次世代暗号・認証方式の研究・開発に関する調査報告

－量子暗号に関する調査・研究報告書－

平成 13 年 3 月

情報処理振興事業協会

目 次

(1) はじめに

この章では、最初に量子暗号に関する調査研究の背景と目的について述べる。

調査研究の背景

インターネットの急速な普及に伴って、新しい情報のインフラストラクチャが構築される中、情報セキュリティの確保は重要な課題である。なかでも、暗号技術は電子化された情報の秘匿性及び非改竄性の確保や電子認証を実現する基盤技術であり、電子政府の構築においてもそのセキュリティ確保のために必要不可欠な技術とされている。しかしながら、現在利用されている既存の暗号技術の多くには２つの問題点がある。１つはその技術が計算量理論に基づいて安全性が評価されている点である。これは暗号技術の解読には膨大な計算量、すなわち、膨大な計算時間がかかることに安全性の根拠をおいているが、将来量子計算機のような超高速計算機が実用化されると、その安全性の前提が崩れてしまいかねないという危険性を含んでいる。もう１つの問題点は、既存の技術では盗聴者の存在、つまり盗聴という攻撃を受けたことが検知できないことである。このことは、攻撃を受けた時点では安全であっても非常に長い時間スケールでセキュリティを要求されるサービスに対しては、我々の有する暗号技術が十全な保証をできるかという疑問を投げかける。このため、多様なサービスが出現してくる今後のネットワーク社会においてはより頑強な安全性を保証できる暗号技術に対する希求が一層高まりつつある。

調査研究の目的

当初は理論的側面の強かった量子情報処理技術は近年になり急速な実用化の可能性が開けてきた。この量子情報処理技術の情報セキュリティへのインパクトは 2 つはある。1 つは暗号解読の強力なツールとなる量子コンピュータ、そして、もう 1 つは絶対的な安全性を保証できる量子暗号である。あたかも現代の矛と盾であるこの 2 つの量子情報処理技術のうち、上記背景に述べられた問題点を鮮やかに解決するのが量子暗号である。即ち、計算量ではくなくハイゼンベルクの不確定性原理に代表される量子力学により安全性の保証された量子暗号は盗聴検知機能も自然に備えている。
従って、本調査研究では、次世代の暗号技術を考える上で、上記背景の２つの問題点を解決することが有力視されている量子暗号技術について調査研究を行う。

(2) 量子鍵配送

(2)-① BB84 プロトコル

(2)-①-a) BB84 プロトコルの概要

(2)-①-a)-1. BB84 プロトコル登場の経緯

BB84 プロトコルとは量子暗号のプロトコルの中で最も有名でしかも最も古くからあるプロトコルである。誤解の無いようにあらかじめ断っておくが、BB84 プロトコルは正確に言うと量子鍵配送プロトコルであって、2 者間で直接暗号文のやり取りができるわけではなく、暗号に必要な鍵データを安全に共有できるというものである。鍵を安全に共有できれば、あとは One-Time Pad 法を使って暗号文を送受信したり、共通鍵暗号を使って送受信したりすることができる。特に前者は情報理論的に完全な安全性を有しているため、量子暗号が絶対に安全であるという根拠の一つになっている。量子暗号の考えは今から 30 年ほど前の 1970 年代初頭の S. Wiesner の着想に端を発する。しかし不幸にも彼のアイデアはその後 10 年以上もの間日の目を見ることはなかった。(実際彼の論文が掲載されたのは 1983 年になってからである[5]。) そのうちに Wiesner のアイデアを聞いていた Bennett と Brassard が具体的なシステムを提案し、実際にデモを行い世の中の注目を集めた。Bennett らが最初に提出した論文は 1982 年のものであるが[6]、実質的な成果と捉えられている論文[1]は 1984 年のもので、この中に通称“BB84”と呼ばれているプロトコルが初めて登場する。その後 1990 年には Bennett、Bessette、Brassard、Salvail、Smolin が"Experimental quantum cryptography"という論文でこのプロトコルを実装し、1992 年にその改訂版が Journal of Cryptology に掲載され[3]、量子暗号技術が実用的な技術として広く認知されることになる。彼らの最初の実験システムは空気中を 32㎝離して量子暗号通信に成功したものであった。それ以降さまざまな量子暗号プロトコルが提案され、また実験技術の方も大きく発展して行った。1991 年には EPR 効果を用いたプロトコル“E91”が Ekert により提案され[4]、また 1992 年には後に“B92”と呼ばれるプロトコル[2]、さらには実験系ではこれまでの光子の偏光を用いた方式に代わって、位相変調を用いたシステムなどが次々と提案され現在に至っている。

(2)-①-a)-2. BB84 プロトコルの一般論

BB84 プロトコルが実現するのは、これまで遭ったこともない見ず知らずの他人同士が、物理的に離れた場所で完全に安全な通信を行えるようにすることである。先ほども少し述べたが、このプロトコルによって両者の間でランダムなビット列(鍵)が共有でき、そのビット列と、送りたい文章をビット変換したものとで Exclusive OR(XOR)を取り、情報理論的に安全であることが証明されている One-Time Pad 暗号として送

受信を行うことで絶対に安全な通信が行えるというものである。但し鍵は１回ずつの使い捨てでなければならない。One-Time Pad 暗号は送りたい文章の長さと、XOR を取るランダムなビット列の長さが同じであるときにその安全性が情報理論的に証明されているので、問題はランダムなビット列をどのように量子暗号プロトコルを用いて共有できるかである。もちろん公開鍵暗号を使ってもまったくの見ず知らずの他人同士で安全な通信が行える。しかしその場合の安全性は計算量的なものであり、現在の技術では解読できなくても、コンピュータ技術が進歩した将来においても安全であるとは言い切れない。事実 P. Shor の結果[10]から、量子コンピュータが完成すると、現在考えられているほとんどの公開鍵暗号は役に立たなくなると考えられている。

(2)-①-a)-3. BB84 プロトコルの詳細

BB84 プロトコルは量子通信路上での処理と、その後の公共回線上での処理（誤り訂正処理とプライバシー増幅処理）の２つが存在する。

(ア)量子通信路上の処理

（１） まず Alice は Bob との間で共有されるビット列の元になる、ランダムなビット列を作成する。今それを仮に”11100100101１”という 12 ビットあるとしよう。

（２） 次に Alice は（１）で作成したビットを水平－垂直、45°－135°の 2 つの偏光基底をランダムに用いて光子の偏光状態にビットを翻訳する。このとき、水平－垂直基底では、0 は水平方向の偏光、1 は垂直方向の偏光とし、また 45°－135°基底では 0 は 45°方向の偏光、１は 135°方向の偏光と決めておく。

水平－垂直基底 （以後＋基底と呼ぶ）	0 = ―	1 = ｜
45°－135°基底 （以後 X 基底と呼ぶ）	0 = ／	1 = ＼

したがって上のビット列は次のような偏光状態の光子列に置き換えられる。

Alice の作成したビット列	1	1	1	0	0	1	0	0	1	0	1	1
Alice が選んだ偏光基底	X	+	+	X	+	X	+	+	+	X	X	+
光子列にコード化された状態	＼	｜	｜	／	―	＼	―	―	｜	／	＼	｜

（3） Alice はこの光子の偏光列を量子暗号通信路を用いて送信し、Bob は2つの偏光基底をランダムに用いて受信する。

Alice の作成したビット列	1	1	1	0	0	1	0	0	1	0	1	1
Alice が選んだ偏光基底	X	+	+	X	+	X	+	+	+	X	X	+
光子列にコード化された状態	＼	｜	｜	／	―	＼	―	―	｜	／	＼	｜
Bob が任意に選んだ基底	X	X	＋	X	＋	＋	＋	X	＋	X	＋	X
Bob が得られた光子列	＼	／	｜	／	―	―	―	／	｜	／	｜	／
Bob が得られたビット列	1	0	1	0	0	0	0	0	1	0	1	0
Alice の作成したビット列	1	1	1	0	0	1	0	0	1	0	1	1
Alice が選んだ偏光基底	X	+	+	X	+	X	+	+	+	X	X	+
光子列にコード化された状態	＼	｜	｜	／	―	＼	―	―	｜	／	＼	｜
Bob が任意に選んだ基底	X	X	＋	X	＋	＋	＋	X	＋	X	＋	X
Bob が得られた光子列	＼	／	｜	／	―	―	―	／	｜	／	｜	／
Bob が得られたビット列	1	0	1	0	0	0	0	0	1	0	1	0
公共回線でチェック	○		○	○	○		○		○	○		

（4） Bob は公共の回線を使って Alice にどのタイプの基底を用いて観測したかを伝え、Alice はどの時刻の測定の型が正しいかを教える。

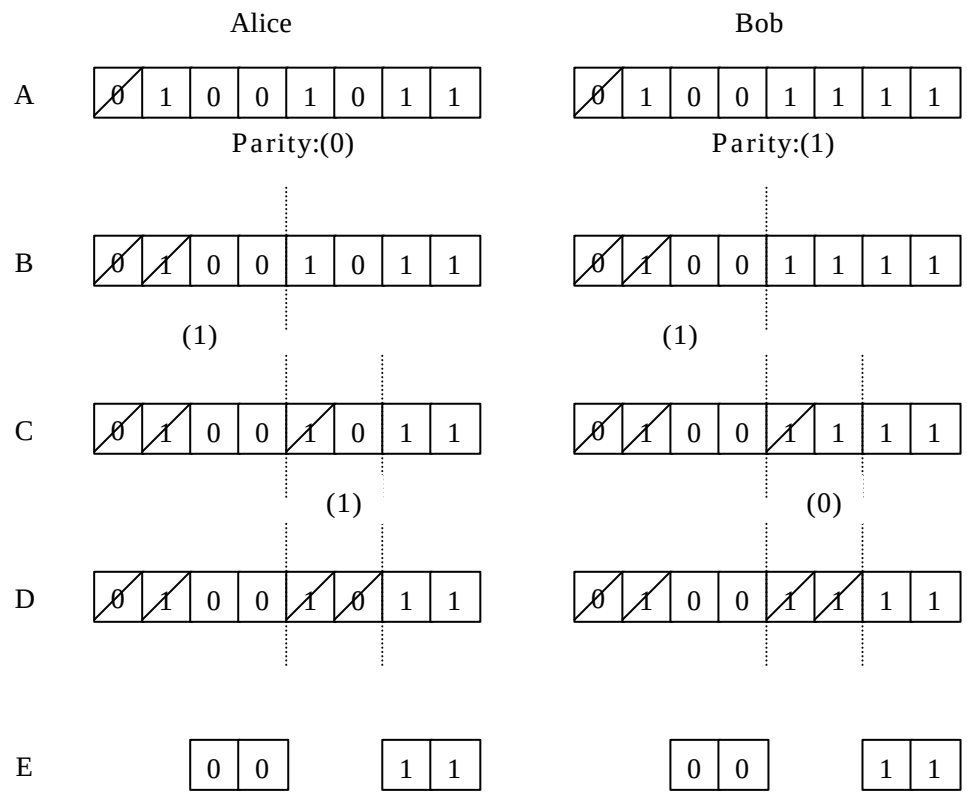
（5） 違う測定器を使ってしまった個所及び、測定器が何らかの理由で検出できなかった場合を除外し､同じ測定器を用いて観測した個所のデータを Alice と Bob の共有データとする。但し Eve の検証のため、この共有データの一部を犠牲にして最終的な確認を行い、その残りを真の共有データとする。

厳密に言うと最後の段の公共回線でチェックという項目を除いた部分が BB84 プロトコルの量子通信路上の処理である。 しかしこれだけではよほど想像力を働かせないと、量子暗号の利点を理解することはできないであろう。したがって少し具体的に上記プロトコルを考えてみる。具体的にと言ったのは盗聴者 Eve が存在する場合を考えてみるということである。Eve が盗聴に際して Bob と同様、測定器で測定する以外に知識を持っていないとすれば、Eve が選択できる最良の盗聴方法は次の通りである。彼女は Bob が受け取るように途中で盗聴し、盗聴した結果の光子列をそのまま Bob に送信するというものである。なぜなら盗聴の段階では Eve はどの測定器が正しいかわからないからである。「もちろん２つのタイプの測定を同時に行うことは不確定性原理から不可能である。」したがって Eve が盗聴時にビットを誤る確率は 1/2 であり、それを再送信する際に、盗聴時に正しい測定器で測定したビットはそのまま正しい偏光状態で送信できるが、間違った測定器のビットは間違った偏光状態で Bob に送信せざるを得ない。この段階では Bob は Eve が存在することは知らないので、全てのデータは Alice から送られてきたものと思い受信していく。このため Alice の偏光を Eve が偶然正しく受信し、それをそのまま再送した場合、その光子列の内の半分は Bob も正しく読めるはずである。しかし Alice と Bob の間で見ると、両者が正しい基底を用いている場合、原理的には 100 パーセント正しくビットが伝わっていなければおかしい。ところが Eve の介在により、そのうちの半分のデータが壊れてしまうことになる。このことから Eve の存在を Alice と Bob が検知できる。これが BB84 量子鍵共有プロトコルのコンセプトである。

(イ)誤り訂正処理

我々の行った実験においてはビット誤り率は１～数%あった。一般に 1%でもエラーがあるとシステムとしては成り立たないことの方が多い。特に暗号通信における鍵データの共有などでは 1 ビットたりとも誤りがあってはならない。そこで公共の回線を使ってその誤りを取り除き、しかも盗聴者に情報をできるだけ漏らさずに行う方法が考案された。それがこの誤り訂正処理である。

原理は簡単で、最初にAliceとBob間で誤りを若干含んだ共有データがあるとする(図(2)-①-a)-1.段階Aでは左から6ビット目が異なっている場合を紹介している)。これを幾つかのブロックに分けて、そのブロックごとにパリティ値を比較する。図(2)-①-a)-1.は 8 ビットのブロックに分けた例を示してある。パリティの比較の際、公共の回線を用いるので、盗聴者 Eve にもパリティ情報、即ち１ビットの情報が漏れる。したがって情報理論的にみて、漏洩してしまった情報量との帳尻をあわせるため、共有データの１ビットを後で捨てる（図(2)-①-a)-1.段階 E)。パリティの合わなかったブロックはそのブロックをさらに２分割して同様なパリティチェックを行い、パリティが一致するまで２分木探索を行い、最終的に誤りのあるビットを修正する（実際には最後まで残ったビットは盗聴者に推定可能なため、利用できない)。こうして２分探索に用いた数プラス１個（前述の理由から）だけビットを捨て、残ったビットを共有情報の候補とする。候補といったのは同じブロック中に偶数個誤りがあると、たまたまパリティが一致してしまうので、そのような場合も取り除くためには、元の共有データのビットを適当に置換して、同様の処理を最初から何度か行うことで、確実に誤っ



図(2)-①-a)-1. 誤り訂正処理の流れ

たビットを取り除くことができる。
(ウ)プライバシー増幅処理

（イ）の誤り訂正処理で誤りを取り除いた後の共有データには僅かであるが、盗聴者に漏洩したビットが存在する可能性がある。プライバシー増幅処理とは部分情報が漏洩しているビット列から、ビットの長さを短くすることにより、盗聴者が部分情報の盗聴に成功する確率を低下させることを目的としている。　基本的には Bennett、Brassard、 Robert[7]及び Chor、 Goldreich、 Hastad、 Freidmann、 Rudich、Smolensky[11]によって独立に導入された t-resilient 関数を利用することでプライバシーの向上は達成できる。以下に t-resilient 関数とその構成法について説明する。

f をブール関数で　$\mathrm{Z}_2^n \mapsto \mathrm{Z}_2^m (n > m)$ なるものとする。
f が balanced（または equitable）であるとはすべての　m ビット列　y に対して　f の逆像　$f^{-1}(y)$ が　2^{n-m} 個の元を持つことと定義される。これは　y が出力であるときに入力　x をランダムに選んだときに　$f(x) = y$ となる確率を　$\mathrm{P}(y)$ とすれば、すべての　m ビット列　y に対して　$\mathrm{P}(y)$ が　2^{-m} となることと同値である。

今、f への入力　x の内　t ビットは固定されていると仮定する。つまり、$x_{i_1} = c_1, \cdots, x_{i_t} = c_t$ とする。確率 $\mathrm{P}(y \mid x_{i_1} = c_1, \cdots, x_{i_t} = c_t)$ を $x_{i_1} = c_1, \cdots, x_{i_t} = c_t$ の条件において　$f(x) = y$ となる確率とする。

f　が“correlation-immune of order t”であるとは、すべての　$x, y, c_1, c_2, \cdots, c_t$ に対して $\mathrm{P}(y \mid x_{i_1} = c_1, \cdots, x_{i_t} = c_t) = \mathrm{P}(y)$ となることと定義する。

直感的には　n ビット列　x において　t 個のビットが盗聴者に漏れていても　f を作用させることで結局盗聴者が　$f(x) = y$　を類推する確率は　$\mathrm{P}(y) = 2^{-m}$ となり、これは何も情報が漏れていない場合と同じになる。エントロピーを用いて言えば　t 個のビットが盗まれていようといまいと、　f を作用させることで盗聴者から見れば m ビットの共有鍵は　m ビットのエントロピー（類推する確率が 2^{-m}）を持つことになる。

f が t-resilient 関数であるとは　f が balanced であり、 correlation-immune of order t　であることと定義する。これはすべての可能な変数に対して

$\mathrm{P}(y \mid x_{i_1} = c_1, \cdots, x_{i_t} = c_t) = 2^{-m}$ となることと同値である。

即ち直感的には　n ビット列　x のいくつかのビット（　t 以下）が情報として漏れていても　f を作用させて、n ビットから　m ビットにビット長を短くする。このとき x（　n ビット列）においては何ビットか漏洩しているので盗聴者から見れば　n ビット列の　x を類推する確率は　2^{-n} よりも小さい。つまり完全な安全性が達成されていないことになる（　n ビットの列　x の完全な安全性とは　x を類推する確率が丁度 2^{-n} であること）。

一方　$y = f(x)$（　m ビット列）においては、盗聴者が類推する確率は丁度　2^{-m} である。つまり　m ビットのエントロピーがある。
以上より　t は量子通信において Eve がエラーの幅程度に紛れ込んで盗聴していてもかまわないビットの数の最大と考えられる。　t の値はエラー率により決定される。

したがって　m が十分大きなものになるように　n を決定し、さらにエラー率から　t を決定し t-resilient 関数を構成して通信プロトコルを設計すれば、鍵交換においていくつかのビットが盗聴者に漏れていても、t-resilient 関数を利用することにより、完全な安全性（m をセキュリティパラメータとすれば、盗聴者が　m ビットの鍵を類推する確率が丁度　　2^{-m} になること）を達成できる。

ちなみに t-resilient 関数の構成方法は盗聴者に知られていてもかまわない。つまり t-resilient 関数は公開情報である。

このように t-resilient 関数が構成できれば完全な安全性を達成できるのであるが、しかし t-resilient 関数はその構成方法がすべてのパラメータについてわかっているわけではないという問題点がある。そこで t-resilient 関数について分かっている幾つかの事実を以下に示す。

$m = 1,2,3$　の場合には以下のことが知られている。つまりこの時には具体的な構成方法が知られている。

定理１　$f : \mathrm{Z}_2^n \mapsto \mathrm{Z}_2$　が t-resilient 関数であるためには
$t \le n - 1$ が必要十分条件

定理２　$f : \mathrm{Z}_2^n \mapsto \mathrm{Z}_2^2$　が t-resilient 関数であるためには

$t \le \frac{2n}{3} - 1$であることが必要十分条件

定理３　$f : \mathrm{Z}_2^n \mapsto \mathrm{Z}_2^{23}$　**が t-resilient 関数であるためには**

$t \le \frac{4n}{7} - 1$　**かつ**　$n \neq 2 (\mathrm{mod}\, 7)$　**または、**

$t \le \frac{4n}{7} - 2$　**かつ**　$n = 2 (\mathrm{mod}\, 7)$　**が必要十分条件**

これら以外については、いろいろ知られていることもあるが、全ての場合について t-resilient 関数の構成方法が明確にわかっているわけでない。

(2)-①-a)-4．BB84 プロトコルの応用の見通し

鍵共有プロトコルである BB84 プロトコルは現在のところ、数十キロ程度の通信しかできない。一般のマーケットに浸透するには 100 倍程度通信距離を伸ばす必要があるといわれている。またその鍵共有レートは 1kbps 程度である。つまり 1 秒間に 1000 ビットの鍵が共有できるオーダーである。しかも実際にはこの後で誤り訂正やらプライバシー増幅処理を行う必要があり、これを加味するととてつもなく遅い。これに対して現在の通信はもうすぐ数千ギガビットに届こうとしている。量子暗号だけで絶対に安全な通信を行うには One-Time Pad 法が不可欠であるが、そうした場合にはこの10^{10}以上のギャップをどうにかしなければならないだろう。

参考文献

[1] C. H. Bennett and G. Brassard, ”Quantum Cryptography: Public key Distribution and Coin Tossing”, Proc. of IEEE int. Conf. On Comp. Sys. And Signal Proc., Bangalore, India, 1984.

[2] C. H. Bennett, “Quantum Cryptography Using Any Two Nonorthogonal States”, Phys. Rev. Lett., Vol.68, No.21, 1992.

[3] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, ”Experimental Quantum Cryptography”, Journal of Cryptology, Vol.5, pp.3-28, 1992.

[4] A. K. Ekert, “Quantum Cryptography Based on Bell's Theorem”, Phys. Rev. Lett., Vol.67, No.6, 1991.

[5] S. Wiesner, S., "Conjugate coding", Sigact News, vol. 15, no. 1, 1983, pp. 78 - 88

[6] C. H. Bennett, G. Brassard, S. Breidbart and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens", Advances in Cryptology: Proceedings of Crypto 82, August 1982, Plenum Press, pp. 267 - 275.

[7] C. H. Bennett, G. Brassard and J-M. Robert, "Privacy amplification by public discussion", SIAM Journal on Computing, vol. 17, no. 2, April 1988, pp. 210 - 229.

[8] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion", Advances in Cryptology | Eurocrypt '93 Proceedings, May 1993, to appear.

[9] C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer, "Generalized privacy amplification", to appear in IEEE Transactions on Information Theory, 1995.

[10] P. W. Shor, "Algorithms for Quantum Computation: Discrete Log and Factoring", Proc. of the 35th Annual IEEE Symposium on Foundations of Computer Science, 1994.

[11] B. Chor, O. Goldreich, J. Hastad, J. Freidmann, S. Rudich and R. Smolensky, “The bit extraction problem or t-resilient functions,” 26th IEEE Symp. Foundations of Computer Science, 1985, 396-407

(2)-①-b)　BB84 プロトコルの安全性

(2)-①-b)-1．安全性とは？

現代の暗号の世界で安全性と言う場合、それは全て計算量的な安全性を指す。したがって計算機が一層高速化したり、画期的な解読アルゴリズムが発見されたりしたときにはその暗号は別のものに取って代わられる必要がある。そこで現代の暗号開発者は少なくとも安全性の観点からは次の２点を考え暗号を設計することになる。

① 現在知られている全ての暗号解読アルゴリズムにおいて、設計した暗号が計算量的に安全であること。
② ある実用耐年数を仮定し、その期間中の計算機の進歩の速度を見積もり、上述の全ての解読アルゴリズムに対してその期間中、安全な暗号となるよう安全性マージンを決める。このとき新種の解読アルゴリズムはそもそも考慮できないので、はじめから考えない。

勿論、暗号を総合的に設計するには他に、処理速度や回路規模、使用目的等考えなければならない別のファクターも幾つかあるが、安全性に関しては簡潔に上述の要件を満足すればよい。但しこのようにして安全性を標榜してみても、次のような問題は依然として解決されない。それは盗聴者がリアルタイムには、計算機のパワーが足りずに解読をあきらめたとしても、何年か後に再びそのとき記録しておいた暗号データを暗号解読器にかけて解読することが可能なことである。言うまでもないがその時代には計算機の能力が向上していたり、新しい解読アルゴリズムが開発されていたりする状況を仮定している。

これに対して量子暗号で言う安全性とは計算量的な安全性ではなく、不確定性原理といった自然の物理法則に基づいた安全性である。原理的にはその物理法則が否定されない限り安全であり、またその物理法則が正しい限り確実に盗聴行為をリアルタイムに検出できるというのが量子暗号である。このことは理論的に証明されている。したがって原理的には計算機の進歩とは無関係に安全であり、しかも盗聴したデータを後の世で高性能な計算機にかけて解読することもできない。なぜなら暗号通信のテスト段階でリアルタイムに盗聴が検出されるので、その時点で暗号通信は中止されるからである。その結果一度量子暗号システムを導入してしまえば、機械的に壊れない限り半永久的に使用でき、しかも誰かに盗聴されているかもしれないという杞憂もなくなる。

このように原理的には絶対に安全な量子暗号であるが、現実の技術レベルや実際の運用上の問題、機械の精度などから必ずしも絶対に安全とは言えない。Brassard らに

よれば現実のシステムで絶対に安全と呼べるものはないということであるし、どこまでが許容できるか量子暗号の安全性が多角的に厳密に議論されつつある。

(2)-①-b)-2．盗聴戦略

(イ)具体的な盗聴戦略

① Intercept/Resend Attack

これは誰もが最初に思いつく攻撃法である。量子ではない普通の通信では途中の通信路で Eve がいくら盗聴していても、通信者である Alice と Bob は気づかない。つまりその通信路にはたくさんの光子が同じ情報を表すのに使われ、その中から盗聴によって幾つか光子を取り出しても、もともと検出器の精度がそうした大雑把なものを想定しているため、Alice と Bob 間で情報の欠損として現れないように Eve はいくらでも工夫することができるのである。しかし話が微細な量子の世界に入ってくると、Eve の盗聴により Alice の送った光子が Bob に届かないようなことが起きる。特に光子１個に情報が乗っかっているような量子鍵配送通信では、光子１個を検出可能な検出器を使用しており、また複製不可能定理から、物理的にもその光子を分割して同粒子の状態をコピーすることができない。したがって Eve に許される攻撃法としては、１度通信路中の光子を捕捉してその量子状態を観測し、その結果を別の光子に焼き直して再送する手段が考えられる。しかし観測する基底はこの時点では分らない Eve は２つの基底を適当に変えて測定するしか手段はなく、したがって非直交な２つの物理量を同時に観測することはできないという不確定性原理の要請から、Eve の盗聴を検出することができる。しかし現実の量子鍵配送において、もともと存在する装置の誤り率程度の盗聴は看過される。そこで誤り訂正手法やプライバシー増幅方法により、現実的には古典的な手法で盗聴者の得られる情報を限りなく小さくするように処理を加える。但しこの時点で絶対的な安全性を有するとは言えないだろう。もちろん実用的な安全性ではあるのだが。

② Beam-splitting Attack

これも現実的な盗聴法である。現在のところ量子暗号を実現するアイテムの１つに単一光子発生源があげられる。しかし現実にはそうした有効な単一光子発生源はないので単に光源にフィルターをかぶせただけのもので代用している。するとどうしてもパルスあたりに光子を２個含むような場合が出てくる。このような場合にどちらか 1 方の光子を分離して保存しておき、もう一方の光子を何事もなかったかのように Bob に送る攻撃が考えられる。もともとこの２つの光子はエンタ

ングルしていると考えられるので、基底の公開まで観測せずに保持しておけば、そもそも Alice と Bob で基底の合わなかったものを除き、Eve が保持した光子の約半分はビットを読めることになる。この攻撃も基本的には防ぎようがない。Intercept/Resend 攻撃同様、古典的手法により安全性を向上させる。

(ウ)理論的な盗聴

① Incoherent Attack

これは別名 Individual particle attack と呼ばれ、以下のような制限のあるタイプの攻撃法である。即ち、盗聴者は１度に１個の光子にだけ、自分の持っている量子プローブ $\wp_i$ をエンタングルさせる（絡ませる）ことができ、そのエンタングルされた光子を Bob が観測し、そのデータが Alice と Bob の間で公衆回線で交換されるまで、Eve は観測せずに盗聴したプローブを保持しておくことができるという方法である。実際 Alice と Bob は、Eve のこうしたエンタングルのような操作は Bob が観測してもしなくても分らない。したがって最大限情報を引き出すためには当然 Eve は公衆回線での情報交換まで自分の観測を遅らせるのである。しかし Incoherent attack は Eve の個々のプローブ $\wp_i$ に対して次のような制約がある。

つまり $\left|E\right\rangle_i$ を Eve のプローブの初期状態とし、Alice から飛んでくる光子とプローブ $\wp_i$ をエンタングルさせるような一般的なユニタリー変換を U とすると、BB84 プロトコルで偏光基底として⊕基底(水平－垂直基底、$\left|0°\right\rangle, \left|90°\right\rangle$)を用いた場合、

数式 1

$$\left|E\right\rangle_i \left|90°\right\rangle \xrightarrow{U} \left|E_{00}^{\oplus}\right\rangle \left|90°\right\rangle + \left|E_{01}^{\oplus}\right\rangle \left|0°\right\rangle$$

数式 2

$$\left|E\right\rangle_i \left|0°\right\rangle \xrightarrow{U} \left|E_{10}^{\oplus}\right\rangle \left|90°\right\rangle + \left|E_{11}^{\oplus}\right\rangle \left|0°\right\rangle$$

と言ったユニタリー変換を行う。但し $\left|E_{ij}^{\oplus}\right\rangle$ はプローブ $\wp_i$ の規格化されていない状態である。

$\left|E\right\rangle_i$ は $\left|E_{ij}^{\oplus}\right\rangle_{ij}$ の中から選ぶことができるので、プローブ $\wp_i$ はそれぞれのプローブが２キュビットで表される４次元ヒルベルト空間で記述できる。またAliceが⊗基底（45°－135°、$\left|45°\right\rangle,\left|135°\right\rangle$）を送った場合は、数式 1 および数式 2 とその線形性から次のようにユニタリー変換を記述できる。

数式 3

$$\left|E\right\rangle_i\left|45°\right\rangle \xrightarrow{U} \left|E_{00}^{\oplus}\right\rangle\left|45°\right\rangle+\left|E_{01}^{\oplus}\right\rangle\left|135°\right\rangle$$

数式 4

$$\left|E\right\rangle_i\left|135°\right\rangle \xrightarrow{U} \left|E_{10}^{\oplus}\right\rangle\left|45°\right\rangle+\left|E_{11}^{\oplus}\right\rangle\left|135°\right\rangle$$

但し、

数式 5

$$\left|E_{00}^{\otimes}\right\rangle=\frac{\left|E_{00}^{\oplus}\right\rangle+\left|E_{10}^{\oplus}\right\rangle+\left|E_{01}^{\oplus}\right\rangle+\left|E_{11}^{\oplus}\right\rangle}{2}$$

数式 6

$$\left|E_{01}^{\otimes}\right\rangle=\frac{\left|E_{00}^{\oplus}\right\rangle+\left|E_{10}^{\oplus}\right\rangle-\left|E_{01}^{\oplus}\right\rangle-\left|E_{11}^{\oplus}\right\rangle}{2}$$

数式 7

$$\left|E_{10}^{\otimes}\right\rangle=\frac{\left|E_{00}^{\oplus}\right\rangle-\left|E_{10}^{\oplus}\right\rangle+\left|E_{01}^{\oplus}\right\rangle-\left|E_{11}^{\oplus}\right\rangle}{2}$$

数式 8

$$\left|E_{11}^{\otimes}\right\rangle=\frac{\left|E_{00}^{\oplus}\right\rangle-\left|E_{10}^{\oplus}\right\rangle-\left|E_{01}^{\oplus}\right\rangle+\left|E_{11}^{\oplus}\right\rangle}{2}$$

である。Eve はUをこのように選び、さらに盗聴を間欠的に行い、通常の通信エラーレートよりも小さい程度に抑えて盗聴を気付かれないようにする。つまり$i \neq j$の時に$\left\langle E_{ij}^{\oplus} \middle| E_{ij}^{\oplus} \right\rangle$と$\left\langle E_{ij}^{\otimes} \middle| E_{ij}^{\otimes} \right\rangle$の非対角成分が小さい、つまり擾乱が小さいことが必要となる。

また Eve は公衆回線を盗聴し、使われていた基底に関する情報を用いて、盗聴したビットを最大限正しく読もうとする。つまり古典通信路で盗聴した基底を使ってプローブの観測を行う。例えば Eve はi番目の光子が⊕基底で送られたことが分れば、もし Alice がその基底を使って 0 を送ったのであれば、上述のプローブ$\wp_i$は次のような混合状態になっていると考える。

数式 9

$$\rho_0 = \mathrm{Tr}_{photon}[(U\left|E\right\rangle_i\left|90^\circ\right\rangle)(U\left|E\right\rangle_i\left|90^\circ\right\rangle)^\dagger = \left|E_{00}^{\oplus}\right\rangle\left\langle E_{00}^{\oplus}\right| + \left|E_{01}^{\oplus}\right\rangle\left\langle E_{01}^{\oplus}\right|$$

同様に、もし Alice がビット 1 に対応する$\left|0^\circ\right\rangle$の状態の光子を送っていたなら、Eve のプローブの状態は次の混合状態にあると思う。

数式 10

$$\rho_0 = \mathrm{Tr}_{photon}[(U\left|E\right\rangle_i\left|0^\circ\right\rangle)(U\left|E\right\rangle_i\left|0^\circ\right\rangle)^\dagger = \left|E_{10}^{\oplus}\right\rangle\left\langle E_{10}^{\oplus}\right| + \left|E_{11}^{\oplus}\right\rangle\left\langle E_{11}^{\oplus}\right|$$

したがって Eve は彼女のプローブが状態ρ_0にあるのかρ_1にあるのかをできるだけ確実に決めるために、プローブ$\wp_i$上で観測を実施する。観測結果はその固有ベクトルにより決まり、今の場合$\rho_0 - \rho_1$となり、これにより Alice の送ったビットを推定できる。

Eve の持つプローブのエンタングルメントの最適化は、様々な単一光子を用いた量子暗号鍵配布プロトコルで議論されている。そして量子通信路のエラー率と Eve の得られる最大情報量との間に密接な関係があることが知られている。この関係から一般的なプライバシー増幅法を使って、望みどおりの秘匿性を保証するパラメータτを計算できる。こうして情報の漏洩が精製中の鍵の長さに比べ、ある値以下の場合に安全であるという議論が成立する。

② Coherent Attack

これは別名 Joint attack と呼ばれ、Eve は伝送された光子の全ての系列に対して、あらゆる次元、あらゆる状態（混合状態、純粋状態）のプローブを、あらゆるユニタリー変換を使って、エンタングルさせることができる攻撃のことである。彼女はこの巨大なエンタングルさせた状態のプローブを公衆回線での通信が終わるまで保持し、彼女の選択する最も広範な測定を行う。その最も広範な測定のクラスは Positive Operator Valued Measures(POVM or POM)として知られていて、詳細は[8]に示されている。この攻撃が現状の技術からみて、実現するのが非常に難しいことは言うまでもない。

Collective attack は概念として Coherent attack に含まれる。Alice の光子 i は個々のプローブ $\wp_i$ に対して個別にエンタングルされる。したがってここまでは Incoherent attack と同じである。Incoherent attack と異なるのは、公衆回線での議論が済むと、Eve には単一の巨大な量子システムとして考えられる全てのプローブ上でのあらゆる POVM の実施が許されることである。

Coherent attack に対する安全性については証明が非常に難しい。したがってインタラクティブな誤り訂正コードよりも線形な誤り訂正コードを使った場合のみ扱われている。Collective attack に対するプロトコルの安全性の証明は[19]に見られ、また一般的な Coherent attack に対する証明は[16][17][3][18]に与えられている。但し、[16]は量子計算機の存在を仮定した証明であり、それ以外は現実的な設定の上での証明となっている。

(2)-①-b)-3. 情報理論的安全性

次に古典的な通信部分である誤り訂正に関して情報理論的な議論を行う。いま Alice と Bob がエラー率 e のデータ（ビット長 n）を共有しているとする。これを公衆回線を使ってデータを修正する場合、その最小の交換ビット数 r はシャノンの符号化定理から次のように求められる。エラーは独立に起きるものと仮定すると、

数式 11

$$r = n(-e\log_2 e - (1-e)\log_2(1-e))$$

として与えられる[15]。n を 1 に規格化した場合を図 (2)-①-b)-1． 誤り訂正の情報理論的限界に示した。縦軸は r、横軸はエラー率eである。

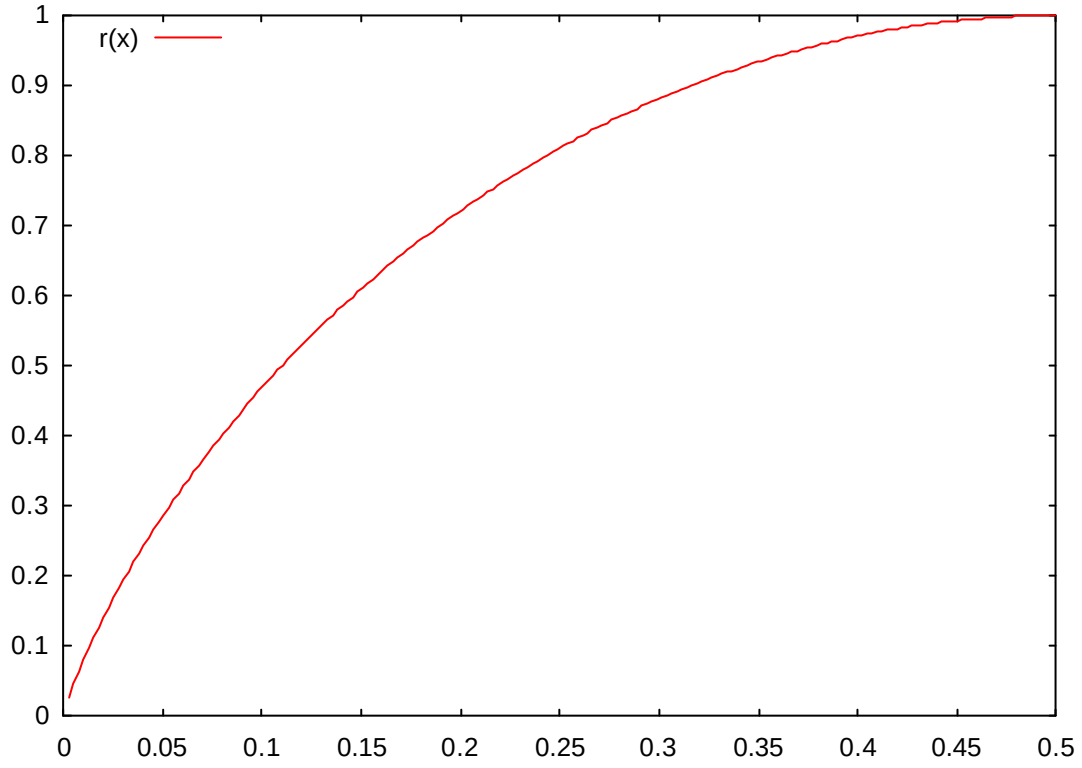


図 (2)-①-b)-1． 誤り訂正の情報理論的限界

このグラフから例えばビット長が 100 ビットであり、エラー率が 10%(0.1)であれば、最良で約 45 ビットの情報を交換して誤り訂正できることになる。またエラー率が 1%であれば、およそ 5 ビット程度の情報交換のみで良いことが分る。しかしこの定理は非構成的な証明であり、どのような手立てで実現すれば良いかは分っていない。一般の線形誤り訂正符号ではむしろ非効率になることが分っており、これに対して Bennett らはこの Shannon 限界により近づける実用的な方法を示した[10][6]。

参考文献

[1]C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing", Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175 - 179.

[2]C. H. Bennett, "Quantum cryptography using any two nonorthogonal

states", Physical Review Letters, vol. 68, no. 21, 25 May 1992, pp. 3121 - 2124.

[3]E. Biham, M. Boyer, P. O. Boykin, T. Mor and V. Roychowdhury, “A proof of the security of quantum key distribution”, In Proc. of the Thirty-Second Annual ACM Symposium on Theory of Computing. ACM Press, New York, 1999. arXiv:quant-ph/9912053.

[4]A. K. Ekert, “Quantum Cryptography Based on Bell’s Theorem”, Phys. Rev. Lett., Vol.67, No.6, 1991.

[5]A. Peres, “Quantum Theory: Concepts and Methods”,Kluwer Academic Publishers, Boston, 1993.

[6]C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography", Journal of Cryptology, Vol. 5, pp. 3 – 28, 1992.

[7]C. H. Bennett, G. Brassard, S. Breidbart and S. Wiesner, “Qunatum cryptography, or unforgeable subway tokens.” In Advances in Cryptology: Proceedings of Crypto 82, pp. 267 – 275, Plenum Press, 1982.

[8]C. H. Bennett, G. Brassard, S. Breidbart and S. Wiesner, "Eavesdrop-detecting quantum communications channel", IBM Technical Disclosure Bulletin, vol. 26, no. 8, January 1984, pp. 4363 - 4366.

[9]B. Chor, O. Goldreich, J. Hastad, J. Freidmann, S. Rudich and R. Smolensky, “The bit extraction problem or t-resilient functions.” In 26th IEEE Symp. Foundations of Computer Science, pp. 396 – 407, 1985.

[10]C. H. Bennett, G. Brassard and J-M. Robert, "Privacy amplification by public discussion", SIAM Journal on Computing, vol. 17, no. 2, April 1988, pp. 210 - 229.

[11]U. M. Maurer, “Secret key agreement by public discussion from common information”, IEEE Transactions on Information Theory, vol. 39, no. 3, May 1993, pp. 733 - 742.

[12]G. Brassard and L. Salvail, “Secret-key reconciliation by public discussion.” Advances in Cryptology, Eurocrypt '93 Proceedings, 1993

[13]C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer, "Generalized privacy amplification", IEEE Transactions on Information Theory, 1995.

[14]C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wooters, Phys. Rev. A. 54, pp. 3824-3851(1996)

[15]D. Bouwmeester, A. Ekert and A. Zeilinger, editors. “The Physics of Quantum Information”, Springer, 2000.

[16]H. K. Lo and H. F. Chau. “Unconditional security of quantum key distribution over arbitrarily long distances.”, Science, Vol. 283, pp. 2050-2056, 1999. arXiv: quant-ph/9803006.

[17]D. Mayers. “Unconditional security in quantum cryptography”, arXiv: quant-ph/9802025.

[18]P. W. Shor and J. Preskill. “Simple proof of security of the bb84 quantum key distribution protocol”, arXiv: quant-ph/0003004, 2000.

[19]E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, “Security of quantum key distribution against all collective attacks”, arXiv: quant-ph/9801022, 1998.

(2)-①-c) 実験系の構成と提案

(2)-①-c)-1. 概要

実際に量子暗号の鍵共有プロトコルを実現しようとした場合、どのような実験構成を考えたら良いのか、またどのような検討項目があるのか、また実現方法はどのようなものがあるのかについてここで簡単に説明しよう。この節では BB84 プロトコルの実験系に関して説明するが、他の鍵共有プロトコルに関しても基本的にほとんど同様に考えられることを述べておく。

まず情報の媒体であるが、量子暗号実験では通常現在の光通信に倣って、光子が用いられる。さらに光子を用いた実験を考える場合、大きく次の３つの基本構成要素からなる。すなわち光源、伝送路、検出器の３つである。下記に簡単にまとめた。

[光　源]

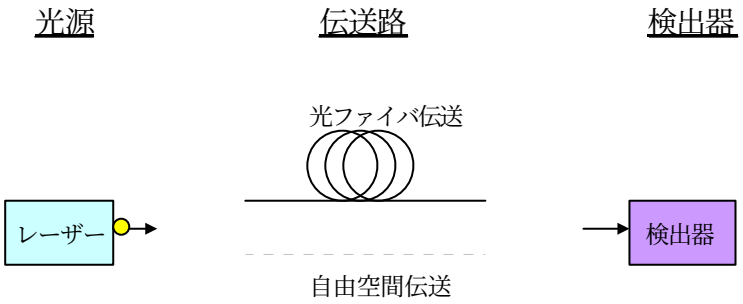
微弱レーザー光（短波長帯、長波長帯)、パラメトリック蛍光光子

[伝送路]

光ファイバ（短波長帯、長波長帯)、自由空間

[検出器]

Si-APD、光電子増倍管、冷却 APD(Si, Ge, InGaAs)



図(2)-①-c)-1. 光通信の基本イメージ

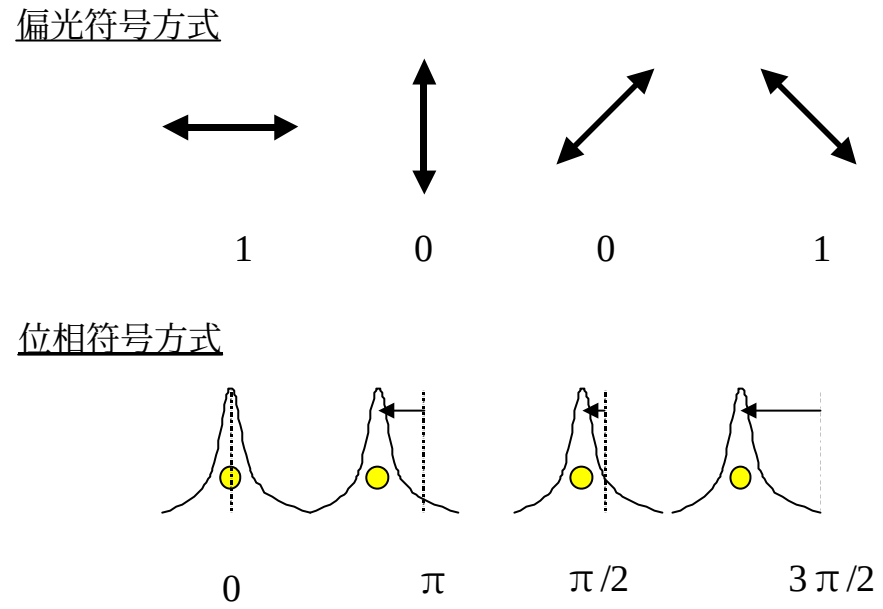
基本的には、各々使用する光源の波長帯に依存して特徴が異なることに注意しよう。光ファイバは、短波長帯では挿入損失が約 3dB/km と比較的大きいが、長波長帯では 0.3dB/km であり長波長帯の方が有利である。しかしこれに対して、検出器に関しては量子効率が高い短波長帯の検出器が存在するが、長波長帯では-100～-200 度まで冷却をしてようやく数%程度の効率が達成され短波長帯の方が有利である。このため、量子暗号実験を行おうとした場合、どちらにもメリット・デメリットがある。

また、これら基本構成要素に加えて、量子暗号実験で大事な点として、0,1 といった

デジタル情報を光子のどのような状態に対応させて伝送するかということが上げられる。下記の次の 2 つの方法に分けられる。

[情報の載せ方]

偏光状態制御（偏光符号方式）、位相変調制御（位相符号方式）



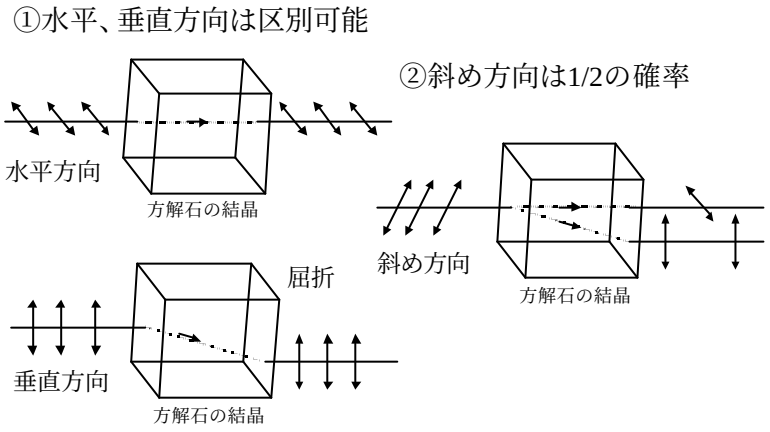
図(2)-①-c)-2.　偏光符号化、位相符号化のイメージ例

偏光状態制御とは、例えば縦偏光を 1、横偏光を 0（また、45 度偏光を 1 に 135 度偏光を 0）というように符号化することである。これを受信測定器で測定する。また位相変調制御方式では、例えば 1 はπだけ位相変調する、0 は位相変調しない（1 は 3π/2 だけ変調する、0 はπ/2 だけ変調する）ことにして、検出では干渉系を作って干渉効果を測定する。

(2)-①-c)-2. **偏光符号方式**

この方式では、デジタル情報を光子の偏光状態に対応させて載せて、情報伝送するものである。この実現方式では、偏光光子発生器（送信器）、0-90 度偏光光子測定器（受信器）、45-135 度偏光光子測定器（受信器）が必要である。

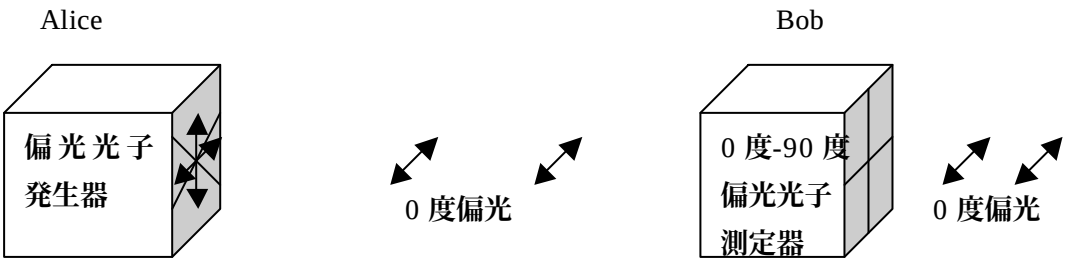
このとき例えば、イメージとして下図のような特徴を持つ方解石の結晶を使用することで、0-90 度偏光光子測定器（受信器）を、またこの方解石を 45 度傾けて 45-135 度偏光光子測定器（受信器）を用意することができる。



図(2)-①-c)-3. 方解石の結晶の仕組み

Alice **側で、ランダムに** 0,45,90,135 **度のいずれか１つの方向に偏光した光子を発生させ、**Bob **側に送る。**Alice **はランダムに** 4 **通り（**0,45,90,135 **度）の送信するパターンが存在し、そのとき** Bob **は各々の場合に対して** 2 **種類の受光器（**0-90 **度、**45-135 **度）で受光するパターンが存在するため、**4×2=8 **通りのパターンが存在する。**
下記に簡単な例を２つ示す。

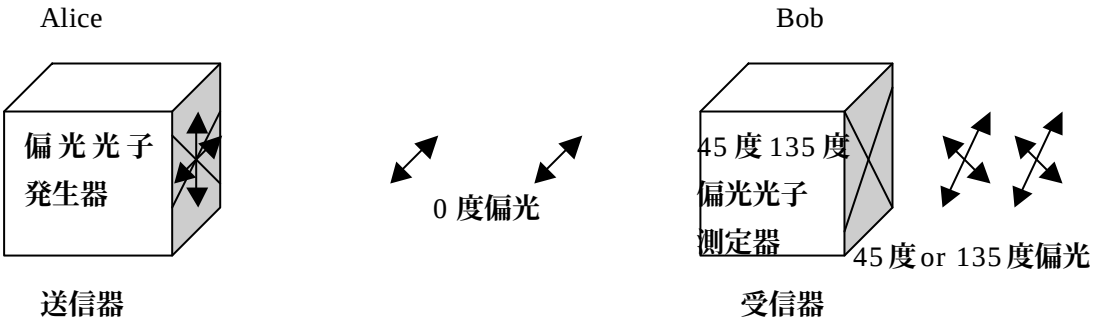
・Alice **が** 0 **度偏光の光子を発生させ** Bob **に送信し、**Bob **が** 0-90 **度偏光光子測定器（受信器）で受信した例**



送信器　　受信器

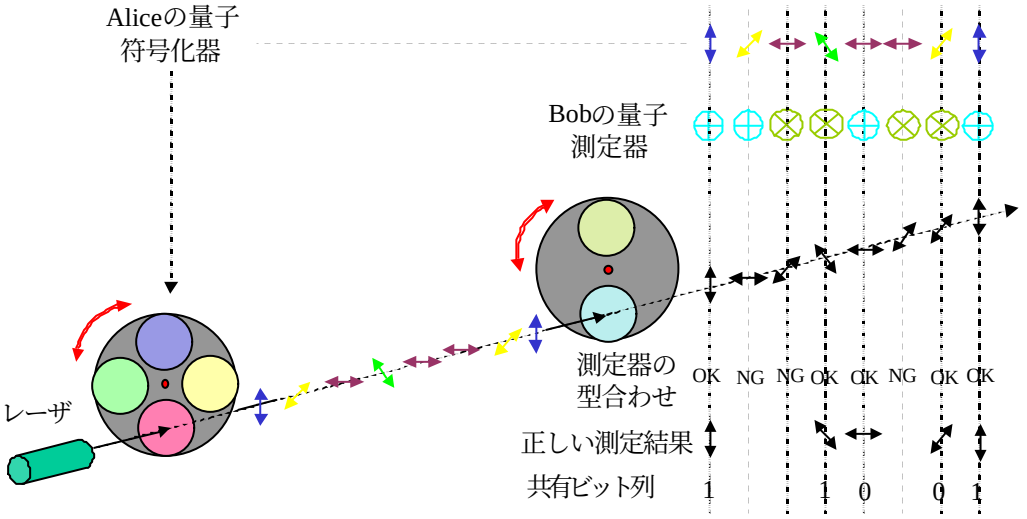
このとき、必ず Bob 側では 0 度偏光を測定する。

・Alice が 0 度偏光の光子を発生させ Bob に送信し、Bob が 45-135 度偏光光子測定器（受信器）で受信した例



このとき、Bob 側では 1/2 の確率で、45 度偏光か 135 度偏光を測定する。

BB84 プロトコルの実験系を実際に構築しようとする場合は、下記の図のようになる。即ちレーザから光を発し、4 種類の偏光状態（縦、横、45 度、135 度）に符号化する符号化器が存在する。これは例えば各々4 つの方向に偏光した偏光子を通る光路を用意し、光スイッチでランダムに切り替えることで実現できる。この光は伝送路である、自由空間や光ファイバを通り、Bob 側に伝わる。Bob は 2 種類の量子測定器をランダムにスイッチングで選択しその測定結果を記録する。このような実験系を構築することにより偏光符号方式による BB84 プロトコルが実現できる。



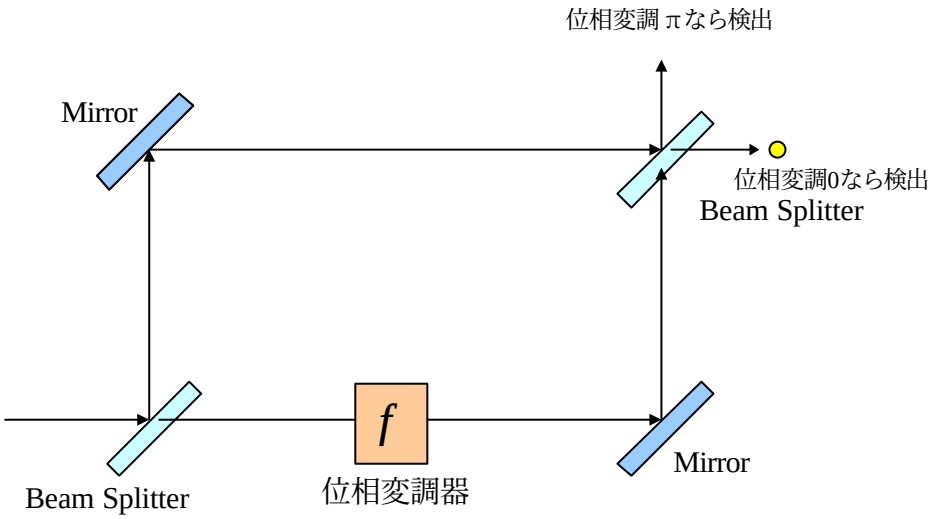
図(2)-①-c)-4. BB84 プロトコルの実験系イメージ

但し、長距離伝送して偏光状態を安定に保つことは物理的に難しい。すなわち揺らぎが生じる。そのため次ぎの位相変調方式による実現がよく用いられる。

(2)-①-c)-3. 位相変調方式

この方式では、デジタル情報を光子の位相状態に対応させて載せて、情報伝送するものである。長距離光ファイバ通信などでは、情報を位相情報として載せる方式の方が、安定性を保つのが比較的容易なためこちらの方式が実用化という観点から考えると優れている。

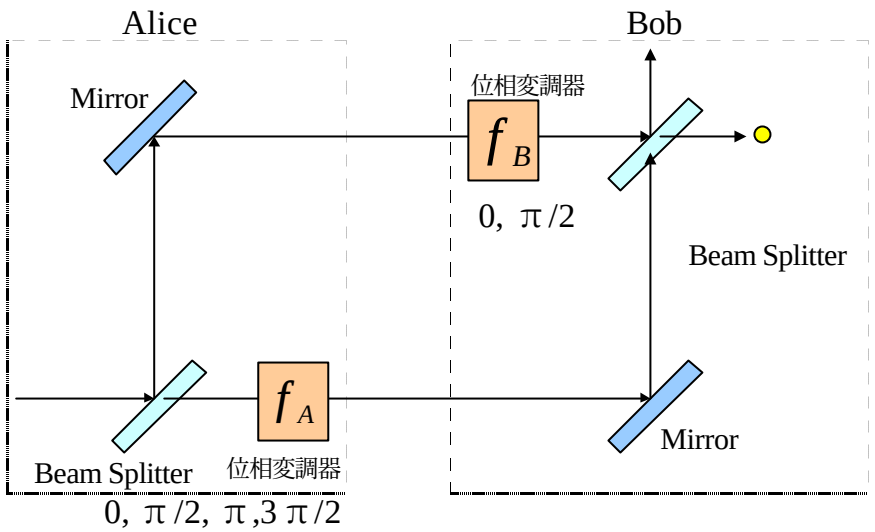
位相変調量は、通常の偏光と異なりそのものを検出するというのではなく、干渉系を組んで、その観測結果から位相情報を読み取ることになる。例えば、干渉系として次の Mach-Zehnder 干渉系を考えよう。



図(2)-①-c)-5. Mach-Zehnder 干渉系

即ち、図中の位相変調器で位相変調量が 0 かπの時、Beam Splitter の異なった方向から観測される。また位相変調量がπ/2、3π/2 の時は確率 1/2 でどちらかから検出されるのである。

この性質を利用して、Mach-Zehnder 干渉系を利用した BB84 プロトコルを次に示す。

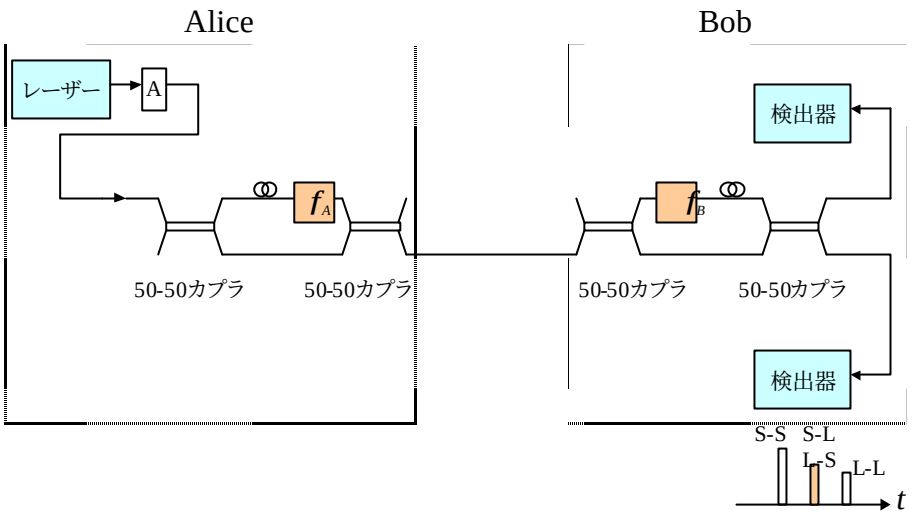


図(2)-①-c)-6. Mach-Zehnder 干渉系を利用した BB84 プロトコルの実験系

[Mach-Zehnder 干渉系を利用した BB84 プロトコル例]

1. Alice と Bob は 0,1 のランダムな列を生成する。
2. Alice からパルス光を一定の時間間隔で発し、Bob 側に送信する。
3. Alice 側では生成した 2bit 乱数に対応して位相変調量（0、π/2、π、3π/2）だけ変調する。例えば乱数 00 なら 0、01 ならπ、10 ならπ/2、11 なら 3π/2 と対応させる。
4. Bob は信号を受け取るときに、自分の生成した 1bit 乱数に対応して位相変調量（0、π/2）だけ変調する。例えば乱数が 0 なら 0、1 ならπ/2 と対応させる。
5. Bob 側で、Beam Splitter のどちらのポートから光子が検出されたかを観測する。例えば、下側だと 0、上側だと 1 というように測定結果を記録する。
6. Alice が送信し終わったあと、公開通信路を用いて、Alice は(0, π)か(π/2, 3π/2)のどちらの組かを Bob に伝え、Bob は 0 かπ/2 かを Alice に伝える。位相差が 0 かπのときのみ値を記録する。このデータを用いて共有鍵データを作り出す。

ここに、位相変調方式を用いた BB84 プロトコルの具体的な実験系を示す。



図(2)-①-c)-7. 位相変調方式を用いた BB84 プロトコルの構成例

Alice、Bob 各々１つづつ光カプラ（光分岐器）を持つことで、Alice から Bob への光路が 4 種類でき、そのうち２つの光路長が同じで位相変調量が異なる光の干渉効果を利用する構成である。残りの 2 つの光に関しては、観測タイミングで区別する。

参考文献

[1]C.H.Bennett, G.Brassard: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, Indiea(IEEE, New York, 1984) 175.

(2)-①-d) BB84 プロトコルの課題

(2)-①-d)-1．理論的課題

(ア)プロトコルの改良に関するもの

BB84 プロトコル[1]は暗号通信のための鍵共有プロトコルであって、暗号文そのものを送るものではない。暗号文はその鍵データと基本的には排他的論理和（XOR）を取って One-time-pad として送信される。したがって1度使った鍵データは２度と使えないし、送信したいメッセージと鍵の長さは同じでなければならない。そこで主に効率の観点から、メッセージを直接伝送するというアイデアが提案されている[7]。これは量子暗号で共有される鍵データを使い回しをしようとするもので、また通信に用いる光子を無駄なく使おうという発想である。具体的には鍵で暗号化されたメッセージそのものを量子通信路で送るもので、盗聴者の有無は常にモニターするというものである。盗聴者がいない限りにおいては同じ鍵を何度も用いて暗号通信を行うが、ひとたび盗聴者が検出された場合に限って、同じ鍵を用いないように制御するものである。また文献[8]のような BB84 プロトコルの改良提案もある。これは送受信者間の予備通信によりあらかじめ基底情報を共有しておこうとするものである。

(イ)安全性に関するもの

安全性の観点から、量子暗号を実現する課題を次の 3 つに分けて考える。即ち信号発生源を実現し、Bob に対してその信号を送信し、さらにその信号を効率的に測定するという３つである。

信号発生源における課題は、単一光子源ができないことからくる安全性の課題である。つまり今の段階では、単なる減光したパルスレーザを用いており、確率的に１パルスに２個以上の光子に情報が運ばれる可能性をゼロにできないことに原因がある。なぜなら盗聴者は何も擾乱を引き起こさず、２つの光子のうちの 1 つを抜き取り、完全な情報を得ることができるからである。

次に問題となるのが伝送路中のロスである。伝送の際の大きな信号のロスは、強い参照光を用いないと危険である。強い参照光は B92 プロトコル[2]がオリジナルである。つまりこれによって、盗聴者 Eve が Bob に真空状態を送って、エラーを起こさず気づかれないようにしようとする陰謀を反故にすることができる。即ち強い参照パルスは、そのような真空状態が存在できないことの証となる。

最後に光子検出器に関しては、系を単一光子状態に近づけようとすると、コヒーレント状態にある光の振幅をある値以下に小さくしなければならない。Bob の光子検出器はその検出器が開いている時間に比例した、ある決まった確率でダークカウントを検出することになる。つまり弱いパルス光を使うということは実際の光子数よりもダークカウントを増加させることにつながり、またダークカウント自体はランダムな測定結果を与えるので、結局エラーレートを増加させることにつながる。

(ウ)その他

BB84 プロトコルに比べて、Ekert の方法[3]による量子鍵共有は「量子」プライバシー増幅が使えるというメリットがある。これは通常得られる鍵よりもさらに低いエラーレートの第 0 次鍵データを得ることができるということであり、逆に雑音の多い通信路であったなら、通常の限界のエラーレートよりもさらにエラーが多くても量子暗号通信できることになる。しかし残念ながら、量子プライバシー増幅を行うのに必要なバッファやデバイスは現在のところ存在していない。

(2)-①-d)-2．実験的課題

(ア) 伝送距離

これまでシリコン・アバランシュ・フォトダイオード（APD）を使った市販の単一光子検出モジュールは波長 800㎚ 帯周辺のものだけであった。この帯域のデバイスは高い検出効率（約 50%）と低い雑音特性を持っている。しかし残念なことにこの周波数帯での光ファイバーのロスは非常に高い(2dB/㎞)。したがって長距離の通信を目指して実験をするには、現在利用されている商業的な通信波長帯 1300㎚ もしくは 1550㎚ のどちらかを用いる必要がある。なぜならこの波長帯でのロスはそれぞれ 0.35dB と 0.2dB だからである。しかしこれまではこの周波数帯での有効な市販の単一光子計数モジュールはなく、ゲルマニウムかガリウム砒素を冷却して用いたアバランシュ・フォト・ダイオードを研究所で作成しなくてはならなかった。

(イ)中継技術

量子暗号を実用的なものにするための幾つかのハードルのうちの一つはこの中継技術であると思われる。一般に遠く離れたノード間において通信のボトルネックとなるのは、ノードを結ぶ通信路の長さにエラーレートが大きく左右されることである。光ファイバーの場合、光子の吸収とデコヒーレンスの両方の確率がファイバーの長さに対

して指数関数的に増大する。整理すると次の２つの課題があると考えられる。（i）吸収されることなく光子を伝送するには、ファイバーの長さの指数関数程度の試行回数が必要。（ii）たとえ光子が検出されても、転送された状態の信頼性はファイバーの長さに対して指数関数的に小さくなる。２番目の問題は一般的な誤り訂正やプライバシー増幅精製手法を用いることで回避することができると考えられる。しかし精製手法は作用させるには，必要最低限のデータの長さが必要であり，これはファイバーの長さが限度を超えて長くなれば達成できない。

(ウ)単一光子源

量子暗号等において用いられる単一光子について、それをきっちり１つずつ発生させることのできる単一光子源を開発することは今のところ難しい技術である。現在行われている実験の大半は単一光子源というよりは、フィルターを通して減光しただけの微弱な光パルスを用いている。そこでは 1 パルス当たり平均して 0.1 個の光子が存在できるようにしている。しかしこのように減光しても 2 個やそれ以上の光子がパルスに含まれる可能性がある。これが盗聴者に盗聴の余地を与えてしまう。盗聴者 Eve はビームスプリッターを使ってそのビームを 2 つに分け、その一方を測定してもう一方を Bob に送れば良い。もちろんこうした攻撃が可能なのはビームにパルス当たり 1 個以上の光子を含んでいる場合のみである。したがって 1 パルス当たり 0.1 個と言うような微弱な光パルスを用いることで、このようなビーム分割による盗聴の成功確率を小さくしている。また Alice と Bob はこうした攻撃を想定して Eve への情報漏洩の上限を求め、さらに誤り訂正やプライバシー増幅を使って完璧な安全性を保てるように得られた鍵データの精製を行う。

その他、地上と衛星間の量子暗号の場合、Bob の光子検出効率は 10^{-3} から 10^{-4} 程度に低くなる。そのような低い検出効率でも、原理的にビーム分割攻撃により Eve はこの量子鍵配布プロトコルを破ることができる。光子源から放出される光子数に関して、ポアソン分布を仮定すると、光子 1 個の放出確率が約 0.1（10 パルスに 1 個の光子）であれば、2 個の光子が放出される割合は約 0.05 である。つまり Eve はビーム分割攻撃を使って量子信号の 5%を得ることができる訳だ。仮に Bob の収集効率が 5%よりもさらに少ない場合、Eve は理論的にはビームの分割に失敗した全ての信号を堰き止め、分離に成功した信号の中から幾つかを、ロスのない理想的な通信路を使って Bob に再送信するような戦略が考えられる。これにより Eve は Bob が受け取るものと完全に同じコピーを持つことができ、Alice と Bob によって作られた鍵に対する完全な情報を得ることができる。このことから考えて QKD においては、より良い（単一）光子源を用い

ることが重要であることが分かる。良い光子源としていわゆるパラメトリック・ダウン・コンバージョンから得られる EPR ペアがある。これはある 1 つの光子が非線形結晶を通過すると、低い周波数のエンタングルした 2 つの光子に変換される現象である。2 つの光子のうちの 1 方は、少なくともその時点で 1 つの EPR ペアが生成されたことのトリガー信号として用いることができる。非線型結晶への入力は単一光子よりもむしろ弱いレーザーパルスがしばしば用いられることから、パラメトリック・ダウン・コンバージョンは 2 つ以上の EPR ペアもゼロでない確率で存在する。しかし光子対が存在しない場合は、送信者側のデバイスのトリガー信号が無いので除外することができる。つまり光子源エラーとしてあらかじめ取り除くことができるのである。

(エ)光子検出器

一般の通信波長帯で量子暗号を実現する意味は、主に実用化に近づけるということである。それにより既設の回線を使って量子暗号を実験することも可能になるし、フィールド試験用に特別に準備する必要もなくなる。そのためにも長波長帯への移行は必然と考える。ところで光子検出器の感度をあげるには、上述のように冷却する以外に APD 型の光子検出器の性能自体の改善や、APD 以外の全く別の方式も検討することが考えられる。前者は半導体物性の改良であるが、これは巨額な開発費を伴い、あまり現実的な解ではないかも知れない。これに対して、量子光学の方面から全く別の考えで光子を検出できる可能性がでてきた。それがホモダイン測定と呼ばれるもので、文献[9]などに提案さている。

(オ)実現方式（コード化手法、システム構成等）

実験的な量子暗号においてはそのコーディング手法に 2 つの大きなタイプがある。それは偏光コーディングと位相コーディングである。適用する実験によってそれぞれ使い分けなければならない。これまで偏光コーディングの方は縷縷説明してきたので、ここでは位相コーディングがどんなものか簡単に示す。位相コーディングのアイデアはある干渉計に異なる 2 つの経路から光子を送ることである。2 つの経路は位相コーディング手法においては 2 つの直交状態を表す。ある光子を 50 対 50 のビームスプリッターを通すことにより、その 2 つのパスの干渉した重ね合わせを作ることができる。

$$\left|u\right\rangle = \frac{1}{\sqrt{2}}\left|Path1\right\rangle + \frac{i}{\sqrt{2}}\left|Path2\right\rangle$$

これに位相の違いを入れることで情報をコード化することができる。

$$|u\rangle = \frac{e^{if}}{\sqrt{2}}|Path1\rangle + \frac{i}{\sqrt{2}}|Path2\rangle$$

φを0とπ/2の間でランダムに選ぶことによって、この手法はB92手法と等価になる。Bobも同様の干渉計を使って情報を読み出すことができる。

(カ)ノイズ対策

たとえ同じ基底がAliceとBobの間で使われたとしても、AliceとBobが共有するはずのデータは様々な要因に基づくエラーによって異なってくる。その原因の１つは光子検出器におけるダークカウントである。光子検出器は光子がないときも偶然反応する。これをダークカウントと言い、このエラーを取り除くには、ある光子パルスが到着すると期待される特定の時刻に、シャッターを用意し、そのシャッターの窓枠に入らなければその受光器の反応を無視するといった方法が用いられる。ついでに言うと弱い光パルスを使ったパラメトリック・ダウン・コンバージョンEPRソースを用いると、EPRペアの一方が送信者であるAliceから検出器にトリガーを与えられるという利点がある。つまりそのタイミングの時だけBobは自分のデータに注目すればよく、トリガーのないときのダークカウントを捨てることができる。

参考文献

[1]C. H. Bennett and G. Brassard, ”Quantum Cryptography: Public key Distribution and Coin Tossing”, Proc. of IEEE int. Conf. On Comp. Sys. And Signal Proc., Bangalore, India, 1984.

[2]C. H. Bennett, “Quantum Cryptography Using Any Two Nonorthogonal States”, Phys. Rev. Lett., Vol.68, No.21, 1992.

[3]A. K. Ekert, “Quantum Cryptography Based on Bell’s Theorem”, Phys. Rev. Lett., Vol.67, No.6, 1991.

[4]L. Goldenberg and L. Vaidman, “Quantum Cryptography Based on Orthogonal States”, Phys. Rev. Lett., Vol.75, No.7, 1995.

[5]B. Huttner, N. Imoto, N. Gisin and T.Mor, “Quantum cryptography with coherent states”, Phys. Rev. A, Vol.51, No.3, 1995.

[6]M. Koashi and N. Imoto, “Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps”, Phys. Rev. Lett.,

Vol.79, No.12, 1997.

[7]K. Shimizu and N. Imoto, “Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps”, Phys. Rev. Lett. Vol.79, p.2383, 1997.

[8]工藤，臼田，内匠，畑,“量子暗号原理を応用した盗聴検出可能なデータ通信”,第２回量子情報技術研究会(QIT99)，No.41，1999．

[9]T. Hirano, T. Konishi and R. Namiki, “Quantum cryptography using balanced homodyne detection”, quant-ph/0008037, 2000.

(2)-② B92 プロトコル

(2)-②-a)B92 プロトコルの概要

(2)-②-a)-1．基本原理

【背景】

1992 年頃の量子暗号の状況は、1984 年に BB84 プロトコルが提案され[1]、引き続いて 1989 年にはこのプロトコルを用いた実験が発表された[2]他、EPR ペアという特殊な量子状態を用いた E91 プロトコルが既に提案された[3]ところである。このような状況下において BB84 プロトコルの提案者の１人である Bennet は上記２プロトコルで用いられている量子状態を一般化し、任意の２つの非直交状態を使うことで量子鍵配送が可能であることを示した。言い換えると、BB84 プロトコルと E91 プロトコルが 4 つの非直交状態を用いているのに対したった 2 つの非直交状態だけで量子鍵配送ができることを提示したのである。これが現在 B92 プロトコルと呼ばれている。

【原理】

量子鍵配送プロトコルにおいても、通常の鍵配送プロトコルと同様に Alice と Bob という 2 人のエンティティが登場する。量子版のプロトコルにおいて、この 2 者の大きな違いは Alice が量子状態を生成し、Bob は受け取った量子状態を検出するという点である。

図(2)-②-a)-1.　量子プロトコルの物理構成

B92 プロトコルにおいて Alice が生成する量子状態を以下の 2 つの非直交状態である：

$$|u_0\rangle, \quad |u_1\rangle$$

このように量子状態はケットベクトルと呼ばれるヒルベルト空間上のベクトルで記述される[5]。このケットベクトルは線形ベクトル空間を張り、その双対空間上のベクトルをブラベクトルと呼ぶ。例えば上記 2 つのケットベクトルに対応する(共役な)ブラベクトルは

$$\langle u_0|, \quad \langle u_1|$$

と表記される。このケットベクトルとブラベクトルの間には複素数値をとる内積が定義されており、上記例を用いると、

$$\langle u_0 | u_0 \rangle, \quad \langle u_1 | u_1 \rangle, \quad \langle u_0 | u_1 \rangle, \quad \langle u_1 | u_0 \rangle$$

のように表記される。
ここで、各量子状態を表現するケットベクトルを以下のように規格化しておくと便利である：

$$\langle u_0 | u_0 \rangle = \langle u_1 | u_1 \rangle = 1$$

これは、波動関数の二乗が確率として解釈されることに対応している。
さて、非直交状態を以下はのように定義される：

$$\langle u_0 | u_1 \rangle = \langle u_1 | u_0 \rangle^* \neq 0$$

逆にいうと直交状態は内積が 0 になる。ここで*は複素共役をあらわす。

このような 2 つの状態$|u_0\rangle$、$|u_1\rangle$を Bob は観測するので、その観測の仕方を規定する。一般に量子状態の観測には POMV(正定値作用素測定)が用いられ、ここでは以下の 2 つの射影演算子を用いる：

$$P_0 \equiv 1 - |u_1\rangle\langle u_1|, \quad P_1 \equiv 1 - |u_0\rangle\langle u_0|$$

もちろん、この 2 つの演算子は非可換、

$$[P_0, P_1] \neq 0$$

であるので、同時観測不可能である。更に以下の性質、

$$P_0 |u_1\rangle = 0, \quad P_1 |u_0\rangle = 0$$

から、P_0で$|u_1\rangle$を観測しても消滅してしまうので検出できない。P_1で$|u_0\rangle$を観測しても消滅してしまうので検出できないことが分かる。

但し、P_0で$|u_0\rangle$を観測したときに検出できる確率は、

$$\langle u_0 | P_0^\dagger P_0 | u_0 \rangle = 1 - |\langle u_0 | u_1 \rangle|^2 < 0$$

となり 1 以下になっている。即ち、P_0で$|u_1\rangle$を観測した場合は絶対に検出しない。$|u_0\rangle$を

観測した場合、検出できたときは確実に$|u_0\rangle$と識別できるが、検出できない場合も存在する。同様なことはP_1で観測した場合にもいえる。このように正しい観測をしても必ずしも検出できないことにより、誤った観測と正しい観測の区別がつけられないことが安全性の根拠となる。

(2)-②-a)-2.**プロトコルの記述**

【プロトコル】

1.Alice は、0、1 からなる乱数列を準備し、その並びにあわせて量子状態$|u_0\rangle$、$|u_1\rangle$を生成し、Bob に向けて伝送する：

1	0	1	1	0	1	0	0	0	1
$\|u_1\rangle$	$\|u_0\rangle$	$\|u_1\rangle$	$\|u_1\rangle$	$\|u_0\rangle$	$\|u_1\rangle$	$\|u_0\rangle$	$\|u_0\rangle$	$\|u_0\rangle$	$\|u_1\rangle$

2. Bob は、0、1 からなる乱数列を準備し、その並びにあわせて観測方式P_0、P_1を定める：

0	0	0	1	0	1	1	0	1	1
P_0	P_0	P_0	P_1	P_0	P_1	P_1	P_0	P_1	P_1

3. Bob は検出できた並びを Alice に伝える：

-	○	-	-	-	○	-	○	-	-

4. Alice と Bob は、検出された乱数列を共有する：

-	0	-	-	-	1	-	0	-	-

(2)-②-a)-3.**微弱コヒーレント光**

実験系を構築するにあたり、非直交 2 量子状態として微弱なコヒーレント光(1 パルスあたりの平均光子数: μ=0.1 位)を用いる方式が提案されている。コヒーレント光とはレーザーからでる光であり、光子検出器で検出されるような光子を 1 個、2 個、...であらわす状態(光子数状態)：

$$|0\rangle,\quad |1\rangle,\quad |2\rangle,\quad \cdots$$

を用いて記述すると(この状態群は完全直交系をなしている。ちなみに$|0\rangle$は光子数 0 の状態すなわち真空状態。)、コヒーレント状態α(複素数αで記述)は

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle \cong \left(1-\frac{|\alpha|^2}{2}\right)|0\rangle + \alpha|1\rangle + \frac{\alpha^2}{2}|2\rangle + O(\alpha^3) \qquad (|\alpha|^2 << 1)$$

で与えられる[6]。

この状態の平均光子数は$|\alpha|^2$であるので$|\alpha|^2 \approx 0.1$の場合を考える。2 つの非直交状態として通例、αの位相が 0 とπの状態：

$$|\alpha\rangle, \quad |-\alpha\rangle$$

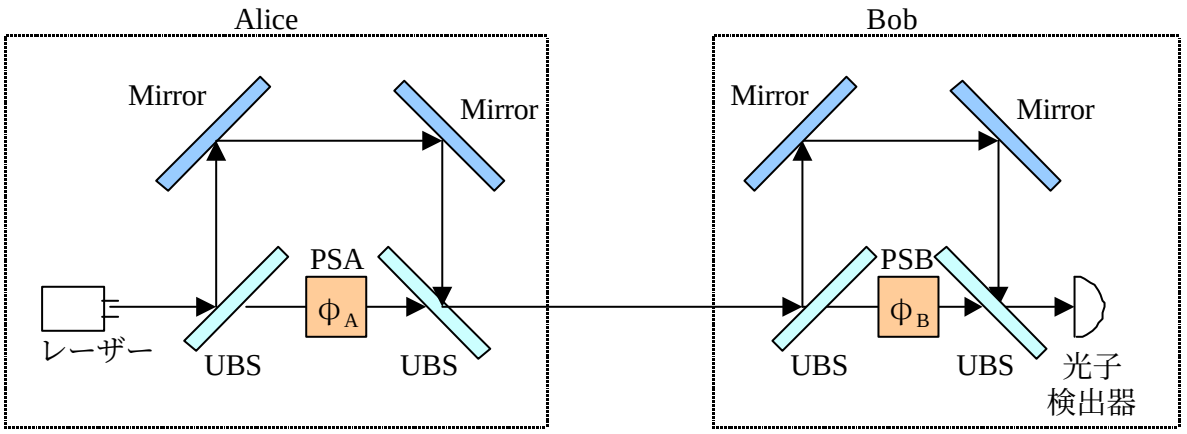
が用いられる。この 2 つの状態の内積は

$$\langle -\alpha|\alpha\rangle = \exp(-2|\alpha^2|) \neq 0$$

であるように非直交である。

(2)-②-a)- 4.実験系の記述

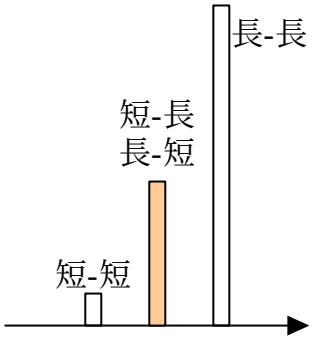
このような微弱レーザー光の量子状態を用いて、干渉系を組むことで 2 つの状態を識別する方式が当初から提案されている[4]：



図(2)-②-a)-2. B92 プロトコルの光学系

ここで、UBS は非対称ビームスプリッタ、PSA、PSB は位相変調器である。UBS は、入射パルス光を微弱パルス光と強パルス光に分割する。Alice と Bob の光路いずれも微弱パルス光の方が位相変調器 PSA、PSB を通るように設置される。従って 4 つの光路が存在することになる。PSA、PSB が設置されている方の光路をそれぞれ短光路、もう一方の光路を長光路と呼べば、短短光路、短長光路、長短光路、長長光路の４つである。このうち短短

光路を通る光は非常に微弱になり検出できなく実験には寄与しない。短長光路と長短光路を通った光が干渉することで鍵共有に寄与する。長長光路を通った光は強い光である参照光の役目を果たす。



図(2)-②-a)-3. 光路によるタイミングと強度の違い

PSA で 0、πの位相変調をかけることで 2 つの非直交状態が生成される。
PSB で 0、πの位相変調をかけることで観測方式が規定される。対応関係は以下の通り、

表(2)-②-a)-1. 位相変調と量子状態、観測方式の関係

PSA	量子状態	PSB	射影演算子	検出器
0	$\|u_0\rangle$	0	P_0	○
0	$\|u_0\rangle$	π	P_1	-
π	$\|u_1\rangle$	0	P_0	-
π	$\|u_1\rangle$	π	P_1	○

ここで、検出器が○印のある組み合わせが光子検出される可能性があるが、平均光子数 0.1 程度のレーザー光を用いているので、理想的な検出器でも 10 パルスに 1 個しか検出できないことになる。これはレーザー光の約 9 割が真空状態であることに起因する。

参考文献

[**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.

[2]C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology 5 (1992), pp.3.

[3]A. Ekert, Phys. Rev. Lett. 67,(1991)pp.661.

[4]C. H. Bennett, Phys. Rev. 68,(1992)pp.3121.

[5]**例えば，メシア，量子力学** 1-3**，東京図書**(1983).

[6]**例えば，松岡正浩，量子光学，東京大学出版会**(1996).

(2)-②-b)B92 プロトコルの課題

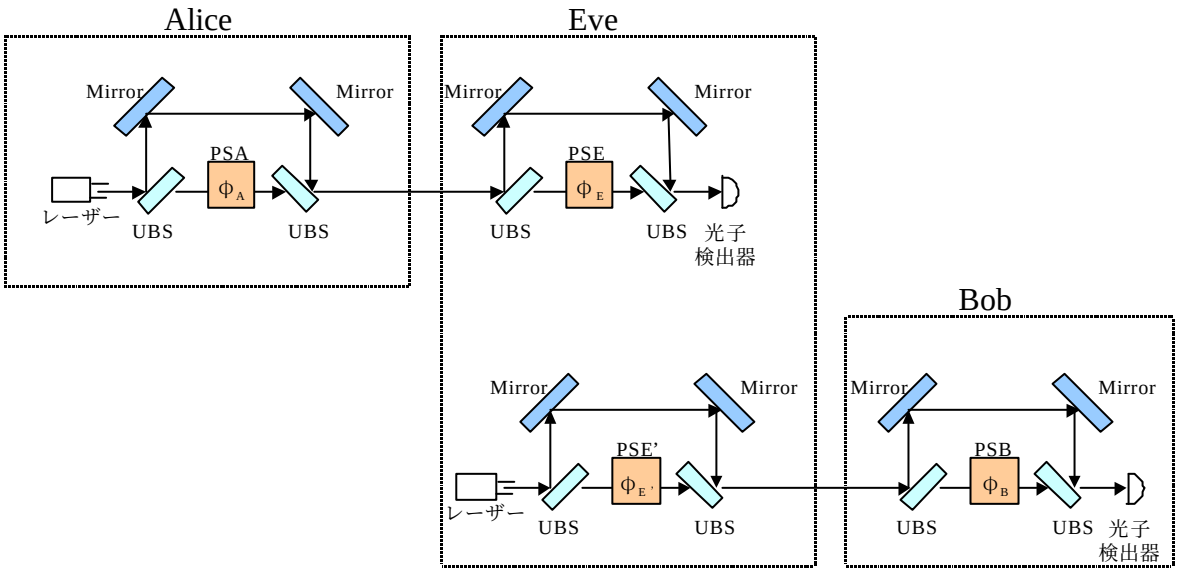
(2)-②-b)-1．安全性に関する議論

量子暗号の安全性は情報伝送の担い手となる量子に対してその状態を知ることなく量子状態を複製できないという no-cloning 定理[1]が如何になりたっているかにかかっている。これにより量子暗号の基本的特徴である盗聴検知機能が保証されるからである。

安全性の観点からは同等なことがしめされている BB84 プロトコル[2]と E91 プロトコル[3]については不確定性原理から no-cloning 定理が直接導かれるが、B92 プロトコル[4]に関してはどうであろうか。

B92 プロトコルにおける量子状態と BB84 プロトコルの量子状態の大きな違いは、観測者が理想的な量子検出器を保有していて、正しい観測方法を知っていても B92 プロトコルの場合は必ずしも量子を検出できないことである。これは本質的に情報のキャリアとして 2 つの非直交量子状態を用いていることに起因する。つまり、(2)-②-a)「B92 プロトコルの概要」でみたようにある状態について正しく観測を試みたとしても検出できる確率が原理的に 1 未満であることがポイントである。例えば、平均光子数 0.1 のレーザ光を用いた場合、かつ、量子効率が 100%である理想的な光子検出器を用いたとしても、その量子状態を検出する確率は 0.1 というように 1 未満となっている。

これがどのように効いてくるか具体的に示そう。盗聴者 Eve は Bob と全く同じ装置を用意し、Alice からの量子状態をトラップする。つぎに、Alice と全く同じ装置を用意して、観測結果に応じて量子状態を偽造し Bob に送りつける：



図(2)-②-b)-1. B92 プロトコルにおける Eve の盗聴

このとき、Eve が完璧に Alice からの量子状態を複製できないことが以下に示される。量子伝送に用いられる微弱レーザ光の平均光子数を一般にμ(<0.1)とすると、そのレーザー光に

真空$|0\rangle$が占める確率は$P(|0\rangle)=1-m$である。1 粒子状態$|1\rangle$が占める確率は$P(|1\rangle)=m$である。平均光子数を十分に小さく取っているので 2 粒子以上の状態は無視できる。いま、Eve が Alice からの量子をあてずっぽうで観測するとして、正しく観測する確率は1/2であるので、Eve が量子状態を検出し、正しく量子状態を推定できる確率は

$$\frac{1}{2}P(|1\rangle)=\frac{1}{2}m<<1$$

というようにμに依存する小さな確率にすぎない。
一方、Eve がその観測において量子検出をできない確率は、

$$\frac{1}{2}P(|0\rangle)+\frac{1}{2}=1-\frac{m}{2}\cong 1$$

である。このとき 2 つの場合が考えられる。1つはまちがった観測をした場合、もう 1 つは正しい観測をしたのだけれど検出できなかった場合である。
検出できなかったという事象が起きたときにそれがまちがった観測をした場合の確率は、

$$\frac{\frac{1}{2}}{1-\frac{m}{2}}\cong\frac{1}{2}(1+\frac{m}{2})\cong\frac{1}{2}$$

検出できなかったという事象が起きたときこれが正しい観測である場合の確率は

$$\frac{\frac{1}{2}(1-m)}{1-\frac{m}{2}}\cong\frac{1}{2}(1-\frac{m}{2})\cong\frac{1}{2}$$

となる。

従って、量子検出ができない殆ど多くの場合、Eve は全く Alice から送られた量子状態を判別不可能なまま、Bob に偽造した量子状態を送りつけなければならない。Eve から Bob に送りつけられた量子の半分は誤った状態にあり、Alice と Bob の間で行われる誤り訂正処理において、ビットエラーレートの不自然な増加が検出され Eve による盗聴行為が検知される。

以上のことから、B92 プロトコルにおける no-cloning 性は微弱レーザ光の強度(平均光子数)μに依存することが分かった。μが小さければ小さいほど no-cloning 性が強くなる。つまり、μは 1 種のセキュリティパラメタとなっている。

より一般的には 2 つの非直交量子状態の非直交性

$$\left|\langle u_0|u_1\rangle\right|^2<1$$

が 1 に近ければ近いほど no-cloning 性が強くなり安全性が高くなる。逆にいうとこの値が十分に大きい 2 つの非直交状態を選択しなければならない。

図(2)-②-b)-2. 2 つの非直交量子状態

(2)-②-b)-2．実験上の課題

光子を用いた量子暗号実験を構成する上での一般的な課題は、光子源、及び、検出器の性能でありこれは B92 プロトコルにおいてもなんら状況は同じである。

【光子源】

光子源として何を用いるかであるが、このプロトコルでは 2 つの非直交量子状態を実現しなければならないことが重要なポイントである。

このため、BB84 プロトコルでは理想的な光源とされた単一光子源は用いられないことがわかる。もし単一光子源を用いると位相 0 の状態と位相πの状態は直交状態になってしまうのである。従って、B92 プロトコルでは微弱コヒーレント光のように微弱なレーザー光が積極的に採用される。レーザー光においても強度の強いレーザー光においては位相 0 の状態と位相πの状態は十分に直交しているので使えない。もちろん平均光子数が 1 を超えているといくらでも盗聴者は光子を盗むことができることも無視できない。

では、弱ければ弱いレーザー光ほど(1)-②-b)-1 の議論から安全性は高まることがわかるがどれくらいμの値を小さくすればよいだろうか。

実は、μの値は量子暗号装置の性能にも絡んでいるパラメタであり、鍵共有ビットレート R に以下のように寄与する[5]：

$$R = q\mu n h_t h_d$$

ここで、q はプロトコル依存の因子であり、ここでは 1/2 となる。n はレーザーパルスの繰返し周波数（Hz）である。h_t は通信路上でどれだけレーザー光が減衰せずに伝わるかという伝送効率であり通信路固有のパラメタである。h_d は光子検出器の量子効率とよばれる検出器固有のパラメタであり後述する。従って、ビットレート R を大きくするためにはできるだけ大きなμにすることが望ましい。

つまり、μの値をどのくらいに設定するかは安全性と性能のトレードオフの関係にあるので、実際に量子暗号装置を運用する場合非常にセンシティブな問題となる。特に B92 プロトコルにおいては、BB84 プロトコルに比して安全性によりシビアに絡んでくるので注意したい。

なお、報告されている実験では、よく $m = 0.1$ の値が用いられている[6]。

【光子検出器】

B92 プロトコルに特定されることなく一般に量子暗号装置用の光子検出器として要求される性能は、たった 1 個の光子が検出器に入射されたとき、取りこぼしなく捕らえ電気信号に変えて出力することである。従って、2 つの特性値が規定される：

①量子効率：h_d

②ダークカウント率：n_{dark}

である。

ここで①量子効率とは 1 個光子が検出器に入射したときに出力信号がでる確率である。理想的な量子効率は 1(もしくは 100%)であり必ず出力信号がでる。しかし、光子検出器においては、市販の波長 830nm 用光子検出器で高々50%くらいである。一般に通信用光ファイバに用いられる 1550nm 用 APD(光子検出器のコアとなるアバランシェフォトダイオードという素子)では数%位にしかならなく、一般の光ファイバー通信に量子暗号を載せるための大きな課題となっている。

②ダークカウント率とは、逆に光子が入射しないのに検出器から偽の出力信号が単位時間当たりに出力される確率である。従って n_{dark} が大きいとビットエラーレートが大きくなってしまう。ビットエラーレートおよびビットレートの観測により盗聴検知を行う量子暗号では、従ってできるだけこのダークカウント率を小さくすることが望まれる。しかしながら、量子効率とダークカウント率の間には一般に正の相関が認められるので、よりよい光子検出器を手に入れることは難しく量子暗号実用化のもっとも大きな問題となっている。

【光学系】

B92 プロトコルの代表的な実現方式は光学的には微弱コヒーレント光を用いた干渉系を構成することで実現される。遠く離れた Alice と Bob で干渉系を構成することは、伝送路上での位相揺らぎが無視できないため技術的に困難な課題を提供している。実際にそれなりの性能をもつ光子検出器を得られたとき量子暗号装置のビットエラーレートを支配するのはこの干渉明瞭度(Visibility)の悪さによる寄与である。（ダークカウントに関してはレーザーパルスの時間幅を十分シャープにとることで観測に寄与する正味のカウントを桁違いにちいさくできる。）この位相揺らぎに対して安定な干渉系を得ようとする試みとしてファラディーミラーという光学素子を用いて自動的に揺らぎを補償する方式が提案されビットエラーレートを 0.15%にまで抑えた実験が報告されている[6]。

参考文献

[1]W. K. Wooters and W. H. Zurek、 Nature 299, (1982),pp.802.

[2]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.

[3]A. Ekert, Phys. Rev. Lett. 67,(1991)pp.661.

[4]C. H. Bennett, Phys. Rev. 68,(1992)pp.3121.

[5]H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, G. Ribordy, Appl. Phys. B67, (1998),pp.743.

[6]H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and, W. Tittel, Electron Lett. 33,(1997), pp.335

(2)-③　E91 プロトコル

(2)-③-a)E91 プロトコルの概要

(2)-③-a)-1. 基礎概念

E91 プロトコルのアイディアは、量子相関を利用することにより、鍵の配布と保管の双方に安全性を保証する暗号体系を作り出すということである。ここで量子相関（量子もつれあい）として EPR 効果（アインシュタイン・ポドルスキー・ローゼ、Einstein-Podolsky-Rosen）をうまく利用して実現する。

EPR 効果は､例えばある Source から量子力学的に相関のあるもつれ合った光子のペアが発生した時、生じる。2 個の光子は、偏光がまだ決まっていない初期の状態において生成される。しかし初期状態が対称であるために、2 個の光子は同じ型の検出器で測定すれば反対方向に偏光していることになる。例えば、Alice と Bob が＋測定器を使って測定すると、2 人は 0（水平偏光）か 1（垂直編光）かを同じ確率で記録する。もしアリスが 0 を得たなら、ボブは確実に 1 を得るはずであり、その逆も真である。

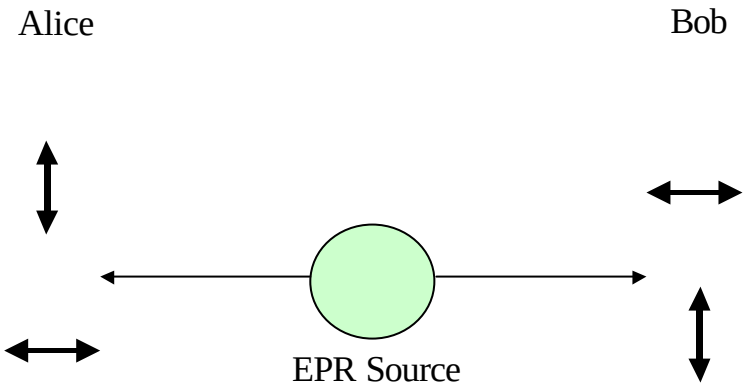
EPR 効果の非常に重要な点は、2 個の光子の一方が測定されるや否や両方の偏光が確定することであり、測定以前には確定しない。すなわち、一方（例えば Alice）が観測して観測値が決定した瞬間に、遠く離れているもう一方（例えば Bob）の状態が決まってしまうわけである。情報が光速を超えて、瞬時に伝わっているような錯覚すら抱かせる奇妙な物理現象である。

ここで、量子もつれ合った 2 粒子状態を下記に式とイメージ図で示す。

[2 粒子]

EPR 状態

$$|f\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle|\leftrightarrow\rangle - |\leftrightarrow\rangle|\updownarrow\rangle)$$



図(2)-③-a)-1. EPR 対のイメージ

ではここで簡単に E91 の処理イメージを説明する。E91 プロトコルの簡易版の処理の流れは次の通り。

[E91 プロトコルの簡易イメージ]

1) source がもつれ合った光子対(pair of entangled photons)を発生する
2) Alice と Bob は各々いくつかこの光子対を保つ
3) Alice と Bob は、盗聴者がいるかテストのために、その偏光状態のいくつかを測定する
4) テストせずに残った光子対は測定せずに貯めておく
5) 鍵が必要なとき、観測して、貯めている光子対のいくつかを比較する
6) tampering がなければ、各々の対の偏光は反対となる
7) テスト光子対に対して、これが実際正しいことを Alice と Bob は確認する
8) 残りの光子対の偏光をランダムに 2 つの base を独立に測定する
9) BB84 と同じく privacy amplification で鍵を精製する

(2)-③-a)-2. **プロトコル詳細**

この節では、より詳しくプロトコルを追っていくことにする。前述の通り、量子もつれ合いを利用した E91 **プロトコルは、例えば次のような偏光の光子対を使って実現される。**

$$|f\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle|\leftrightarrow\rangle - |\leftrightarrow\rangle|\updownarrow\rangle)$$

[**プロトコルの詳細な流れ**]

step1. **もつれ合った光子対を** source **から発生し** Alice **と** Bob **に送信する**

step2. 3 **つの観測基底（下記の通り）のうち** 1 **つを選択して** Alice **と** Bob **は測定する**

Alice：＋**基底を** z **軸方向に** $f_1^a = 0$、$f_2^a = p/4$、$f_3^a = p/8$**だけ回転させた基底**

Bob ：＋**基底を** z **軸方向に** $f_1^b = 0$、$f_2^b = -p/8$、$f_3^b = p/8$**だけ回転させた基底**

（**このとき、 次の量** $E(f_i^a, f_j^b)$ **が** Alice **の** f_i^a **だけ回転した観測基底での観測結果と**

Bob **の** f_j^b **だけ回転した観測基底での観測結果の相関係数となる**

$$E(f_i^a, f_j^b) = P_{++}(f_i^a, f_j^b) + P_{--}(f_i^a, f_j^b) - P_{+-}(f_i^a, f_j^b) - P_{-+}(f_i^a, f_j^b)$$

$$E(f_i^a, f_j^b) = -\cos[2(f_i^a - f_j^b)] \quad)$$

step3. **次の量** S **が** Alice **と** Bob **が異なる方向の測定器を使った場合の相関係数からなる値として定義できる**

$$S = E(f_1^a, f_3^b) + E(f_1^a, f_2^b) + E(f_2^a, f_3^b) - E(f_2^a, f_2^b)$$

（**この値** S **は** Clauser, Horne, Shimony, Holt **によって一般化された** Bell **の定理の提案したときの** S **と同じで、**CHSH inequality **として知られている。量子力学の原理により、** $S = -2\sqrt{2}$ **となる。**）

step4. **量子通信後、**Alice **と** Bob **は個々の測定時に選択した測定器の方向を公開する**

step5. また測定結果を 2 つのグループに分ける

first group　異なる方向の測定器を使った測定結果

second group　同じ方向の測定器を使った測定結果

step7. Alice と Bob または、片方一方が観測に失敗した測定は全て捨てる

step8. Alice と Bob は first group（異なる方向の測定器使用）の測定結果のみ公開する

step9. これより、Alice と Bob が異なる方向の測定器を使った場合の相関係数 S を計算する

（もし、粒子が直接的にまたは間接的に擾乱（disturb）されていなければ、$S = -2\sqrt{2}$ となるはずである。）

step10.これにより、正規の通信者(legitimate users)は second grou から得られた結果が逆相関(anti-correlated)していることが保証され、これらを秘密のビット列（共有鍵）に変換することができる

以上の手順により、盗聴者検出及び絶対安全に鍵共有ができることになる。

この後、通常の他の鍵共有プロトコルで行うようにプライバシ増幅（privacy amplification）処理を行うことで共有データを精製する。

参考文献

[1]A.K.Ekert: Phys. Rev. Lett. 67 (1991) 661.

[2]C.H.Bennett, G.Brassard, N.D.Mermin: Phys. Rev. Lett. 68 (1992) 557

[3]J.F.Clauser, M.A.Horne: Phys. Rev. D 10 (1974) 526

[4]A.Garg, N.D.Mermin: Phys. Rev. D 35 (1987) 3831

[5]J-A.Larsson: Phys. Rev. A 57(1998) 3145

(2)-③-b)E91 プロトコルの課題

盗聴者の存在は、公開通信路(public channel)でやりとりして、Bell の不等式(Bell's inequality)が満たされているか否かでわかる。すなわち Bell の不等式が成立していたら、盗聴者(Eve)の存在が検知できる。また Bell の不等式が成立していない場合は、盗聴者(Eve)は存在していないということになる。

実際の実験では、光源や検出器の信頼性まで含めて鍵共有プロトコルを評価する場合には、チャンネルロスや検出器の非効率はプロトコルの安全性に大きな影響を与えることに注意する必要がある。これはもちろん、もつれ合った状態を利用した E91 プロトコルの場合でも同様である。特に E91 プロトコルでは、Bell の不等式による量子力学的非局所性の実験的証明において問題になる、detection loophole の問題（すなわちチャンネルロスや検出器の非効率により、局所的な隠れた変数モデルが排除できない問題）と関連しているため、ある一定以上の量子効率が必要になるなど注意が必要である。

参考文献

[1]A.K.Ekert: Phys. Rev. Lett. 67 (1991) 661.

[2]C.H.Bennett, G.Brassard, N.D.Mermin: Phys. Rev. Lett. 68 (1992) 557

[3]J.F.Clauser, M.A.Horne: Phys. Rev. D 10 (1974) 526

[4]A.Garg, N.D.Mermin: Phys. Rev. D 35 (1987) 3831

[5]J-A.Larsson: Phys. Rev. A 57(1998) 3145

(2)-④ **その他のプロトコル**

(2)-④-a) GV **プロトコルの紹介**

(2)-④-a)-1.**基本原理**

これまで述べてきた代表的な量子鍵配送プロトコルでは、安全性の根拠として非直交量子状態に依拠する no-cloning **定理に基づいている。従って、直交状態を用いた方式は考えられてこなかったのだが、**1995 **年になり** Goldenberg **と** Vaidman **は直交状態を用いても安全な量子鍵配送プロトコルを構成できることを示した**[1]**。これが提案者にちなんで** GV **プロトコルと名付けられたプロトコルである。ではこのプロトコルの安全性は何に基づき、どのように構成していくのであろうか。**

まず、no-cloning **定理を軽くおさらいすると、盗聴者** Eve **が情報を盗み見しようと量子状態の観測を試みたとき、被観測状態が** 2 **つの非直交量子状態であれば正しい観測を試みたときのみ正しく観測できるのであるが、まちがった観測を試みたときはその観測結果が正しいのか、間違っているのかも判別できない。よって、正しい量子状態を複製し** Bob **に送り付けることができないので、**Alice **と** Bob **はビットエラーレートの変化により盗聴検知をしてしまうのであった。もし、被観測状態が直交状態であるとすると、正しい観測、間違った観測という区別は存在しなくなり、**Eve **は常に正しく量子状態を識別することができ、正しい量子状態を複製し** Bob **に送りつけることができる。従って、**Alice **と** Bob **はなんら** Eve **が盗聴したという事象を検知できなくなってしまう。**

では、上記のような問題を GV **プロトコルではどのように克服したかというと以下の時間に関するポイント** 2 **点に基づき解決している：**

i.) **局所量子状態の時間差伝送**

ii) **ランダム時間伝送**

まず、量子状態として時間的に局所化された 2 **つの波束：**$|a\rangle$**、**$|b\rangle$**を用意する：**

$$\langle a|a\rangle = \langle b|b\rangle = 1, \quad \langle a|b\rangle = 0$$

この 2 **状態を基に、情報のキャリアとして以下の** 2 **状態を定義する：**

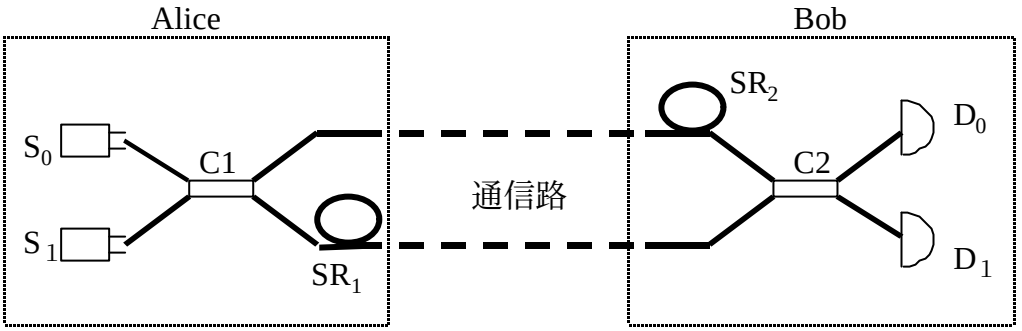
$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle),$$

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle),$$

ここで添字の 0**、**1 **は伝送すべき情報ビットに対応する。従って、この** 2 **状態は直交している。量子生成、量子検出するときは**$|\Psi_0\rangle$**、**$|\Psi_1\rangle$**の状態で行われるが伝送時は**$|a\rangle$**、**$|b\rangle$**の状**

態で行われ、しかも$|a\rangle$、$|b\rangle$は同時に伝送路に入射されるのではなくある固定された時間差tをおいて順々に入射される。このとき、Alice から Bob への伝送時間qに比べて$t > q$であるとする。即ち、$|b\rangle$が伝送路上に現れるのは既に$|a\rangle$が Bob 内に取り込まれた後であり、伝送路上にこの２つの状態が同時に存在することはない(厳密にいうとtのこのような制限はきつすぎである)。

では、このような特性を実現する実験系の構成図を下記に示す。



図(2)-④-a)-1.GV プロトコルの光学系

これは Mach-Zehnder 干渉系を応用したもので、Alice は S0、S１という 2 つの光子源をもっている。S0 から発生する状態が$|\Psi_0\rangle$、S１から発生する状態が$|\Psi_1\rangle$である。Alice は０を送信したいときは S0 から光子を発射、1 を送信したいときは S1 から光子を発射する。同時に 2 つの光子源から光子が発射されることはない。いずれから発射された光子も方向性結合器 C1 において２つに分離される。このとき上側の光路を通過する波束が$|a\rangle$、下側の貯蔵リング SR_1があるほうの光路を通過する波束が$|b\rangle$となる。この貯蔵リングの長さが時間差tを決定する。この時間差tが第 1 のポイントであった。伝送時間qは通信路の長さ(破線部分)により決まる。2 つの波束は方向性結合器 C2 において再結合され直交状態$|\Psi_0\rangle$、$|\Psi_1\rangle$を再生する。このため$|a\rangle$が通る光路上に設置された貯蔵リング SR_2 は干渉が起こるように SR_1に合わせてうまく調整しておく。結果として$|\Psi_0\rangle$が再生されたときは光子検出器 D0 で光子が検出され、$|\Psi_1\rangle$が再生されたときは光子検出器 D1 で検出される。

なお、Alice は S0、S1 いずれの光子源を用いて光子を発生するときもランダムなタイミングで光子を発生する。このとき、その発生時刻t_sを記録しておき。Bob は光子を検出したとき、その検出時刻t_rを記録することが第 2 のポイントであった。

Alice と Bob が行う盗聴検知の戦略は以下の 2 つである：

i)タイミングテスト

ii)ビットエラーテスト

タイミングテストというのは、発生時刻t_sと検出時刻t_rとの関係：

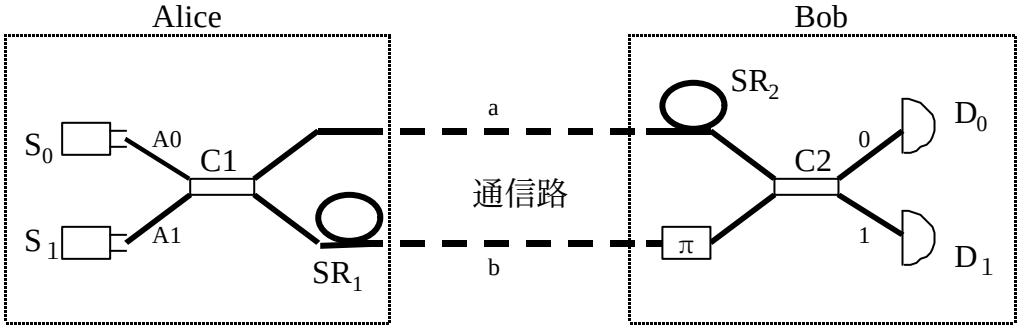
$$t_r = t_s + \boldsymbol{t} + \boldsymbol{q}$$

を確認するものである。これにより、Eve が波束$|a\rangle$をトラップしておき波束$|b\rangle$が出てくるの待って直交状態$|\Psi_0\rangle$、$|\Psi_1\rangle$を特定するという攻撃を検出できる。ここで、発生時刻のランダムさがダミーの波束$|a\rangle$を使うという攻撃を妨げている。($\boldsymbol{t}$ の大きさの制限はこのタイミングテストが有効である大きさまで小さくできる。つまり、t_s、t_rの時間精度Δtに対して$\boldsymbol{t} > \Delta t$となる)。

2 番目のビットエラーテストは、BB84 プロトコル等で用いられるビットエラーレートからの盗聴検知と同じである。

(2)-④-a)-2.改良 GV

GV プロトコルのポイントとしてランダムタイミングで光子発生を行うことにより Eve がダミーの波束を発生させることで盗聴検知を無効化するという攻撃を防いでいたのだが、1997 年に小芦と井元は 2 本ある伝送路に非対称性を持ち込むことでランダムタイミングとそれに伴うタイミングテストの不要な方式を提案した。



図(2)-④-a)-2.改良 GV プロトコルの光学系

以下、上記構成図をもとに説明する。なお、この図は GV プロトコル図と殆ど同じであるが方向性結合器 C1、C2 が分岐比 50：50 ではなく T：R(T+R=1)である点、Bob 側の光路

b側に位相シフタがあり位相がπシフトされている点が異なっている。なお、図中 A0、A1、0、1、a、b は方向性結合器のポート、もしくは光路をあらわしている。

まず、方向性結合器 C1 を通過した光子の状態は、S0、S1 からの光子それぞれ

$$|\Phi_0\rangle = \sqrt{T}|0\rangle_a|1\rangle_b - i\sqrt{R}|1\rangle_a|0\rangle_b$$

$$|\Phi_1\rangle = \sqrt{T}|1\rangle_a|0\rangle_b - i\sqrt{R}|0\rangle_a|1\rangle_b$$

となる。ここで、$|0\rangle_a$、$|1\rangle_a$ は光路 a 上に光子数がそれぞれ 0 個、1 個ある状態をあらわす。

同様に$|0\rangle_b$、$|1\rangle_b$は光路b上に光子数がそれぞれ 0 個、1 個ある状態をあらわす。

次に、光路 b 上にある位相シフタのおかげで伝送路を通る 2 つの状態$|1\rangle_a|0\rangle_b$、$|0\rangle_a|1\rangle_b$ は方向性結合器 C2 を通過するとそれぞれ、

$$|1\rangle_a|0\rangle_b \rightarrow \sqrt{T}|0\rangle_0|1\rangle_1 - i\sqrt{R}|1\rangle_0|1\rangle_1$$

$$|0\rangle_a|1\rangle_b \rightarrow -(\sqrt{T}|0\rangle_0|1\rangle_1 - i\sqrt{R}|1\rangle_0|1\rangle_1)$$

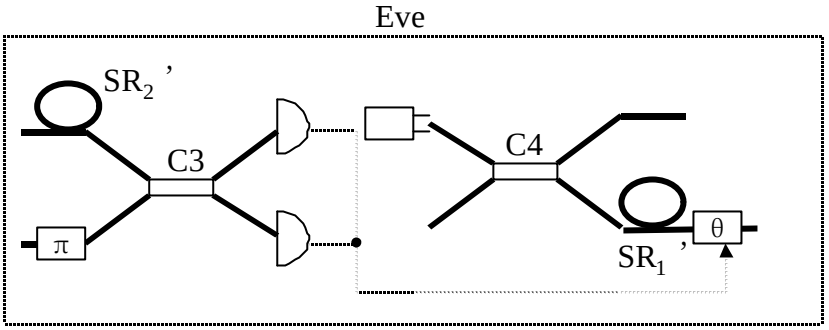
のようになる。結果として S0、S1 から出た光子状態$|\Phi_0\rangle$、$|\Phi_1\rangle$はそれぞれ

$$|\Psi_0\rangle = -|1\rangle_0|0\rangle_1$$

$$|\Psi_1\rangle = |0\rangle_0|1\rangle_1$$

となり D0、D1 で検出される。

ここで、T=R のときは光子状態$|\Phi_0\rangle$、$|\Phi_1\rangle$の違いは全体の位相を除けば GV プロトコルで情報のキャリアとなった状態そのものであり、当プロトコルが GV プロトコルを拡張したものであることがわかる。では、Eve の攻撃を考察することでどのような違いがあるかをみよう。Eve の攻撃法として以下の図のように Bob と同型の量子受信装置と Alice の量子送信装置を若干改造したものを Alice と Bob の通信路上に挿入することが考えられる。



図(2)-④-a)-3．Eve の盗聴装置

このような装置を用いて盗聴を試みたとき Eve の戦略としては、光子検出器の結果に従って、Alice が送信した光子状態$|\Phi_0\rangle$、$|\Phi_1\rangle$を判定し、同じ状態を Bob に送るように貯蔵リング SR_1'からでた光子に位相変調器θで位相変調をかけるのである。この装置を使えば、予めダミー光子を Bob に向けて発射しておいて、Alice からの光子を検出後に位相変調かけることが可能になる。従って、GV プロトコルでは光子の発射タイミングをランダムにする必要があった。ところが、改良プロトコルの場合ダミー光子を発射して位相変調をθかけた場合、Bob の受取る量子状態はその非対称性のため、

$$|\Psi_f\rangle = -\frac{1}{\sqrt{2}}(\sqrt{T}e^{iq}+\sqrt{R})|1\rangle_0|0\rangle_1 + \frac{i}{\sqrt{2}}(\sqrt{R}e^{iq}-\sqrt{T})|0\rangle_0|1\rangle_1$$

のような 2 つの状態の重ね合わせとなる。これからビットエラーとなる確率は間違った方の状態となる確率：

$$\frac{1}{2}(\sqrt{T}-\sqrt{R})^2 = \frac{1}{2}-\sqrt{TR}$$

で与えられ盗聴検知が可能となる。従って、ランダムタイミングで光子を発射しなくてもよいのである。

(2)-④-a)-3.**鍵配送プロトコルの体系化**

さて、これまでに鍵配送プロトコルとして代表的な BB84 プロトコル、B92 プロトコル、E91 プロトコル、GV プロトコルについて述べてきたがどのように分類することができるであろうか、最近、井元、小芦のグループにより見通しのよい知見が得られいるのでその点について触れておきたい[3,4]。

これは量子状態への情報の載せ方を no-cloning **定理との関係から分類したもので、**Alice **と** Bob **の間でやりとりされる情報に着目したものである**

表(2)-④-a)-１伝送情報に基づくプロトコルの分類

	プロトコル	特長
量子状態のみ	B92	非直交 2 量子状態
量子状態＋古典情報	BB84,E91	古典情報の時間差をつけた伝送
量子状態＋量子情報	GV，改良 GV	量子情報の時間差をつけた伝送

このように分類されると理論的にはほぼ網羅されてきたといってよい。もちろん実験的には変調方式による位相変調と偏光変調方式、光子源に単一光子源とコヒーレント光源を用いる方式という具合にまだまだ多くの方式の提案がなされる可能性がある。

参考文献

[1]L. Goldenberg and L. Vaidman, Phys. Rev. Lett. 75, (1995), pp.1239.

[2]M. Koashi and N. Imoto, Phys. Rev. Lett. 79, (1997), pp.2383

[3]井元，小芦，日本物理学会誌 56, (2001),pp.17.

[4]小芦，レーザー研究 28, (2000), pp.677.

(3) **現実的な仮定に基づく安全な量子ビットコミットメント**

(3)-① **量子ビットコミットメントの不可能定理**

(3)-①-a) **ビットコミットメント**

(3)-①-a)-1. **ビットコミットメントとは**

いま、Alice **と** Bob **がネットワークを介して次のコイン投げゲームを行うことを考える。**

Alice **と** Bob **はそれぞれ独立に** 1 **ビットの値を選び、その排他的論理和が** 1 **ならば** Alice **の勝ち、**0 **ならば** Bob **の勝ちとする。**

ここで公平性の観点からは、Alice **と** Bob **が対称であること、したがって、**Alice **の値と** Bob **の値が同時に開示されることが重要である。しかし、とくにネットワーク上で通信をしているような場合にはその同時性を確保することは困難であり、必然的に** Alice **と** Bob **の情報の開示に時間差が生じることになる。したがってこのような場合、その時間差を利用して先に情報を得た方がその情報をもとに自分の値を偽る不正（いわゆる「後出し」)ができないようなスキームを考える必要がある。実際のコイン投げでは、まず** Alice **が値を決め（コインを投げ)、次に** Bob **が値を決め（表裏を選択し)、最後に** Alice **が値を開示することになるが、ここで公平性の観点から重要なのは、**Bob **が表か裏かを決める際に** Alice **のコイン投げの結果がわからないこと（** Bob **の不正が不可能)、**Alice **がコイン投げの結果を公開する際にいかさまができないこと（**Alice **の不正が不可能)、の** 2 **点である。実際のコイン投げでは、**Alice **と** Bob **が実際にそのコイン投げに立ち会うことによりいわば物理的にこの問題を解決しているが、暗号技術的にこの問題を解決する一つの方法がビットコミットメント** BC(b,r) **（ただし、**b **はコミットするビット、**r **は乱数）である。**

ここでビットコミットメントとは、以下の 2 **つの性質(**P1)、(P2)**をみたす関数** BC:{0,1}$\times\{0,1\}^{k}\rightarrow\{0,1\}^{l}$ **のことである。**

(P1) BC(b,r)=BC(b',r')**となるような**(b',r'), b≠b'**を求めるのが困難である。**

(P2) X **の値（ただし、**X=BC(b,r)**）から、**b **を求めるのが困難である。**

ここで、性質(P1)**は** Alice **の不正が不可能であること（拘束性)、(**P2)**は** Bob **の不正が不可能であること（秘匿性）に対応している。この** BC(b,r)**を用いて、以下のようにコイン投げプロトコルを構成することができる。**

1) A **は、ランダムなビット** b $\in_U$\{0,1\}**、乱数** r **を選び、**X=BC(b,r)**を計算する。**A **は** X **を** B **に送る。**

2) B **は、ランダムなビット** c $\in_U$\{0,1\}**を選び、**c **を** A **に送る。**

3) A は、(b,r)を B に送る。

4) B は、X=BC(b,r)が成立するかどうかを検証する。

ビットコミットメントは、上記コイン投げプロトコルのほかにも電子入札や電子投票など多様な応用が考えられる重要な暗号プリミティブである。

(3)-①-a)-2. ビットコミットメントの安全性

ビットコミットメントが安全であるためには、Alice、Bob 双方の不正が不可能でなければならない。したがって、ビットコミットメントが性質(P1)、(P2)をみたすとき安全であると定義する。性質(P1)、(P2)においては計算の困難性が仮定されているが、ここで問題となるのは、Alice と Bob がどの程度の計算能力を持つかということである。ビットコミットメントは、Alice と Bob の計算能力の仮定に関して、次の 2 つのタイプに分類される。

タイプ 1：

A が確率的多項式時間チューリング計算機（B は無限の計算能力を持ってよい）とした場合に安全

タイプ２：

B が確率的多項式時間チューリング計算機（A は無限の計算能力を持ってよい）とした場合に安全

代表的な構成法は、それぞれ、

タイプ 1：$BC(b,r)=g^b h^r \bmod p \ (h=g^a)$

タイプ 2：$BC(b,r)=g^b \| r \bmod p$

で与えられる。計算能力に対する仮定としては、もちろん無限の計算能力を持ってよいとする仮定が最も弱く、それゆえ安全性の観点からは最も安全である。したがって、A、B ともに無限の計算能力を持ってよいとする仮定が、最も安全な仮定ということになるが、この仮定をみたすようなビットコミットメントは存在しないことが知られている。

ビットコミットメントの安全性

	タイプ 1	タイプ 2	存在しない
A の計算能力	多項式時間	∞	∞
B の計算能力	∞	多項式時間	∞

参考文献

[1] **岡本龍明，山本博資：現代暗号，産業図書** (1997)

[2] J. Gruska: Quantum computing, Mc Graw Hill (1999).

(3)-①-b) 量子ビットコミットメント

(3)-①-b)-1. 量子ビットコミットメントとは

ビットコミットメントの安全性のところで具体的に挙げた構成法は、どちらも離散対数問題を解くのが困難であるとするいわゆる計算量的安全性に基づく方式である。この他にも、現在標準的に用いられている暗号技術の多くは、離散対数問題や素因数分解を解くのが困難であるとする仮定に基づいている。これらの仮定は、通常の計算機上では妥当であると広く信じられているが、通常とは異なる原理に基づく計算機上で妥当であるとは限らない。実際、量子計算機上では素因数分解や離散対数問題は簡単に（多項式時間で）解かれてしまうことが示されている。ここで量子計算機とは、量子効果を利用することにより格段に情報処理能力が向上した（と期待される）計算機のことである。この他にも量子効果を利用することによって、無限の計算能力を持つ盗聴者にも解読不能な量子鍵配送、古典的な情報伝送レートの限界であるいわゆるシャノン限界をも超える量子通信など、革新的な情報技術が提案されている。

ビットコミットメントの安全性に関しては、Alice、Bob ともに無限の計算能力を持つ場合でも安全（無条件に安全）であるものは存在しないことはすでに述べたが、これはあくまで古典的な情報技術に基づいた場合のことであり、量子情報技術を用いた場合のその存在性については自明ではない。すなわち、量子効果を利用することによって、無条件に安全なビットコミットメントが構成できる可能性があることになる。実は、量子効果を利用しても無条件に安全なビットコミットメントを構成することは不可能であることが示されているが、量子効果を利用することによってその安全性が計算量的な仮定に拠らないビットコミットメントを構成することは可能である。このようなビットコミットメントのことを量子ビットコミットメントと呼ぶ。

(3)-①-b)-2. 無条件に安全な量子ビットコミットメントの不可能定理

以下では、無条件に安全な量子ビットコミットメントが存在しないという Lo and Chau [1]および Mayers[2]の結果について概説する。

まず、通信を行う二者、Alice と Bob は事前にセキュリティパラメータ s を決めておく。次に Alice はコミットする値 b を{0,1}から選ぶ。もし、b=0 の場合には直線偏光基底により、b=1 の場合には円偏光基底によりｓ個の光子に乱数値 r を符号化し Bob に送るものとする。Bob は、光子ごとに直線偏光基底か円偏光基底かをランダムに選んで s 個の光子を測定する。Bob はこの測定結果からただちに Alice のコミットした値 b を知ることはできないが、あとで Alice が乱数値 r を開示したときにはこの測定結果から b の値を検証することができる。これにより、量子ビットコミットメントが構成されたようにも思われるが、以下で述べるように Alice はコミット値 b を Bob への開示直前に覆すことができる。すなわち、Alice は完全にエンタングルした光子対(EPR pair)を s 組用意し、対の片方の光子群を Bob に送り、残りを手元に保管しておく。そして、Bob からの開示要求が

あってからコミット値 b を選択し、b に対応する基底により手元の光子群を測定し、その結果を乱数値 r として Bob に送ることによって Bob の検証を欺くことが可能となる。以上具体例により説明したが、一般に、エンタングル状態を利用することにより Alice 側の不正（コミット値の反転）が可能であることが示されている。

参考文献

[1] H.-K. Lo and H. F. Chau: Phys. Rev. Lett. 78 (1997) pp.3410.
[2] D. Mayers: Phys. Rev. Lett. 78 (1997) pp.3414.

(3)-② 改良量子ビットコミットメントプロトコル

(3)-②-a) 安全な量子ビットコミットメントの実現の検討

(3)-②-a)-1. 安全な量子ビットコミットメントは不可能か

すでに説明したように、無条件に安全な量子ビットコミットメントは不可能であることが証明されているので、量子ビットコミットメントの研究は終わりかというとそれは早計である。そこで証明されているのは、あくまで、ビットコミットメントを実現するどのような量子プロトコルに対しても原理的にそれを破る攻撃法が存在する、ということであって、そのような攻撃法が現実的に実現可能かどうかということはまた別の問題になっているからである。例えば、ある量子ビットコミットメントを破るのに大規模な量子計算機が必要であることがいえれば、それは現在の技術レベルから考えて当分の間十分に安全であるとみなすことができる。したがって、ここで重要なのは、どのような条件を仮定すれば十分な安全性（とくに、 Alice、Bob ともに無限の計算能力を持つ場合における安全性）を確保できるか、ということを明らかにすることである。

(3)-②-a)-2. 量子ビットコミットメント実現のための仮定

暗号系を構成する上で重要なことは、できるだけ弱い仮定で十分な安全性を達成することである。その意味で、暗号プロトコルに量子効果を利用することによる利点の一つは、通常よりも弱い仮定、あるいは、通常とは独立な仮定に基づく安全性が達成されうることであるといえる。とくに量子系は観測により状態が変化するので、これを利用することによってある限られた期間（プロトコルを実行している間）だけ成り立っていればよい仮定（一時的な仮定と呼ぶことにする）に基づく安全な量子暗号プロトコルを構成することができる。そこで、安全な量子ビットコミットメント実現のための仮定としてこの「一時的な仮定」に注目し、その中で現実的に妥当であると思われるものについて以下でとりあげることにする（[1]参照）。

参考文献

[1] J. Muller-Quade and H. Imai: ISITA2000 (2000) pp.665.

[2]井元信之，小芦雅斗：日本物理学会誌 56 (2001) pp.17.

(3)-②-b) **改良量子ビットコミットメントプロトコルの提案**

(3)-②-b)-1. **量子メモリに関する仮定に基づく改良プロトコル**

一時的な仮定を得るために鍵となることは、不正を行うことのできるパーティーが量子レベルですべての操作を行えないようにすることである。これは、送信者の量子レベルでの操作の能力が限られているとすることで簡単に実現可能である。例えば、送信者が量子メモリを持っていなければ、たとえ情報をコミットした後で量子メモリが利用可能になったとしても不正を行うことができない。これと同様の効果を持つ一時的仮定には、量子メモリの容量や量子ビットの保持時間を限定する方法などがある。

(3)-②-b)-2. **観測能力に関する仮定に基づく改良プロトコル**

Salvail[1]により提案された、送信者が高々n 個の量子ビットしかコヒーレントに観測することができないという仮定は、プロトコルを若干修正することにより一時的仮定として用いることができる。ここで必要とされることは、情報をコミットした後、送信者が開示する前に n 個より多数の量子ビットをコヒーレントに観測しなければ受信者に送る検証情報を情報量的に知ることができないようにしてやることである。そこで以下のプロトコルを考える。送信者はランダムビット $b_1,\ldots,b_m$ をコミットした後ただちにその中のいくつかを公開するものとする。このとき送信者は、高々n コヒーレント観測しかできないので、不正を成功させることは情報量的に不可能である。そしてコミットフェーズの最後に、送信者は残りのビットの中のどれがコミットしたい値と同じか受信者に伝える。その後送信者に対する制限を解除することができる。

(3)-②-b)-3. **公開データベースに関する仮定に基づく改良プロトコル**

Yao の結果[2]により、量子チャンネル上ではビットコミットメントを用いて任意の二者間通信を実現できることが示された。ここで用いられているビットミットメントは、短時間のみ拘束性を持てばよいが、すべての操作を量子レベルで行うことは不可能でなければならない。

そこで一つの可能性として考えられるのが、コミットフェーズが完了するまでに完全に探索することが不可能な大規模公開データベースに基づいたビットコミットメントである。このデータベースのもとで、短時間拘束性、情報量的秘匿性をもつビットコミットメントを構成できる。送信者はコミットフェーズが完了するまでにすべてのデータを閲覧することはできないので、情報をコミットする際にデータベースのどの部分を用いるか決めなければ成らない。この決定は量子レベルのみで行うことは不可能であるので、送信者は Yao のプロトコルに従うよう拘束されることになる。その後この仮定をなくして送信者にすべてのデータの閲覧を許してよいが、それにより不正が可能となることはない。

参考文献

[1] L. Salvail: Crypto'98 (1999) pp.338.

[2] A. Yao: Proc. of the 27th Symposium on the Theory of Computing (1995) pp.67.

[3] J. Muller-Quade and H. Imai: ISITA2000 (2000) pp.665.

(4)その他の量子暗号プロトコル
(4)-①量子紛失通信プロトコル
(4)-①-a)量子紛失プロトコルの概念設計
(4)-①-a)-1．量子紛失通信プロトコルとは

通常の紛失通信（Oblivious Transfer: OT)とは、送信者 Alice が通信文を受信者 Bob に送るときに、50%の確率で受信者 Bob に伝わるが、それが伝わったかどうかは送信者の Alice には分からないというものである。このような通信路は Rabin により素因数分解の困難性に基づき提案された[1]。 続いて Even、 Goldreich、 Lempel により 1-out-of-2 Oblivious Transfer(OT)($\binom{2}{1}$–OT)が発明された[2]。これは例えば次のような状況を想定したプロトコルである。即ち Alice と Bob が次のようなゲームを行うとする。Alice は 2 つの 1 ビットメッセージを選び、その 2 つのメッセージを Bob に送るが、Bob の方はその 2 つのメッセージの両方ともを得ることはできず、そのうちの片方のみのメッセージを非常に小さな誤り確率で読むことができるというものである。もちろんこの時 Alice は Bob がどちらのメッセージを読んだのかは分からない。この 2 つの OT は、どちらかをインプリメントできればもう一方もそれによりインプリメントできるという意味で等価であることが示されている[3]。したがってどちらか一方を実現すればよい。

OT はとても奇妙なアイデアに見えるが、しかしいろいろな興味深いプロトコルを構成するための基本的な構成要素となっている。例えば 2 者間での Oblivious Circuit Evaluation（Alice も Bob もそれぞれ自分だけが知っている秘密 x と y を持ち、それぞれがお互いの秘密情報を相手に漏らすことなく、お互いに関数 f(x,y)の値を計算できるプロトコルで、勿論個人の秘密情報から f(x,y)を推定することができないもの）などといったプロトコルを実現する基本的な要素でもある。

ここで古典的な OT の問題点について指摘しておこう。まず古典的な OT では Alice と Bob のどちらかがそこに使われている暗号を破ることができたらなら、相手に気づかれること無く相手をだますことができる。さらに古典的な OT プロトコルはオフラインで相手を欺くことを必然的に与えてしまっている。つまりたとえばスーパーコンピュータを使って何日も計算を行い、プロトコルに使われている暗号を破ったりすると、この古典的 OT プロトコルはもはや使えない。さらに重要なのは今現在は大丈夫でも、新しい解読アルゴリズムが発見されると、それは過去に遡って解読されてしまう可能性があるということである。つまり盗聴者が盗聴データのコピーを何年もの間保管していて、そのデータを後の新しい技術で解読することができる。

これに対して量子 OT プロトコルでは一般に光子を保管する技術の難しさから、攻撃はオンラインで行われなければならず、古典的な OT のような問題点は無い。しかしこれに類したマジックプロトコルの１つであり、非常に基本的なプロトコルであるビットコミットメントが、量子を用いて実現することが不可能であるとの証明が相次いでなされ、それ以降本当にその他のマジックプロトコルも安全なのか危ぶむ声もある。実際、ロスアラモスにある量子関係のプレプリントサーバーにおいては、９６年以降量子 OT プロトコルに関する論文が激減している。このビットコミットメント不可能定理は量子暗号全体に暗い影を落としていると言わざるを得ない。しかしここではとりあえず、現在までに提案された量子 OT プロトコルについて幾つか紹介する。

まず Rabin の OT の量子版について単純に考える。考えるベースとしては[4]の鍵共有プロトコルで用いた光子の偏向を用いる。即ち、水平-垂直基底と 45°-135°基底を用いたものである。まず Alice は 2 つの基底のうちどちらかをランダムに選び、Bob に対してその基底でビット情報を１つの光子にエンコードして送る。Bob はランダムに観測基底を選び観測し、最後に Alice が正しい基底情報を教える。これにより Bob は Alice のビットを 50%の確率で読むことができ、また逆に 50%の確率で読めないことになる。また Alice はどちらの状態を Bob が読んだのか分からない。

ところがこのプロトコルはその成功確率が Bob の検出器の非効率性やノイズにより大きく影響されてしまうという問題点や、水平-垂直基底と 45°-135°基底の中間の基底、例えば θ=22.5°といった基底を Bob が測定することにより、いつでも Alice のビットに関する部分情報を Bob が少なからず得られるという問題点があり、プロトコルとしては不十分であった。

これに対して 1-out-of-2 量子 OT プロトコルを Cr peauと Kilian[5]が 1988 年に提案した。これは上述のような問題点はないものの、検出器のエラーや、光源が単一光子でないなどの現実的な条件の元ではうまくいかないものであった。

その後単一光子ではなく、弱い光パルスを用いた 1-out-of-2 量子 OT プロトコルが Bennett、Brassard、 Cr peau Skubiszewska[6]によって提案された。このプロトコルは実用的な観点から構成されたもので、 次章にその詳細を記す。

それではまず非現実的ではあるが、基本的な量子 OT プロトコルを紹介する。問題設定は送信者 Alice が受信者 Bob に 1-out-of-2 Oblivious Transfer を行うものである。Alice は b_0 と b_1 の 2 つのビットを Bob に送り、Bob はそのうちのどちらかのビットを受信する(n)。このとき Alice は Bob の選択 w を知ることができず、また Bob も選択しなかった方のビット $b_{\bar{w}}$

を知ることができない。尚、量子暗号通信路の他に所謂一般の通信路も利用できるものとする。

i. Alice は長さnのランダムなビット列 $q^n = (q_1, q_2, \cdots, q_n)$ と $r^n = (r_1, r_2, \cdots, r_n)$ を選ぶ。

ii. Bob はn回分の測定に必要な測定器の種類 $\Theta = (q_1, q_2, \cdots, q_n), q_i \in \{0°系, 45°系\}$ をランダムに選ぶ。

iii. Alice は $(r_i \times 45° + q_i \times 90°)$ に基づき偏光させた光子を Bob に送り、Bob は q_i の測定器のタイプでその光子を測定する。

iv. Alice は r^n を Bob に知らせる。

v. Bob は $i = 1,2,\cdots,n$ を正しく測定できた時刻（ $r_i = 0$ のとき 0° 系で、$r_i = 1$ のとき 45° 系で測定）の集合と正しく測定できなかった時刻の集合に分割し、その分割を Alice に知らせる。但し、正しく測定できた（できなかった）集合がどちらであるかは Alice に知らせない。$q_i, (i = 1,2,\cdots,n)$ をその２つの集合に分割し、一方の集合のパリティを x_0、他方の集合のパリティを x_1 とする。このとき Bob はそのうちの一方（正しく測定できた方）のパリティ $x_d\,(d = 0 \text{ or } 1)$ を知ることができる。他方 Alice は x_0 と x_1 の 2 つの値を知ることができるが、Bob がどちらの集合のパリティを知っているかは分からない。

vi. Bob は Alice に Bob の選択 w が $w = d$ であるか否かを通知する。

vii. Alice は $w = d$ なら $(x_0 \oplus b_0, x_1 \oplus b_1)$ を $w = \bar{d}$ なら $(x_0 \oplus b_1, x_1 \oplus b_0)$ を Bob に送る。Bob はこれと x_d から b_w を求める。

ところで手順 vi で Bob は自分の選択を Alice に伝えているが、Alice は Bob の選択 d が 0 であるか 1 であるか知らないため、Alice は Bob の選択を知ることはできない。また Bob は 0° 系から 22.5° 傾けた測定器で測定すれば、$\cos^2(22.5°)$ の確率で q_i の値を知ることができるが、そのn個のパリティが 0（または１）になる確率は、nが大きくなるとともにランダムに近づくため、x_0 と x_1 を両方知ることはできない。

(4)-①-a)-2. その他の量子紛失通信プロトコル

上述のプロトコルは単一光子を仮定したものであり、検出器の効率 100%を想定した非現実的なものである。これに対して次に紹介するプロトコルは、弱い光パルスを用いた現実的なプロトコルである。ちなみに最初のステップは Bob　の光子検出器の物理的性能限界を知

りプロトコルの調整を行うために必要なものである。以下でb_0とb_1を Alice の選んだビットとし、cを Bob の選んだビットとする。

viii. Bob は Alice に自分の検出器の量子効率qとダークカウントレートdを告げる。もしこれらの値が満足の行くものであれば、次に Alice は Bob に光パルスの強度mを教え、それを使って以降の通信を行う。Alice はこれから送信するパルス列のa割が Bob に正しく伝わるものと考え、またビットエラーレートeを予想し、ダークカウントやノイズにより誤ったデータを修正できるかどうか判断する。また彼女はセキュリティパラメータ N を次のように決め Bob に伝える。即ち Alice と Bob は予想されるビットエラーレートeの通信路上で、 N ビットワードを伝送したとき、それを高い確率で誤り訂正できる、線形バイナリ誤り訂正コードを用いて通信することを合意し、このことから必然的に N が決まる。
これらのことをもう少し正確言うと、まずaの値は普通$a = (1 - e^{-(mq+2d)} \approx mq)$と取る。この値は強度μの光の中に１個もしくはそれ以上の光子を検出するポアソン確率から求まる。しかし実際には Alice と Bob の間の光学系のロスにより、もっと弱い光が使われることになる。同様にeも通常は$d/a \approx d/mq$と見積もられる。これは Bob の持つ 2 つの光子検出器のダークカウントから見積もられるのだが、実際には他のノイズ源に打ち勝つためにもっと高い値に設定される。これらのことからμの値が決まる。ところで理論的には安全な OT は次のエントロピー関数[数式 12]

数式 12

$$\mathrm{H}(p) = p\log\frac{1}{p} + (1-p)\log\frac{1}{1-p}$$

を用いて、$H(2e) < \frac{1}{2} - (1 - e^{-m} - me^{-m})/2a$を実現した時に達成できることが知られている。もしこの条件が満たされていなければ Alice はプロトコルを中止する。そして最後に Alice と Bob はテストを実行する。そのテストとは前もって決めておいた系列で Alice が強度mのパルス列を送り、Bob がそれを正しい基底で読みとり、aよりも大きい確率でパルスを検出でき、eより小さい誤り率であることを確認するというものである。

ix. Alice は Bob に４つの偏向状態にエンコードされた$2N/a$個の弱い光パルス列を送る。

x. Bob はランダムに 2 種類の基底から観測基底を決め、その基底とパルスが検出されたとき（確率～a）の測定結果を表に記録する。したがって Bob は２N 個のパルスを連

続的に受けることになる。もしも Bob が少し多く受け取ったならば、その超過分を無視し、もし少し少なく受け取れば、ランダムな推測を行い表を埋める。したがっていつでも 2N 個のエントリーが完成する。Bob は Alice に全２N パルス中、データの存在する箇所、つまりコミットした時間を報告する。ここでは観測に使用した基底情報や Bob の測定結果そのものではないことに注意。

xi. Alice は Bob の受け取ったパルスに関してそれぞれ送信時の基底情報を教える。

xii. Bob は自分のパルス列を正しい基底で測定した“正しい”集合と、間違った基底で測定した“間違った”集合に分ける。こうして Bob は Alice との間で正しい集合に属する１ワード、つまり N ビットストリングを共有し、間違った集合に属する１ワードに関しては共有できないことになる。Alice はどちらのワードを Bob と共有しているのかは分からない。(それは Bob が受け取ったパルスの数の統計的な揺らぎのため、Bob が N 個の正しいパルス列を完全に受け取ることができなかったことによる。その値は２N よりは少ないであろうし、正しい基底で測定したパルス数に比例するが、またそれは 1/2 より僅かに下回ると思われる。しかし N が十分大きいとき、正しいデータの集合の中に含まれるエラーは、ノイズに基づくエラーと比較して無視できるものと考える。)

xiii. ステップ viii で選んだ誤り訂正コードを使って、Alice は各集合に対する性質を計算し、それから彼女はその結果を Bob にエラーのない古典通信路を使って送る。この値を受け取ると Bob は正しいデータに対応する、オリジナルを復元することができ、間違ったデータのほうは勿論復元できない。
さらに Alice はそれぞれの集合のランダムな部分集合に対するパリティを計算し、Bob にそのランダムな部分集合の定義を通知する。このときパリティは通知しない。Bob はこれにより正しいデータ集合の中のパリティが計算できる。Alice は勿論両方のパリティを知っているが、Bob が知っているのがどちらかは分からない。ここで x_0 と x_1 をそれぞれこれらのパリティビットとし、$\hat{c}$ を Bob の知っているパリティビットとする。

xiv. Bob は Alice に $c = \hat{c}$ かどうかを尋ねる。

xv. もしも $c = \hat{c}$ なら、Alice は $(x_0 \oplus b_0, x_1 \oplus b_1)$ を、そうでなければ $(x_0 \oplus b_1, x_1 \oplus b_0)$ を Bob に送る。これから Bob は b_c を抽出する。

(4)-①-a)-3．まとめ

量子 OT の基本的なプロトコルを 2 つ紹介した。１つは単純に机上の方式を述べたもので、2 つ目は実際のインプリメントまで考えた方式である。次の章ではこのプロトコルの具体的な実現方法について考えていく。尚、量子紛失通信プロトコルの安全性に関しては文献[6, 9, 10]に幾つか議論されているので参考にされたい。最後にそれに関連して安全性の面から切り離せないビットコミットメントとの関係について述べる。量子ビットコミットメントが量子 OT を用いて実現可能であることは Yao によって文献[7]で示されている。また Kilian は通常の OT が２者間の安全な計算を実現すればインプリメントできることを示した。したがってこの２つの結果から量子ビットコミットメントが無条件に安全な 2 者間の安全な計算を導くものと予想されたが、 実際には不可能であることが証明された訳である。したがって量子 OT の安全性に関しても様々な角度から検討する必要があるが、ビットコミットメント不可能定理の存在により、その研究はかなり下火になっていると言える。

参考文献

[1]M. O. Rabin, “How to exchange secrets by oblivious transfer”, Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[2]S. Even, O. Goldreich and A. Lempel, “A randomized protocol for signing contracts”, Advances in Cryptology: Proceedings of Crypto’82, August 1982, Plenum Press, pp. 205-210.

[3]C. Crépeau, “Equivalence between two flavors of oblivious transfer (abstract)”, Advances in Cryptology: Proceedings of Crypt ’87, August 1987, Springer-Verlag, pp. 350-354.

[4]C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, ”Experimental Quantum Cryptography”, Journal of Cryptology, Vol.5, pp.3-28, 1992.

[5]C. Crépeau and J. Kilian, “Achieving oblivious transfer using weakened security assumptions”, Proceedings of 29th IEEE Symposium on the Foundations of Computer Science, October, 1988, pp. 42-52.

[6]C. H. Bennett, G. Brassard, C. Crépeau and M-H. Skubiszewska, "Practical quantum oblivious transfer", Advances in Cryptology, Crypto '91 Proceedings, August 1991, Springer - Verlag, pp. 351 - 366.

[7]A. Yao, “Security of Quantum Protocols Against Coherent Measurements”, in Proc. of 26th Annual ACM Symposium on Theory of Computing, 1995.

[8]J. Kilian, Proc. of 1988 ACM Annual Symposium on Theory of Computing, 1988.

[9]D. Mayers, “On the Security of the Quantum Oblivious Transfer and Key Distribution Protocols”, Proc. of Crypto'95, LNCS963, Springer-Verlag, pp. 124-135, 1996.

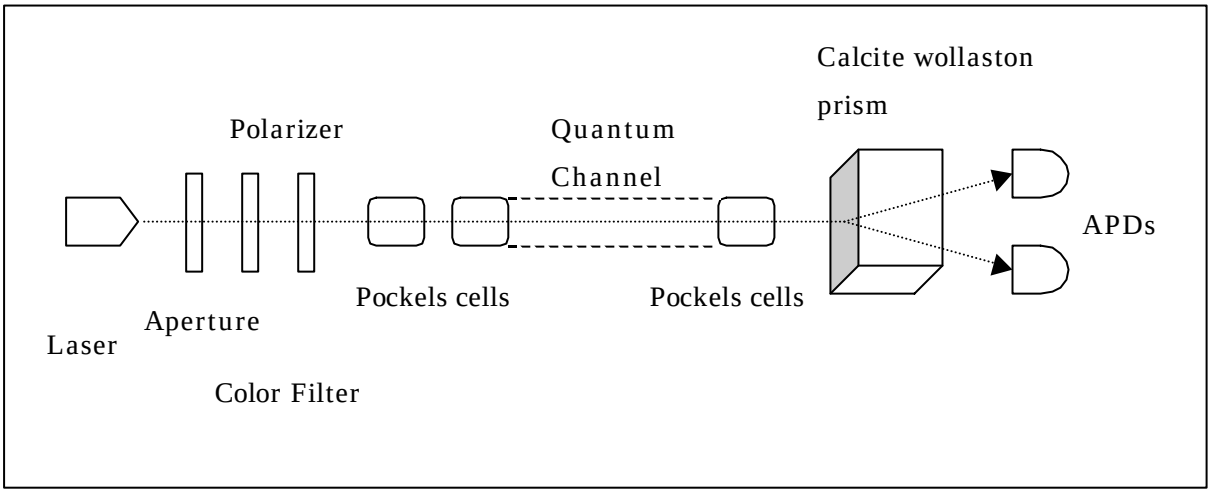
[10]D. Mayers, “Quantum Key Distribution and String Oblivious Transfer in Noisy Channels”, arXiv: quant-ph/9606003.

(4)-①-b)量子紛失プロトコルの物理構成とデータ処理

(4)-①-b)-1.量子紛失通信プロトコルを実現する光学系の概要

前節で紹介した量子紛失通信(Oblivious Transfer（OT）)プロトコルの実装について考えてみる。まず Rabin の提案する OT は次のようなものである[1]。送信者 Alice が通信文を受信者 Bob に送るときに、50%の確率で受信者 Bob に伝わるが、それが伝わったかどうかは送信者の Alice には分からないというものである。

このプロトコルは以下のように BB84 プロトコルと同様な物理系で構成できる。



つまり Alice は 2 つの偏光基底(水平-垂直基底と 45°-135°基底）のどちらか１つを選び、1 ビットの情報を BB84 同様、光子にエンコードし、それを Bob に量子通信路を用いて送信する。Bob はそれをやはり 2 種類の偏光基底のうちの１つを使ってデコードする。理想的な状況下では Bob が Alice と同じ基底で観測した時は正しく情報は伝わり、異なる基底で観測した場合には情報は伝わらない。したがって確実に１つの光子の情報を載せることができれば、50%の確率で Bob に情報が伝わり、それが伝わったかどうかは Alice は分からない。

このように一見、これで実現できるように思う。しかし実は次のような 2 つの落とし穴がある。まず１つはこの方法ではプロトコルの成功確率は、Bob の検出器の光子検出効率（量子効率という）と通信路上のノイズにより大きく影響されてしまうという点である。実際の測定器や通信路上にどのくらい障害があるかというと、まず検出器の量子効率はせいぜい 30%程度である。またノイズ等による誤検出も 10^{-5} くらい存在する。したがって 50%の確率で情報を伝達するためには、系に対する事前知識が不可欠となる。また Bob が水平－垂直基底と 45°-135°基底の中間の基底、例えば θ=22.5°といった基底を測定すると、Alice のビットに関する部分情報を $\cos^2(22.5°)$ の確率で Bob は得られてしまう（しかしこちらの方は(4)-①-a）に示したような解決法がある)。したがってこの OT を実現する物理

系は不十分であるといわざるを得ない。これに対して Bennett らのプロトコルは同じような物理系を用いていても上述の問題点を回避することができる 0。それを次章に示す。

(4)-①-b)-2.同光学系を駆動するデータ処理系の仕様

光学系を同様なものを用いていても、次のようにプロトコルを改良することで１で示した問題点が回避される。またプロトコルは 1-out-of-2 OT とする。まず送信するデータを N ビット列の 2 つとし、統計的に処理することで Bob が 50%の確率でどちらかのビット列を選択できるようにした点である。即ち、Alice は Bob に４つの偏向状態にエンコードされた 2N 個の弱い光パルス列を送る。Bob はランダムの受信するから、次のような表ができる。但し、偏光基底とビットの対応は次の通りとし、また表には測定できなかった箇所のデータを除いてある。

水平－垂直基底 （以後＋基底と呼ぶ）	0 = ―	1 = ｜
45°－135°基底 （以後 X 基底と呼ぶ）	0 = ／	1 = ＼

時間	1	3	6	7	11	12	15	16	19	21	25	27	29	30	31	33
Alice が選んだビット列	0	1	0	1	1	0	0	0	1	1	0	1	1	1	1	0
Alice の選んだ偏光基底	＋	×	×	×	＋	＋	×	＋	＋	＋	×	＋	×	×	＋	×
光子の偏光	―	＼	／	＼	｜	―	／	―	｜	｜	／	｜	＼	＼	｜	／
Bob の選んだ偏光基底	×	×	×	＋	×	＋	＋	×	＋	×	×	＋	×	＋	×	×
Bob の観測結果	1	1	0	0	0	0	0	1	1	1	0	1	1	1	0	0

正しい基底と間違った基底で測定したものの集合に分割。

時間	3	6	12	12	25	27	29	33	1	7	11	15	16	21	30	31
Alice が選んだビット列	1	0	0	0	0	1	1	0	0	1	1	0	0	1	1	1
Alice の選んだ偏光基底	×	×	＋	＋	×	＋	×	×	＋	×	＋	×	＋	＋	×	＋
光子の偏光	＼	／	－	－	／	｜	＼	／	－	＼	｜	／	－	｜	＼	｜
Bob の選んだ偏光基底	×	×	＋	＋	×	＋	×	×	×	＋	×	＋	×	×	＋	×
Bob の観測結果	1	0	0	0	0	1	1	0	1	0	0	0	1	1	1	0
パリティを取る部分集合	*			*	*	*		*	*			*	*		*	
パリティ	0								1							

最後に Bob はどちらかの集合のパリティを Alice に訪ねる。Alice は両方の集合のパリティは分かるが、Bob がどちらの集合を選んでいるのかは分からない。このパリティ情報に Alice の選んだビットを XOR して送れば、50%の確率で情報が伝達できるという仕組みである。

(4)-①-b)-3. 課題とまとめ

量子 Oblivious Transfer の物理的実現について概観してみた。実はこのプロトコルだけでは現実のインプリメントには対応できない。現実の量子 OT を実現するためにはこれに誤り訂正処理とプライバシー増幅処理を付け加える必要がある。

参考文献

[1]M. O. Rabin, “How to exchange secrets by oblivious transfer”, Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[2]C. H. Bennett, G. Brassard, C. Cr peau and M-H. Skubiszewska, "Practical quantum oblivious transfer", Advances in Cryptology, Crypto '91 Proceedings, August 1991, Springer - Verlag, pp. 351 - 366.

(4)-②量子コイン投げプロトコル

(4)-②-a)量子コイン投げプロトコルの概念設計

(4)-②-a)-1.コイン投げの紹介と計算量的実現法

コイン投げプロトコルが初めて提案されたのは 1982 年の Blum の論文による[1]。表題は「電話によるコイン投げ」というもので、遠く離れた Alice と Bob が通信回線を使って交互に交信しながら公平なコイン投げを行うプロトコルを提案している。その基本原理はビットコミットメントを応用したものである。但し、ビットコミットメントを応用したプロトコルは量子コイン投げプロトコルの経緯とも絡んでいるので次節で触れたい。

とりあえず、コイン投げプロトコルの一般的な要件を整理しておく[2]：

i) 信頼できる第 3 者を仮定しない

ii) Alice は Bob が推測する前にコインを投げる

iii) Alice は Bob の推測を聞いた後コインを再度投げることはできない

iv) Bob は推測をする前に投げられたコインの結果を知ることはできない

これを実現するビットコミットメント以外の計算量的実現法を以下に示す。

【一方向性ハッシュ関数を用いたコイン投げ】[2]

①Alice は乱数 x を選択し、そのハッシュ値 $y = H(x)$ を計算する。ここで、$H(\bullet)$ は一方向性ハッシュ関数である。

②Alice は y を Bob に送る。

③Bob は x のパリティを推測し、その値を Alice に送る。

④Bob の推測が正しければコインの表とし、推測が間違っていればコインの裏とする。その結果を Alice はアナウンスし、x を Bob に送る。

⑤Bob はハッシュ値 $y = H(x)$ を確認する。

(4)-②-a)-2.ビットコミットメントに基づく試み

1984 年 Bennett と Brassard は量子鍵配送だけでなく量子ビットコミットメントプロトコルも提案し、その中でビットコミットメントの応用としてコイン投げプロトコルの提案もしている[3]。彼らのビットコミットメントプロトコルを基にしたコイン投げプロトコル「BB-cointoss」は以下のような構成となっている：

①Alice は 1 ビット b_0 を決めて、量子ビットコミットメントプロトコルのコミットメント・フェーズ「BB-commit(b_0)」を Bob に対して行う。

②Bob は 1 ビット b_1 を決めて、Alice に送る。

③Alice と Bob は量子ビットコミットメントプロトコルの開示フェーズ「BB-open(b_0)」を行う

④Bob が勝つのは $b_1 = b_0$ の条件を満たすときのみである。

ここで BB-commit(b)は以下のような量子プロトコルである：

①Alice は長さ s のランダムビット列 $B=(b_1,b_2,\ldots,b_s)$ を決める。

②Bob は s 個の偏光測定系列 $\Theta=(q_1,q_2,\ldots,q_s)$ を選択する。ここで、q_i は $\oplus$, $\otimes$ のいずれかでありお互いに 45° 傾いた測定系である。

③Alice は s 個発射する光子の偏光状態をコミットメントビット b の値により

$b=0$ のときは、	0 度偏光	―	at $b_i=0$
	90 度偏光	|	at $b_i=1$
$b=1$ のときは、	45 度偏光	／	at $b_i=0$
	135 度偏光	＼	at $b_i=1$

のように変調し Bob に送る。

Bob は送られた光子列を偏光測定系列 Θ に従った測定系で観測する。

観測結果は、0 度偏光、45 度偏光のときは $b_i'=0$ とし、90 度偏光、135 度偏光のときは $b_i'=1$ として記録しておく。

④Bob は秘密に Θ と $B'=(b_1',b_2',\ldots,b_s')$ を保持しておく。

⑤Alice は開示フェーズまで、b と B を秘密に保持しておく。

また、開示フェーズにおける BB-open(b)は以下のような量子プロトコルである：

①Alice は Bob に b と B を開示する。

②Bob は、b の値に基づき偏光測定系のあっていた観測のみを取り出し、 $b_i'=b_i$ であるかどうかを検査する。

③この検査がすべてクリアできたとき Bob は Alice のコミットを受理する。そうでなければ否決する。

このように彼らの BB-cointoss は量子プロトコルとしての本質的な部分は量子ビットコミットメントプロトコルの部分にある。

しかし、残念ながら量子ビットコミットメントプロトコルは原理的に不可能なことが証明されてしまったので[4,5]、上記の量子コイン投げプロトコルも安全ではない。EPR 対のように量子論的に絡み合った量子状態(エンタングル状態)を使うことで Alice が Bob を騙せることが示されている。

それでは、安全な量子コイン投げプロトコルを実現することは不可能であろうか。

(4)-②-a)-3.無条件安全性を有する方式

Mayers、Salvail、河野のグループは、量子ビットコミットメントプロトコルとともに不可能と思われていた量子コイン投げプロトコルに安全性を保証出来る方式があることを示した[6,7]。それはまず量子コイン投げというタスクを 4 つに大きく分類し、不可能なタスクと可能なタスクを分けることから始まる。

i) 厳密な通常のコイン投げ

ii) 非厳密な通常のコイン投げ

iii) 厳密な素朴な定義のコイン投げ

iv) **非厳密な素朴な定義のコイン投げ**

まず、「素朴」と「通常」の違いは「素朴」が利用者のいかなる不正行為にも関わらず勝敗の確率が五分五分であるようなプロトコル、「通常」が一方の利用者がボイコットを働けるようなプロトコルの中止を許すプロトコルである。「厳密」と「非厳密」の違いは「厳密」が勝敗の確率の上限が厳密に守られるプロトコル。「非厳密」は勝敗確率にバイアスを許すプロトコルである。この場合セキュリティパラメタが存在し、その値により漸近的にバイアスを小さくしていくことができる。

このうち、厳密な素朴な定義のコイン投げは既に不可能であることが示されている[8]**が、**Mayers、Salvail**、河野のグループは非厳密な通常のコイン投げのカテゴリーに属する無条件に安全なプロトコルを提案したのである。この特長は一言でいうと** Slow Coin Tossing **であり、**Alice **と** Bob **がビット値を徐々に開示していき、相手のビット値がある程度読めるようになったときは、自分のビット値もある程度よまれてしまうような不思議なプロトコルである。**

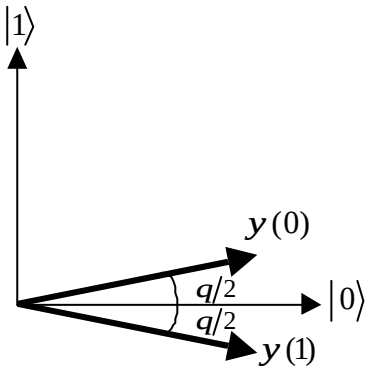
【原理】

・Alice **と** Bob **は** m **個のビット情報** a_j, b_j **を用意し** 1 **ラウンド毎に** 1 **ビットずつ提供しあう。従って** m **ラウンドにわたるプロトコル。**

・**勝敗の決着は全ビットのパリティ** $z = \oplus_j a_j \oplus b_j$ **で与えられる。**

・2 **つの非直交量子状態** $\psi(0)$, $\psi(1)$ **：**

$$\psi(0) = c|0\rangle + s|1\rangle, \quad \psi(1) = c|0\rangle - s|1\rangle$$



図(4)-②-a)-1 2 つの非直交量子状態

を用いる。ここで、$|0\rangle$, $|1\rangle$ **は正規化された直交状態。**$c = \sin \theta/2$, $s = \sin \theta/2$

はこの２つの非直交状態間がなす角度に相当する。1 粒子のこの非直交量子状を識別できる確率は非常に小さいとする。

・コイン投げにはｎ粒子状態 $\Phi(0)=\otimes_{k=1}^{n}\psi(0),\quad \Phi(1)=\otimes_{k=1}^{n}\psi(1)$ を用いる。この 2 つの状態間のなす角 Θ は $\cos\Theta=\cos^{n}\theta$ で与えれるので、十分 n が大きければこの 2 つの状態 $\Phi(0)$ と $\Phi(1)$ は直交状態に近づく。従って、ビット判定が確実にできることになる。

・上記 2 つのｎ粒子状態 $\Phi(0)$ と $\Phi(1)$ を観測する 2 つの正定値作用素測定 POVM は以下の通り：

$(E_0,\quad E_0^{\perp})$：

$$E_0=[1+\cos\Theta]^{-1}\left|\Phi(0)\right\rangle\left\langle\Phi(0)\right|$$
$$E_0^{\perp}=1-E_0$$

$(E_1,\quad E_1^{\perp})$：

$$E_1=[1+\cos\Theta]^{-1}\left|\Phi(1)\right\rangle\left\langle\Phi(1)\right|$$
$$E_1^{\perp}=1-E_1$$

観測者はいずれか 1 つを選択して観測を行い、$\Phi(0)$ か $\Phi(1)$ の状態を判別する。

より具体的にいうと、$E_0^{\perp}$ に対して出力があれば確定的に $\Phi(0)$ の状態にないこと、同様に、$E_1^{\perp}$ に対して出力があれば確定的に $\Phi(1)$ の状態にないことが判別する。

【プロトコル】

①Alice は m 個のランダムビット列 $a_j\quad (j=1,\ldots m)$ を選ぶ。

Bob は m 個のランダムビット列 $b_j\quad (j=1,\ldots,m)$ を選ぶ。

②Alice は mn 個のランダムビット $c_{ij}\quad (i=1,\ldots n,\quad j=1,\ldots m)$ を選び、mn 個の粒子対 $\psi(c_{ij})\otimes\psi(\bar{c}_{ij})$ を生成し、Bob に送る。ここで、$\bar{c}$ は c のビット反転である。

同様に、Bob は mn 個のランダムビット $d_{ij}\quad (i=1,\ldots n,\quad j=1,\ldots m)$ を選び、

mn 個の粒子対$y(d_{ij})\otimes y(\bar{d}_{ij})$を生成し、Alice に送る。

③Alice と Bob は以下の操作を 1 ラウンドとし、$i=1,\ldots n$ まで n ラウンドを繰り返す：

Alice は m 個のビット $e_{ij}=a_j\oplus c_{ij}$ (i は固定)を Bob に送信する。Bob は e_{ij} の値に従って、②でもらった粒子対のうち m 個の粒子を Alice に送り返し、対応する m 個の粒子を保持する。そのルールは以下の通り：

$e_{ij}=0$ の場合：　$y(\bar{c}_{ij})(=y(\bar{a}_j))$ が Alice に返却。

$y(c_{ij})(=y(a_j))$ を Bob は保持。

$e_{ij}=1$ の場合：　$y(c_{ij})(=y(\bar{a}_j))$ が Alice に返却。

$y(\bar{c}_{ij})(=y(a_j))$ を Bob は保持。

ここで、i には依存していないこと、a_j でみた状態が e_{ij} の値によらないことに注意。

同様に Bob は m 個のビット $f_{ij}=b_j\oplus d_{ij}$ (i は固定)を Alice に送信する。Alice は f_{ij} の値に従って、②でもらった粒子対のうち m 個の粒子を Bob に送り返し、対応する m 個の粒子を保持する。そのルールは以下の通り：

$f_{ij}=0$ の場合：　$y(\bar{d}_{ij})(=y(\bar{b}_j))$ が Bob に返却。

$y(d_{ij})(=y(b_j))$ を Alice は保持。

$f_{ij}=1$ の場合：　$y(d_{ij})(=y(\bar{b}_j))$ が Bob に返却。

$y(\bar{d}_{ij})(=y(b_j))$ を Alice は保持。

ここで、i には依存していないこと、b_j でみた状態が f_{ij} の値によらないことに注意。

従って、Alice がnラウンド後に持っている状態はそれぞれm組の n 粒子状態 $\Phi(b_j)$ と $\Phi(\bar{a}_j)$ である。同様に Bob がnラウンド後に持っている状態はそれぞれm組の n 粒子状態 $\Phi(a_j)$ と $\Phi(\bar{b}_j)$ である。

④Alice は1からmまでに順に a_j を Bob に開示し、Bob は各 j ごとにその値に従い n 粒子状態 $\Phi(a_j)$ に POMV $(E_{a_j},\ E_{a_j}^{\perp})$ を施し観測を実行する。$\Phi(a_j)$ ではないことが検出された場合は Alice が不正を働いたとみなしプロトコルを終了する。そうでない場合は $(E_0,\ E_0^{\perp})$ か $(E_1,\ E_1^{\perp})$ に従い、0、1を $\tilde{a}_j$ に記録する。

同様に、Bob は1からmまでに順に b_j を Alice に開示し、Alice はその値に従い n 粒子状態 $\Phi(b_j)$ に POMV $(E_{b_j},\ E_{b_j}^{\perp})$ を施し観測を実行する。$\Phi(b_j)$ ではないことが検出された場合は Bob が不正を働いたとみなしプロトコルを終了する。そうでない場合は $(E_0,\ E_0^{\perp})$ か $(E_1,\ E_1^{\perp})$ に従い、0、1を $\tilde{b}_j$ に記録する。

⑤Alice は1からmまで順に Bob から返却された n 粒子状態 $\Phi(\bar{a}_j)$ に POMV $(E_{\bar{a}_j},\ E_{\bar{a}_j}^{\perp})$ を施し観測を実行する。$\Phi(\bar{a}_j)$ ではないことが検出された場合は Bob が不正を働いたとみなしプロトコルを終了する。同様に Bob は1からmまで順に Alice から返却された n 粒子状態 $\Phi(\bar{b}_j)$ に POMV $(E_{\bar{b}_j},\ E_{\bar{b}_j}^{\perp})$ を施し観測を実行する。$\Phi(\bar{b}_j)$ ではないことが検出された場合は Bob が不正を働いたとみなしプロトコルを終了する。

このようにして、Alice の得る最終的なビット値は、

$$A \oplus \tilde{B} = (\oplus_j a_j) \oplus (\oplus_j \tilde{b}_j)$$

であり、Bob の得る最終的なビット値は

$$\tilde{A} \oplus B = (\oplus_j \tilde{a}_j) \oplus (\oplus_j b_j)$$

である。

こうして実現される無条件に安全な量子コイン投げプロトコルのセキュリティパラメタはmである。現在見積もられている最適な攻撃において 2 者のうち一方が有利となる度合い、具体的には勝敗確率の 1/2 からのずれは、$O(1/m^3)$となることが知られており、mを十分に大きくとれば安全性も十分に大きくなっていく。

参考文献

[1]M. Blum, Proc. of COMPCON, IEEE, (1982), pp.137

[2]B. Schneier, Applied Cryptography 2nd Ed., John Wiley & Sons, Inc., (1996), pp.89.

[3]C. H. Bennett and G. Brassard, Proc. of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India., (1984), pp.267.

[4]D. Mayers, Phys. Rev. Lett.78, (1997), pp.3414.

[5]H. -K. Lo and H. F. Chau, Phys. Rev. Lett.78, (1997),pp.3410.

[6]D. Mayers, L. Salvail, and, Y. Chiba-Kohno, quanta-ph/9904978, (1999).

[7] D. Mayers, L. Salvail, and, Y. Chiba-Kohno, QIT99-40, (1999), pp.151

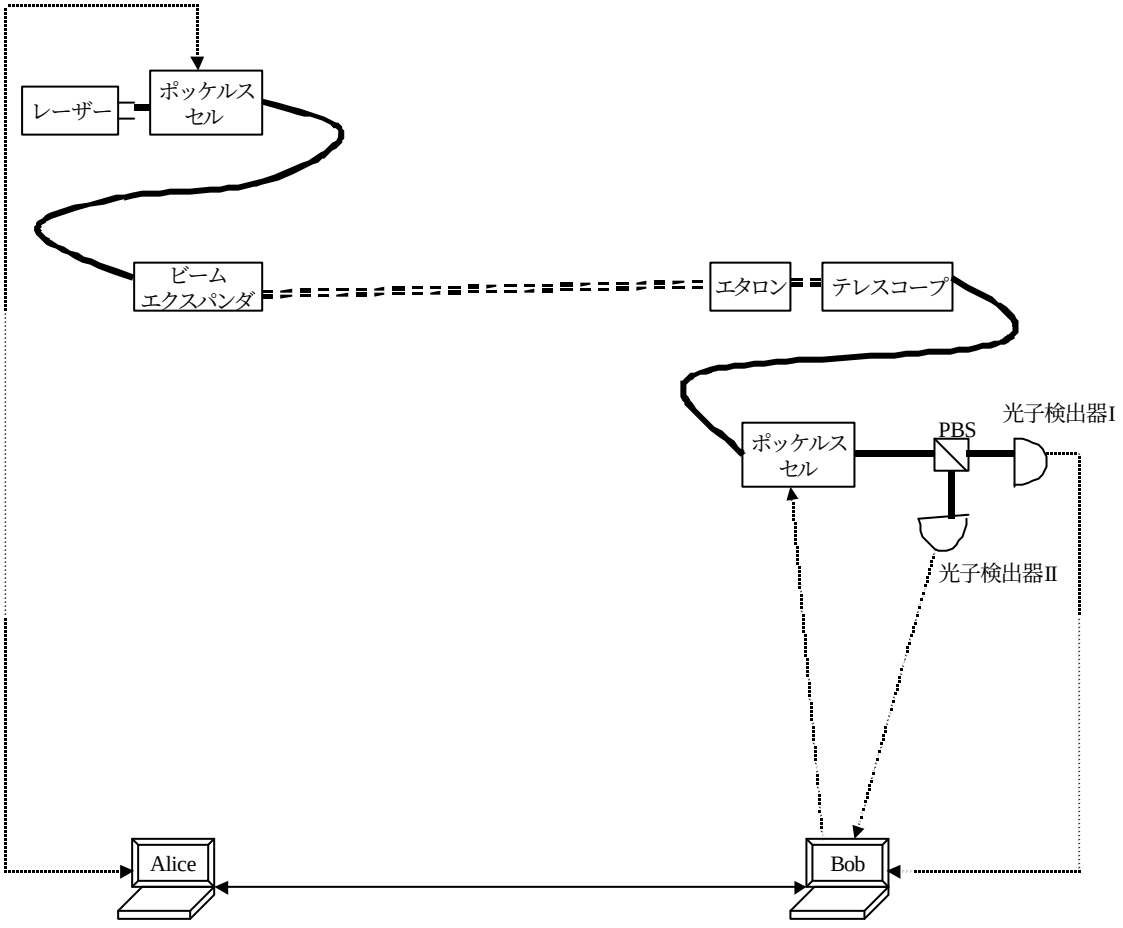
[8] H. -K. Lo and H. F. Chau, quanta-ph/9711065, (1997).

(4)-②-b)量子コイン投げプロトコルの物理構成とデータ処理

(4)-②-b)-1. 量子コイン投げプロトコルを実現する光学系の概要

前節 a)「量子コイン投げプロトコルの概念設計」では2つの量子プロトコルを紹介した。無条件に安全性の保証された Mayers、Salvail、河野が提案したプロトコルの[1,2]光学系を構成することは非常に興味深いのであるが、いざ実験系を構成しようとすると様々な問題があることに突き当たる。従って、その問題を後述する b)-3. 「課題とまとめ」 で触れ、ここでは安全性に問題があるが現在の我々の技術で十分構成可能な BB-cointoss[3]を実現する光学系についてその概要を述べる。

BB-cointossを実現する光学系は鍵配送プロトコルである BB84 プロトコルを実現する光学系とほぼ同じである。ここでは air で BB84 プロトコルを実現した光学系を基に構成してみよう[4]：



図(4)-②-b)-1. BB-cointoss 実験系構成図

この構成は、air で光子を伝送し、光子の偏光状態に情報を載せる方式に基づいている。図中の二重破線が正に空中を光子が伝送することを示している。太線は光ファイバを表し Alice、Bob の量子送受信装置内はほぼ光ファイバで光学系が組まれている。ここで矢印付

点線は光学系とコンピュータ間の電気信号線を表す。矢印付実線は Alice と Bob のコンピュータ間の公開通信路である。

Alice の量子送信装置は、光子源であるレーザと偏光変調を行なうポッケルスセルおよび光ファイバからでる光(口径数μm)を口径 1cm 程のビームに広げて空中に送り出すビームエクスパンダからなる。レーザはパルスレーザである。ポッケルスセルとは印加される電圧により結晶中の屈折率が変わるポッケルス効果を応用したもので、その効果が異方性を有するため偏光面の回転が生じる。Alice のポッケルスセルでは 4 種類の電圧が印加できるように設定されており、偏光面が印加電圧により、0 度、45 度、90 度、135 度回転するようになっている。Bob の量子受信装置は、外光とシグナル光を分離するためにエタロンという一種の周波数フィルタを用いる。これによりシグナル光のみが受信装置内に入光する。入光したビーム状のシグナル光はテレスコープにより集光され光ファイバ内に送られる。Bob のポッケルスセルでは偏光面を 0 度、45 度回転するように印加電圧が設定されている。ここで偏光面の回転を受けた光子は偏光ビームスプリッタ PBS によりポート 1、ポート 2 のいずれかに振り分けられる。ポート 1 の光子検出器 I で受光した場合は 0 度か 45 度偏光、ポート 2 の光子検出器 II で受光した場合は 90 度か 135 度偏光であるように設定されている。なおそれぞれ２つのうちのいずれであるかは Bob のポッケルスセルにより偏光面が何度回転を受けたかによる。

(4)-②-b)-2. 同光学系を駆動するデータ処理系の仕様

ここでは、図(3)-②-b)-1.におけるデータ処理系の仕様を記述する。留意点は量子鍵配送と同様に実装レベルにおいてはエラーが不可避である点である。このため、観測量としてビットレートとビットエラーレートを測定することになる。

①Alice と Bob は当該光学系における量子鍵配送の意味でのビットレート、ビットエラーレートを測定し、以下のコイン投げプロトコルにおいてそれぞれの閾値を予め合意しておく。

②セキュリティパラメタとなる乱数の長さｓを二者間で合意しておく。

③Alice と Bob のコンピュータはそれぞれ独立にビット長ｓの乱数列を生成する。

Alice：$a_1, a_2, \ldots, a_s$

Bob： $b_1, b_2, \ldots, b_s$

④Alice は 1 ビット a_0 を決めて自分のコンピュータに入力する。

⑤Alice のコンピュータはポッケルスセルに a_0 と a_i の値により表(4)-②-b)-1.に従

い偏光面を回転するように信号を送る。これを $i=1$ から s まで繰り返す：

表(4)-②-b)-1．Alice のポッケルスセル制御表

a_0	a_i	偏光面の回転角
0	0	0 度
	1	90 度
1	0	45 度
	1	135 度

⑥Bob は Alice から飛来した光子 1 個 1 個に対して、ポッケルスセルを用いて偏光面を回転させる。回転の大きさは b_i により表(4)-②-b)-2.に従って、Bob のコンピュータがポッケルスセルに信号を送る：

表(4)-②-b)-2.Bob のポッケルスセル制御表

b_i	偏光面の回転角
0	0 度
1	45 度

⑦Bob のコンピュータは光子検出器の検出結果からビット列

$$a_1', a_2', \ldots, a_s'$$

を記録する。記録ルールは光子検出器 I が検出したときは 0、光子検出器 II が検出したときは 1 を記録する。光子検出器が光子を検出しなかったとき、もしくは両方の検出器が検出したときは f (空)とし区別できるようにしておく。
このときビットレートを測定する。ビットレートの定義は有意に検出したビットの s に対する割合。この値がその閾値より小さければ以下の処理を中止する

⑧Bob は 1 ビット b_0 を決めて自分のコンピュータに入力する。Bob のコンピュータは公開通信路を通じて Alice のコンピュータにその値を通知する。

⑨開示フェーズにおいて、まず Alice のコンピュータは 1 ビット a_0 とビット列 a_i を公開通信路を使って Bob のコンピュータに開示する。

⑩Bob のコンピュータは検出ビット列のうちから有効ビットのみをそのままとする。他のビット f とする。有効ビットの条件は f でなく、かつ、$b_i = a_0$ を満たすもの。

⑪Bob のコンピュータは有効ビットのみを Alice から開示されたビット列a_iとを比較する。有効ビットにおいて$a_i' = a_i$であれば OK とし、そうでなければ NG とする。このときビットエラーレートを測定する。ビットエラーレートの定義は NG の数の有効ビット数に対する割合。この値がその閾値より大きければ以下の処理を中止する。小さければコイン投げの勝負が確定する。$b_0 = a_0$であれば Bob の勝ちであり、そうでなければ Alice の勝ちである。

表(4)-②-b)-3.BB-cointoss のデータ例

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_i	0	1	0	0	1	1	0	1	0	0	0	1	1	0	1	0
b_i	1	1	1	1	0	1	0	0	1	0	1	0	0	0	1	1
量子状態		|	―	―	|	|	―	|	―	―	―	|	|	―	|	―
観測基底		⊗	⊗	⊗	⊕	⊗	⊕	⊕	⊗	⊕	⊗	⊕	⊕	⊕	⊗	⊗
測定結果		／	φ	φ	|	φ	―	φ	φ	φ	＼	―	φ	―	φ	φ
検出 bit:a'		0	φ	φ	1	φ	0	φ	φ	φ	1	0	φ	0	φ	φ
bit rate		R＝6/15=40%														
有効 bit		φ	φ	φ	1	φ	0	φ	φ	φ	φ	0	φ	0	φ	φ
ビット検査		φ	φ	φ	OK	φ	OK	φ	φ	φ	φ	NG	φ	OK	φ	φ
bit error rate		BER=1/4=25%														

表(4)-②-b)-3.は BB-cointoss の１データ例である。これは s =15 である。Alice と Bob はビットレートとビットエラーレートの値からこの結果を受理するか、拒絶するかが判断される。受理する場合、$b_0 \neq a_0$であるので Bob の負けとなる。

(4)-②-b)-3. 課題とまとめ

前節までは、比較的実装の容易な BB-cointoss の実装に関して具体的に記述してきた。残念なことに理論的に量子ビットコミットメントプロトコルが不可能なことが証明されたためこの BB-cointoss も絶対的な安全性が保証されているわけではない。しかしながら、BB-cointoss の実装は 2 つの点で考察する価値がある。１つは量子プロトコルにおいてはエラー存在が不可避であること、もう１つはデータ処理としてのエラーへの対処法をプロトコルに組み込んでおかなければならないことである。既に前節において量子鍵配送で提案されているエラー処理がそのまま適用できないことが確認できた。量子コイン投げプロトコルならではのエラー処理の考察が必要となり、そのためのテストベンチを提供してくれる。

次に、Mayers、Salvail、河野による無条件に安全性の保証された量子コイン投げプロト

コルの実装であるが大きく 2 つの困難な点が予想される。この方式の特長として、量子状態を Alice と Bob の間でキャッチボールし、しかも、量子状態をしばらく貯蔵しなければことがあるので、あたかもまるでネットワークコンピュータの量子版ような処理を要求される。これが簡単な量子プロトコルと異なる問題点を引き起こす：

i)量子の貯蔵

Alice は Bob から受取った量子状態を暫く貯蔵しておかなければならない。光子をその量子状態を保ったまま保存しておく技術が必要になる。光ファイバを貯蔵リングとして用いる方式が簡単であるが、この場合、光子を受取った順に処理しなければならないのだが、当プロトコルではそのようではない処理も要求されるので簡単には適用できない。しかも、ファイバ内の光の減衰を考えるとファイバ長はせいぜい 50Km であり、時間にして 250 μsec 位しかならない。量子コンピュータで使用されるような量子レジスタが必要と思われる。

ii)エラー対策

Alice と Bob の 2 者は遠く隔てていることを前提にしているので、必ず伝送途中のエラーを考慮しなければならない。更に検出器のエラーも考慮していかなければならない。直感的には誤り訂正符号的な処理を行えばよいと思われるが、取り扱う量子状態の並びが二次元的に配置されており、送信元では横並びに処理するのに対し、受信側では縦並びに処理するので二次元符号的な取り扱いが要求されそうである。従って、簡単なプロトコルにおけるビットレート、ビットエラーレートに対応する物理量の定義と観測等、それに対する考察が必要になろう。

以上のように複雑なプロトコルになるほど、高度な量子操作技術が要求され、また、その観測結果を意味のあるものとするエラー処理等のデータ処理も検討すべきことが多々あることが判明した。十分な安全性を有する量子コイン投げプロトコルを実装は多くの課題を提議し解決を迫ってきている。

参考文献

[1]D. Mayers, L. Salvail, and, Y. Chiba-Kohno, quanta-ph/9904978, (1999).

[2] D. Mayers, L. Salvail, and, Y. Chiba-Kohno, QIT99-40, (1999), pp.151

[3]C. H. Bennett and G. Brassard, Proc. of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India., (1984), pp.267.

[4]B. C. Jacobs and J. D. Franson, Optics Lett. 21, (1996), pp.1854.

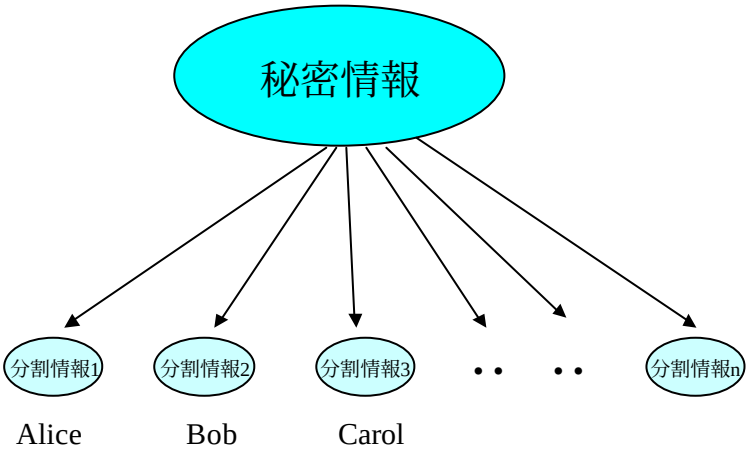
(4)-③ 量子秘密分散プロトコル

(4)-③-a)量子秘密分散プロトコルの概念設計

(4)-③-a)-1. 量子秘密分散プロトコルとは？

1998 年に M.Hillery らは量子秘密分散プロトコル(quantum secret sharing)の概念を導入した。この量子秘密分散プロトコルとは、計算量に基づく秘密分散プロトコルの考えかたを、量子力学の性質を利用して実現した量子プロトコルである。では、まず最初に通常いう秘密分散プロトコル(secret sharing)について、ここで簡単に復習しよう。

最初にメッセージを複数の部分に分け、部分部分のみではメッセージを読むのみ十分ではないが、いくつか集まるとメッセージが読めるというように設定する方式である。もっとも単純な秘密分散の基本的なアイディアは、2 者（例えば Alice と Bob）の間で秘密を分散して所有する状況である。そして、この秘密情報は 2 者が協力してはじめて再構築することができるわけである。これをより一般化すると、例えば $m-out-of-n$ プロトコル（(m,n)-閾値秘密分散プロトコル）というものになる。すなわち秘密情報を n 人の参加者が分割して所有し、そのうち m 人が（ここで $1 \le m \le n$ ）分割情報を持ち寄ることで秘密情報を再構成できるというものである。



図(4)-③-a)-1. 秘密分散のイメージ

これらの計算量の世界での概念を量子効果を利用して実現する。では具体的にどのような状態を利用して実現していくのだろうか。

最初に提案した M.Hillery らは、3 粒子が量子もつれ合った状態である GHZ 状態(Greenberger-Horne-Zeilinger state)を用いて実現できることを示した。また A.Karlsson らは､秘密分散プロトコルが 2 粒子のもつれ合い状態を使って構築できると提案している。次に具体的に量子秘密分散プロトコルについて見てみよう。

(4)-③-a)-2. **量子秘密分散プロトコルの詳細**

この節では、2 粒子の量子もつれ合い状態を利用した実現方法例を詳しく説明しよう。

[2 **粒子の量子もつれ合い状態を利用した実現方法例**]

準備

$|z+\rangle$、$|z-\rangle$ **は例えばスピン固有状態**(spin eigenstate)**と考える。この** z **軸方向の基底** $\{|z+\rangle,|z-\rangle\}$ **で状態を表現しよう。この場合** Bell state **は次のように書ける。**

4 つの Bell state

$$|f^{+}\rangle=\frac{1}{\sqrt{2}}(|z+\rangle_A|z+\rangle_B+|z-\rangle_A|z-\rangle_B)$$

$$|f^{-}\rangle=\frac{1}{\sqrt{2}}(|z+\rangle_A|z+\rangle_B-|z-\rangle_A|z-\rangle_B)$$

$$|y^{+}\rangle=\frac{1}{\sqrt{2}}(|z+\rangle_A|z-\rangle_B+|z-\rangle_A|z+\rangle_B)$$

$$|y^{-}\rangle=\frac{1}{\sqrt{2}}(|z+\rangle_A|z-\rangle_B-|z-\rangle_A|z+\rangle_B)$$

これを x-spin **固有状態**(x-spin eigenstate)**で書きなおしてみよう。すなわち次の関係を用いて書きなおしてみる。**

$$|x+\rangle=\frac{1}{\sqrt{2}}(|z+\rangle+|z-\rangle)$$

$$|x-\rangle=\frac{1}{\sqrt{2}}(|z+\rangle-|z-\rangle)$$

すると、結果のみ書くと次のように x-spin **固有状態で表現できる。**

$$|f^{+}\rangle=\frac{1}{\sqrt{2}}(|x+\rangle_A|x+\rangle_B+|x-\rangle_A|x-\rangle_B)$$

$$|f^{-}\rangle=\frac{1}{\sqrt{2}}(|x+\rangle_A|x-\rangle_B+|x-\rangle_A|x+\rangle_B)$$

$$|y^{+}\rangle=\frac{1}{\sqrt{2}}(|x+\rangle_A|x+\rangle_B-|x-\rangle_A|x-\rangle_B)$$

$$|y^{-}\rangle=\frac{1}{\sqrt{2}}(|x-\rangle_A|x+\rangle_B-|x+\rangle_A|x-\rangle_B)$$

また次のような 2 つの Bell 状態の線形結合を定義する。

$$\left|\Psi^{+}\right\rangle = \frac{1}{\sqrt{2}}(\left|f^{-}\right\rangle + \left|y^{+}\right\rangle)$$

$$= \frac{1}{\sqrt{2}}(\left|z+\right\rangle_A \left|x+\right\rangle_B + \left|z-\right\rangle_A \left|x-\right\rangle_B)$$

$$= \frac{1}{\sqrt{2}}(\left|x+\right\rangle_A \left|z+\right\rangle_B + \left|x-\right\rangle_A \left|z-\right\rangle_B)$$

$$\left|\Phi^{-}\right\rangle \equiv \frac{1}{\sqrt{2}}(\left|f^{-}\right\rangle - \left|y^{+}\right\rangle)$$

$$= \frac{1}{\sqrt{2}}(\left|z+\right\rangle_A \left|x-\right\rangle_B - \left|z-\right\rangle_A \left|x+\right\rangle_B)$$

$$= \frac{1}{\sqrt{2}}(\left|x+\right\rangle_A \left|z-\right\rangle_B - \left|x-\right\rangle_A \left|z+\right\rangle_B)$$

これから次の状態からなる集合を考えよう。

$$\{y^{+}, f^{-}, \Psi^{+}, \Phi^{-}\}$$

この状態間では次のような関係があることがわかる。

$$\left\langle y^{+} \middle| f^{-} \right\rangle = 0$$

$$\left\langle \Psi^{+} \middle| \Phi^{-} \right\rangle = 0$$

非直交関係(nonorthogonal)

$$\left\langle y^{+} \middle| \Psi^{+} \right\rangle \neq 0$$

$$\left\langle y^{+} \middle| \Phi^{-} \right\rangle \neq 0$$

$$\left\langle f^{-} \middle| \Psi^{+} \right\rangle \neq 0$$

$$\left\langle f^{+} \middle| \Phi^{-} \right\rangle \neq 0$$

それではこれらの準備をふまえて、次に実際のプロトコルの手順を説明する。

プロトコルの手順

$\{y^+, f^-, \Psi^+, \Phi^-\}$**を考えよう。**

step1. Trent**（秘密の情報の発信者）は情報として、下記を送信する**

$$\{|0\rangle, |1\rangle\} \Leftrightarrow \{|y^+\rangle, |f^-\rangle\} \quad \text{と} \quad \{|0'\rangle, |1'\rangle\} \Leftrightarrow \{|\Psi^+\rangle, |\Phi^-\rangle\}$$

Alice **と** Bob **は** z **軸方向か** x **軸方向のどちらかで観測する**

step2. Alice **と** Bob **公開通信路で盗聴されているかのテストのために使われたビットの集合の測定結果**(measurement outcome)**を公表する**
この後、テストビットとして使われたものと秘密に分散されたビット各々の観測基底を公表する
テストビットに関しては、最初に観測結果(measurement outcome)**を伝えた方（例えば** Alice**）が基底を相手（例えば** Bob**）より後に公表するようにする**

step3. **いくつかのビット（観測結果と観測基底）を公開した後、**Trent **は二つの基底どちらの集合に属するものを送ったか** Alice **と** Bob **に明らかにする。但し、どの状態を送ったかは当然明らかにしない。また** Trent **はテストビットとして、どの状態を送ったかを教える。すべての場合の中で半分は** Alice **と** Bob **は彼らの結果を捨てなくてはいけないが、残りの半分は有効な結果として所有する。(表** 1 **に** Trent **からある状態が発信されたとき、** Alice **と** Bob **の観測結果の相関特性を示した。)**

step4. Step3 **の後、**Alice **と** Bob **はお互い独立に盗聴者がいるかテストできる。盗聴者テストでもしエラーがなければ、**Alice **と** Bob **は** Trent **の基底が公表されているの残りビットから、表**(4)-③-a)-1 **から推測できるように、秘密の鍵を再構築することができる。**

表(4)-③-a)-1. Alice **と** Bob **の間の相関関係**

Alice/Bob	z+	z-	x+	x-
z+	f^-	y^+	Ψ^+	Φ^-
z-	y^+	f^-	Φ^-	Ψ^+
x+	Ψ^+	Φ^-	y^+	f^-
x-	Φ^-	Ψ^+	f^-	y^+

[3 粒子の量子もつれ合い状態を利用した実現例]

もつれ合った 3 粒子の GHZ 状態を利用しても秘密分散プロトコルは基本的に同様に実現できる。

参考文献

[1]M.Hillery, V.Buzek, A.Berthiaume: quant-ph/9806063 (1998)

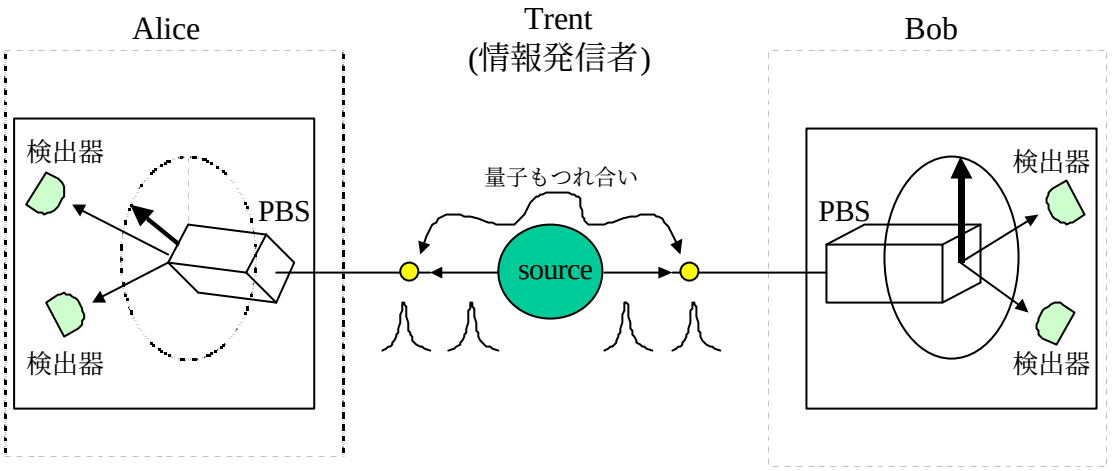
[2]A.Karlsson, M.Koashi, N.Imoto: Phys. Rev. A 59 (1999) 162

(4)-③-b)量子秘密分散プロトコルの物理構成とデータ処理

(4)-③-b)-1. 物理構成

ここでは、量子秘密分散プロトコルの物理構成について説明していこう。量子秘密分散プロトコルでは、2 粒子や 3 粒子の量子もつれ合い状態を使って実現するのは既に説明した通りである。

下記に一例として、2 粒子の量子もつれ合い状態を使った物理構成例を示した。



図(4)-③-b)-1. 量子秘密分散プロトコルの物理構成例

この例では、2 者（ここでは Alice と Bob）で秘密を分散することを考えている。
エンティティは、下記のように Alice、Bob、Trent の 3 者存在する。

[Trent] 情報（具体的には量子もつれあい状態）を生成するのは、センターに相当するこのエンティティ（ここでは Trent）である。こちらで情報を作り出し、Alice と Bob に送り出す。
プロトコルの説明時の例でいうと、送信する情報とは次のようになる。

$$\{|0\rangle,|1\rangle\} \Leftrightarrow \{|y^{+}\rangle,|f^{-}\rangle\} \quad と \quad \{|0'\rangle,|1'\rangle\} \Leftrightarrow \{|\Psi^{+}\rangle,|\Phi^{-}\rangle\}$$

[Alice] Alice は観測基底の方向をランダムに選んで測定し状態を観測する装置を所有する。例えば、測定装置とは、PBS（偏波依存ビームスプリッタ）が内部にあり軸からある角度を振れるようなものであり、これにより観測基底が変更できる装置である。（スピンの固有状態の場合は、z 軸方向や x 軸方向に沿って状態を観測できるもの。）

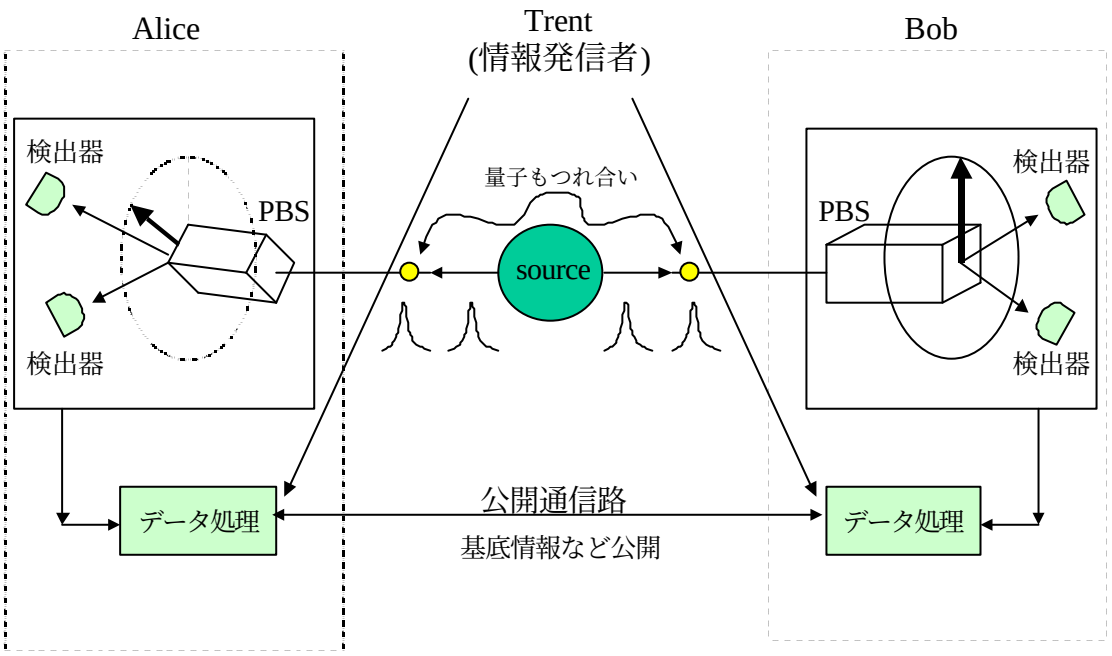
[Bob] Bob は観測基底の方向をランダムに選んで測定し状態を観測する装置を所有する。Alice と同様に例えば、測定装置とは、PBS（偏波依存ビームスプリッタ）

が内部にあり軸からある角度を振れて、観測基底が変更できる装置である。（スピンの固有状態の場合は、z 軸方向や x 軸方向に沿って状態を観測できるもの。）

光学的な物理構成としては、基本的にはこれらの構成要素で実現できる。もちろん、実際はこれ以外に公開通信でテストに関する情報や観測結果、基底情報などを伝えるデータ処理（古典的なデータの流れ）が必要である。次にデータ処理まで含めた全体図を見てみよう。

(4)-③-b)-2.データ処理

光学的な前述の物理構成に加えて量子秘密分散プロトコルを機能させるためには、公開通信路およびそこで得た情報などをもとにデータ処理する部分が当然必要である。下の図が、データ処理まで含めた全体図である。



図(4)-③-b)-2. データ処理まで含めた量子秘密分散プロトコルの全体イメージ図

公開通信路でのやりとりは、具体的には、プロトコルの手順の step2、step3 で必要になってくる。

例えば、step2 では、テストビットとして使用されたものの測定値を公開する。また、観測基底も公表する。このとき注意する必要があるのは、テストビットの観測結果と基底の

伝える順番である。例えば、Alice が最初に観測結果を伝えたら、基底は Bob より後に伝えるというようにしなければならない。

また、step3 でも Trent が Alice と Bob に 2 つの基底のどちらの集合を送ったかを公表したり、どの状態を送ったかを教えたりする。

参考文献

[1]M.Hillery, V.Buzek, A.Berthiaume: quant-ph/9806063 (1998)
[2]A.Karlsson, M.Koashi, N.Imoto: Phys. Rev. A 59 (1999) 162

(5) まとめ

本調査報告において量子暗号技術に関して、大きく 3 つの軸：量子鍵配送、ビットコミットメント、その他のプロトコルに視点をあてて調査研究をおこなった。ここでは、まとめとして、実用化に向けての今後の課題と更なる調査研究が必要な領域を整理して述べておく。

実用化に向けての今後の課題

量子暗号プロトコル実用化への一般の共通課題として 3 つの基本的な課題がつねにつきまとう。1 つは単一光子源の入手であり、2 つは量子効率の高い、かつ、ダークカウントの低い光子検出器の入手、そして、3 つめは安定性の高い光学系の構築である。更にエラー処理が不可避であることからより効率の高いデータ処理系の実現が性能向上のための課題として続く。このほか、量子鍵配送に関していえば長距離化と高速化という課題がある。ビットコミットメントに関していえば、純量子力学的原理だけでは安全性が保証されないので、個々の実装レベルでの安全性要件の抽出が課題であろう。その他のプロトコルに関していえば、複雑なプロトコルほど実用化にはより高度な量子工学技術の進歩が望まれる。

更に調査研究が必要な領域等

量子鍵配送の盗聴攻撃に関していえば、理論と実験に関して適用できる攻撃技術に乖離が大きく、見通しのよい体系化を進める必要がある。この体系化が進むことにより、安全性の議論にも統一的な見通しが得られるであろう。現在、量子暗号の長距離化の限界は 100Km 以内にあり、それ以上の距離で量子暗号を可能とするためには、量子リピーターのような量子物理よりの研究がまだまだ必要である。

ビットコミットメントに代表される量子鍵配送以外のプロトコルに関していえば、思いの外「不可能定理」が大きな存在となっている。しかしながら、このことはこの領域が痩土であることを意味するわけではない。むしろ、本報告にみられるように、我々が既存の暗号技術において培ってきた知見をもとに実用的な方式を模索していくことで量子情報と情報セキュリティの新しい研究領域が開拓される可能性をもっている。

付録 用語解説

誤り訂正処理

二者間において同じデータを共有するにあたり、伝送エラーの存在が無視できなくなる。このようにエラーが存在するデータに関して誤りを除去する処理。誤り訂正符号がポピュラーであるが、量子暗号の分野では独自の処理が要求される。

位相(光の)

光の状態の表す物理量の１つ。光子レベルでは量子化され離散的な状態しかもちえない。

位相変調器

光学素子、印加電圧の大きさに従い、通過する光の位相に変調をかける。結晶の屈折率が外部から印加される電場により変化するポッケルス効果を利用。

一時的仮定(temporary assumptions)

ある限られた期間の間だけ成り立っていればよい仮定。当然もとの仮定よりも弱い。

エタロン

光学素子、特定波長の光のみを透過させる。一枚の石英板の両面に反射膜を蒸着したものでファブリ・ペロー干渉計の原理を利用。

エンタングル状態

2 つ以上の粒子の量子状態が特定の組み合わせで相関をもった量子状態。EPR ペアとよばれる 2 粒子状態が有名。

干渉明瞭度(visibility)

干渉系において、干渉のハッキリさ加減を表す尺度。

ケットベクトル

量子状態を記述するのに用いられる複素ベクトル、Dirac によりはじめて導入された。

コイン投げプロトコル

遠く離れた二者間においてコイン投げを交互に通信することで実現するためのプロトコル。

拘束性(binding)

送信者がコミットした値を覆していないことを検証できること。

光電子増倍管

光子検出器の１つ。APD を用いた光子検出器に比べて大規模な装置となる。

コヒーレント光

レーザーから放射される光、もしくは、その光の状態。波長、位相が揃っているため可干渉性が高い。

射影演算子

量子状態であるベクトルをある平面に射影するための演算子。

正定値作用素測定(ＰＯＶＭ)

つねにその固有値が正となる作用素を用いた測定。

ダークカウント

光子検出器において、全く入射光のない状態で出力信号がでる度数。

単一光子源

1 パルスあたり 1 個の光子しか放出しない光源。量子暗号における理想的光源と考えられている。

短波長帯

光ファイバー通信において用いられる波長帯の１つ。830nm の前後。近距離用通信に使用。

長波長帯

光ファイバー通信において用いられる波長帯の１つ。1300、 1550nm の前後。長距離用通信に使用。

パラメトリック・ダウン・コンバージョン

非線形光学現象。単一光子源の発生メカニズムとして有力視されている。ポンプ光である入射光が振動数の低い 2 つの放射光、シグナル光とアイドラー光に変換される。

非直交状態

複素ベクトルである２つの量子状態においてその内積が 0 ではない状態

光カプラ

光学素子、光分岐器、方向性結合器、2 つの光を合わせたり、1 つの光を分離したりするの用いる。2 入力 2 出力方向性結合器は物理的にはビームスプリッタと同じ作用をする。

ビットコミットメント(bit commitment)

送信者が、自分の伝えたい情報（ビット値）を、そのままでは受信者はその値について分からない（秘匿性）が、あとからさらに証拠となる情報を送ることによってその値について検証できる（拘束性）ように符号化して送る方式。

秘匿性(concealing)

受信者が、送信者による開示の前にコミットされた値についての情報を得ることができないこと

秘密分散プロトコル

１つのメッセージを複数に分け、部分のみではメッセージを復元できないが、幾つか集まるとメッセージが復元できるプロトコル

ファラディーミラー

光学素子、入射光の偏光面をある決まった角度だけ回転して反射する。磁場により偏光面が回転するというファラディー効果を利用。

不確定性原理

ハイゼンベルクの不確定性原理、同時に正確に測定できない物理量があることを示す。

不可能定理(no-go theorem)

ビットコミットメントを実現するどのような量子プロトコルに対しても、原理的にそれを破る攻撃法に存在することを述べた定理。1997年に、Lo and Chau およびMayersらにより独立に示された。これは、現実的な仮定のもとでの安全な量子ビットコミットメントの存在を否定するものではない。

プライバシー増幅処理(privacy amplification)

量子暗号において二者間で鍵共有をおこなうとき、若干の情報が盗聴者に漏洩していると仮定して、二者間で共有するデータから盗聴者には全く情報が漏れていないような共有

データを精製する処理。

ブラベクトル

ケットベクトルの双対ベクトル。

紛失通信プロトコル

送信者から受信者に通信文を送るとき、50%の確率で受信者に伝わるが、送信者は伝わったかどうか分からないような通信プロトコル。

ベルの状態(Bell States)

量子相関にある 2 粒子状態を記述する

偏光

光の状態の表す物理量の１つ。光子レベルでは量子化され離散的な状態しかもちえない。

方向性結合器

「光カプラ」参照

ポッケルスセル

光学素子、印加電圧の大きさに従い、通過光の偏光面を回転する。ポッケルス効果を利用。

ユニタリ変換

量子力学における基本的な変換。量子状態にユニタリ変換を施しても内積は不変である。

量子鍵配送

量子暗号の代表的プロトコル、2 者間において安全な鍵共有を実現する。

量子効率

光子検出器において、光子が入射したときに出力信号がでる確率。

量子コンピュータ

量子情報処理の量子暗号と並ぶもう 1 つの成果。最近になり既存の公開鍵暗号が量子コンピュータにより解かれる可能性が発見され注目を浴びている。

量子状態

量子力学により記述される状態。量子力学においては、観測量はこの量子状態に観測量に対応する演算子を作用させることによって得られる。

量子ビットコミットメント(quantum bit commitment)

量子効果を取り入れることによって安全性を向上させたビットコミットメント。

APD

光子検出器に用いられる半導体素子。アバランシェフォトダイオード(Avalansh photo diode) の略。

BB84 プロトコル

量子鍵配送プロトコルの 1 つ。Bennet、Brassard により 1984 年に提案された。

B92 プロトコル

量子鍵配送プロトコルの 1 つ。Bennet により 1992 年に提案された。

EPR ペア(EPR 効果)

Einstein、Podolsky、Rosen により提案された量子相関を持った特殊な 2 粒子状態。エンタングル状態の１つ。もしくはその 2 粒子による量子相関効果

E91 プロトコル

量子鍵配送プロトコルの 1 つ。Ekert により 1991 年に提案された。

GHZ 状態(Greenberger-Horne-Zeilinger state)

エンタングルした 3 粒子状態。

no-cloning 定理

量子状態を観測することなく、複製することができないという定理

One-Time Pad 法

情報量的に安全性の保証された暗号。平文と鍵の排他的論理和をとったものが暗号文。従って、平文と同じ長さの鍵が必要。安全な鍵配送を如何に行うかに課題がある。

POVM(正定値作用素測定)

「正定値作用素測定」参照。