simeq \frac{1}{2}$ となり、Eve は $f(X)$ の値を推測することができないことになる。

次に $\mathcal{Y}$ が M ビットである場合を考えよう。これは、Hashing Lemma と呼ばれる Vazirani の XOR Lemma と似た方法を用いて上記の 1 ビットの場合を経由して示されるが、ここではゆるい条件ではあるが別の方法を用いて考えてみよう。まず、推定問題について Helstrom の公式に対応する簡単な公式は 1 ビット以外の場合には存在しない。(形式的な必要十分条件は Helstrom 自身と Holevo により得られている。また、誤り確率を最小にするという条件とは異なる条件においての推定問題も現在も活発に議論されている。) さて、Eve は Hash function f が公開された後で、それに対応して何か最適な POVM (Positive Operator Valued Measure) を用いて $f(X)$ の値を推測しよう

とする。今、この POVM を $E(f) := \{E(f)_a\}_{a\in\mathcal{Y}}$ と書こう。すると、推定正解確率は

$$P(Guess) = \sum_f P(f)P(Guess|f) = \sum_f P(f)\sum_a P_a(f)\mathrm{tr}(\rho_a(f)E_a(f))$$

とかける。今、この値を $\frac{1}{2^M}$ と比較したいので、$P_a(f)\rho_a(f) = \left(P_a(f)\rho_a(f) - \frac{\mathbf{1}}{2^q 2^M}\right) + \frac{\mathbf{1}}{2^q 2^M}$ と分解する。すると、

$$P(Guess|f) = \frac{1}{2^M} + \sum_a \mathrm{tr}\left(\left(P_a(f)\rho_a(f) - \frac{\mathbf{1}}{2^M 2^q}\right)E_a(f)\right)$$

がなりたつ。ここで、Hilbert-Scmidt 内積に対する Cauchy-Schwarz の不等式を用いると、

$$P(Guess|f) \le \frac{1}{2^M} + \sum_a \mathrm{tr}\left(\left(P_a(f)\rho_a(f) - \frac{\mathbf{1}}{2^M 2^q}\right)^2\right)^{1/2}\mathrm{tr}(E_a(f)^2)^{1/2}$$

となる。また、a に対する和について普通の Euclid 内積についての Cauchy-Schwarz の不等式を適用すると、

$$P(Guess|f) \le \frac{1}{2^M} + \left(\sum_a \mathrm{tr}\left(P_a(f)\rho_a(f) - \frac{\mathbf{1}}{2^M 2^q}\right)^2\right)^{1/2}\left(\sum_b \mathrm{tr}(E_b(f)^2)\right)^{1/2}$$

ここで、$E_b(f)^2 \le E_b(f)$ と $\sum_b E_b(f) = \mathbf{1}$ を用いると、

$$\begin{aligned} P(Guess|f) &\le \frac{1}{2^M} + 2^{q/2}\left(\mathrm{tr}\sum_a \left(P_a(f)\rho_a(f) - \frac{\mathbf{1}}{2^M 2^q}\right)^2\right)^{1/2} \\ &= \frac{1}{2^M} + 2^{q/2}\left(\mathrm{tr}\left(\sum_a P_a(f)^2\rho_a(f)^2\right) - \frac{\mathbf{1}}{2^M}\right)^{1/2} \end{aligned}$$

となる。今、f について平均をとり、Jensen の不等式を用いると、

$$\begin{aligned} P(Guess) &\le \frac{1}{2^M} + 2^{q/2}\left(\mathrm{tr}\left(\sum_f P(f)\sum_a P_a(f)^2\rho_a(f)^2\right) - \frac{\mathbf{1}}{2^M}\right)^{1/2} \\ &= \frac{1}{2^M} + 2^{q/2}\left(\sum_{x,x'} \nu_{x,x'}P_X(x)P_X(x')\mathrm{tr}(\rho_x\rho'_x)\right) \end{aligned}$$

となる。但し、$\nu_{x,x'} := Prob(f(x) = f(x')) - \frac{1}{2^M}$ である。これは、$x \neq x'$ については、two-universal Hash function の定義により $\nu_{x,x'} \leq 0$ となるので、結局、

$$P(Guess) \leq \frac{1}{2^M} + 2^{-\frac{R(X)-q}{2}}$$

となる。すなわち、$R(X) \gg q$ であれば、Eve の推測はやはり成功しない。

さて、以下に、この議論の応用例として有限メモリ下での量子紛失通信の説明を行う。

2.6.3 有限量子メモリ下での Rabin Oblivious Transfer

前節の量子論における秘匿性増強の議論の応用として Fehr,///らによる紛失通信の研究を紹介する。量子論を用いても紛失通信やビットコミットメントを無条件安全には行えないことが示されている。しかしながら、ノイズのある通信路を仮定したり、なんらかの仮定をすれば安全性が保証される場合がある。ここでは、不正なユーザの量子メモリが制限されているとき、やはり安全性が保証されることを示す。なお、古典のメモリが制限されているときにも安全な紛失通信は行えるが、量子メモリを制限するほうが、実際のテクノロジーを鑑みるとより自然な仮定であるといえよう。前に示した確率型不確定性関係 [34] は特殊な状況設定（N-qubit 系であること、x と z という unbiased な観測量に適用範囲がとどまっていたこと）によっていた。ここではまず、彼らの関係式を一般化した定理を導く。

定理 7 任意の量子系およびその上の状態と、二つの $POVM$ $\{A_i\}$ と $\{B_j\}$ を考える。すると、任意の i, j について

$$\langle A_i \rangle + \langle B_j \rangle \leq \ 1 + \langle \{A_i, B_j\} \rangle$$

が成り立つ。

この定理は Massen と Uffink によって導かれた Landau-Pollak 型の不確定性関係を Naimark extension により一般化することによって証明される。この定理が実際にこれまでの確率型不確定性関係の一般化になっていることは、以下の定理を導くことからわかる。

定理 8 N-*qubit* 系とこの上の任意の状態を考える。今、各 *qubit* について z 軸に沿った観測（対応する基底は $\{|i\rangle\}$）を行ったときに得られる測定値の（$\{0,1\}^N$ 上の）確率分布を $Q^+(\cdot)$、ある別の軸に沿った観測（対応する基底を $\{|\bar{i}\rangle\}$ と書く）を行ったときに得られる測定値の確率分布を $Q^\times(\cdot)$ と書く。すると、$L^+ \subset \{0,1\}^N$、$L^\times \subset \{0,1\}^N$ について、

$$Q^+(L^+) + Q^\times(L^\times) \leq \left(1 + \sqrt{p^N |L^+||L^\times|}\right)^2$$

が成り立つ。但し、ここで

$$p := \max_{i,j=0,1} |\langle i|\bar{j}\rangle|^2$$

は *biasedness* をあらわす量であり、1/2 から 1 までの値をとる。($p = 1/2$ の場合が元の定理に対応している。)

二者間プロトコルの primitive である Oblilvious Trasfer は、量子論を用いても無条件には実現できないことが知られている [17]。I.Damgaard, S.Fehr, L.Salvail, C.Schaffner は [34] において、量子メモリが限定されていれば、という条件付でそれが可能であることを示した。彼らの結果は N 個の qubit を用いる場合、不正な Receiver が $N/2$ 以下の qubit しか長時間保存することができなければ、N が大きい場合に安全な Oblivious Transfer ができるといったものである。彼らのプロトコルにおいては、unbiased な状態を用いることを仮定しているが、我々は biased な状態を用いる場合についてそれを拡張する。以下で具体的に扱うのは Rabin Oblivious Transfer と呼ばれるプロトコルである。これは erasure channel を実現するプロトコルであり、以下の二つの要件を満たさなければならない（正確な表現については [34] 参照)。

privacy 条件 Sender は何をどうやっても、自分の選んだ数 $c \in \{0,1\}$ が Receiver に伝わったのかどうかはわからない。

obliviousness 条件 Receiver が何をどうやっても、少なくとも確率 1/2 で、Receiver には Sender が何を送ったのかわからないような状況となっている。

まず、状況設定について述べる。これは、先の BB84 プロトコルの簡略版と似ているが、今回の登場人物は Sender と Receiver の二者である。Honest な Sender と Receiver は以下のプロトコルに従う。1 つの量子ビット $\mathbf{C}^2$ において、基底 $b := \{|0\rangle, |1\rangle\}$ とその「共役な」基底 $\bar{b} := \{|\bar{0}\rangle, |\bar{1}\rangle\}$ を導入する。これらは理想的な場合には、mutually unbiased な関係を満たしているが、今、その必要はない。Sender は乱数 $i \in \{0,1\}^N$ を等確率 $p(i) = \frac{1}{2^N}$ で選び、それをエンコードするために基底 b もしくは $\bar{b}$、を選び、対応する状態を準備し Receiver に送る。たとえば今、Sender が基底 b を選び、数列 $i = i_1 i_2 \cdots i_N$ を生成した場合を考える。すると、彼女は対応した状態 $|i\rangle = |i_1\rangle \otimes |i_2 \otimes \cdots \otimes |i_N\rangle \in \mathbf{C}^2 \otimes \cdots \otimes \mathbf{C}^2 =: \mathcal{H}_A \simeq \mathcal{H}_B$ を 1-qubit ずつ Receiver に送る。また、もし共役な基底 $\bar{b}$ と数列 $i = i_1 i_2 \cdots i_N$ を Sender が選んだ際には、$|\bar{i}\rangle = |\overline{i_1}\rangle \otimes |\overline{i_2}\rangle \otimes \cdots \otimes |\overline{i_N}\rangle \in \mathcal{H}_A$ を 1-qubit ずつ Receiver に送ることになる。Honest な Receiver は基底 b か $\bar{b}$ のどちらかを選択する。彼は量子メモリを持っている必要はなく、qubit が送られてくるそばから、その決めた基底に沿って観測を行う。Sender は、送りたい数 $c \in \{0,1\}$ 及び、ハッシュ関数 f を一つ選び、Receiver が実際に N 個の量子ビットを受け取ったということを確認した後、どちらの基底を用いたか、と $c \oplus f(i)$ を古典通信路で知らせる。Receiver は、もし自分の選んだ基底と Sender の選んだ基底が一致していれば、自分の得たデータにハッシュ関数を作用させ、送られてきた $c \oplus f(i)$ と足すことにより c を計算して得る。もし基底が一致してなければこの結果は "erase" であり、実際 Receiver は Sender がどちらの値を選んだのかは全くわからない。

このプロトコルは non-interactive であるため privacy 条件を満たすことをみるのはたやすい。しかしながら、仮に不正な Receiver が N-qubit の量子メモリを持っていたとすると、obliviousness 条件は明らかに満たされない。実際、Receiver は Sender が自分の選んだ基底を知らせてくれるのを待ってから送られてきた N-qubit を測定すれば、常に c の値を知ることができる。量子メモリの大きさが限られている場合にはどうなるか、は全く自明ではないが、I.Damgaard, S.Fehr, L.Salvail, C.Schaffner は以下の定理を示した。

定理 9 *[34] Sender* の用いる基底 b と $\bar{b}$ が *unbiased* な場合、任意の $\epsilon > 0$ について、不

正な *Receiver* の量子メモリが $\left(\frac{1}{2}-\epsilon\right)N$ 以下であれば上のプロトコルは *Rabin Oblivious Transfer* の安全性条件を（N が大きい場合、漸近的に）満たしている。

彼らのこの定理の証明において key となるのは、確率型不確定性関係である。一般化された確率型不確定性関係を用い、彼らの結果を biased な基底の組へと拡張することができる。

定理 10 *Sender* の用いる基底 b と $\bar{b}$ の *biasedness* を p とする。すなわち、

$$p := \max_{i,j=0,1} |\langle i|\bar{j}\rangle|^2$$

とおく。すると、任意の $\epsilon > 0$ について、不正な *Receiver* の量子メモリが $\left(-\frac{\log p}{2}-\epsilon\right)N$ 以下であれば上のプロトコルは *Rabin Oblivious Transfer* の安全性条件を（N が大きい場合、漸近的に）満たしている。

2.6.4 安全性証明

秘匿性増強をここまで考えてきたが、残る部分はこれを鍵分配プロトコルのそれまでの部分とうまくつなげることである。Christandle らは [35]、エラー率を見極めることにより ρ のランクが十分よく推定できることを示した。すなわち、エラー率が十分小さければ、Eve にわたっている状態のランクは十分小さい。その後、エラー訂正を行い、上記の秘匿性増強を行う。エラー訂正はやはり Hash 関数を用いた古典論において良く知られたプロトコルを行えばよい。また、このエラー訂正をあらかじめ共有された秘密鍵によって暗号化して行うという方法も提案されている。無論、たとえばエラー率 p である状況で N ビットの訂正を行うのに、だいたい $Nh(p)$ ビットの秘密鍵を消費しなければならないことに注意しなければならない。

2.7 BB84 プロトコルの究極的安全性

さて、前節までにエラー訂正・プライバシー増幅の方法、また安全性の証明の骨子となる情報ー攪乱定理を紹介した。この節では、この究極的安全性の証明の概略を示そう。

前節の情報ー攪乱定理の証明では無視したが、実際にはランダムに選ばれるテストビットと残りのビット（情報ビットとよぼう）がある。前者に関しては添え字 T を、後者に関しては添え字 I をつけてあらわすと、

$$\sum_{i_T,c_T,b} P(Test = pass, i_T, c_T, b) I(A : E|i_T, c_T, b)$$
$$\leq N\sqrt{\frac{1}{2^N}\sum_{b} P\left((|c_I| > (p+\epsilon)N/2) \cap (|c_T| \leq pN/2)\right)}$$

が成り立つ。（p は適当な値。）ところで、テストビットはランダムに選ばれるので $P\left((|c_I| > (p+\epsilon)N/2) \cap (|c_T| \leq pN/2)\right)$ は N について指数的に減少することが示される。そこで、結局、

$$P(Test = pass\ and\ I_{Eve} \geq Ae^{-\beta N}) \leq Be^{-\nu N}$$

となる。このテストを通過した場合には、含まれる誤りも十分すくなく、エラー訂正とプライバシー増幅が適用できるのがわかる。証明の詳細に関しては論文を参考にされたい。

RSA などの公開鍵暗号方式は、計算量的複雑性にその礎を置いている。素因数分解など、一方向関数が本当に一方向であれば、計算量的観点からこの方式が安全であることが示されるのであった。これに対して、情報理論的暗号という概念がある。これは、前もって Alice と Bob が秘密の情報を共有することによって、Eve には情報が足らず、解読ができないというような、秘密鍵方式のような状況のことをさす概念である。量子鍵分配はこっちの部類に入るプロトコルである。さて、この節では、後で説明するように量子鍵分配によって何とかして Alice と Bob が不完全な情報を共有したときに、どのようにこれを訂正・蒸留することによって、完全に秘密な、しかも一致した

鍵を共有しうるか、ということを説明する。

エラー訂正プロトコル

さて、何とかして Alice と Bob は不完全ながら情報を共有しているものとしよう。この共有は、次に述べる量子鍵分配の方法や、あるいは例えば雑音のある通信路（盗聴者 Eve がいるのかもしれない）によって行われる。今、Alice はこの通信路を通して N ビットを送りたい。Alice の手にしているビット列を $a := a_1a_2\cdots a_N$、Bob の手にしたビット列を $b := b_1b_2\cdots b_N$ と書こう。このままでは、お互いにもつビット列は一致しておらず、暗号の鍵として使うことはできない。しかし今、これらのハミング距離 $d(a,b)$ は Np 以下であるということはわかっているとしよう。Alice が部分的な情報を与えることによって、Bob のもつビット列を訂正して、Alice のものと一致させることはできないだろうか。これを実現するのが、エラー訂正プロトコルである。直感的にいうと、これは、エラーで損なわれている部分を Alice が公開することにより、Bob は自分のもつ情報を訂正できるという方法である。ここでは、現実的なプロトコルではないが、一番簡単なものを紹介する。

i) Alice は $\{0,1\}^N$ から $\{0,1\}^M$ への関数 f （ハッシュ関数と呼ばれる）をランダムにえらぶ。ここで、$M \leq N$ である。(後でその具体的な値については論ずる。)

ii) a を持っている Alice は f と $f(a)$ を公開する。

iii)　b をもつ Bob は $f(b') = f(a)$ となる b' のうち、b と最もハミング距離が近いものを計算して求める。

さて、実際にこれがうまくいくということを説明しよう。今、F というのをこのプロトコルが失敗する（すなわち、得られた b' と a が一致しない）という事象をあらわす確率変数としよう。このプロトコルがうまくいく場合というのは、ハミング距離の関係式 $d(b',a) \leq d(b,a)$ を満たす $b' \neq a$ がすべて $f(b') \neq f(a)$ であるときである。つまり、このような b' は f によってすべて $f(a)$ 以外の $2^M - 1$ 個の中に移されなければならない。ひとつ b' を取り上げたときに、それがたまたま、$f(a)$ と同じものに移されてしまう確率は $1/2^M$ だから、うまくいくのは $1 - 1/2^M$ の確率である。これが、$d(b',a) \leq d(b,a)$

を満たす $b' \neq a$ についてすべて成り立つのだが、この数は $\sum_{j=1}^{d(b,a)} {}_nC_j$ であるから、

$$P(notF) = \left(1 - \frac{1}{2^M}\right)^{\sum_{j=1}^{d(b,a)} {}_nC_j}$$

が成り立つ。$d(b,a) \leq Np$ であったからこれは、

$$P(notF) \geq \left(1 - \frac{1}{2^M}\right)^{\sum_{j=1}^{Np} {}_nC_j}$$

を導く。(但し、Np が整数で無い場合は、Np は Np より大きい最小の整数に置き換えられる。) よって、

$$P(F) \leq 1 - \left(1 - \frac{1}{2^M}\right)^{\sum_{j=1}^{Np} {}_nC_j}$$

が成り立つ。今、M として $\log \delta_N + Nh(p+\epsilon_N)$ 以上の最小の整数、但し、$\epsilon := 1/\log N$、δ_N は $\log N$ 以上の最小の整数、を採用する。（$h(p) := -p \log p - (1-p)\log(1-p)$ である。）すると、

$$P(F) \leq 1 - \exp\left(-2^{Nh(p+\epsilon_N)-M}\right)$$

となり、これは N が大きければ、ゼロに近づく。すなわち、Alice は大体 $Nh(p)$ ビットの情報を Bob に送れば、Bob は N が大きいときにはほぼ確実にエラーを訂正することができるのである。現実的には、全ての写像からランダムに選ぶということをするのではなく、線形符号化等、確実に誤りが訂正できるようなプロトコルが用いられることが多い。

秘匿性増強

さて、上記のようにしてエラー訂正を行い、Alice と Bob は一致した長さ N のビット列を共有した。しかし、これは完全に秘密であるというわけにはいかない。実際、エラーが生じていた原因は Eve の存在のせいかもしれず、またそうでなくても、エラー訂正プロトコルにおいて Alice は $Nh(p)$ ビットの情報を公開してしまっている。すなわち第三者、Eve も何がしかの情報を得てしまっていると考えてよいだろう。そこで、このような状況から Alice と Bob は協力して、Eve が全く情報をもっていない短いビッ

ト列を共有することはできないだろうか。つまり、Eveが現在もっている情報が全く無力となるような、短いビット列を蒸留することができないだろうか。もし、これが可能であれば、AliceとBobは完全に一致した、しかも第三者には完全に秘密なビット列を共有することができる。これは秘密鍵として使うことができるだろう。これは実際可能であり、プライバシー増幅と呼ばれる。以下にこれを説明する。

さて、具体的なプロトコルの説明に入る前にいくつか概念を導入しておく。まず、何か確率変数 X があったときに、このとりうる値の確率分布 $P_X(x)$ が定まるが、このレニーエントロピーと呼ばれる量 $R(X)$ を

$$R(X) := -\log \sum_x P_X(x)^2$$

で定義する。これは、シャノンエントロピー $S(X)$ と

$$R(X) \leq S(X)$$

という大小関係がある。また、同様に、何か他の確率変数 Y も与えられているときに、条件付レニーエントロピー $R(X|Y)$ を

$$R(X|Y) := \sum_y P_Y(y) R(X|Y=y)$$

で定義する。但し、$R(X|Y=y)$ は条件付確率 $P(x|y)$ について定義されるレニーエントロピーである。さて、レニーエントロピー $R(X)$ は X が確定値を持つときに限りゼロである。また、等確率分布しているときに最も大きな値をとる。

次に、普遍的関数族と呼ばれる概念を定義しよう。今、$\{0,1\}^N$ から $\{0,1\}^L$ へのある関数族 $\mathcal{G}$ を考える。但し、$L \leq N$ とする。これが、普遍的関数族であるとは、今、任意の $x, y \in \{0,1\}^N$ を決めて、$\mathcal{G}$ からランダムに一つ関数 g を選んだとき、これが $g(x) = g(y)$ を満たす確率はせいぜい 2^L であるという性質をみたすことを言う。普遍的関数族の例としては、前にも用いたハッシュ関数のあつまり、すなわち $\{0,1\}^N$ から $\{0,1\}^L$ への関数全ての集合がある。実際、今、ある $x, y \in \{0,1\}^N$ を固定したときに、それがある $z \in \{0,1\}^L$ に写像される確率はそれぞれ $1/2^N$ である。このような z が 2^L 個あるのだ

k ら一致する値をとる確率は $1/2^{2N-L}$ である。$N \geq L$ の条件よりこれは普遍的関数族の条件をみたしている。

さて、いよいよプロトコルに入るが状況を整理しよう。今、Alice と Bob の共有する N ビット列を表す確率変数を X と書く。Eve はこれについて何がしかの情報を持っている。Eve の確率変数を V と書こう。しかし、Eve の持っている情報は完全ではなく、ある $c > 0$ について、Eve のもつ X についての情報の不完全さをあらわすレニーエントロピーは $R(X|V=v) \geq cN$ という関係式を満たしていることが、Alice と Bob に知られているとする。そこで、Alice と Bob は以下のプロトコルを実行する。

i)Alice は適切な L（具体的な値は後に述べる）について普遍的関数族 $\mathcal{G}$ を設定する。

ii)Alice は $\mathcal{G}$ の中から一つ関数をランダムに選ぶ。この関数値確率変数を G と書こう。

iii)Alice は G の値 (どの関数を選んだか) を公開する。G を X に適用したものは公開しない。

iv)Alice と Bob は G を X に適用し、共通の秘密を手にする。

このように行って得られる確率変数 $G \circ X$ の値は Eve にとっては全く未知のものであることを示そう。まず、

$$\begin{aligned}
R(G(X)|G, V=v) &= \sum_g P_G(g) R(G(X)|G=g, V=v) \\
&= \sum_g P_G(g)(-\log \sum_{z \in \{0,1\}^L} P(g(X)=z|V=v)^2) \\
&\geq -\log \left(\sum_g P_G(g) \sum_{z \in \{0,1\}^L} P(g(X)=z|V=v)^2 \right)
\end{aligned}$$

となる。これは

$$
\begin{aligned}
& \sum_g P_G(g) \sum_{z\in\{0,1\}^L} P(g(X)=z|V=v)^2 \\
= \; & \sum_g \sum_{z\in\{0,1\}^L} P_G(g) \sum_{x:g(x)=z} \sum_{y:g(y)=z} P_X(x|V=v)P_X(y|V=v) \\
= \; & \sum_g P_G(g) \left(\sum_x P_X(x|V=v)^2 + \sum_{x\neq y:g(x)=g(y)} P_X(x|V=v)P_X(y|V=v) \right) \\
\leq \; & \sum_x P_X(x|V=v)^2 + (1-\sum_x P_X(x|V=v)^2)2^{-L} \\
\leq \; & 2^{-R(X|V=v)} + 2^{-L} \\
= \; & 2^{-L}\left(1+2^{L-R(X|V=v)}\right)
\end{aligned}
$$

と抑えられ、両辺の対数をとり関係 $\log(1+y) \leq \log y/\ln 2$ を用いると、

$$
R(G(X)|G,V=v) \geq L - \frac{2^{L-R(X|V=v)}}{\ln 2}
$$

を得る。$S(G(X)|G,V=v) \geq R(G(X)|G,V=v)$ と $R(X|V=v) \geq cN$ を用いると、これは

$$
S(G(X)|G,V=v) \geq L - \frac{2^{L-cN}}{\ln 2}
$$

を導く。結局 $L=kN$ としたときに $k<c$ であれば、大きな N に対して Eve の情報を全くカットすることができるのである。

この章では、量子鍵分配の方式などによって Alice と Bob がある程度情報を共有したときに、どのようにして彼（女）らが一致した完全に秘密な情報を訂正・蒸留し共有できるか、について述べた。実際には、上に述べた方法より、計算の手続きとして簡単なものが存在するし、また上の二つの方式をつないでうまくいく条件などを求めなければならないだろう。それについては、この本では詳細には立ち入らないので、原論文を参照してほしい。

関連図書

[1] M.N.Wegman and J.L. Carter, Journal of Computer and System Sciences, Vol.22, 1981, pp.265.

[2] R.Konig, U.Maurer, R.Renner,On the Power of Quantum Memory IEEE Transaction on Information Theory, vol. 51, no. 7, pp. 2391-2401, Jul 2005,

[3] C.W.Helstrom, Detection theory and quantum mechanics (II). Information and Control, 13(2):156-171, August 1968.

[4] A. メシア「量子力学 (1、2、3)」, 東京図書 (1981 年)

[5] C.H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in: *Proc. of the IEEE Inst. Conf. on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York,1984) p.175

[6] C.H. Bennett, G. Brassard, C. Crepeau, and U. Maurer *Generalized Privacy Amplification* IEEE Transaction on Information Theory, vol. 41, no. 6, pp. 1915-1923, Nov (1995)

[7] C.H.Bennett, G.Brassard, S.Popescu, B.Schumacher, J.A.Smolin, W.K.Wootters, *Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels*, Phys. Rev. Lett. **76**,722 (1996)

[8] E. Biham, M. Boyer, P.O. Boykin, T. Mor, and V. Roychowdhury, *A proof of the security of quantum key distribution*, Proc. 32nd Ann. ACM Symposium on the Theory of Computing, 715-724, ACM press, (2000)

[9] C.Cachin and U.Maurer, *Linking Information Reconciliation and Privacy Amplification*, Advances in Cryptology - EUROCRYPT '94, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, pp. 266-274, (1994)

[10] T.M. Cover and J.A. Thomas, *Elements of Information Theory*, Wiley (1991)

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

[12] Bennett92

[13] N. Gisin and S. Massar, *Optimal quantum cloning machines*, Phys.Rev.Lett. 79, (1997), p.2153.

[14] H. Inamori, *Security of EPR-based Quantum Key Distribution*, Algorithmica 34(4): 340-365 (2002)

[15] Hoi-Kwong Lo, H. F. Chau, *Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances*,Science, vol. 283, p. 2050 (1999).

[16] H. Maassen and J.B.M. Uffink, *Generalized entropic uncertainty relations* Phys. Rev. Lett. **60**, 1103 (1988)

[17] D. Mayers, *Unconditional security in Quantum Cryptography*,JACM, vol 48, no 3, May 2001, p 351-406

[18] P.W.Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J.Comut.26 1484 (1997)

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

[20] S. Wiesner, *Conjugate coding*, SIGACT News, 15:1, pp.78-88. (1983)

[21] W.K. Wooters and W.H. Zurek, *A single quanta cannot be cloned*, Nature, 299, (1982), pp.802-803.

[22] H-K. Lo and H-F. Chau. *Science*, 283, pages 2050–2056, 1999.

[23] C. A. Fuchs and A. Peres. *Phys.Rev.A*, 53(4), pages 2038–2045, 1996.

[24] C. A. Fuchs. *Fortschritte der Physik*, 46(4,5), pages 535–565, 1998.

[25] M. Christandl and A. Winter. *IEEE Trans Inf Theory*, 51(9), pages 3159–3165, 2005.

[26] P. O. Boykin and V. P. Roychowdhury. *QIC: Quantum Information and Computation*, 5(5), pages 396–412, 2005.

[27] T. Miyadera and H. Imai, Information-Disturbance Theorem for Unbiased Observables, *Phys.Rev.A.* 73, pages 042317 2006.

[28] M. A. Nielsen, and I. L. Chuang, *Quantum Computation and QUantum Information*, Cambridge press. 2000.

[29] D. Deutsch, *Phys.Rev.Lett.* 50,631 (1983).

[30] M. Krishna and K. R. Parthasarathy, *Sankhya, Series A,* 64(3), 842 (2002).

[31] L. Hughston, R. Jozsa, and W. Wootters, *Phys. Lett. A.* 183 pages 14 (1993).

[32] H. Halvorson, *J. Math. Phys.* 45, pages 4920 (2004).

[33] M. Hayashi, *Phys. Rev. A.* 74, pages 022307 2006.

[34] I. Damgaard, S. Fehr, L. Salvail and C. Schaffner. Cryptography In the Bounded Quantum-Storage Model, *Proceedings of the 46th IEEE Symposium on Foundations of Computer Science - FOCS 2005*, pages 449–458, 2005.

[35] M. Christiandl, R. Renner, and A. Ekert,“ A Generic Security Proof for. Quantum Key Distribution, ” 2004, quant-ph/0402131.

第3章　実用化に向けた技術開発におけるトレンド —デコイに関するまとめ—

3.1　実使用環境下における量子暗号通信の実現に向けて

現在、広く社会で利用されている暗号方式は、解読に必要な計算量が大きく、実際上、短い時間内にそれを完了することが不可能であることをもって、その安全性を保証している。このことは、今後、計算機の能力が飛躍的に伸び、解読アルゴリズムが改良されると、その安全性の基盤が揺らぐことを意味している。夢の量子コンピュータが実現されるとなれば、その脅威はさらに深刻さを帯びることになろう。

これに対し、1984 年に Bennett と Brassard が新しい暗号方式 BB84 [1] を提案すると、新しい可能性が拓かれた。量子暗号の出現である [2–5]。量子暗号では、暗号鍵を量子状態に乗せて配布する。例えば BB84 [1] では、暗号鍵 1 ビット分の 0・1 を、1 光子の偏極の縦・横にエンコードする。その情報を盗聴しようとする者があれば、その量子状態を測定、もしくはコピーしなければならないが、量子力学の基本原理——不確定性原理——によると、その状態を擾乱することなく正確にその目的を達成することは不可能である。すなわち、盗聴の痕跡が残るので、盗聴者の存在を見抜くことができるのである。

このように、量子暗号の安全性は計算量ではなく自然法則の基本原理に基づいているため、その自然法則が正しい限り、絶対的な安全性が保証される [6–10]。BB84 [1] の提案をきっかけに、様々な量子暗号プロトコルが提案され [2–5]、次世代の暗号方式の実現に向けて、また、量子情報技術の最初の実用として、理論・実験の両面から精

力的に研究が進められている。世界中に張りめぐらされている光ファイバー網の利用を想定し、光ファイバー・ケーブルを光子の伝送路に使用した実験 [11–15] や、ケーブルを通さずに大気中に光子を飛ばす実験 [14, 16–18]、地上と人工衛星との間の鍵配送実験 [19][[[**日本の他の実験**]]] など、鍵配送の長距離化が試みられるとともに、商品化の動きも既に出てきている [20–22]。

しかしながら、その絶対安全性を現実のシステムで即実現できるかとなると、注意が必要である。現実の使用環境は、量子暗号の理論が要求する条件すべてを満足するのには厳しすぎるからである。例えば、100% の伝送率を現実に達成することは不可能であり、また、ビット・エラーも少なからず起こる。量子暗号においては、鍵を運搬する媒体の量子性が重要であるが、日常の生活環境下においてそれをきれいに実現することも、長距離の伝送に耐えて維持することも大変困難な課題である。量子暗号システムの実用化、さらに長距離鍵配送の実現に向けては、こうした非理想的要素を考慮に入れた上で安全性が保証されていなければならない。

特に、BB84 では、1 ビットを 1 光子に乗せることを想定しており、その光子の量子性を安全性の拠所にしている。この要件を満たすために、単一光子源の開発が精力的に進められてきた [23–25]。しかし、それには大変な技術を要し、広く実用に用いるのには程遠いのが現状である。そこで、実際には、本当の単一光子ではなく、光子数 1 個以下相当にまで光源強度を落としたレーザー・パルス (弱コヒーレント光) でそれに代用している場合がほとんどである。つまり、真の単一光子に鍵を乗せているのではなく、時として複数個の光子が担う形になってしまっているのである。

この単一光子の擬似性が BB84 の安全性の脅威となりえることが具体的に指摘されると、これは大きな問題になった。「光子数分岐攻撃 (Photon-Number-Splitting Attack; PNS Attack)」に対する脆弱性 [26–30] である。Alice が配送する暗号鍵を受け取る Bob には、光子を捕らえる検出器が必要である。光子数をカウントすることも技術的に難しく、通常、量子暗号鍵配送実験に用いられている検出器は、ただパルスが来たことを捕らえるのみである。Bob は、それが真に単一光子であったかどうかは判断していない。盗聴者 Eve はこの点を突き、複数個の光子を含むパルスから、いくつかの光子

を盗み取ってしまうのである。残りの光子は乱されることなく Bob のところに到着するが、Bob は光子数をカウントしないため、途中で光子が抜き取られたことに気が付かない。こうして、Eve は Bob に気が付かれることなく鍵を盗み取ることができるのである。

このように、擬似単一光子パルスを使用する通常の道具立てでは、BB84 の安全性が自明でなくなってしまう。そこで、この単一光子源の擬似性とともに、有限の伝送率、ビット・エラー率なども考慮に入れたより現実的な設定の下で安全性が議論されている [31,32]。例えば、最終的に抽出可能な安全な鍵の生成率として、

$$R \geq qY_\mu \left\{ -H_2(E_\mu) + (1-\Delta)\left[1 - H_2\left(\frac{E_\mu}{1-\Delta}\right)\right]\right\} \tag{3.1}$$

という式が提出されている [31,32]。ここで、

$$H_2(x) = -x\log_2 x - (1-x)\log_2(1-x) \tag{3.2}$$

であり、q は通常の BB84 プロトコルに対しては

$$q = \frac{1}{2}, \tag{3.3}$$

Y_μ は送られてきたレーザー・パルスを Bob が検知する割合 (収率; 伝送効率と暗計数率を含む) で、E_μ は量子ビット・エラー率。そして、Δ が、多光子パルスが寄与する割合を表し、単一光子源の擬似性を取り入れる量である。Bob がすべての多光子パルスを受け取ってしまう最悪のケースまでを想定して、

$$\Delta = \frac{P_{\mathrm{multi}}}{Y_\mu} \tag{3.4}$$

(P_{multi} は Alice が多光子パルスを発してしまう確率) とされている [31,32]。いずれのパラメータも、通常の装置で測定可能な量である点が重要である。R の下限 [不等式 (3.1) の右辺] が 0 よりも大きければ、それは安全な鍵を有限ビット数生成可能であることを意味しており、より現実的な設定の下でも安全性が保証される。一方、Δ が大きくなって R の下限が 0 を下回ることになると、安全な鍵配布が保証されないことになる。標準的な実験設定 (例えば、[11,13,33–35]) では 20 km や 30 km がその限界と言われ、こ

のことから、擬似単一光子源による安全で長距離な鍵配布は困難であると考えられてきた。

ところが、最近 (2003 年) になって、この問題にブレーク・スルーがもたらされた。Hwang が提案した「デコイ法による量子鍵配送 (Decoy-State Quantum Key Distribution)」である [36]。そのアイデアは、時折あえて多光子パルス (decoy; おとり) を送ってみて、PNS 攻撃が行われているか探りを入れようというものである。すなわち、鍵を乗せる弱コヒーレント光パルスとは異なる強度のコヒーレント光パルスをパルス列に忍ばせておくのである。Eve には、どの多光子パルスが鍵の情報を乗せた擬似単一光子パルスのもので、どれがデコイのものなのか区別がつかないため、彼女は両者に対して同じ攻撃手続きをとる。Alice と Bob は、鍵を乗せたビットとデコイのビットが Bob のところにどれだけ届いたかを確認することによって、PNS 攻撃を感知し、安全な鍵が保証されるか否かを明確にできるのである。

あるいは、別の言い方をすると、その多光子パルスがどれほど関与してしまうかが安全性を大きく左右することになるのだが、通常の装置でその寄与を正確に見積もることは不可能である。光子数をカウントできる測定器は、そうそうないからである。ところが、Hwang が提案したように、信号用の光源強度とは異なる強度のレーザー・パルスを飛ばしてみて、それぞれの強度のレーザー・パルスの収率を測定から知ると、多光子パルスの寄与を幾分正確に評価できるのである。その結果、式 (3.1) よりも厳しい不等式を証明することができ、より高いレートの安全鍵生成が保証できるようになるのである。

この考えは Wang [37,38] や Lo ら [39–42]、さらにはロス・アラモスと NIST のグループ [43] によって推し進められ、デコイとして挿入するレーザー・パルスの強度の種類を増やすことで、さらに厳しい制限を与えられることが示されると、安全性を保証できる鍵配送距離が格段に伸びた。単一光子源を用いずとも、従来広く用いられてきた擬似単一光子源で、100 km を超える長距離の安全な鍵配送が可能なのである。このことで、量子暗号鍵配送システムの実用化に向けてのハードルが劇的に低くなった。その後、理論的研究がさらに進められるとともに [44, 45]、早速、実験も行われており、

昨年から今年にかけて立て続けにその結果が論文発表 [46–51] されるなど、現在最も注目を集めている量子暗号方式の一つとなっている。

上述の Wang の研究も含め、日本でも精力的に研究が進められている。先行研究のいくつかの仮定をさらに緩めてより現実に即した形で理論の再構築、定量的評価を行うとともに [52]、その理論を実装して、誤り訂正、秘密増幅をも施して実際に安全な最終鍵を生成することに成功したとの発表が最近なされた [53]。

本章では、最近の量子暗号研究の中から特に注目を集めているこのデコイ法に焦点を当て、その基本的アイデアから実験の現状までを報告する.[1]

[1]デコイ法以外にも、擬似単一光子源を用いた暗号鍵配送の安全性を高める方策が提案されている [54–58]。

3.2　光子数分岐攻撃

デコイ法のアイデアを理解するために、まず、「光子数分岐攻撃 (Photon-Number-Splitting Attack; PNS Attack)」[26–30] を簡単に振り返っておこう。

Alice が Bob に BB84 プロトコルで暗号鍵を配送することを考える。あいにく、Alice は理想的な単一光子源を持っておらず、強度を弱めたコヒーレント光 (擬似単一光子源) でそれに代用する。そのため、多くのパルスは光子 1 つのみからなるものの、コヒーレント光の強度で決まるある一定の確率 P_{multi} で、複数個の光子を含むパルスを発してしまうことになる。この、単一光子源の擬似性に起因する脆弱性が、ここでの話題である。転送するビット値は、パルスの偏極に乗せる。このとき、1 つのパルスを構成する複数個の光子は、すべて同じ偏極状態になっている。

Bob は、それぞれのパルスに含まれる光子数をカウントできるような優れた検出器は持っておらず、パルス全体がある特定の偏極状態にあったか否かが判別できるに過ぎない。また、パルスを伝送する現実のチャンネルは完璧なものではなく、いくらかの損失を容認しなければならない。距離が伸びれば伸びるほど、伝送率 Y_μ は低下するであろう。簡単のため、ここではビット・エラーは起こらないものとする。Bob の検出器の感度も、理想的なものとしよう。

さて、このような設定の下、Eve がたくらむ PNS 攻撃は、以下のようなものである。優れた能力を持つ Eve は、各パルスに含まれる光子数をカウントできるものとする。伝送路の途中でパルスを横取りし、もし、それが単一光子であれば、その場で捨ててしまう。もし、それが複数個の光子を含んでいれば、そのうちの一つを手元に残して、残りを (Eve であれば準備可能な) 伝送率 100% のチャンネルで Bob に送る。後ほど、Alice が使用した基底が公表されたとき、それに合わせて Eve も手元の光子の偏極状態を測定する。そうすることで、Eve も、Alice や Bob とビット情報を共有できる。

さらに話を簡単にするために、次のような状況を考えよう。仮に、多光子パルスが発生してしまう確率が $P_{\mathrm{multi}} = 10\%$ で、伝送率も $Y_\mu = 10\%$ であるとする。すると、Eve が PNS 攻撃を行った場合、信号パルス列のうちの 90% を占める単一光子パルスは捨てられ、残りの 10% のパルスが、Eve によって 1 つの光子が引き抜かれた後、伝送率

100% の伝送路ですべて Bob に届く。つまり、Bob にパルスが届く割合は、Eve の PNS 攻撃が行われていないときも行われているときも 10% となり、Alice と Bob に気が付かれることなく、ビット情報を盗めてしまうのである。

多光子パルスが発生してしまう確率 P_{multi} が大きければ大きいほど、Eve の PNS 攻撃は容易になる。Eve が Bob に送り直すパルス数を、Eve が適当に調節して少なくすればいいだけのことだからである。逆に、P_{multi} が十分に小さく、

$$Y_\mu > P_{\mathrm{multi}} \tag{3.5}$$

であれば、PNS 攻撃は不可能である。Eve が単一光子パルスをブロックして捨てると、それだけで Bob のところに届くパルスの割合が、攻撃を受けない場合の Y_μ を下回ってしまうからである。Eve は、この割合を Y_μ にまで回復させることはできない。したがって、Alice と Bob が、Bob のところに届くパルスの数から伝送率を割り出すと、通常の値 Y_μ と異なるため、PNS 攻撃を見抜くことができるのである。

つまり、式 (3.5) が成立していれば、PNS 攻撃に対しても安全性が保証されることになる。一方で、この式から明らかなように、伝送率 Y_μ が小さくなればなるほど、光源に対する要求が厳しくなる。鍵配送距離が長距離になると、現在広く用いられている通常の擬似単一光子パルスでは、安全性を保証することができなくなるのである。このことが単一光子源の開発を駆り立ててきた [23–25]。しかし、依然として単一光子源を広く汎用として利用できるまでには至っておらず、実用的な長距離鍵配送の実現に向けて、大きな壁となっていた。

3.3　デコイ法による量子鍵配送

2003年にHwangは、PNS攻撃の検知感度を上げ、伝送損失が比較的大きな状況でもPNS攻撃に対する安全性を保証できるようにしようと、新しい鍵配送方式を提案した [36]。「デコイ法による量子鍵配送プロトコル」である。その基本的アイデアを振り返った後に、Wang [37, 38] やLoら [39–42] による改良・発展を概観しよう。

3.3.1　Hwangによる最初の提案

Hwangの最初のアイデアは、次のようなものであった [36]。PNS攻撃の際、Eveは単一光子パルスをブロックして捨ててしまう。この点に着目し、あえて光子を多く含むパルスをデコイ (おとり) として投げてみようというのである。光子数が大きめのパルスが来ても、それが鍵を乗せた擬似単一光子パルスに確率的に含まれるものなのか、デコイ・パルスのものなのかの区別はEveにはつかない。そのため、Eveは両者に対して同じ手続きを取ることになろう。すると、単一光子成分が切り捨てられる鍵パルスがBobに受け取られる収率と、デコイ・パルスの収率とでは、前者が圧倒的に小さくなるに違いない。もし、その違いが有意に確認されれば、PNS攻撃を受けていると判定できるだろう。

問題を定式化しよう。鍵を乗せる光源は、完璧な単一光子源ではなく、確率 p_n で n 個の光子を発してしまうようなものである。ただし、$n = 0, 1, 2, \ldots$ であり、

$$\sum_{n=0}^{\infty} p_n = 1. \tag{3.6}$$

以下では、特にコヒーレント状態 $|\mu e^{\theta}\rangle$ を発生する光源を考える。その位相 θ がランダムな場合には、発信されるパルスは、混合状態

$$\rho_\mu = \int \frac{d\theta}{2\pi} |\mu e^{\theta}\rangle\langle\mu e^{\theta}| \tag{3.7}$$

で記述されよう。これを数表示で書けば、

$$\begin{cases} \rho_\mu = \displaystyle\sum_{n=0}^{\infty} p_n(\mu)|n\rangle\langle n|, \\ p_n(\mu) = \dfrac{\mu^n e^{-\mu}}{n!} \end{cases} \tag{3.8}$$

のように、光子数が確定した状態 $|n\rangle$ の古典的な重ね合わせで与えられる。これを我々の光源として話を進めよう。

さて、鍵の情報を乗せるパルスは擬似単一光子パルスで、

$$\mu < 1 \tag{3.9}$$

のコヒーレント光 (弱コヒーレント光) である。一方で、デコイ・パルスとしては、あえて光子を多く含ませ、

$$\mu' > 1 \tag{3.10}$$

としよう。これ以降、デコイ・パルスに関する量には、μ' のように $'$ を付すことにする。

通常の装置で Alice と Bob が測定できるのは、途中の伝送率、Bob の測定器の感度、その他 Eve の所作の影響も含め、Alice が送ったパルスのうち Bob が受け取ったパルス数の割合、すなわち、収率 Y_μ, $Y_{\mu'}$ である。n 個の光子を含むパルスの収率を y_n, y'_n と記すと、

$$Y_\mu = \sum_{n=0}^{\infty} p_n(\mu) y_n, \tag{3.11a}$$

$$Y'_{\mu'} = \sum_{n=0}^{\infty} p_n(\mu') y'_n \tag{3.11b}$$

と書かれる。この段階で、

$$Y_\mu \ll Y'_{\mu'} \tag{3.12}$$

が確認されれば、PNS 攻撃を受けていると判断できるであろう。そうでない場合には、もう少し詳細な議論が必要だ。

それでは、どのような場合に、PNS 攻撃の可能性を排除できるであろうか？それは、

$$Y_\mu > \max Y_\mu^{\mathrm{multi}} \tag{3.13}$$

が成立するときである。ただし、

$$Y_\mu^{\mathrm{multi}} = \sum_{n=2}^{\infty} p_n(\mu) y_n \tag{3.14}$$

は、2個以上の光子を含むパルスの (Alice が送った全パルスに対する) 収率であり、max は、Eve が PNS 攻撃を隠すために最大限の努力をした場合の値をとることを意味する。つまり、測定された Y_μ が式 (3.13) を満たしていることが確認されれば、PNS 攻撃を否定できるのである。

ここで重要なのは、Bob の測定器は光子数を判別できないので、y_n や y'_n は直接測定できない量であるということである。したがって、式 (3.14) の Y_μ^{multi} も測定できない。そもそも、Y_μ^{multi} を測定できるのであれば、デコイ・パルスを利用せずとも、PNS 攻撃の有無を即座に判定することができる。また、それができないからこそ、Eve が最良の攻撃をした場合までを想定し、式 (3.13) の右辺で max を考えなければならないのである。

この Y_μ^{multi} を直接測定することはできないものの、デコイ・パルスの収率 $Y'_{\mu'}$ を用いると、その上限を評価できてしまうところがデコイ法の真髄である。その際、n 個の光子を含むパルスが、鍵を乗せたパルスのものなのかデコイ・パルスのものなのかの区別が Eve にはつかない点が重要である。つまり、

$$y_n = y'_n \tag{3.15}$$

の関係が、デコイ法において最も重要な式である。したがって、$Y'_{\mu'} = Y_{\mu'}$ と言える。

さて、式 (3.14) を考えよう。この上限が、デコイ・パルスの収率 $Y_{\mu'}$ でどう評価されるかが問題だ。Eve の目指すところは、可能な限り Y_μ^{multi} が大きくなるように工夫し、式 (3.13) の成立を難しくすることである。このことは、

$$A = \frac{Y_\mu^{\mathrm{multi}}}{Y_{\mu'}^{\mathrm{multi}}} = \frac{\sum_{n=2}^{\infty} p_n(\mu) y_n}{\sum_{n=2}^{\infty} p_n(\mu') y_n} \tag{3.16}$$

を可能な限り大きくすることと等価である。

その上限は、実は

$$A \leq \frac{p_2(\mu)}{p_2(\mu')} \tag{3.17}$$

で与えられる。このことを示すためには、$\mu < \mu'$ に対して、

$$\frac{p_n(\mu)}{p_n(\mu')} > \frac{p_m(\mu)}{p_m(\mu')} \qquad \text{for} \qquad n < m \tag{3.18}$$

であることを知っておくとよい。実際、式 (3.8) の確率分布に注意すると、

$$\frac{p_n(\mu)}{p_n(\mu')} = \frac{\mu^n e^{-\mu}/n!}{\mu'^n e^{-\mu'}/n!} = (e^{-\mu}/e^{-\mu'})(\mu/\mu')^n \tag{3.19}$$

であり、これは n の単調減少関数であって、式 (3.18) の成立を示している。すると、

$$\frac{p_2(\mu)}{p_2(\mu')} - A = \frac{\sum_{n=2}^{\infty} y_n[p_2(\mu)p_n(\mu') - p_2(\mu')p_n(\mu)]}{p_2(\mu')\sum_{n=2}^{\infty} p_n(\mu')y_n} \geq 0 \tag{3.20}$$

が結論され、式 (3.17) が示される。

この結果、

$$Y_\mu^{\text{multi}} \leq \frac{p_2(\mu)}{p_2(\mu')} Y_{\mu'}^{\text{multi}} \leq \frac{p_2(\mu)}{p_2(\mu')} Y_{\mu'} \tag{3.21}$$

が得られる。すなわち、式 (3.13) で関心があり、直接の測定で知ることができない Y_μ^{multi} の上限が、測定可能なデコイ・パルスの収率で評価できるのである。したがって、式 (3.13) を満足しようと思ったら、

$$Y_\mu > \frac{p_2(\mu)}{p_2(\mu')} Y_{\mu'} \tag{3.22}$$

となっていればよい。この条件が満足されていれば、PNS 攻撃を否定できるのである。改めて、この条件式が測定可能量と既知の量とからなっていることを強調しておこう。

仮に、Eve の攻撃を受けていないものとして、式 (3.22) をもう少し見てみよう。1 光子の伝送効率を η とする。これは、伝送距離や Bob の測定器の効率などに依存する。多光子パルスに含まれている光子のうち、いくつかが失われても、Bob には関係ない。パルスがやってきたとカウントするであろう。Bob は光子数を数えないからである。n 個の光子を含むパルスが失われるというのは、その n 個すべてが失われることである。その確率は $(1-\eta)^n$ で与えられる。したがって、n 光子パルスが Bob に捕らえられる割合 (収率) y_n は、

$$y_n = 1 - (1-\eta)^n \tag{3.23}$$

である。この式を用いると、光強度 μ のレーザー・パルスの収率 (3.11) は、

$$Y_\mu = 1 - e^{-\eta\mu} \tag{3.24}$$

と計算される。伝送効率が悪く η が小さい場合、$Y_\mu \simeq \eta\mu$ と近似されるので、式 (3.22) は

$$\frac{\mu e^{-\mu}}{\mu' e^{-\mu'}} < 1 \tag{3.25}$$

と簡略化される。例えば、$\mu = 0.3,\ \mu' = 1.0$ とすると、この左辺は 0.6 となって、不等式を満たす。このとき、式 (3.25) から η が姿を消している点が注目である。一方、デコイに拠らない (3.5) の評価式では

$$\eta\mu > P_{\mathrm{multi}} = 1 - e^{-\mu} - \mu e^{-\mu} \tag{3.26}$$

となって、η が小さくなればそれだけこの条件を満足することが難しくなる。式 (3.25) は、依然として小さな μ を要求している式のようにも見えるが、伝送効率の低下に対するデコイ法の頑強さを示唆しており、擬似単一光子源による長距離鍵配送への可能性を期待させる式である。

3.3.2　Wang の 2 デコイ・プロトコル

擬似単一光子源による鍵配送プロトコルの安全性は、多光子パルスの寄与 [式 (3.13) の右辺、すなわち、Y_{multi} の上限] を、どれだけ正確に評価できるかにかかっている。この量が直接測定できない量である点が問題だ。Hwang が与えた評価は、式 (3.21) だ。これに対し、Lo らは、Hwang のアイデアを発展させ、複数種類のデコイ・パルスを織り交ぜることで、より正確な Y_{multi} の評価が可能になることを示唆した [39,40]。Wang は、そのアイデアを 2–3 種類のデコイ・パルスを用いるプロトコルで具体的に検証し、実際に、Hwang の (3.21) よりも厳しい制限を Y_μ^{multi} に与えることができることを示した [37,38]。Hwang の条件 (3.22) よりも緩いパラメータ領域まで、鍵配送の安全性を保証できるのである。

2 種類のデコイ・パルスを用いる場合で、Wang の議論を見てみよう [37,38]。2 種類といっても、そのうちの一つは “真空” (パルスを送らない) である。したがって、用意

する光源強度は、μ (鍵用) と μ' (デコイの一つ) の 2 種類である (真空の “0” も含めると 3 種類)。実は、$Y_\mu^{\rm multi}$ に対する良い評価を得るためには、Hwang が思い描いたように $\mu<1,\ \mu'\geq 1$ である必要はない。以下、

$$\mu<\mu' \tag{3.27}$$

とだけ仮定して話を進めよう。

光源の状態 (3.8) を

$$\rho_\mu=p_0(\mu)|0\rangle\langle 0|+p_1(\mu)|1\rangle\langle 1|+\rho_\mu^{\rm multi} \tag{3.28a}$$

と分解しよう。$\rho_\mu^{\rm multi}$ は、2 光子以上を含む (規格化されていない) 状態である。デコイ・パルスの $\rho_{\mu'}$ は、次の凸結合で書ける:

$$\rho_{\mu'}=p_0(\mu')|0\rangle\langle 0|+p_1(\mu')|1\rangle\langle 1|+\frac{p_2(\mu')}{p_2(\mu)}\rho_\mu^{\rm multi}+\tilde{\rho}_{\mu',\mu}. \tag{3.28b}$$

実際、

$$\tilde{\rho}_{\mu',\mu}=\rho_{\mu'}^{\rm multi}-\frac{p_2(\mu')}{p_2(\mu)}\rho_\mu^{\rm multi}=p_2(\mu')\sum_{n=3}^{\infty}\left(\frac{p_n(\mu')}{p_2(\mu')}-\frac{p_n(\mu)}{p_2(\mu)}\right)|n\rangle\langle n| \tag{3.29}$$

であるが、式 (3.27) の下で

$$\frac{p_n(\mu')}{p_2(\mu')}-\frac{p_n(\mu)}{p_2(\mu)}=2({\mu'}^{n-2}-\mu^{n-2})/n!>0\quad(n>2) \tag{3.30}$$

であることから、凸分解ができている。

さて、Alice と Bob が測定で知ることのできる量は、$Y_0,\ Y_\mu,\ Y_{\mu'}$ の収率である。それぞれ、Alice が送ったパルスのうち Bob がいくつを受け取ったかを確認すればよい。式 (3.11) にしたがって、

$$\begin{cases} Y_0=y_0, \\ Y_\mu=p_0(\mu)y_0+p_1(\mu)y_1+Y_\mu^{\rm multi}, \\ Y_{\mu'}=p_0(\mu')y_0+p_1(\mu')y_1+\dfrac{p_2(\mu')}{p_2(\mu)}Y_\mu^{\rm multi}+\tilde{Y}_{\mu',\mu} \end{cases} \tag{3.31}$$

と書こう。ここでも、式 (3.15) が重要である。ここで、$\tilde{Y}_{\mu',\mu} \geq 0$ に注意すると、第 3 式から

$$Y_\mu^{\mathrm{multi}} \leq \frac{p_2(\mu)}{p_2(\mu')}[Y_{\mu'} - p_0(\mu')y_0 - p_1(\mu')y_1]. \tag{3.32}$$

さらに、

$$Y_\mu^{\mathrm{multi}} \leq \frac{p_2(\mu)}{p_2(\mu')}[Y_{\mu'} - p_0(\mu')y_0] \leq \frac{p_2(\mu)}{p_2(\mu')}Y_{\mu'} \tag{3.33}$$

が帰結できるが、これは、Hwang の (3.21) にほかならない。

同時に、この式 (3.33) は、今回の 2 デコイ・パルス・プロトコルで、Hwang の (3.21) よりも厳しい制限を Y_μ^{multi} に与えることができることを示している。今回のプロトコルでは $Y_0 = y_0$ を測定するため、式 (3.33) の中間の不等式を利用できるからである。話はこれにとどまらない。式 (3.33) の導出には式 (3.31) の第 3 式のみを利用したが、第 2 式も考慮に入れるとさらに厳しい評価式が得られるのである。

実際、式 (3.31) の連立方程式を解くことで

$$\begin{pmatrix} Y_\mu^{\mathrm{mutli}} \\ y_1 \end{pmatrix} = \frac{1/p_2(\mu')}{p_1(\mu)/p_2(\mu) - p_1(\mu')/p_2(\mu')} \begin{pmatrix} -p_1(\mu') & p_1(\mu) \\ p_2(\mu')/p_2(\mu) & -1 \end{pmatrix} \times \begin{pmatrix} Y_\mu - p_0(\mu)Y_0 \\ Y_{\mu'} - p_0(\mu')Y_0 - \tilde{Y}_{\mu',\mu} \end{pmatrix} \tag{3.34}$$

を得るが、$\tilde{Y}_{\mu',\mu} \geq 0$ と、式 (3.27) の下で $p_1(\mu)/p_2(\mu) - p_1(\mu')/p_2(\mu') = 2/\mu - 2/\mu' > 0$ に注意すると、

$$\begin{cases} Y_\mu^{\mathrm{mutli}} \leq \dfrac{\mu}{\mu' - \mu}\left(\dfrac{\mu e^{-\mu}}{\mu' e^{-\mu'}}Y_{\mu'} - Y_\mu\right) + \dfrac{\mu e^{-\mu}}{\mu'}Y_0, \\ y_1 \geq \dfrac{1}{\mu' - \mu}\left(\dfrac{\mu'}{\mu e^{-\mu}}Y_\mu - \dfrac{\mu}{\mu' e^{-\mu'}}Y_{\mu'}\right) - \dfrac{\mu' + \mu}{\mu\mu'}Y_0 \end{cases} \tag{3.35}$$

が得られる。これが、Wang が導いた評価式である [37, 38]。

式 (3.33) は、$y_1 \geq 0$ であるという最低限の知識で式 (3.32) から導かれた。ところが、2 種類のデコイ・パルスの情報を活用すると、式 (3.35) の第 2 式のように、y_1 の下限が底上げできるのである。その結果、Y_μ^{multi} の範囲を式 (3.33) よりもきつく評価することができるのである。

Wangの上限(3.35)が、Hwangの(3.21)に比べてどれほど良い評価を与えているかを、

$$\Delta = \frac{Y_\mu^{\mathrm{multi}}}{Y_\mu} \tag{3.36}$$

の量を通じて見てみよう。Eveの攻撃が存在せず、信号パルスの伝送効率がηで、暗計数率y_0を考慮に入れれると、y_nは式(3.23)の代わりに

$$y_n = y_0 + 1 - (1-\eta)^n \tag{3.37}$$

で与えられ、収率Y_μは、式(3.24)の代わりに

$$Y_\mu = y_0 + 1 - e^{-\eta\mu}, \tag{3.38a}$$

$$Y_\mu^{\mathrm{multi}} = Y_\mu - y_0 e^{-\mu} - (y_0+\eta)\mu e^{-\mu} \tag{3.38b}$$

となる。Hwangが与えるΔの上限は、式(3.21)の右辺より、

$$\Delta_{\mathrm{H}} = \frac{\mu^2 e^{-\mu}}{\mu'^2 e^{-\mu'}} \frac{Y_{\mu'}}{Y_\mu}. \tag{3.39}$$

これに対し、Wangが与えるΔの上限は、式(3.35)の右辺より、

$$\Delta_{\mathrm{W}} = \frac{\mu}{\mu'-\mu}\left(\frac{\mu e^{-\mu}}{\mu' e^{-\mu'}}\frac{Y_{\mu'}}{Y_\mu} - 1\right) + \frac{\mu e^{-\mu}}{\mu'}\frac{Y_0}{Y_\mu} \tag{3.40}$$

だ。これらΔ, Δ_{H}, Δ_{W}を式(3.38)を用いて計算した結果を、図3.1に示す。HwangのΔ_{H}は、$\mu' \simeq 1$で最適な評価を与え、WangのΔ_{W}は、μ'が小さいほど良い。

図3.1に見られるΔ_{H}とΔ_{W}の差が、安全性評価にどれほどの影響があるかを知ろうと思ったら、最終的に生成可能な安全鍵の生成率を評価するとよいであろう。Wangは、式(3.36)で定義したΔを式(3.1)に当てはめることで、安全な鍵の生成率を評価することを提案した。デコイ法に拠らない従来の評価やHwangの評価に対して、Wangの評価がどれほど長距離の鍵配送の安全性を保証するかを定量的に議論できる。これに対して、Loらは、式(3.1)を用いるのよりも厳しい評価式を提示し、さらに長距離の鍵配送の安全性が保証できることを示した[39–42]。次節で、そのLoらの議論[39–42]を整理しよう。

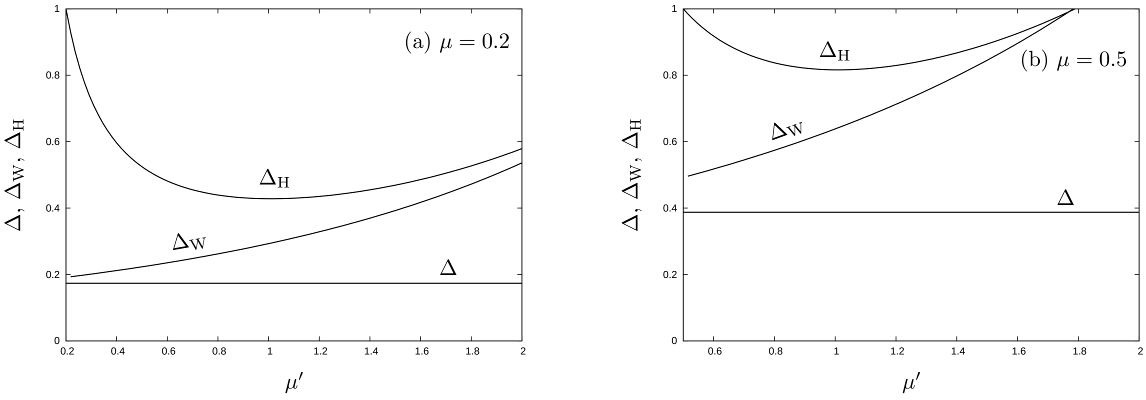

図 3.1: Eve の攻撃が存在せず、信号パルスの伝送効率が $\eta = 10^{-4}$ で暗計数率が $y_0 = 10^{-6}$ 場合の Δ と、Hwang、Wang が与えるその上限 $\Delta_{\rm H}, \Delta_{\rm W}$。(a) は、$\mu = 0.2$ の場合。(b) は、$\mu = 0.5$ の場合。

3.3.3　Lo らによる一般的枠組みと最適化

Wang が安全な暗号鍵の最終生成率を式 (3.1) で評価することを提案した [37, 38] のに対し、Lo らは、

$$R \geq q\{-Y_\mu f(E_\mu)H_2(E_\mu) + p_1(\mu)y_1[1 - H_2(e_1)]\} \tag{3.41}$$

を用いることで、より正確な評価が可能であることを指摘した [39–42]。ここで、$f(e)$ (>1) は、エラー訂正プロトコルが一般に最適な効率を達成できないことを盛り込む関数で、式 (3.1) では $f(E_\mu) = 1$ とされていた。重要なのは、式 (3.41) には、式 (3.1) には見られない e_1 (単一光子パルスに乗せられたビットにビット・エラーが生じる割合) が含まれていることである。デコイ・パルスを用いない従来の議論 [31,32] では、y_1 や e_1 は実際には測定ができない量なので、それらを緩く評価して、式 (3.1) としていた。Wang の提案は、デコイ法で y_1 の (すなわち Δ の) 評価精度が向上することで、式 (3.1) を用いた評価がより正確になる、ということであるが、Lo たちは、デコイ法によれば e_1 もきつく評価できるので、さらに高い精度が達成できることを指摘したのだ [39–42]。

さらに、Lo らは、デコイ・パルスの種類を限定しない一般的枠組みを提示し、パラメータの最適化を実行、現実的な実験パラメータを用いて、安全な暗号鍵配送を保証できる配送距離の上限を評価した [39–42]。この節では、これら Lo たちの議論を紹介

しよう。

Lo らは、Hwang のデコイ法のアイデアを拡張し、(1 種類ではなく) 複数種類のデコイ・パルスを用いることを考えた。メインの信号パルスの強度を μ とし、デコイ・パルス用の光源強度を $\nu_1, \nu_2, \ldots$ とする。我々は、それぞれのパルスの収率 $Y_\mu, Y_{\nu_1}, Y_{\nu_2}, \ldots$ と、ビット・エラー率 $E_\mu, E_{\nu_1}, E_{\nu_2}, \ldots$ を測定から知ることができる。それらは、以下の式で与えられる:

$$Y_\mu = \sum_{n=0}^{\infty} p_n(\mu) y_n, \qquad E_\mu Y_\mu = \sum_{n=0}^{\infty} p_n(\mu) e_n y_n, \tag{3.42a}$$

$$Y_{\nu_1} = \sum_{n=0}^{\infty} p_n(\nu_1) y_n, \qquad E_{\nu_1} Y_{\nu_1} = \sum_{n=0}^{\infty} p_n(\nu_1) e_n y_n, \tag{3.42b}$$

$$Y_{\nu_2} = \sum_{n=0}^{\infty} p_n(\nu_2) y_n, \qquad E_{\nu_2} Y_{\nu_2} = \sum_{n=0}^{\infty} p_n(\nu_2) e_n y_n, \tag{3.42c}$$

$$\vdots \qquad \qquad \vdots \tag{3.42d}$$

e_n は、n 光子パルスに乗せられたビットにエラーが生じるレートである。

結局、問題は、これらの測定可能量 $Y_\mu, Y_{\nu_1}, Y_{\nu_2}, \ldots, E_\mu, E_{\nu_1}, E_{\nu_2}, \ldots$ から、式 (3.41) で必要とされる y_1 と e_1 をいかに精度良く評価するかということに集約される。原理的には、無限種類のデコイ・パルスを用いれば、式 (3.42) の連立方程式を解くことでその目標は達成される [39–42]。これが、デコイ法の真髄だ。

ただし、実際には、無限種類のデコイ・パルスを準備し、それらすべての収率とエラー率を測定するのは現実的とはいえない。そこで、少数種類のデコイ・パルスを用いるプロトコルで y_1 と e_1 を評価することを考えよう。それでも依然として、比較的高い精度の評価が可能である。

2 デコイ・プロトコル 2 種類のデコイ・パルスを用いる場合で、y_1 と e_1 の評価を具体的に実行してみよう。まずは、前節で議論した Wang の 2 デコイ・プロトコルと違って、2 種類のデコイ・パルスともに真空でない場合を考える。前節の式 (3.28) に習い、

$$\mu > \nu_1 \geq \nu_2 \geq 0 \tag{3.43}$$

として、凸分解しよう:

$$\begin{cases} \rho_{\nu_2} = p_0(\nu_2)|0\rangle\langle 0| + p_1(\nu_2)|1\rangle\langle 1| + \rho_{\nu_2}^{\text{multi}}, \\ \rho_{\nu_1} = p_0(\nu_1)|0\rangle\langle 0| + p_1(\nu_1)|1\rangle\langle 1| + \dfrac{p_2(\nu_1)}{p_2(\nu_2)}\rho_{\nu_2}^{\text{multi}} + \tilde{\rho}_{\nu_1,\nu_2}, \\ \rho_{\mu} = p_0(\mu)|0\rangle\langle 0| + p_1(\mu)|1\rangle\langle 1| + \dfrac{p_2(\mu)}{p_2(\nu_1)}\left(\dfrac{p_2(\nu_1)}{p_2(\nu_2)}\rho_{\nu_2}^{\text{multi}} + \tilde{\rho}_{\nu_1,\nu_2}\right) + \tilde{\rho}_{\mu,\nu_1}. \end{cases} \tag{3.44}$$

これに対応して、

$$\begin{cases} Y_{\nu_2} = p_0(\nu_2)y_0 + p_1(\nu_2)y_1 + Y_{\nu_2}^{\text{multi}}, \\ Y_{\nu_1} = p_0(\nu_1)y_0 + p_1(\nu_1)y_1 + \dfrac{p_2(\nu_1)}{p_2(\nu_2)}Y_{\nu_2}^{\text{multi}} + \tilde{Y}_{\nu_1,\nu_2}, \\ Y_{\mu} = p_0(\mu)y_0 + p_1(\mu)y_1 + \dfrac{p_2(\mu)}{p_2(\nu_2)}Y_{\nu_2}^{\text{multi}} + \dfrac{p_2(\mu)}{p_2(\nu_1)}\tilde{Y}_{\nu_1,\nu_2} + \tilde{Y}_{\mu,\nu_1} \end{cases} \tag{3.45}$$

と書くと、$\tilde{Y}_{\nu_1,\nu_2}, \tilde{Y}_{\mu,\nu_1} \geq 0$ だ。

$$\begin{pmatrix} 1 & \nu_2 & 1 \\ 1 & \nu_1 & \nu_1^2/\nu_2^2 \\ 1 & \mu & \mu^2/\nu_2^2 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ e^{\nu_2}Y_{\nu_2}^{\text{multi}} \end{pmatrix} = \begin{pmatrix} e^{\nu_2}Y_{\nu_2} \\ e^{\nu_1}(Y_{\nu_1} - \tilde{Y}_{\nu_1,\nu_2}) \\ e^{\mu}(Y_{\mu} - \tilde{Y}_{\mu,\nu_1}) - (\mu^2/\nu_1^2)e^{\nu_1}\tilde{Y}_{\nu_1,\nu_2} \end{pmatrix} \tag{3.46}$$

と整理して、これを解くと、

$$\begin{aligned} \begin{pmatrix} y_0 \\ y_1 \\ e^{\nu_2}Y_{\nu_2}^{\text{multi}} \end{pmatrix} &= \frac{1}{(\mu-\nu_1)(\mu-\nu_2)(\nu_1-\nu_2)} \begin{pmatrix} \mu\nu_1 & -\mu\nu_2 & \nu_1\nu_2 \\ -(\mu+\nu_1) & \mu+\nu_2 & -(\nu_1+\nu_2) \\ \nu_2^2 & -\nu_2^2 & \nu_2^2 \end{pmatrix} \\ &\quad \times \begin{pmatrix} (\mu-\nu_1)e^{\nu_2}Y_{\nu_2} \\ (\mu-\nu_2)e^{\nu_1}(Y_{\nu_1} - \tilde{Y}_{\nu_1,\nu_2}) \\ (\nu_1-\nu_2)[e^{\mu}(Y_{\mu} - \tilde{Y}_{\mu,\nu_1}) - (\mu^2/\nu_1^2)e^{\nu_1}\tilde{Y}_{\nu_1,\nu_2}] \end{pmatrix} \end{aligned} \tag{3.47}$$

であり、

$$\begin{aligned} y_0 &= \frac{1}{(\mu-\nu_1)(\mu-\nu_2)(\nu_1-\nu_2)} \\ &\quad \times \Big[\nu_1\nu_2(\nu_1-\nu_2)e^{\mu}Y_{\mu} - \mu\nu_2(\mu-\nu_2)e^{\nu_1}Y_{\nu_1} + \mu\nu_1(\mu-\nu_1)e^{\nu_2}Y_{\nu_2} - \nu_1\nu_2C_0\Big], \end{aligned} \tag{3.48a}$$

$$\begin{aligned} y_1 = &\frac{1}{(\mu-\nu_1)(\mu-\nu_2)(\nu_1-\nu_2)} \\ &\times \Big[(\mu^2-\nu_2^2)e^{\nu_1}Y_{\nu_1} - (\nu_1^2-\nu_2^2)e^{\mu}Y_{\mu} - (\mu^2-\nu_1^2)e^{\nu_2}Y_{\nu_2} + C_1\Big], \end{aligned} \tag{3.48b}$$

$$\begin{aligned} e^{\nu_2}Y_{\nu_2}^{\mathrm{multi}} = &\frac{\nu_2^2}{(\mu-\nu_1)(\mu-\nu_2)(\nu_1-\nu_2)} \\ &\times \Big[(\nu_1-\nu_2)e^{\mu}Y_{\mu} - (\mu-\nu_2)e^{\nu_1}Y_{\nu_1} + (\mu-\nu_1)e^{\nu_2}Y_{\nu_2} - D\Big] \end{aligned} \tag{3.48c}$$

を得る。ここで、

$$\begin{cases} C_0 = (\nu_1-\nu_2)e^{\mu}\tilde{Y}_{\mu,\nu_1} - (\mu\nu_2/\nu_1^2)(\mu-\nu_1)e^{\nu_1}\tilde{Y}_{\nu_1,\nu_2}, \\ C_1 = (\nu_1^2-\nu_2^2)e^{\mu}\tilde{Y}_{\mu,\nu_1} - (\nu_2^2/\nu_1^2)(\mu^2-\nu_1^2)e^{\nu_1}\tilde{Y}_{\nu_1,\nu_2}, \\ D = (\nu_1-\nu_2)e^{\mu}\tilde{Y}_{\mu,\nu_1} + (1/\nu_1^2)(\mu-\nu_1)(\mu\nu_1-\mu\nu_2-\nu_1\nu_2)e^{\nu_1}\tilde{Y}_{\nu_1,\nu_2} \end{cases} \tag{3.49}$$

であるが、式 (3.29)–(3.30) に注意すると、

$$\begin{aligned} \tilde{Y}_{\mu,\nu_1} &= \mu^2 e^{-\mu}\sum_{n=3}^{\infty}\frac{1}{n!}(\mu^{n-2}-\nu_1^{n-2})y_n \\ &= \mu^2(\mu-\nu_1)e^{-\mu}\sum_{n=3}^{\infty}\frac{1}{n!}(\mu^{n-3}+\mu^{n-4}\nu_1+\mu^{n-5}\nu_1^2+\cdots+\mu\nu_1^{n-4}+\nu_1^{n-3})y_n \end{aligned} \tag{3.50}$$

であるから、

$$\begin{aligned} C_0 &= \mu(\mu-\nu_1)(\nu_1-\nu_2)\sum_{n=3}^{\infty}\frac{y_n}{n!}\Big[\mu(\mu^{n-3}+\mu^{n-4}\nu_1+\cdots+\mu\nu_1^{n-4}+\nu_1^{n-3}) \\ &\qquad\qquad - \nu_2(\nu_2^{n-3}+\nu_2^{n-4}\nu_1+\cdots+\nu_2\nu_1^{n-4}+\nu_1^{n-3})\Big] \\ &\geq \mu(\mu-\nu_1)(\nu_1-\nu_2)\sum_{n=3}^{\infty}\frac{y_n}{n!}(\mu-\nu_2)(\mu^{n-3}+\mu^{n-4}\nu_1+\cdots+\mu\nu_1^{n-4}+\nu_1^{n-3}) \geq 0, \end{aligned} \tag{3.51a}$$

$$
\begin{aligned}
C_1 &= (\mu-\nu_1)(\nu_1-\nu_2)\sum_{n=3}^{\infty}\frac{y_n}{n!}\Big[\mu^2(\nu_1+\nu_2)(\mu^{n-3}+\mu^{n-4}\nu_1+\cdots+\mu\nu_1^{n-4}+\nu_1^{n-3})\\
&\qquad\qquad -\nu_2^2(\mu+\nu_1)(\nu_2^{n-3}+\nu_2^{n-4}\nu_1+\cdots+\nu_2\nu_1^{n-4}+\nu_1^{n-3})\Big]\\
&\geq (\mu-\nu_1)(\nu_1-\nu_2)\sum_{n=3}^{\infty}\frac{y_n}{n!}[\mu^2(\nu_1+\nu_2)-\nu_2^2(\mu+\nu_1)]\\
&\qquad\qquad \times(\mu^{n-3}+\mu^{n-4}\nu_1+\cdots+\mu\nu_1^{n-4}+\nu_1^{n-3})\geq 0,
\end{aligned}
\tag{3.51b}
$$

$$
\begin{aligned}
D &= (\mu-\nu_1)(\nu_1-\nu_2)\sum_{n=3}^{\infty}\frac{y_n}{n!}\Big[\mu^2(\mu^{n-3}+\mu^{n-4}\nu_1+\cdots+\mu\nu_1^{n-4}+\nu_1^{n-3})\\
&\qquad +(\mu\nu_1-\mu\nu_2-\nu_1\nu_2)(\nu_2^{n-3}+\nu_2^{n-4}\nu_1+\cdots+\nu_2\nu_1^{n-4}+\nu_1^{n-3})\Big]\\
&= (\mu-\nu_1)(\nu_1-\nu_2)\sum_{n=3}^{\infty}\frac{y_n}{n!}\Big[\mu^2(\mu^{n-3}+\mu^{n-4}\nu_1+\cdots+\mu\nu_1^{n-4}+\nu_1^{n-3})\\
&\qquad +[(\mu+\nu_1)(\mu-\nu_2)-\mu^2](\nu_2^{n-3}+\nu_2^{n-4}\nu_1+\cdots+\nu_2\nu_1^{n-4}+\nu_1^{n-3})\Big]\geq 0.
\end{aligned}
\tag{3.51c}
$$

したがって、

$$
\begin{aligned}
y_0 &\leq \frac{1}{(\mu-\nu_1)(\mu-\nu_2)(\nu_1-\nu_2)}\\
&\quad\times\Big[\nu_1\nu_2(\nu_1-\nu_2)e^{\mu}Y_\mu-\mu\nu_2(\mu-\nu_2)e^{\nu_1}Y_{\nu_1}+\mu\nu_1(\mu-\nu_1)e^{\nu_2}Y_{\nu_2}\Big],
\end{aligned}
\tag{3.52a}
$$

$$
\begin{aligned}
y_1 &\geq \frac{1}{(\mu-\nu_1)(\mu-\nu_2)(\nu_1-\nu_2)}\\
&\quad\times\Big[(\mu^2-\nu_2^2)e^{\nu_1}Y_{\nu_1}-(\nu_1^2-\nu_2^2)e^{\mu}Y_\mu-(\mu^2-\nu_1^2)e^{\nu_2}Y_{\nu_2}\Big],
\end{aligned}
\tag{3.52b}
$$

$$
\begin{aligned}
e^{\nu_2}Y_{\nu_2}^{\mathrm{multi}} &\leq \frac{\nu_2^2}{(\mu-\nu_1)(\mu-\nu_2)(\nu_1-\nu_2)}\\
&\quad\times\Big[(\nu_1-\nu_2)e^{\mu}Y_\mu-(\mu-\nu_2)e^{\nu_1}Y_{\nu_1}+(\mu-\nu_1)e^{\nu_2}Y_{\nu_2}\Big]
\end{aligned}
\tag{3.52c}
$$

の評価式が得られる。

あとは、e_1 を評価できればよい。式 (3.42) より、

$$\begin{cases} e^{\mu}E_{\mu}Y_{\mu} = e_0y_0 + \mu e_1y_1 + \sum_{n=2}^{\infty}\dfrac{\mu^n}{n!}e_ny_n, \\ e^{\nu_1}E_{\nu_1}Y_{\nu_1} = e_0y_0 + \nu_1e_1y_1 + \sum_{n=2}^{\infty}\dfrac{\nu_1^n}{n!}e_ny_n, \\ e^{\nu_2}E_{\nu_2}Y_{\nu_2} = e_0y_0 + \nu_2e_1y_1 + \sum_{n=2}^{\infty}\dfrac{\nu_2^n}{n!}e_ny_n \end{cases} \tag{3.53}$$

であるから、例えば、第 2–3 式から

$$e^{\nu_1}E_{\nu_1}Y_{\nu_1} - e^{\nu_2}E_{\nu_2}Y_{\nu_2} = (\nu_1-\nu_2)e_1y_1 + \sum_{n=2}^{\infty}\frac{(\nu_1^n-\nu_2^n)}{n!}e_ny_n \geq (\nu_1-\nu_2)e_1y_1. \tag{3.54}$$

したがって、

$$e_1 \leq \frac{e^{\nu_1}E_{\nu_1}Y_{\nu_1} - e^{\nu_2}E_{\nu_2}Y_{\nu_2}}{(\nu_1-\nu_2)y_1} \leq \frac{e^{\nu_1}E_{\nu_1}Y_{\nu_1} - e^{\nu_2}E_{\nu_2}Y_{\nu_2}}{(\nu_1-\nu_2)y_1^{\mathrm{L}}} \tag{3.55}$$

と評価すればよい。y_1^{L} は、y_1 の下限値 [式 (3.52b) の右辺] である。他に 2 通りの組み合わせが考えられるので、それらを総合して、

$$e_1 \leq \min\left(\frac{e^{\nu_1}E_{\nu_1}Y_{\nu_1} - e^{\nu_2}E_{\nu_2}Y_{\nu_2}}{(\nu_1-\nu_2)y_1^{\mathrm{L}}}, \frac{e^{\mu}E_{\mu}Y_{\mu} - e^{\nu_1}E_{\nu_1}Y_{\nu_1}}{(\mu-\nu_1)y_1^{\mathrm{L}}}, \frac{e^{\mu}E_{\mu}Y_{\mu} - e^{\nu_2}E_{\nu_2}Y_{\nu_2}}{(\mu-\nu_2)y_1^{\mathrm{L}}}\right) \tag{3.56}$$

が得られる。

こうして得られた y_1 の下限 (3.52b) と e_1 の上限 (3.56) を鍵生成率の評価式 (3.41) に代入すればよい。$R \geq 0$ であれば、安全な鍵配送が保証される。

真空デコイ　ここで、

$$\nu_1, \nu_2 \to 0 \tag{3.57}$$

としてみよう。式 (3.52) は、

$$y_0 \leq Y_0 = y_0, \qquad y_1 \geq Y_0 + \left.\frac{\partial Y_{\nu_1}}{\partial \nu_1}\right|_{\nu_1=0} = y_1, \qquad e^{\nu_2}Y_{\nu_2}^{\mathrm{multi}} \leq 0, \tag{3.58}$$

e_1 の上限 (3.56) は、

$$e_1 \leq \min\left(e_1, \frac{\sum_{n=1}^{\infty}(\mu^n/n!)e_ny_n}{\mu y_1}\right) = e_1 \tag{3.59}$$

となる。つまり、それぞれの評価式が、マージンなく正確な値を与えている。すなわち、式 (3.57) の極限が、最適なデコイ法を与えるのである。

しかし、現実的には、2 種類のデコイ・パルスとしてともに真空を採用することはできない。したがって、一方のみを真空にした

$$\nu_1 > 0, \qquad \nu_2 = 0 \tag{3.60}$$

が、2 デコイ・プロトコルでは最適だ。これこそ、前節で議論した Wang のプロトコル [37] にほかならない。

式 (3.52) で $\nu_2 \to 0$, $\nu_1 \to \nu\,(> 0)$ とすると、

$$y_0 \leq Y_0 = y_0, \tag{3.61a}$$

$$y_1 \geq \frac{1}{\mu - \nu}\left(\frac{\mu}{\nu e^{-\nu}} Y_\nu - \frac{\nu}{\mu e^{-\mu}} Y_\mu\right) - \frac{\mu + \nu}{\mu\nu} Y_0. \tag{3.61b}$$

これは、前節で導いた評価式 (3.35) を再現している。さらに、この結果を利用すると、式 (3.36) で定義される Δ は

$$\begin{aligned}\Delta &= \frac{Y_\nu - e^{-\nu} y_0 - \nu e^{-\nu} y_1}{Y_\nu} \\ &\leq \frac{Y_\nu - e^{-\nu} Y_0 - \nu e^{-\nu}\left[\frac{1}{\mu-\nu}\left(\frac{\mu}{\nu e^{-\nu}} Y_\nu - \frac{\nu}{\mu e^{-\mu}} Y_\mu\right) - \frac{\mu+\nu}{\mu\nu} Y_0\right]}{Y_\nu} \\ &= \frac{\nu}{\mu - \nu}\left(\frac{\nu e^{-\nu}}{\mu e^{-\mu}} \frac{Y_\mu}{Y_\nu} - 1\right) + \frac{\nu e^{-\nu}}{\mu} \frac{Y_0}{Y_\nu}\end{aligned} \tag{3.62}$$

と評価され、これは、Wang の評価式 (3.40) にほかならない。e_1 は、式 (3.56) から、

$$e_1 \leq \min\left(\frac{e^\nu E_\nu Y_\nu - e_0 Y_0}{\nu y_1^{\mathrm{L}}}, \frac{e^\mu E_\mu Y_\mu - e^\nu E_\nu Y_\nu}{(\mu - \nu) y_1^{\mathrm{L}}}, \frac{e^\mu E_\mu Y_\mu - e_0 Y_0}{\mu y_1^{\mathrm{L}}}\right) \tag{3.63}$$

となる。

1 デコイ・プロトコル　Lo らは、さらに、最も簡単な場合として、1 デコイ・プロトコルを提示した [42]。式 (3.31), (3.45) に戻って、

$$\begin{cases} e^\nu Y_\nu = y_0 + \nu y_1 + e^\nu Y_\nu^{\mathrm{multi}}, \\ e^\mu Y_\mu = y_0 + \mu y_1 + \dfrac{\mu^2}{\nu^2} e^\nu Y_\nu^{\mathrm{multi}} + e^\mu \tilde{Y}_{\mu,\nu} \end{cases} \tag{3.64}$$

が、このプロトコルで測定できる量である。これを、これまでのように y_1 と Y_ν^{multi} に関して解きたいのだが、今回は y_0 に関する情報がない。そこで、

$$\begin{cases} e^\nu E_\nu Y_\nu = e_0 y_0 + \nu e_1 y_1 + \displaystyle\sum_{n=2}^{\infty} \frac{\nu^n}{n!} e_n y_n, \\ e^\mu E_\mu Y_\mu = e_0 y_0 + \mu e_1 y_1 + \displaystyle\sum_{n=2}^{\infty} \frac{\mu^n}{n!} e_n y_n \end{cases} \tag{3.65}$$

で補おう。

これまでと同様にして、

$$\begin{cases} y_1 \geq \dfrac{1}{\mu - \nu} \left(\dfrac{\mu}{\nu e^{-\nu}} Y_\nu - \dfrac{\nu}{\mu e^{-\mu}} Y_\mu \right) - \dfrac{\mu + \nu}{\mu\nu} y_0, \\ Y_\nu^{\mathrm{mutli}} \leq \dfrac{\nu}{\mu - \nu} \left(\dfrac{\nu e^{-\nu}}{\mu e^{-\mu}} Y_\mu - Y_\nu \right) + \dfrac{\nu e^{-\nu}}{\mu} y_0. \end{cases} \tag{3.66}$$

式 (3.65) より、

$$y_0 \leq \min\left(\frac{e^\mu E_\mu Y_\mu}{e_0}, \frac{e^\nu E_\nu Y_\nu}{e_0} \right) \tag{3.67}$$

なので、この右辺を y_0^{U} として、

$$\begin{cases} y_1 \geq \dfrac{1}{\mu - \nu} \left(\dfrac{\mu}{\nu e^{-\nu}} Y_\nu - \dfrac{\nu}{\mu e^{-\mu}} Y_\mu \right) - \dfrac{\mu + \nu}{\mu\nu} y_0^{\mathrm{U}}, \\ Y_\nu^{\mathrm{mutli}} \leq \dfrac{\nu}{\mu - \nu} \left(\dfrac{\nu e^{-\nu}}{\mu e^{-\mu}} Y_\mu - Y_\nu \right) + \dfrac{\nu e^{-\nu}}{\mu} y_0^{\mathrm{U}}. \end{cases} \tag{3.68}$$

さらに、この第 1 式の右辺を y_1^{L} として、

$$e_1 \leq \min\left(\frac{e^\mu E_\mu Y_\mu}{\mu y_1^{\mathrm{L}}}, \frac{e^\nu E_\nu Y_\nu}{\mu y_1^{\mathrm{L}}} \right). \tag{3.69}$$

e_0 は真空のビットエラー率であるが、バックグラウンドがランダムであれば、それは

$$e_0 = \frac{1}{2} \tag{3.70}$$

で良いであろう。

この 1 デコイ・プロトコルは、決して最適な評価を与えられるものではないが、実装するのには最もシンプルであり、実際、Lo らによる最初の実験は、この 1 デコイ・プロトコルであった [46, 47]。

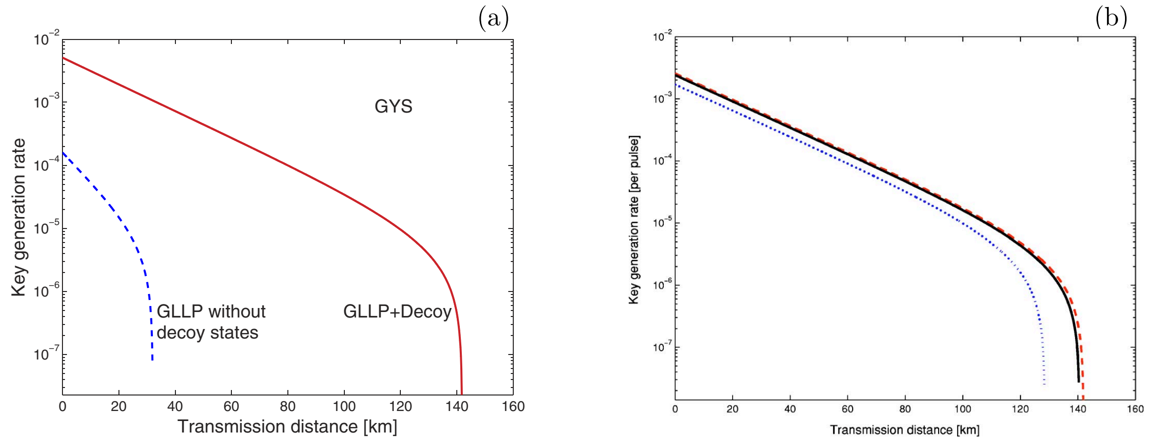

図 3.2: 文献 [11] の実験設定を元に評価された鍵生成率 R。(a) デコイ法を用いない、式 (3.1) による評価 (破線) と、無限種類のデコイ・パルスを用い、式 (3.41) で評価した場合 (実線) の比較。従来の評価では 30 km 程度しか保証できなかった安全性が、デコイ法を用いると 140 km にまで伸びる。文献 [41] より転載。(b) 無限種類のデコイ・パルスを用い、式 (3.41) で評価した場合 (破線)、2 デコイ・プロトコル ($\mu = 0.48$, $\nu_1 = 0.05$, $\nu_2 = 0$) を利用し、式 (3.41) で評価した場合 (実線)、及び、Wang が提案した、2 デコイ・プロトコルと式 (3.1) を組み合わせる評価 (点線) の比較。Lo らの評価 (140 km) は、Wang の評価 (128.55 km) よりも長距離を保証する。文献 [42] より転載。

3.3.4　鍵配送距離の評価

Lo らは、文献 [11] の実験設定を参考に、デコイ法が保証する安全な鍵配送距離を評価してみせた [41, 42]。式 (3.41) に、デコイ法で評価される y_1 や e_1 を代入し、安全鍵の生成率 R を見る。距離に応じて R は低下するが、それが $R = 0$ を下回ってしまうと、それ以上の長距離の鍵配送は、安全性が保証されないことを意味する。図 3.2 は、文献 [41, 42] から転載したグラフである。従来の評価に比べ、安全性が保証される距離が劇的に伸びている点が見て取れるであろう。従来の、30 km 程度までしか安全性が保証できなかった光源で、100 km を超える鍵配送が可能というのである。このことで、デコイ法は一躍注目の鍵配送プロトコルとなった。

3.3.5　デコイ法による量子鍵配送実験の動向

デコイ法は、単一光子源のような特殊な光源を必要としないなど、その実装のしやすさが大きな売りである。早速、実験的研究も進められており、昨年から今年にかけ

表 3.1: デコイ法による量子鍵配送実験の動向。昨年から今年にかけて、6 グループの実験が発表されている。1 デコイ・プロトコル、2 デコイ・プロトコル、及び、3 デコイ・プロトコルが採用されている。光ファイバー・ケーブルを伝送路に使用する実験のみならず、大気中にレーザー・パルスを飛ばして鍵を送る実験も行われている。( ) 内の数値は、式 (3.1) や (3.41) を利用して評価した、理論上に達成可能な数値。

	光源強度			距離	伝送路	最終鍵生成率
	μ	ν_1	ν_2	km		bit/s
Zhao *et al.* [46,47]*	0.80	0.120	——	15(59)	fiber	(165)
Yuan *et al.* [51]	0425	0.204	——	25	fiber	(5,510)
Zhao *et al.* [47]*	0.55	0.152	0	60(68)	fiber	———
Peng *et al.* [50]	0.2	0.6	0	75	fiber	(11.668)
Rosenberg *et al.* [48]	0.487	0.063 9	0.001 05	85	fiber	28.2
Rosenberg *et al.* [48]	0.297	0.099	0.002 57	100(107)	fiber	14.5
Peng *et al.* [50]**	0.2	0.6	0	102	fiber	(8.090)
Schmitt-Manderbach *et al.* [49]	0.27	0.39	0	144	free space	12.8
JST-NEC [53]	(3 デコイ・プロトコル)			20	fiber	2,000

*two-way protocol
**two-detector scheme

て、立て続けに報告がなされている [46–51, 53]。基本的な道具立ては、従来から弱コヒーレント光を用いて行われてきた鍵配送実験とほぼ同様である。新たに導入すべき技術は、発生するレーザー・パルスの光強度を、信号や複数種類のデコイ用に逐一切り替える装置だ。

表 3.1 に、これまでに報告された実験をまとめた。これまでのところ、6 つのグループが発表を行っている。最初の実験は、トロントの Lo らのグループによって、1 デコイ・プロトコルで行われた [46, 47]。1 デコイ・プロトコルは、複数のデコイを用いるプロトコルに比べてその性能は低い [式 (3.68)–(3.69) が与える評価が甘い] ものの、実験は容易だ。ケンブリッジの Yuan らの実験 [51] も 1 デコイ・プロトコルのものだが、主流は真空パルスを含む 2 デコイ・プロトコルとなっている。日本のグループは、最適性の観点から、3 デコイ・プロトコルを採用している [53]。

伝送路は、光ファイバー・ケーブルを使用したものがほとんどであるが、大気中を直接飛ばす実験も、ヨーロッパの SECOQC プロジェクトによって既に行われている。現在の最長距離は、その 144 km となっている。

最終的な暗号鍵の生成レートに関しては、実際には誤り訂正と秘密増幅の作業まで

は行わず、実験で測定した収率から、デコイ法が与える評価式 [例えば、式 (3.61b) と (3.63)] で y_1 の下限や e_1 の上限を評価し、式 (3.1) や (3.41) を通じて鍵生成率 R の下限を見積もっている場合 [46, 47, 50, 51] と、誤り訂正と秘密増幅まで実行して, 実際に鍵を生成してみせている場合 [48, 49, 53] とがあるようだが、詳細に関しては、文献だけからは定かではない。

日本のグループは、式 (3.1) や (3.41) が、無限長のデータを有する場合の漸近的な評価式に過ぎないことを指摘している [52, 53]。現実には有限長のデータから誤り訂正と秘密増幅を行うわけであり、厳密には、式 (3.1) や (3.41) とは異なる評価式が必要だ。さもないと、安全性が保証できているとはいいがたい。日本のグループは、この問題の解決を図り、有限長のデータを想定するとともに、推定の際の統計誤差まで考慮に入れて、デコイ法の理論を再構成した [52]。さらに、その理論の基礎の上で誤り訂正と秘密増幅を行うシステムを構築し、最終鍵生成まで一貫した形でデコイ法の実験を行った [53]。また、その理論は、任意の種類数のデコイ・パルスに対して評価式を与えており、従来の議論 [36–43] のように、1 デコイや 2 デコイなどと数を指定して個別に議論したものを発展させた形になっている。その結果、何種類のデコイ・パルスを利用するのが最適かを議論することが可能であり、3 デコイ・プロトコルを最適なものとして採用している。

以上、最近大きな注目を集めているデコイ法による鍵配送プロトコルの紹介と、実験の現状をまとめた。デコイ法は、安全な鍵配送システムの構築に向けて要請される厳しい技術的要件を劇的に緩和し、実用化に向けての機運を大きく盛り上げるものとなっている。今後、産業界を巻き込んで、実用面に力点を置いて、精力的に研究・開発が進められることであろう。

関連図書

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[2] A. K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Physical Review Letters **67**, 661 (1991).

[3] C. H. Bennett, *Quantum Cryptography Using Any Two Nonorthogonal States*, Physical Review Letters **68**, 3121 (1992).

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum Cryptography*, Reviews of Modern Physics **74**, 145 (2002).

[6] D. Mayers, *Unconditional Security in Quantum Cryptography*, Journal of the Association for Computing Machinery **48**, 351 (2001).

[7] P. W. Shor and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Physical Review Letters **85**, 441 (2000).

[8] H.-K. Lo and H. F. Chau, *Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances*, Science **283**, 2050 (1999).

[9] B. Huttner and A. K. Ekert, *Information Gain in Quantum Eavesdropping*, Journal of Modern Optics **41**, 2455 (1994).

[10] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels*, Physical Review Letters **77**, 2818 (1996).

[11] C. Gobby, Z. L. Yuan, and A. J. Shields, *Quantum Key Distribution over 122 km of Standard Telecom Fiber*, Applied Physics Letters **84**, 3762 (2004).

[12] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, *Single-Photon Interference over 150 km Transmission Using Silica-Based Integrated-Optic Interferometers for Quantum Cryptography*, Japanese Journal of Applied Physics **43**, L1217 (2004).

[13] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, *Quantum Key Distribution over 67 km with a Plug&Play System*, New Journal of Physics **4**, 41 (2002).

[14] E. Klarreich, *Quantum Cryptography: Can You Keep a Secret?*, Nature (London) **418**, 270 (2002).

[15] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, *Long-Distance Quantum Key Distribution in Optical Fiber*, New Journal of Physics **8**, 193 (2006).

[16] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, *Practical Free-Space Quantum Key Distribution over 10 km in Daylight and at Night*, New Journal of Physics **4**, 43 (2002).

[17] Ch. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, *Quantum Cryptography: A Step towards Global Key Distribution*, Nature (London) **419**, 450 (2002).

[18] H. Weier, T. Schmitt-Manderbach, N. Regner, Ch. Kurtsiefer, and H. Weinfurter, *Free Space Quantum Key Distribution: Towards a Real Life Application*, Fortschr. Phys. **54**, 840 (2006).

[19] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, *Ground to Satellite Secure Key Exchange Using Quantum Cryptography*, New Journal of Physics **4**, 82 (2002).

[20] id Quantique, http://www.idquantique.com/.

[21] MagiQ, http://www.magiqtech.com/.

[22] BBN, http://www.bbn.com/.

[23] J. McKeever, A. Boca, A. D. Boozer, R. Miller, J. R. Buck, A. Kuzmich, and H. J. Kimble, *Deterministic Generation of Single Photons from One Atom Trapped in a Cavity*, Science **303**, 1992 (2004).

[24] Z. Yuan, B. E. Kardyna, R. M. Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N. S. Beattie, D. A. Ritchie, and M. Pepper, *Electrically Driven Single-Photon Source*, Science **295**, 102 (2001).

[25] M. Keller, B. Lange, K. Hayasaka, W. Lange, and H. Walther, *Continuous Generation of Single Photons with Controlled Waveform in an Ion-Trap Cavity System*, Nature (London) **431**, 1075 (2004).

[26] B. Huttner, N. Imoto, N. Gisin, and T. Mor, *Quantum Cryptography with Coherent States*, Physical Review A **51**, 1863 (1995).

[27] H. P. Yuen, *Quantum Amplifiers, Quantum Duplicators and Quantum Cryptography*, Quantum and Semiclassical Optics **8**, 939 (1996).

[28] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Limitations on Practical Quantum Cryptography*, Physical Review Letters **85**, 1330 (2000).

[29] N. Lütkenhaus, *Security against Individual Attacks for Realistic Quantum Key Distribution*, Physical Review A **61**, 052304 (2000).

[30] N. Lütkenhaus and M. Jahma, *Quantum Key Distribution with Realistic States: Photon-Number Statistics in the Photon-Number Splitting Attack*, New Journal of Physics **4**, 44 (2002).

[31] H. Inamori, N. Lütkenhaus, and D. Mayers, *Unconditional Security of Practical Quantum Key Distribution*, quant-ph/0107017 (2001).

[32] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, *Security of Quantum Key Distribution with Imperfect Devices*, Quantum Information and Computation **4**, 325 (2004).

[33] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, *Experiments on Long Wavelength (1550 nm) "Plug and Play" Quantum Cryptography Systems*, Optics Express **4**, 383 (1999).

[34] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, *Single-Photon Interference Experiment over 100 km for Quantum Cryptography System Using Balanced Gated-Mode Photon Detector*, Electronics Letters **39**, 1199 (2003).

[35] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, *Faraday-Michelson System for Quantum Cryptography*, Optics Letters **30**, 2632 (2005).

[36] W.-Y. Hwang, *Quantum Key Distribution with High Loss: Toward Global Secure Communication*, Physical Review Letters **91**, 057901 (2003).

[37] X.-B. Wang, *Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography*, Physical Review Letters **94**, 230503 (2005).

[38] X.-B. Wang, *Decoy-State Protocol for Quantum Cryptography with Four Different Intensities of Coherent Light*, Physical Review A **72**, 012322 (2005).

[39] H.-K. Lo, *Extending the Distance of Unconditionally Secure Quantum Key Distribution*, presentation at Quantum Information and Quantum Control Conference, Toronto (2004), http://www.fields.utoronto.ca/programs/scientific/04-05/quantumIC/abstracts/lo.ppt.

[40] H.-K. Lo, in *Proceedings of 2004 IEEE International Symposium on Information Theory (ISIT), Chicago* (IEEE, New York, 2004), p. 137.

[41] H.-K. Lo, X. Ma, and K. Chen, *Decoy State Quantum Key Distribution*, Physical Review Letters **94**, 230504 (2005).

[42] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, *Practical Decoy State for Quantum Key Distribution*, Physical Review A **72**, 012326 (2005).

[43] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, *Enhancing Practical Security of Quantum Key Distribution with a Few Decoy States*, quant-ph/0503002 (2005).

[44] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, *Decoy-State Quantum Key Distribution with Two-Way Classical Postprocessing*, Physical Review A **74**, 032330 (2006).

[45] A. Khalique, G. M. Nikolopoulos, and G. Alber, *Postponement of Dark-Count Effects in Practical Quantum Key-Distribution by Two-Tay Post-Processing*, The European Physical Journal D **40**, 453 (2006).

[46] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, *Experimental Quantum Key Distribution with Decoy States*, Physical Review Letters **96**, 070502 (2006).

[47] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, in *Proceedings of 2006 IEEE International Symposium on Information Theory (ISIT), Seattle* (IEEE, New York, 2006), pp. 2094–2098.

[48] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, *Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber*, Physical Review Letters **98**, 010503 (2007).

[49] T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheidl, 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 144 km*, Physical Review Letters **98**, 010504 (2007).

[50] 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*, Physical Review Letters **98**, 010505 (2007).

[51] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, *Unconditionally secure one-way quantum key distribution using decoy pulses*, Applied Physics Letters **90**, 011118 (2007).

[52] 林正人・富田章久・廣島透也・長谷川淳,「デコイ法によって実現可能な量子鍵配送システムの安全性評価」, presentation at 科研費特定領域研究「情報統計力学の深化と展開」平成18年度研究成果発表会 (2006), http://www.smapip.is.tohoku.ac.jp/ dex-smi/2006/Workshop200612/ExtendedAbstracts/MasatoHayashi.pdf.

[53] 科学技術振興機構 (JST)・日本電気株式会社 (NEC),「安全性を定量的に保証する量子暗号鍵配布システムを開発」, プレス・リリース (2007), http://www.jst.go.jp/pr/announce/20070117/index.html.

[54] M. Koashi, *Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse*, Physical Review Letters **93**, 120501 (2004).

[55] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, *Unconditional Security of the Bennett 1992 Quantum Key-Distribution Scheme with Strong Reference Pulse*, quant-ph/0607082 (2006).

[56] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations*, Physical Review Letters **92**, 057901 (2004).

[57] A. Acín, N. Gisin, and V. Scarani, *Coherent-Pulse Implementations of Quantum Cryptography Protocols Resistant to Photon-Number-Splitting Attacks*, Physical Review A **69**, 012309 (2004).

[58] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, *Security of Two Quantum Cryptography Protocols Using the Same Four Qubit States*, Physical Review A **72**, 032301 (2005).

第4章　標準化動向と電子政府への導入に向けた課題

4.1　量子暗号をとりまく社会状況

近年、究極の安全性を効率よく達成するとされる、量子暗号技術の研究開発は、その基本的成果が徐々に開花しつつあり、商品化を含めた競争的研究開発が加速している。量子光学技術の著しい発展を背景とし、ある種の量子鍵配送プロトコル（ＢＢ８４など）が、実験室レベルを超えフィールドレベルにおいて実装されるまでに至った。またこのようなシステムについては、すでに商品化され販売が行われている。さらに、このような暗号システムの構成に不可欠な部品、あるいはシステムそのものについても、ワッセナーアレンジメントの枠組みのもと、輸出入規制に関する議論が行われてもいる。現在のところ、さまざまな技術的制約により、理論的に「無条件」安全性を達成することができる物理的状況は、通信距離、通信速度の両方の意味で限定されている状況ではあるが、これらの議論は、理論的に最も強い攻撃者（通信路上に存在し、物理法則に矛盾しないあらゆる攻撃が可能な攻撃者）を想定したものであり、実際の攻撃者には技術的制約が存在することを考えると、より高い性能と安定性を以って安全な鍵配布を達成していることが期待できる。

一方、人々の社会活動の根幹を支えるインフラシステム（金融、電力、交通）に対し、その制御・管理を行う「情報神経系システム」は、その役割を日々増大させている。このようなシステムは、いわば「インフラのためのインフラ」として位置づけられ、サイバーテロなどに代表されるある種の攻撃への耐性を配慮した設計・構築が、安全で安定した社会の実現に向け大きな課題の一つとなっている。

これら二つの事情を背景とし、現状達成可能な量子暗号技術を基盤とした情報神経

系システムのアイディアが既に幾つか提案されている。具体的には、信頼できる２パーティ間をＢＢ８４システムを用いて結び、ある種の鍵配送網を構築することにより、既存の情報通信システムへの鍵供給として組み込むものである。鍵を配布されるプレーヤー達は信頼できる、という仮定のもとで、外部の攻撃者に対して備える、という限られた状況ではあるが、全体として広域情報セキュリティ基盤を構築することができる。このアイディアの実用的利点は、暫定的には無条件安全性を達成しないまでも、現在達成可能な量子暗号技術を有効に活かすことにより高度な安全性を提供しつつ、今後達成されるであろう技術革新に応じてシステム全体のアップグレードを行うことにより、無条件安全性を満たす情報セキュリティ基盤への段階的な移行を穏やかに促進することができる点にある。現在国内外で開発が進められているＢＢ８４プロトコルや類似のプロトコルを調査し、攻撃者の現実的な攻撃能力に依存した「条件付」安全性について量子情報理論的な立場から定義を与えることは重要である。以上のタスクにより、量子暗号技術の発展的組込みによる情報セキュリティ基盤の設計という大きなゴールに向け、暫定的で実用的な状況について、理論的な裏打ちのある安全性規準を与えることが重要であろう。また、このような研究の成果は、国内における暗号実装関連技術等の調査・検討を行う暗号モジュール委員会あるいは CRYPTREC への貢献や、今後議論が徐々に進むことが想定される量子暗号技術に関する国際的な標準化活動にも非常に大きな影響を及ぼすことが予想される。

4.2　標準化に関する動向

量子暗号装置が製品として世の中に存在するようになってから久しい。現在、欧米、国内においてベンダーが幾つか存在し、様々な実装による製品が存在している。これらの製品については、現在のところ、大枠としてはＢＢ８４プロトコル（あるいはそのバリアンスとして考えることのできるプロトコル）を実装したものがほとんどである。しかしながら、詳細な物理的条件あるいは各コンポーネントとしてのデバイスの性能、使用条件、さらには鍵共有に必要な古典的なプロセスを比較すると、微妙な差異が存在している。これらの差異も、現在までの主要な製品については、安全性に重要な影響を及ぼすものとは考えにくく、ある意味で各製品の特性として捉えられる範囲ではあるが、より厳密に考えた場合、「何を以って量子暗号が実装された装置と呼ぶか」について、明確なコンセンサスが存在しない状況と捉えることもできる。（例えば、安全性が全く保障できない物理パラメータの領域で装置を実装したもの、あるいは、実際には量子暗号としての安全性を持たないプロトコルを実装した装置などを量子暗号装置、と呼ぶことについて明確な基準を持って否定できないのが現状である。）このような状況は、実システムに量子暗号を導入した際の安全性をどのように考えればよいか、という問題を複雑にするばかりでなく、導入する側のユーザーにとっても利用しにくい状況であり、今後の市場形成にとっても健全であるとは言いがたい。このような背景のもと、量子暗号の標準化が議論されるようになっている。

一方、量子暗号装置に関する現在の市場は萌芽的な段階であり、通常の意味での標準化については時期尚早とのとの意見も存在する。実際、一般的に考えても標準化が必ずしも市場拡大に正の貢献があるわけではなく、その意味からは安直な標準化の導入が今後の量子暗号装置市場の発展にとって望ましいものではない。また、量子暗号自体が非常に高度な安全性を担保すべき状況でのみ使われるのであれば、民生品を対象とした通常の意味での標準化が必要かどうかについても検討が必要である。

以上のような背景もあり、現在のところ通常の意味での標準化を直ちに進めるべし、という強い動きは国際的にも認められない。しかしながら、少なくとも「何を持って量子暗号が実装された装置と呼ぶか」程度の共通認識の必要性は既に認識されており、

いわゆる標準化とは異なった意味での、「合意形成」に向けた取組みがなされているのが現状である。例として、米 MagiQ 社など既存のベンダーのコンソーシアムとして、QCrypto Consortium が形成され、今年度、関連するワークショップが 2 回開催された。以後、表立った活動が想定されている様子はないが、現在も本コンソーシアムのメンバーを中心に、安全性を考慮するうえで考慮すべき現実的な条件に対する合意の形成等に向け議論は続けられており、本コンソーシアムの今後の動向についても注目すべきであると考えられる。

4.3　電子政府への導入に向けた課題

量子暗号は、現在のところ、非常に限られた状況で高度な安全性を達成することができる技術として捉えることができる。このような暗号技術を、電子政府においてどのように活用すべきかについては必ずしも自明な問題ではないが、高度な安全性が求められる状況において極めて有効な技術であることもあり、さらなる技術発展によっては、より使いやすい状況での導入も将来的には想定することができる。技術的な意味においても、限定的な状況であれば、電子政府への導入も直ちに可能な状況でもあり、導入に向けたルールの検討が必要な時期にきていると考えられる。このような状況を受け、ここでは導入に向けたルール策定に向けた課題を整理しておくことにする。

本報告書でも既に述べてきたように、量子暗号、特にＢＢ８４プロトコルなどの幾つかの方式については、その理論的安全性について、既に十分に検討されているものもあり、それらについてはアルゴリズムの意味で、電子政府における使用に対して推奨しうる暗号技術かどうかについての判断はさほど難しいものではないと考えられる。ただし、従来の暗号アルゴリズムが、仕様としてきちんと記述されているのと同様に、それらの量子暗号技術についても仕様としての記述を行わなければならないが、純粋にアルゴリズムの部分のみに注目すれば、この点については学術的知見も十分に蓄積されており、大きな困難は見当たらない。

一方、従来の（数理論的）暗号の場合と同様に、電子政府への導入に向けては、アルゴリズムレベルでの安全性評価にとどまらず、「アルゴリズムを実装したとされる装置そのものの安全性の評価」が重要であり、そのような評価技術は電子政府への導入に向け必須の技術であると考えることができる。特に量子暗号の場合、一つのアルゴリズムに対し、その物理的実装はユニークに決まらないばかりか、その実装方法そのものの物理的特性に安全性が大きく左右されるという事情があり、従来の（数理論的）暗号に対するそれと較べても非常に複雑な問題となることが予想される。このような評価技術手法に関しては、現在までのところ学術的知見も十分でなく、量子暗号の電子政府への導入には今後の発展が必須の分野といえるだろう。またこれと関連し、従来の（数理論的）暗号とやや事情が異なっている点を一つ指摘しておく。従来の暗号と

比較し、量子暗号は実装技術そのものがその安全性を大きく左右しているのは先に述べたとおりであり（少なくとも量子暗号の理想的な実装が期待できない現段階においては特に）、安全性を議論するうえでは純粋なアルゴリズムそのものと、実装形態の切り分けが従来の暗号ほど意味を持たない。即ち、量子暗号の実装技術のキーテクノロジーの多くがほとんどパテント化されているという状況は（安全性評価の意味においては）、従来の（数理論的）暗号におけるアルゴリズムそのもの（あるいはその一部）がパテント化されている状況に近いものとして捉えなければならないことを意味している。これは、（少なくともアルゴリズムそのものについてはパテント化されていない技術が標準的な技術として採用、あるいは安全性評価の対象となる傾向をもつ）従来の暗号技術に対する状況とやや異なっている。この点についても、量子暗号の電子政府への導入の際には注意深い議論が必要とされるだろう。

参考（米NIST、MagiQ社における調査）

NIST(CSD, ITL)の量子暗号の標準化に関する見解

平成18年12月18日（月）〜19日（火）に、米国メリーランド州ゲイザースバーグ（ワシントンDC近郊）にて開催された米国NIST定期会議2006[1]において、NISTにおける量子暗号研究開発、および標準化についての見解を得る機会を得た。

NIST内部の現状としては、量子暗号に関する研究を行っている物理学部門（Physics Laboratory）とコンピュータセキュリティ部門（CSD）、あるいは、暗号技術に関する標準化を検討する情報技術研究所（Information Technology Labratory）は、最近コミュニケーションを図り始めたところである。しかしながら、直ちに、標準化、あるいは、政府機関調達条件としてのルール策定に関して必要性を感じてはいない。CSDの基本的な方針としては、量子暗号関係に割くことのできる人的リソースの制限もあるため、当面見送る見解とのことであり、量子暗号の標準化のスケジュールに関しては未定である。

一方、量子計算機の存在を前提に、量子計算機による攻撃に耐えられる暗号の標準化のための予備検討を開始している。また、メリーランド大学と、多変数多項式暗号ベース、ハッシュ連鎖ベース等の署名の検討を共同研究の形で開始している。NISTは、平成19年度にWorkshopを開催する予定がある。さらに、ポスト量子暗号計算システムに向けに、量子計算機システムが出現した場合にも安全性の確保できる公開鍵暗号系について検討を開始している。具体的には、Latticeベースの暗号系を対象に検討を進めている。

MagiQ Technologies, Inc.の量子暗号に関する見解

平成18年12月20日（水）に、米国マサチューセッツ州サマーヴィル（ボストン近郊）にて、MagiQ Technologies, Inc.と会合し、量子暗号研究開発とその標準化につい

[1]米国の標準化機関である米国国立標準技術研究所（NIST）の情報セキュリティ関連部門CSD（Computer Security Division）と、（独）情報処理推進機構、経済産業省、日本規格協会、NRIセキュアテクノロジーズ、および（独）産業技術総合研究所との定期会議

ての MagiQ Technologies, Inc. の見解を得ることができた。

MagiQ Technologies, Inc. は、コンソーシアムの形をとって標準化活動を行っている。量子鍵配送の実践的な定義について意見交換が進められている。具体的には量子鍵配送システムに対する攻撃者の能力として実際上何を仮定すれば十分かに関する合意形成を行っている。MagiQ Technologies, Inc. としては、Alice と Bob それぞれに、Secure なゾーン（攻撃対象とならない物理的な装置）を仮定するのが、妥当だという見解である。また、原理的にはありえるがあまり極端な攻撃の想定（例：Detector の Quantum efficiency を攻撃者が制御できるような状況）には、興味がない、という視点で活動している。