九州大学学術情報リポジトリ
Kyushu University Institutional Repository

量子暗号理論から見た量子系の諸性質の定量的な理解

小芦, 雅斗
大阪大学大学院基礎工学研究科

https://doi.org/10.15017/18705

出版情報：応用力学研究所研究集会報告. 21ME-S7 (15), 2010-03. Research Institute for Applied Mechanics, Kyushu University
バージョン：
権利関係：

KYUSHU UNIVERSITY

応用力学研究所研究集会報告 No.21ME-S7
「非線形波動研究の現状と将来 — 次の 10 年への展望」（研究代表者　矢嶋　徹）
共催　九州大学グローバル COE プログラム
「マス・フォア・インダストリ教育研究拠点」

Reports of RIAM Symposium No.21ME-S7

Current and Future Research on Nonlinear Waves — Perspectives for the Next Decade

Proceedings of a symposium held at Chikushi Campus, Kyushu Universiy,
Kasuga, Fukuoka, Japan, November 19 - 21, 2009

Co-organized by
Kyushu University Global COE Program
Education and Research Hub for Mathematics - for - Industry

Article No. 15 (pp. 99-106)

量子暗号理論から見た量子系の諸性質の定量的な理解

小芦 雅斗 (KOASHI Masato)

(Received January 29, 2010)

Research Institute for Applied Mechanics
Kyushu University
March, 2010

量子暗号理論から見た量子系の諸性質の定量的な理解

大阪大学基礎工学研究科　　小芦雅斗　(KOASHI Masato)

概 要

量子系に対して測定を行うと、その量子系の状態は一般に変化する。この量子力学の基本的な性質を、盗聴行為の検出に応用することで暗号通信を行う試みが量子暗号である。様々な状況下において、量子暗号のセキュリティを原理的に証明する試みは、測定と状態変化の不可分な関係という量子力学の基本的な性質について定量的に掘り下げることに相当する。その結果、暗号通信という応用的な目標とは別に、量子系の持つ情報の大きさを操作的に定量化する問題への解答や、量子的な相関の大きさについての定量的な理解など、量子系の諸性質の定量的な理解を促進するという基礎的な副産物が生まれている。

1. 序論

量子系に対して測定を行うと、一般にその量子系は測定の反作用を受けて、状態が変化する。このような、測定による情報取得と被測定系への擾乱との間のトレードオフ関係を巧みに利用して、暗号通信に応用しようという試みが、量子暗号である。光パルスは量子系であるから、光通信における盗聴行為は量子系に対する測定行為と見なすことができる。そのため、信号の載せ方を工夫することで、受信された光パルスの状態変化から、盗聴行為の程度を定量的に見積もることが出来る。つまり、状態変化が小さければ、盗聴者への情報の漏洩が小さいことが量子力学の原理に基づいて証明できる、という仕掛けである。

量子暗号の理論研究では、様々な状況下で情報漏洩が小さいことを「証明」することが主眼となるが、この証明は、「原理的に許されるあらゆる盗聴行為」の可能性を取り込まなければならない。このため、応用的な動機にもかかわらず、その理論研究は量子力学の原理に深く切り込むことになる。そこで、本稿では、量子暗号の研究の過程で浮かび上がってきた基礎的な側面に焦点を当て、量子系の基本的な諸性質の定量的な理解の進展について、いくつかの例を紹介したい。

量子系を信号の媒体として見たとき、その情報の「大きさ」はどう決まるのか、という問いは、基本的な問題のひとつである。古典的なデジタル信号では、信号の保存に最低限必要なメモリの容量が、シャノンのエントロピーで与えられる。ところが、これが量子系になると、単純なエントロピーは最低限必要なメモリの容量を必ずしも与えず、何が情報の大きさを決めているのかが謎であった。この問題自体は暗号と無関係に見えるのだが、意外なことに、メモリの容量を与える一般的な公式の発見は、量子暗号理論を契機としてもたらされた。

２つの量子系の間の真に「量子的な」相関とは何か、という基本的な問題に対しては、様々なアプローチが考えられる。最近になって発展した量子情報理論では、通信路で結ばれた２者（Alice と Bob）がそれぞれ部分系を持っている状況を想定し、古典通信だけでは作れない相関をエンタ

ングルメントと呼ぶ。一方、時代を遡って EPR の論文を思い出すと、アリスの持つ系の共役な二つの物理量から、ボブが好きにひとつを選んでその値を予言できる、という性質が議論されている。両方の物理量を同時に予言することは、不確定性原理に反するので禁止される。このように、どちらも実行可能なのに同時には実行不可能という相補的な二つのタスクが存在するという状況も、アリスとボブの系が量子的に相関を持つことに起因している。また、その相関を利用してどのくらい暗号通信ができるか、という視点も、相関の量子性のひとつの見方と言えるだろう。以上のように、古典系とは異なる相関、とひとくちに言っても、そのような相関は多種多様な量子特有の性質に関連しており、全体像を把握することは容易ではない。果たして、これらの性質は全て同じものを違った角度から見ているだけなのだろうか？　それとも、各性質は微妙に、あるいは大幅に異なる源泉を持つのだろうか？　この疑問に対しても、量子暗号の研究を通じて、諸性質の間に一般的に成り立つ美しい定量的な関係が浮かび上がってきている。

2. 擾乱なしの場合と量子情報の大きさ

測定された量子系は、その状態が変化する、という性質はあくまで一般論であって、実際には量子系の初期状態や測定の種類によって変化が起こらない場合もある。極端な例として、０か１かという１ビットの古典情報を、０なら縦偏光の１光子、１なら横偏光の１光子という対応で光パルスの量子系に書き込んだとしよう。この２種類の光子の状態は、状態ベクトルが互いに直交し、原理的に確実に見分けることができる。従って、そのような測定をすれば、書き込まれた情報が得られるし、さらに、測定前の状態が縦偏光、横偏光のどちらであったかについても完全にわかってしまう。そこで、その正しい偏光状態の１光子からなる光パルスを改めて発生させると、測定前と測定後の状態は全く同一になってしまう。つまり、このケースでは、状態変化を引き起こすことなしに、測定によって情報を引き出すことが可能であり、当然ながら暗号通信には使えない。

一方、少し状況を変えて、０なら縦偏光の１光子、１なら斜め４５度偏光の１光子、という対応で書き込んだとしよう。今度は、２状態の状態ベクトルは互いに非直交であり、確実に見分けることは原理的に不可能である。また、０か１か、について僅かでも情報が得られる測定をしてしまうと、状態がどうしても変化してしまうことが簡単に示せる。つまり、このような情報の載せ方をすれば、盗聴行為の痕跡が残ることになるので、暗号通信に応用できる可能性が出てくることになる。もちろん、現実には他のノイズ源がある中でその痕跡を読み出せるか、という問題が浮上するのだが、それについては次節で考えることとし、ここでは僅かでも痕跡が残るか、そうでないか、という違いに着目することにしよう。

以上のように、どのような量子状態の組み合わせに情報を載せるかによって、量子暗号として使えるかどうかが決まる。使う状態を純粋状態に限れば、上記の例がほぼ全てを語りつくしており、互いに非直交な状態の対を含むように量子状態を組み合わせれば量子暗号として使える、という単純な答えでよい。

しかし、量子力学では、純粋状態だけでどんな系の状態も全て表せるわけではなく、混合状態

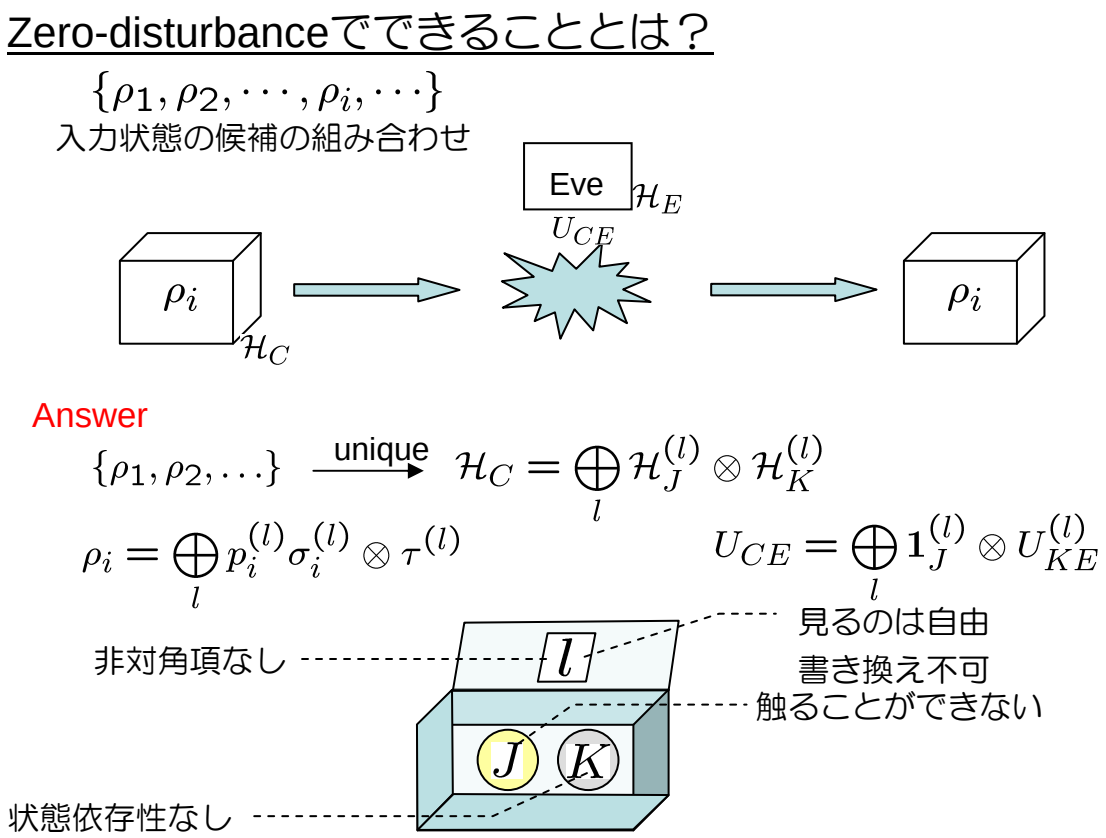
も含めて考える必要がある。混合状態は、純粋状態の確率的な混合に過ぎないことは確かであるが、問題は、ひとつの混合状態を純粋状態の混合に分解するやり方が無数にあって、一意に決まらない点である。とくに、全体として純粋状態にある複合系を構成する部分系ひとつだけを見たときに混合状態に見えるケースでは、どの分解の仕方が正しいか、という問いに答えることもできない。このようなわけで、通信が絡む問題のように、複数の部分系が登場する問題では、純粋状態での結論を単純に混合状態に敷衍することができないのである。

では、混合状態も含めた一般の状態について、どのような量子状態の組み合わせに情報を載せれば量子暗号として使えるか、という一般的な問題に戻ろう。少し問題の体裁を変えて、量子状態の組み合わせが先に与えられたとして、盗聴者（慣例で Eve と呼ぶ）が状態変化なしで行える行為は何か？という問いのほうが扱いやすい。測定を含めた盗聴者の行為は、盗聴者の持つ量子系Ｅと、光パルスの系 C との間のユニタリ変換 U_{CE} で一般に表すことができるので、許される U_{CE} の形は何かが分かればよい。その答え[1]は、数学的にはやや複雑で、次のような形になる（次頁図参照）。信号として使われる量子状態の密度演算子の組から、直和とテンソル積からなるヒルベルト空間の分解の仕方が一意に決まる。この分解のもとで、それぞれの密度演算子は図のような単純な形をしている。状態変化を起こさないためには、U_{CE} は図のような形をしていなければならない。

もう少しわかりやすく紐解くと、どんな状態の組み合わせを取っても、それは箱の中に J、K の２個の粒子が入ったモデルで常に解釈できる。箱には番号 *1* が書かれていて、これは状態変化なしにただで見ることが許される。粒子 J の状態は、少しでも知ろうとすると状態が変化してしまうので、触ることができない。一方、粒子 K の状態は、最初どの量子状態が選ばれていても常に決まった状態であり、覗いても情報が得られない。従って、粒子 J に書き込まれた情報は、量子暗号として使えるということになる。

以上の話は、量子暗号を具体的に行う際の種々の状態の選び方を統一的に理解するために構築された理論であるが、思わぬところに副産物をもたらした。それは、量子情報の大きさの定量化の問題である。信号源の持つ情報量を操作的に定量化する方法として、保存に最低限必要なメモリの大きさを考えるやり方がある。古典信号であれば、確率分布のシャノンエントロピーがこのメモリのビット数に一致する。量子状態からなる信号も、２準位系を量子メモリとして使い、１キュビットという単位で呼ぶことにすれば、同じように操作的に定量化できるだろう。純粋状態のみからなる信号であれば、答えは単純であり、密度演算子の平均をとって、そのフォンノイマンエントロピー S を計算すれば、これが必要なメモリのキュビット数になる。ところが、一般に混合状態を含む信号では、この S よりも少ないメモリに保存できるケースがあり、一般にどういうルールで大きさが決まるのかが不明であった。一見すると、このような情報を圧縮してメモリに保存する話は、暗号と無関係に思える。ところが、保存したものを取り出してもとの状態に解凍する過程を考え、圧縮から解凍までのプロセスをひとつの作業とみなせば、初期状態がそのまま終状態として出てくる過程になっている。すなわち、上記の量子暗号の議論で盗聴者の置かれた状況に酷似しているのである。そう思うと、そこに出てきたヒルベルト空間の分解が圧縮解凍の問題の答えを与えたことはそう不思議ではないであろう。

最低限必要なメモリの大きさの答えは以下のようになる[2]。上述の分解のもとでは、平均密度演算子のフォンノイマンエントロピーは、$S = I_C+I_Q+I_R$ のように３つの項の和に分解される。I_C は箱に付いた番号 l の持つエントロピー、I_Q は粒子 J の持つエントロピー、I_R は粒子 K の持つエントロピーである。このとき、I_C が最低限必要な古典メモリのビット数を与え、I_Q が最低限必要な量子メモリのキュビット数を与える。I_R は保存の必要がない冗長部分の大きさであると解釈できる。このように、どんな量子信号も、古典メモリに保存できる古典的な部分、量子メモリに保存しなければならない量子的な部分、及び冗長部分の３つに綺麗に分けることができる。また、古典的な部分は量子暗号に使えないが、量子的な部分の情報は、「見ると壊れる」という性質があって、量子暗号に使うことができる。前者の分解が先に見出されてから、後者のような性質がわかったのではなく、量子暗号に纏わる後者の性質を追いかけた結果、前者の分解が見出されたというところが面白い。



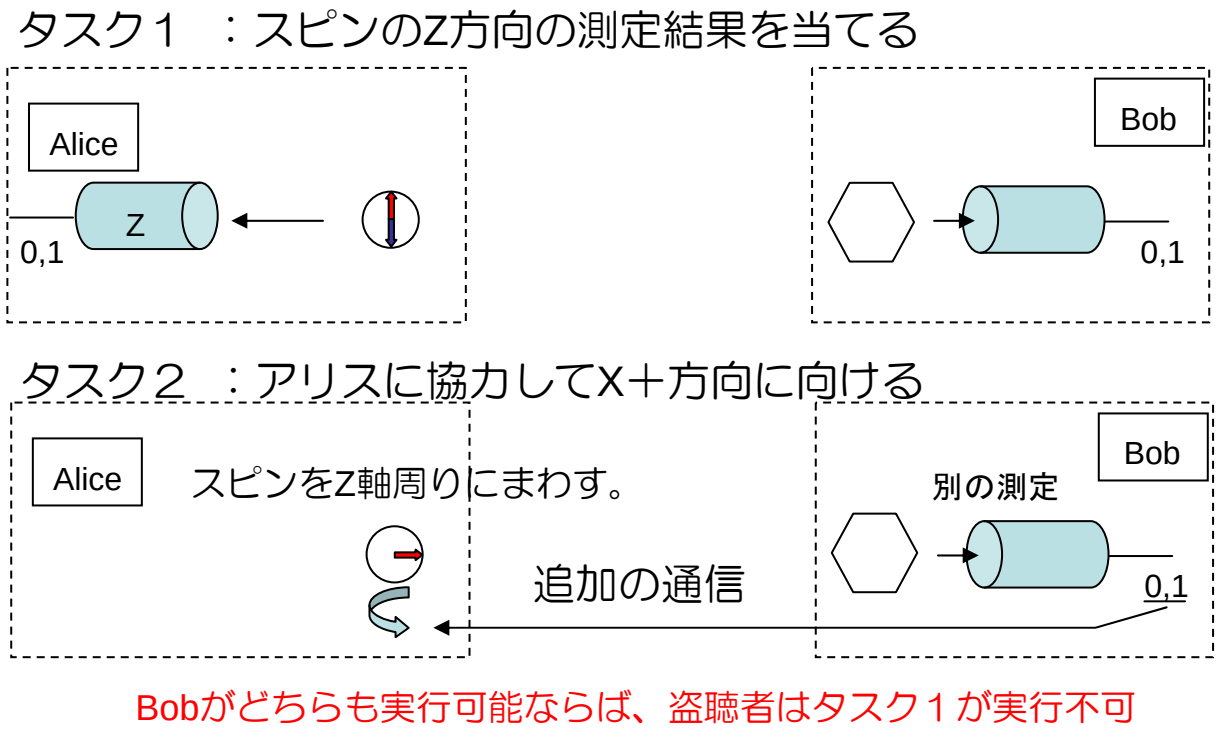
3. 擾乱がある場合と量子力学の相補性

前節では、盗聴行為があると僅かでも何かしら擾乱が起こる条件を考えたが、現実の装置で量子暗号通信を行うためには、それだけでは不十分である。現実的な光源と光検出器を用いて通信を行うと、装置の性能が不十分であったり、ノイズが混入したりするなどの影響で、送信された状態は盗聴行為がなくても変化してしまう。そのため、擾乱があるかないか、という定性的な観

点ではなくて、より定量的な考察、すなわち、擾乱の大きさがこの程度であれば、盗聴によって漏れた情報の大きさは高々これ位のはずだ、という見積もりが必要になる。漏れた情報量がわかっていれば、古典的な通信を用いて送受信者が話し合うことで、漏れていない部分だけを取り出して暗号通信に利用することができる（このプロセスを秘匿性増幅と呼ぶ)。

前節で、盗聴者の行為は、盗聴者の持つ量子系 E と、光パルスの系 C との間のユニタリ変換で一般に表すことができると述べた。そこで、原理的には、全てのユニタリ変換を調べて漏洩情報量の最大値を計算すれば良いように思えるかもしれない。ところが、秘匿性増幅のプロセスでは、送受信者の持つビット列に対して演算を施すために、ビット列を構成する各ビットの間の相関が影響を持つようになる。各ビットは、もともと光パルスの送信によって生成されたものであるから、この相関は、遡れば次々に送信された多数の光パルスの間の相関を引き継いでいる。この状況下で、盗聴者にとって最善の選択は、当然ながら個々の光パルスに対して独立に攻撃することではない。送信された多数の光パルスを一括して攻撃し、その間の相関を制御するほうが、盗聴者にとって有利である。こうなると、考えなければならないユニタリ変換は、何千、何万と送られる光パルス全てに対するユニタリ変換ということになって、全てのユニタリ変換を力技で調べ尽くすのは到底無理な話になってしまう。

この問題を解決するために、量子暗号のセキュリティの理論においては、盗聴者 Eve の盗聴行為を直接考えなくても、送信者(Alice)と受信者(Bob)の手元にある量子系だけに着目することで、情報漏洩の程度が保証できる巧妙なテクニックがいろいろと追及されてきた。ここでは、そのようなテクニックのひとつである、量子力学の相補性を用いた考え方[3]を紹介しよう。



図のように、Alice は二準位系（スピン 1/2 の粒子）を持ち、Bob はその粒子と相関した量子系

（例えば届いた光パルス）を持っているとする。暗号通信を行うために、Alice はスピンの向きを Z 方向に測定してビット値を得る。Bob は、自分の量子系にうまい測定をして、Alice と同じビット値を得ようとする。これをタスク１と呼ぼう。もし、二人の持つビット値が完全に一致し、全くランダムで、しかもその値が Eve には全くわからないとすれば、この相関ビットを用いて１ビットの情報を Eve に漏れないように送ることが可能である。そのような理想的な相関ビットは秘密鍵と呼ばれている。タスク１が達成できるなら、二人の持つビット値が完全に一致することにはなるが、それがランダムかどうか、また、Eve にその値が漏れていないかどうかはわからない。そこで登場するのが相補性である。この考え方では、もし、Alice と Bob が、タスク１を目指すのを辞めて、代わりに別のタスクを行ったらどうなるか、という考察をする。具体的には、追加の通信を好きなだけ用いて、Alice のスピンを Z 軸の周りに回し、終状態が常に右方向を向くようにする、というのがタスク２の目標である。ここで用いる追加の通信は、ビット列を送る古典通信だけでなく、量子系をそのまま手渡すような量子通信でもなんでもよい。例えば、Alice のスピンの向きを X 方向に測定した結果を Bob が自分の系の測定によって完全に予測できるような場合は、その予測を Alice に伝えることで Alice は適切な回転を行い、タスク２を達成できる。

さて、タスク１が達成できただけでなく、タスク２もやろうと思えばちゃんと達成できた、ということが保証されたとしよう。どちらのタスクも、盗聴者 Eve は全く登場していないことに注意して欲しい。それにも関わらず、この場合はタスク１で得られた二人のビット値は秘密鍵であると結論してよい。実は、タスク１と２は、１粒子干渉計における経路の測定と干渉縞の制御のような関係になっている。干渉計で、粒子がどちらの経路を通ったか知ることと、干渉縞を作ることは同時にはできない。同様に、タスク１、つまり Alice のスピンの Z 方向の向きを予測することと、タスク２とは同時には達成できない。仮に、Eve が Alice のスピンの Z 方向の向きを予測できたとすると、Alice と Bob がタスク２を達成できたという前提から、３人合わせて両タスクが同時に達成できてしまうことになる。それは禁止されているので、Eve には Alice のスピンの Z 方向の向きがわからない、という結論に至る。このように、Eve が過去にどんな盗聴行為を行ったのかについて具体的な言及をせずとも、Eve に情報が漏洩していないことを証明できる点がこの考え方の利点で、現実の装置で量子暗号通信を行う際のセキュリティの証明に利用されている。

4. 量子的な相関の大きさ

ここで、２つの部分系の間の真に量子的な相関とは何か、あるいはその大きさはどうやってきめるか、という基礎的な問題を考えてみたい。数学的にいろいろと定義をすることはもちろん可能だが、ここでは、物理的な意味が明白な、操作的な考え方に限ろう。いわゆる量子もつれ(entanglement)という言葉は、最近では、古典的な通信だけでは作れない相関、という意味で使われることが多い。古典的な通信で作れないもっとも典型的な相関は、二つのスピンの１重項状態であり、しばしば量子もつれの大きさの基本単位(ebit)として用いられる。一般の状態についての量子的な相関の大きさは、この基本単位を物差しとして、何個分に相当するか、というように定量化すればよい。すなわち、与えられた状態を古典的な通信で作るには、材料として１重項状

態のスピン対がいくつ必要か、という問題の答えが量子もつれの大きさだと思えばよいだろう。この値(E_C)は entanglement cost と呼ばれる。しかし、話はそれほど単純ではない。コストとは逆の考えで、与えられた状態を材料と考えて、古典的な通信で１重項状態のスピン対をいくつつくれるか？という問題を考えると、distillable entanglement と呼ばれる別の値(E_D)が定義できるが、残念ながらこの二つの値は一般には一致せず、コストのほうが大きくなる。

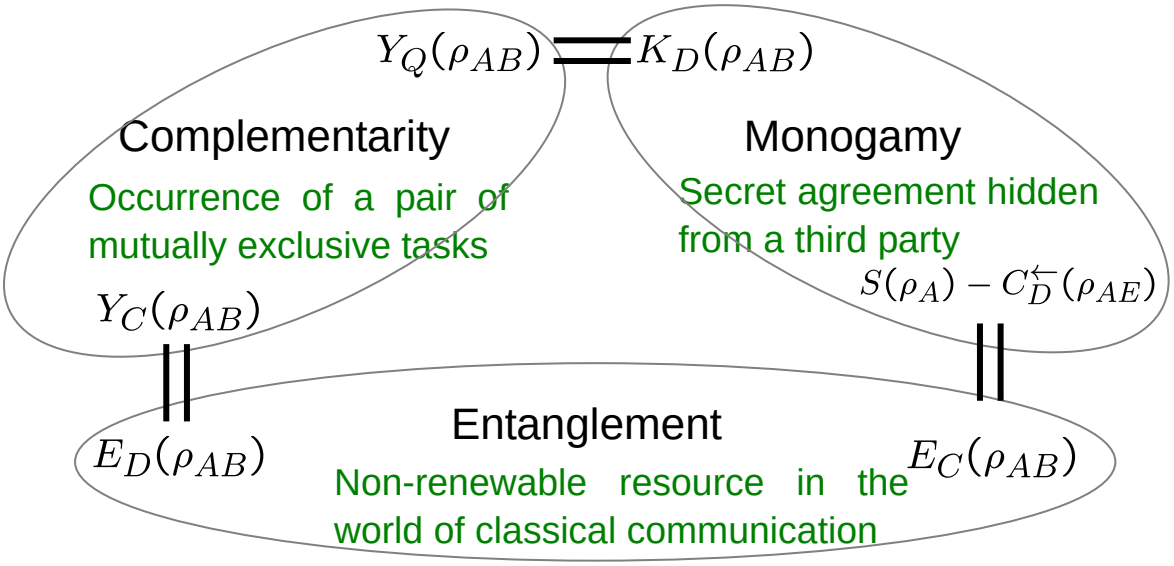
一方、全く別の視点から量子的な相関を考えることもできる。そもそも、量子暗号は、古典論では出来ないことを達成する話であるから、ある相関を材料にして暗号通信が出来たとすれば、それはまさにその相関が量子的であることの証左である。従って、与えられた状態から秘密鍵を何ビット取り出せるか、という値(K_D)も、量子的な相関を計るひとつの物差しだといえる。この量は、distillable key と呼ばれ、第３者には漏れていない、２者間だけに排他的に生じている相関(monogamy)の大きさを操作的に定義したもののひとつと考えられる。その大きさは、上に出てきた E_D とも E_C とも一般には一致しない。このように、真に量子的な相関とは何か、という問いには唯一の正解があるわけではなく、どのような量子的性質に着目するかによって物差しが変わるし、同じ性質に根ざしていても、定義の仕方で複数の物差しができるなど、一筋縄ではいかない。

前節で登場した相補性に関わる性質も、量子的な性質のひとつである。二つの両立しないタスクを好きに選んで実行できるという状況は、量子的な相関を持つ量子系が配られているからこそ生じている。そこで、タスク１とタスク２のような芸当を、Alice の持つスピンの数をどのくらいまで増やしても実行できるか、という値(Y_Q)を考えると、これも量子的な相関のひとつの指標になる。前節では、両タスクが実行可能なら秘密鍵が出来る、という議論をしたが、これは直ちに $Y_Q \leqq K_D$ が成立していることを意味している。面白いことに、逆向きの議論も成り立つことが証明できる。つまり、秘密鍵が出来るなら、いつでも実行可能なタスク１とタスク２が存在する、ということが言えて、その結果、$Y_Q = K_D$ が全ての量子状態について成立することが言える。つまり、相補性をもとに作った物差しと、排他的な相関をもとに作った物差しは、定量的に一致しているのである。

これだけなら、単に排他的な相関と相補性がそもそも同じ性質なのだ、という結論になりそうだが、まだ話には続きがある。タスク２において許される追加の通信を、古典通信のみに限定して、同じように物差し Y_C を定義しよう。タスク自体はより難しくなっているので、一般には $Y_C \leqq Y_Q$ である。この物差しが、実は量子もつれの物差しのひとつである E_D にピタリと一致することが示せる($Y_C = E_D$)。E_D と K_D は、異なる性質に着目して作られた物差しなのだが、相補性という性質はちょうどその二つの橋わたしをしているように見える。似たような話で、排他的な相関の物差しについても、K_D とは別の定義を与えることができる。K_D は、Alice と Bob が秘密鍵を取り出すシナリオであったが、これを、Alice と Eve が相関ビット列を取り出す可能性を、Bob がどの位邪魔しているか、という視点の定義に変える。すると、これが E_C に一致する[4]。

このように、いろいろな量子的な性質をもとに真に量子的な相関の大きさを考えると、一般には、多種多様の物差しが作れて、その値も異なるのだが、その中には、異なる出自の物差しが定量的に一致する場合があり、異なる量子的な性質が定量的にも美しい関係を持っていることを示

唆している。もちろん、図に示したのはたまたまそういった関係が見つかったものを選んで表示しているだけなので、実際には他との関連がない物差しもいろいろと作れてしまう。その意味では、量子的な相関とは何か、という問題はまだまだ混沌としており、もっと高度で美しい構造が隠されている可能性もあるだろう。



5. おわりに

本稿では，量子暗号のセキュリティ理論について、とくにそこから派生した基礎的な問題についての我々の理解の進展を中心に述べた。現実的な装置を用いる場合などを考え始めると、通常なら、応用的な課題となって、基礎的な問題からは遠ざかってしまうものだが、量子暗号の場合には、むしろそういった応用的な課題に真剣に取り組むことで、基礎的な問題への答えも明らかになってくるという面白さがある。考えてみれば、測定とその反作用、という量子力学の本当に核となる性質を利用したものが量子暗号であるから、その応用課題に取り組むことが、量子力学の本質を定量的に理解する上で進むべき道と同じ方向を向いていたとしても、不思議ではないのかもしれない。

---

[1] M. Koashi and N. Imoto, Physical Review Letters **81**, 4264 (1998); M. Koashi and N. Imoto, Physical Review A **66**, 022318 (2002).
[2] M. Koashi and N. Imoto, Physical Review Letters **87**, 017902 (2001); M. Koashi and N. Imoto, Physical Review Letters **89**, 097904 (2002).
[3] M. Koashi and J. Preskill, Physical Review Letters **90**, 057902 (2003); M. Koashi, New Journal of Physics **11**, 045018 (2009).
[4] M. Koashi and A. Winter, Physical Review A **69** 022309 (2004).