量子暗号の話

森前智行（京都大学基礎物理学研究所）

2022 年 4 月 1 日

1　はじめに

量子論には、古典論には無い不思議な現象が多くある。例えば、量子的重ね合わせ、不確定性原理、no-cloning 等である。このような不思議な現象をうまく利用することにより、これまでにないような高性能な情報処理技術を実現するのが量子情報である。特に、計算への応用（量子計算）と暗号への応用（量子暗号）がメジャーな応用例である。本稿の内容は後者の量子暗号に関するものである。

暗号理論においては正確な定義や厳密な証明が重要であるが、本稿では全ての説明は直観的な理解を優先し厳密性は失われたものになっている。詳細や正確な内容が知りたい場合は引用されている文献を参照してほしい。また、量子情報や量子計算の初歩についても知識を仮定する。必要に応じて教科書 [1, 2] を参照していただきたい。

2　量子の不思議な性質

まずは量子の不思議な性質について簡単に復習しておこう。量子の不思議な性質として、主なものに、量子的重ね合わせ、不確定性原理、no-cloning がある。量子的重ね合わせというのは、量子的な系の状態は $|\alpha\rangle$ という状態と $|\beta\rangle$ という状態の任意の複素係数による線形結合で表される状態も取り得るというものである。これは、α という状態と β という状態が古典の確率分布にしたがってランダムに出るということとは違い、古典系には無い量子特有の性質である。特に、重ね合わせの係数がマイナスにもなるおかげで、量子的干渉効果で異なる計算パスを打ち消すことにより高速な計算が実現できるのが量子計算である[1]。量子的重ね合わせは、不確定性原理や no-cloning と違い、量子暗号においてはどちらかというと「困るもの」として出てくるこ

[1]ただし、このように量子的干渉効果で打ち消して高速化できるのは問題の構造をうまく使えた非常に限られた場合のみであり、ほとんどの場合はどうやって打ち消してよいかさっぱり分からない。よく国内の報道に出てくる、実際の社会の現場に現れる様々な組合せ最適化問題を「量子計算機」を使って解きました、という話は量子による高速性に科学的根拠は無いので要注意！

とのほうが多い。量子計算機を持っている攻撃者は、量子的な重ね合わせで「データーベース」にアクセスすることができる。そのような攻撃はこれまでの古典の暗号では考えられてこなかったため、新たにそのような攻撃に対する安全性を証明する必要がある。耐量子暗号の分野ではそのような研究が近年活発に行われてきており、暗号以外にも使えそうな面白い結果もいろいろ出ている [3, 4]。

不確定性原理というのは大雑把にいうと、ある物理量の測定をして値を得ると、他の物理量の情報が完全に失われてしまうというものである[2]。例えば、$|010\rangle$ という状態の各量子ビットを Hadamard 基底で測定すると、計算基底の情報 010 は完全に失われてしまう。この性質は古典に無いものであり、後で見るように様々な量子暗号プロトコルに利用される。

No-cloning というのは、未知の量子状態はコピーできない、というものである。例えば、

$$U(|0\rangle|e\rangle) \to |0\rangle|0\rangle$$
$$U(|1\rangle|e\rangle) \to |1\rangle|1\rangle$$

を満たすユニタリ U が存在するとしよう。($|e\rangle$ は任意のアンシラ状態である。) これはつまり、$|0\rangle, |1\rangle$ のコピーを作れるようなマシンである。ところが、

$$\begin{aligned} U(|+\rangle|e\rangle) &= U(|0\rangle|e\rangle) + U(|1\rangle|e\rangle) \\ &= |0\rangle|0\rangle + |1\rangle|1\rangle \\ &\neq (|0\rangle + |1\rangle)^{\otimes 2} \end{aligned}$$

であるので、このような U は $|+\rangle = |0\rangle + |1\rangle$ という状態のコピーは作ることができない。古典のデータは原理的にコピー可能であるため、コピーできないという量子のみが持つ性質は暗号にとって非常に強力なものである。実際、後で見るように多くの量子暗号プロトコルに使われている。

3 情報理論的安全性と計算量的安全性

量子暗号の話に入る前に、暗号の安全性についても簡単に説明しておこう。暗号の安全性には大きく分けて二つある。情報理論的安全性と計算量的安全性である。情報理論的安全性というのは、攻撃者の計算能力がどんなに高くても安全であるようなものであり、計算量的安全性というのは、攻撃者の計算能力に制限があると仮定したときに成り立つ安全性である。明らかに後者より前者の方が望ましい。後者の場合、将来計算機の能力が発達したり、難しいと信じられていた問題（例えば素因数分解等）を効率的に解く新しい計

[2]不確定性原理はそれ自身が長らく研究されてきている研究対象であり、定義や解釈だけでも一つの解説記事になってしまうが、本稿は量子暗号の解説なので、不確定性原理そのものには深入りしない。

算モデルやアルゴリズムが発見されたりすると安全性が破れてしまう可能性がある。しかしながら、情報理論的安全な暗号はあまりいろいろなことができず、一方で計算量的安全な暗号は非常に様々な機能が実現できるため、計算量的安全な暗号はよく使われる。

情報理論的安全な暗号の最もシンプルな例に、one-time pad がある。今、アリスとボブは共通の鍵として、n ビットのビット列 $k \in \{0,1\}^n$ を持っているとしよう。アリスはボブに n ビットのメッセージ m を送りたいので、$c = k \oplus m$ という暗号文を作りボブに送る。($\oplus$ というのは各ビットを XOR する演算である。例えば $k = 010, m = 111$ だとすると、$k \oplus m = 101$。) ボブは $c \oplus k$ を計算すれば m を復号することができるが、鍵 k を知らない盗聴者イブにとっては c は完全にランダムなビット列であるため、m についての情報を全く得ることができない。これはイブの計算能力がどんなに高くてもそうである。

計算量的安全な暗号の例として、一方向性関数を用いた署名という暗号タスクを考えてみよう。一方向性関数とは、x から $f(x)$ を計算するのは簡単だが、$f(x)$ から x を求めるのは難しいような関数である。一方向性関数の存在はまだ証明されておらず、一方向性関数が本当に存在するのかは分かっていない。アリスは、自分のメッセージ m に「これは確かに自分の文章です」ということを証明するために、署名 σ を付けたいとしよう。簡単のためにメッセージ m は一ビットとする。つまりアリスのメッセージは 0 か 1 である。アリスはランダムに二つのビット列 x_0, x_1 を選び、$y_0 = f(x_0), y_1 = f(x_1)$ を計算する。ここで f は公開された一方向性関数である。アリスは、(y_0, y_1) を署名の検証用の公開鍵として公開する。アリスは $m = 0$ に対しては x_0、$m = 1$ に対しては x_1 を署名 σ として付ける。メッセージと署名のペア (m, σ) をもらったボブは、これが正当な署名であることを検証したい。そのためには公開鍵 (y_0, y_1) を使う。ボブは $f(\sigma)$ を計算し、それが確かに y_m になっていたら、正当な署名であるとしてメッセージ m を受理する。一方向性関数の性質により、(y_0, y_1) から (x_0, x_1) を求めることはできないので、(x_0, x_1) を知らないアリス以外の人間には正当な署名を作ることはできない。この署名の安全性は一方向性関数の性質から来ているので計算量的安全性である。実際、無限の計算能力を持つ攻撃者は、公開されている y_0, y_1 から x_0, x_1 を求めることができる。(全ての x を f に入力してしらみつぶしに探せばよい。)

4　量子暗号の二つの分類

それではここからようやく量子暗号の話に入る。量子暗号というのは最も広く言うと量子と暗号に関する研究を全て指すと思われるが、特に、二つの方向性の研究がある。一つは量子暗号プロトコルの研究であり、もう一つは耐量子暗号である。

4.1 量子暗号プロトコル

量子暗号プロトコルの研究というのは、量子の不思議な性質を利用することにより、古典よりも高性能な暗号タスクを実現したり、そもそも古典ではできない（できないと思われている）暗号タスクを実現するものである。

最も有名なものはよく新聞等にも出てくる量子鍵配送（ＱＫＤ）だろう。QKD については本稿では触れないが、非常に大雑把に言うと、one-time pad の鍵を共有するためにアリスがボブに量子状態（光など）を送るが、もし盗聴者が量子通信を盗聴すると、不確定性原理により、盗聴したことがばれてしまう、というものである。同じような機能（つまり鍵を共有するということ）は古典のみでも可能であるが、その場合は計算量的安全な方法しか知られていない。一方で QKD を使う場合は、情報理論的安全である。また、oblivious transfer というタスク[3]（そして multi-party computation）は古典の場合、一方向性関数よりも強い仮定を必要とするだろうと考えられているが、量子状態を送ることができるのであれば、（耐量子の）一方向性関数のみから実現できることが分かっている [5, 6][4]。

これらの例は、古典でもできるタスクが量子ならより優位性をもってできる（例えば安全性が強力になる等）、というものであるが、そもそも古典ではできない（できないと考えられている）タスクが量子を使えば実現できるという例も多くある。例えば、後で詳しく説明するような、偽造不可能な量子マネーや、サーバーにアップロードしたデーターを削除したことを保証する certified deletion 等である。古典のデータは原理的にはコピーできるため、量子マネーや certified deletion は古典では不可能である。また、クラウド量子計算を安全に行うというタスクは、量子計算を使うため、そもそも古典では不可能である。

量子の不思議な性質というのは量子論から来ているものであり、何か計算量的仮定のもとで成り立つというものではない。（例えば no-cloning は素因数分解が難しいから no-cloning が成り立つというわけでなく、量子論そのものの形から導出されるものである。）したがって、量子の不思議な性質のみを使って実現される量子暗号プロトコルは情報理論的安全なものとなる。計算量的仮定も使った量子暗号プロトコルの研究というのも昔からいくつかあるが（例えば [9]）、大量の結果が出るようになったのはここ数年であり、昔はどちらかというと、量子の性質のみを用いた情報理論的安全な暗号プロトコルの研究がほとんどであった。

---

[3] oblivious transfer というのは、アリスが二つのビット列 m_0, m_1 を持っており、ボブはその一方を得ることができ、アリスはボブがどっちを得たかを知れず、ボブは希望しなかったもう一方については知れない、というものである。

[4] さらについ最近、一方向性関数すら無しでもできる可能性が示唆された [7, 8]

4.2 耐量子暗号

量子暗号の研究を大きく二つに分けたときのもう一つの研究はいわゆる耐量子暗号である。これは、古典の計算機や古典のネットワーク上で動く古典の暗号[5]を量子的な攻撃から守るというものである。ご存じのように、素因数分解等は量子計算機で効率的に解けてしまうので、将来にそなえて、量子計算機でも効率的に解けなさそうな問題に基づいた（古典の）暗号が研究されている。特に、LWE（learning with errors）という、大雑把にいうと、ノイズののった連立線形方程式を解くという問題は量子計算機でも効率的に解けないだろうと信じられており、LWE をベースにしたいろいろな（古典の）暗号が作られている。

量子的な攻撃に対する安全性を考える場合は、単に量子計算機で解け無さそうな難しい問題を用意すればすむわけではない。古典の暗号でこれまで行われてきた安全性の証明は途中に量子が入ってくるともはや成り立つかどうか分からないので、改めて、量子が入っているうえでの安全性証明を再構築する必要がある。例えば、量子計算機を持っている攻撃者はデータベースに量子的な重ね合わせでクエリできるかもしれない。そのような攻撃に対する安全性はこれまで考慮されてこなかったので、きちんと考える必要があり、現在いろいろな研究が行われている[6]。

4.3 ハイブリッド

ここまで、量子暗号の研究には大きく分けて量子暗号プロトコルの研究と耐量子暗号の研究の二つがあると説明してきた。

前者は主に量子情報や物理の人たちが多く行ってきたように見える。その理由は二つ考えられる。一つ目は、量子暗号プロトコルの研究は量子の性質が前面にでてくるため量子の知識が必要だからである。二つ目の理由は、安全性は量子の性質のみから情報理論的に証明できるため、古典の計算量的な暗号の知識が必要でないという点である。一方で、後者はどちらかというと古典の暗号の人たちや数学の人たちがやってきているように見える。その理由は、いったん量子計算機で解けないだろうと信じられる古典の問題が決まると、あとはそこからは完全に古典の暗号あるいは数学の問題になり、量子は全く出てこないからである[7]。

---

[5]暗号の分野で古典暗号というと、公開鍵暗号などの現代暗号より以前の暗号、という別の意味になる。量子の人が古典暗号というときは、量子論が出てこない暗号、という意味であり、公開鍵暗号も古典暗号となる。

[6]例えば [4] は、Proof of quantumness という量子の優位性を古典検証するテクニックをうまく利用して古典では安全であるが量子では安全でない例を構成したエレガントな論文である。

[7]上でも述べたように、耐量子の為には、量子計算機で解けないような問題を用意するだけでは不十分であり、量子的な重ね合わせ攻撃に対しても安全であることを示す必要がある。そのような証明には量子の知識が必要となってくるため、最近では耐量子の研究でも量子が積極的に出てくるようになってきており、逆に暗号以外にも使えそうな新しくて面白いアイデアも現れてきている。

このように、(情報理論的安全な) 量子暗号プロトコルと、耐量子暗号の研究はどちらかというと、それぞれ別のコミュニティで独立に研究されてきたわけであるが、近年、両者の間で活発な交流を見せている。その理由の一つは後で述べるように、Mahadev らによるブレークスルーを通じて、量子の性質のみを使うだけでは実現できないような暗号的タスクが、耐量子暗号 (計算量的仮定) も組み合わせることによって実現できることが分かってきたからである。もともと耐量子暗号は古典の計算を守るための古典の暗号であったが、量子計算機でも破れないということは、量子ネットワークの中にいる量子計算機を騙すのにも使える。そこで、量子計算機が量子ネットワークで繋がったような場面における量子暗号プロトコルにも有用なのである。

5 情報理論的安全な量子暗号プロトコル

さて、ここからは具体的な内容に入る。まずは、量子の性質のみを使った情報理論的安全な量子暗号プロトコルについて解説しよう。そのような量子暗号プロトコルにおいて基礎となるのが BB84 状態である。BB84 状態というのは、$|0\rangle, |1\rangle, |+\rangle = |0\rangle + |1\rangle, |-\rangle = |0\rangle - |1\rangle$ の 4 つの状態である。アリスが BB84 状態をランダムに選んでボブに送るとしよう。アリスは自分で選んだのでどの状態か知っているが、ボブは自分にどんな状態が届いたか分からない。測定しても完全な情報は得られない。(例えば、計算基底で測定して 0 がでたら、$|1\rangle$ でないことは分かるが、他の 3 つのどれであるかは不明である。) また、送ってきた状態のコピーをつくることは no-cloning により不可能である。(一方で、アリスは自分がどんな状態を選んだかの古典的情報を持っているので、それを使って同じ状態のコピーを好きなだけつくることができる。)

このように、アリスはボブに対して優位な状況にある。この非対称性をうまく使うことによりいろいろな暗号タスクが実現できる。以下では 3 つの例を紹介する。

5.1 (privately verifiable) 量子マネー

最もメジャーな量子暗号プロトコルの例に、量子マネーというものがある。上記の BB84 状態を送る設定において、アリスが銀行でボブが一般人に相当する。アリスはランダムに選んだ BB84 状態が埋め込まれたお札 (量子マネー) を作り、流通させる。ボブは、量子状態のコピーが作れないので、お札の偽造ができない、というものである。このアイデアはイスラエルのウィズナーによって 1970 年に提案された [10]。当時はあまりにも画期的過ぎたのか、13 年後にようやく出版されたらしい。(ファインマンの量子計算の提案が 1982 年、ショアーのアルゴリズムが 1994 年である。) このウィズナーの量子マネー

は実は量子を情報処理技術に応用する最初の提案であり、つまり量子情報の一番最初のアイデアであるといわれている。

お札が本物かどうかは、どういう量子状態が埋め込まれているかを知っている銀行しかチェックできないため、お札が本物かどうかを知るには銀行にいちいちもっていかないといけない。このように、秘密の検証鍵を持った特定の人しかチェックできないような量子マネーは privately verifiable 量子マネーと呼ばれている。いちいち銀行にもっていかなくても、誰でもその場で正しさがチェックできるような量子マネーは作れないだろうか？どういう量子状態を埋め込んだかという情報も公開すれば、誰でも正しさがチェックできるようになるが、それだと今度は誰でも偽造できるようになってしまうため、何か工夫が必要である。（ちなみにウィズナーの BB84 を使った量子マネーの場合 public verifiable なものは達成不可能であることが知られている [11]。）このような問題は Aaronson により 2009 年に初めて提示され [12]、publicly-verifiable 量子マネーと呼ばれて研究が続いている。

明らかに、情報理論的安全な publicly-verifiable 量子マネーは不可能である。なぜなら、ボブが自分で量子マネーをチェックすることができるデバイスを持っているわけなので、そのデバイスに適当に作った量子マネーを何度も入力し、本物であるという結果がでるまで繰り返せばよい。指数回かかるかもしれないが、ボブの計算能力は無限なので可能である。後で説明するように、耐量子暗号を利用した publicly-verifiable な量子マネーがいろいろ提案されている。

5.2 Certified deletion

暗号化したデータをサーバにアップロードしたとしよう。しかし結局そのデータは使わないことになったので、セキュリティのためにサーバから削除したい。サーバに削除の依頼を出し、サーバがたしかに削除したという証拠をユーザーに送る。ユーザーはこの証拠をチェックし、もし有効なものであれば、確かにサーバからデータは完全に消去されたと確認できる。このようなものが certified deletion である。明らかに、これは古典の世界では不可能である。なぜなら、悪意のあるサーバはこっそりデータのコピーを取ることができる。（古典のデータは原理的にコピー可能。）ユーザーから削除の依頼がきたら、オリジナルを消して消した証拠を送ればよい。コピーをこっそり保持しているので、時間をかけてこのデータの暗号を解読したり、将来ユーザーがうっかりデータの暗号化に使った秘密鍵を漏洩した際にはその鍵を用いてコピーしたデータを読むことができる。

量子を使うと certified deletion が可能であることが最近 Broadbent と Islam によって示された [13]。アイデアとしては、データ m を $m \oplus u \oplus H(r)$ と暗号化してサーバにアップロードする。ここで、u, r はランダムなビット列であ

り、H はハッシュ関数である。さらに、r の情報を計算基底に隠しているランダム BB84 状態を作り、それもアップロードする。（例えば、$r = 0101$ とすると、$|+\rangle|0\rangle|1\rangle|-\rangle|0\rangle|+\rangle|1\rangle$ のようなランダム BB84 状態を用意する。）ユーザーはデータを削除してほしくなったら、サーバに BB84 状態の全ての量子ビットを Hadamard 基底で測定してもらい、その結果を削除の証拠として送ってもらう。もし Hadamard 基底の箇所の測定結果が全て一致していれば、削除の証拠は有効である。（例えば、上記の例でいうと、測定結果が $+??-?+?$ となっていればよい。）サーバは受け取った BB84 状態のどれが計算基底でどれが Hadamard 基底か分からないので、全ての Hadamard 基底の箇所について正しい測定結果を出すためには、全ての量子ビットを Hadamard 基底で測定する必要があるが、そうすると、計算基底の箇所に埋め込まれている r の情報が消去されてしまうことになる。r の情報が失われてしまうと、たとえ後から u が漏洩してももはや m を知ることはできない。

このように、量子の no-cloning と不確定性原理をうまく使うことにより、古典では不可能な certified deletion が実現できる。しかし、この Broadbent-Islam の方法だと、ユーザーは BB84 状態を作り、サーバに送る必要がある。完全古典のユーザーと古典通信のみでも certified deletion は可能だろうか？これは一見すると不可能なように見える。なぜなら、サーバには古典のデータしか伝わらないため、サーバは好きなだけデータをコピーできるからである。面白いことに、LWE を使うと実は古典通信のみでの certified deletion が可能となる [14]。これについてはまた後で説明する。

5.3　ブラインド量子計算・量子計算の検証

量子計算機は高価で巨大なものなので一家に一台というのはだいぶ先であり、当面はクラウド的に利用されるだろう。つまり、ユーザーは自宅の端末から遠隔にある量子計算機にリモートアクセスし、そこで量子計算を実行するのである。クラウド量子計算が今後普及するうえで、セキュリティが重要になってくる。クラウドに計算内容を知られることなく量子計算を委託できるだろうか（ブラインド量子計算）？また、クラウドが正しい量子計算をしているかどうかチェックできるだろうか（量子計算の検証）？もし、1 量子ビット状態を生成あるいは測定でき、サーバとの間で量子状態を通信できれば、古典のクライアントがブラインド量子計算や量子計算の検証を（情報理論的安全に）行うことができることが知られている [15, 16, 17]。

ブラインド量子計算や量子計算の検証は完全古典のクライアントでしかも古典通信のみでもできるだろうか？実は LWE を使うことにより可能であることが Mahadev により示された [18, 19]。このブレークスルーはある意味、本稿のテーマである耐量子ハイブリッド量子暗号プロトコルの研究の近年のブームのきっかけとなったものである。Mahadev の成果については後で説明する。

5.4 未解決問題

ここまで、量子の性質のみを使った情報理論的安全な量子暗号プロトコルについて説明してきた。耐量子ハイブリッドの話に入る前にここでいったん、著者が日頃考えている二つの未解決問題を紹介したい。

Open problem 1:量子の性質を使って実現できる情報理論的安全な暗号タスクには他にどんなものがあるだろうか？

量子の性質をつかった情報理論的安全な量子暗号プロトコルを作る研究はすでに 51 年の歴史があり、昔から多くのプロトコルが作られてきている。しかしながら、certified deletion のように、つい最近見つかったものもあり、実はまだまだいろいろなものが考えられるのかもしれない。

Open problem 2:これまで知られていない（あるいは使われていない）量子の性質を使って何か新しい暗号タスクが実現できるだろうか？

少なくとも著者の知る限り、全ての情報理論的安全な量子暗号プロトコルは no-cloning と不確定性原理に基づいている。何か他の量子の性質も使えないのだろうか？あるいは結局 no-cloning と不確定性原理しかないのだろうか？[8]

6 耐量子ハイブリッド（量子状態は正しく作られる場合）

さて、ここからは耐量子暗号も使う話になる。量子の性質のみ使っていてはできないタスクの一つに、public verification がある。

6.1 Publicly-verifiable 量子マネー

ウィズナーが提案した量子マネーは秘密の検証鍵を持った銀行しかマネーの正しさをチェックできない。誰でもその場で量子マネーの正しさをチェックすることは可能なのだろうか？

Aaronson と Christiano [20] は subspace 状態を用いた publicly-verifiable な量子マネーを提案した。subspace 状態というのは、ランダムに選んだ $n/2$ 次元 subspace $A \subset \mathbb{F}_2^n$ に対し、$|A\rangle \equiv \sum_{a\in A} |a\rangle$ として定義される状態である。$|A\rangle$ という状態になっているかどうかは A と A の直交補空間 $A^\perp$ の membership をコヒーレントに評価することにより確認できる。つまり、まず $|A\rangle$ に対し、A の membership をコヒーレントに評価すると $|A\rangle|0\rangle \to \sum_{a\in A} |a\rangle|1\rangle$ となるので、第二レジスターを測定すれば確率 1 で 1 を得る。次に、$|A\rangle$ に $H^{\otimes n}$ を

[8] これについては最近、著者らにより面白い結果が得られた [7]。この論文では、疑似ランダム量子状態というものを使うと、一方向性関数無しでもコミットメントや電子署名といった様々な暗号プリミティブを実現できる可能性が示された。量子を使わない場合は、これらの暗号プリミティブには一方向性関数が必要であることが知られているため、何らかの量子の性質が効いているはずであるが、それが何なのかはまだ解明されていない。

作用させると $|A^\perp\rangle$ になるので、$|A^\perp\rangle$ に $A^\perp$ の membership をコヒーレントに評価すると、同様にして確率 1 で 1 を得る。誰でも検証できるためには、$A, A^\perp$ の membership アルゴリズムを公開する必要があるが、そのアルゴリズムを使えば、一つの $|A\rangle$ から $|A\rangle$ のコピーを作ることができるかもしれない。Aaronson と Christiano は、$A, A^\perp$ の membership アルゴリズムがブラックボックス (oracle) として与えられる時、$|A\rangle$ から $|A\rangle^{\otimes 2}$ を作るには oracle に指数回 query しないといけないということを示した。

アルゴリズムをブラックボックスとして公開できるというのはあまり現実的ではない非常に強い仮定である。実際、一般には不可能であることが示されている [21]。Zhandry は、（耐量子）indistinguishability obfuscation というもう少しましな仮定に変えることに成功した [22]。耐量子の標準的な仮定（例えば LWE 等）で publicly-verifiable な量子マネーが構築できるかはまだ分かっておらず、現在も研究が続く未解決の問題である。

6.2 Tokenized signature

Ben-David と Sattath は、一つの $|A\rangle$ と $A, A^\perp$ の membership oracle が与えられたとき、$u \in A$ と $v \in A^\perp$ を同時に得るためには指数回の query が必要なことを示した [23]。これは $|A\rangle$ のコピーを作ることができないということよりも強い。なぜなら、一つの $|A\rangle$ から $u \in A$ と $v \in A^\perp$ を同時に得るのが不可能ならば、コピーを作ることも不可能であることはいえるが[9]、逆はいえるかどうか分からないからである。

これらの性質は、tokenized signature（一回しか使えないはんこ）というものに使える[10]。メッセージ 0 に署名をしたかったら $|A\rangle$ を測定し、$u \in A$ を署名として使い、メッセージ 1 に署名をしたかったら $|A^\perp\rangle$ を測定し、$v \in A^\perp$ を署名として使えばよい。$A, A^\perp$ の membership oracle を使えば誰でも署名の正しさがチェックできる。$u \in A$ なる u と $v \in A^\perp$ なる v を同時に出せないことより、メッセージ 0 に対する署名とメッセージ 1 に対する署名を同時に出すことはできない。Ben-David と Sattath たちは A と $A^\perp$ の membership を oracle として扱っていたが、最近 subspace 状態を修正した coset 状態[11]というものを考えることにより、membership oracle を（耐量子）indistinguishability obfuscation に置き換えることができることが示された [24]。

[9] もしコピーできたら、$|A\rangle$ を計算基底で測定して $u \in A$ を得、もう一つの $|A\rangle$ を Hadamard 基底で測定して $v \in A^\perp$ を得ればよい。

[10] 彼らの論文のアブストラクトは量子はんこを助けた魚からもらう漁夫の昔話仕立てになっている。また、arXiv のアブストラクトのページの Ancillary files の箇所にそのアニメ（！）がある。

[11] $|A_{s,s'}\rangle \equiv \sum_{a\in A}(-1)^{a\cdot s'}|a+s\rangle$ として定義される状態のこと。

7　耐量子ハイブリッド（量子状態は正しく作られるとは限らない場合）

7.1　古典通信で代用できるか？

これまでは、量子状態は正しく作られたと仮定していた。例えば、量子マネーの場合、状態 $|A\rangle$ は正しく銀行が作り、攻撃者はその状態を使って何かする、という設定であった。また、ブラインド量子計算や量子計算の検証の場合も、クライアントが正しい BB84 状態を作ってサーバに送るという設定であった。そして、そのようなプロトコルの安全性には、正しい状態が作られていることが効いている。

ところが、このような設定だと、量子状態を送る量子通信路が必要となる。例えば、量子マネーの場合、量子マネーを流通させるためには量子通信路が必要であるし、ブラインド量子計算や量子計算の検証の場合クライアントとサーバを量子通信路でつなぐ必要がある。量子状態の生成自体も攻撃者にやらせる場合を考えても、意味のある量子暗号タスクができるだろうか？例えば、銀行は完全古典で、量子計算機を持つ一般の人と古典通信のみをやり取りすることにより、一般の人のもとに偽造できない量子マネーを生成することは可能だろうか？あるいは、完全古典のクライアントが量子サーバと古典通信のみを用いて、ブラインド量子計算や量子計算の検証を行うことは可能だろうか？

一見するとこれは不可能なように見える。例えば、量子マネーの例でいうと、銀行からの情報は完全に古典の情報なので、攻撃者はその情報をコピーし放題である。コピーしたそれぞれの古典情報から量子状態を作れば、全く同じ量子マネーを何個も作れるように見える。また、ブラインド量子計算や量子計算の検証の場合も、サーバはクライアントから古典の情報しか貰わないので、それをもとに作った量子状態の情報を完全に得ることが出来そうであり、クライアントはサーバに対して何のアドバンテージもないように見える。

面白いことに、最近、耐量子の（計算量的）古典暗号を使うと、古典通信のみで攻撃者自身に量子状態を作らせる場合であっても、量子マネーやブラインド量子計算、量子計算の検証など、さまざまな量子暗号タスクが可能であることが分かってきている。

7.2　シンプルな例

耐量子の古典暗号を使うことにより、（計算量的に）コピーできない量子状態を古典通信のみで相手方に作ることができる。次のような最もシンプルな例を考えよう。

アリスは claw-free 関数 f をボブに送る。claw-free 関数というのは、$f(x_0) = f(x_1) = y$ なるペア（claw）、(x_0, x_1)、を見つけるのが難しいような関数であ

る。ボブは $\sum_x |x\rangle|f(x)\rangle$ という状態を作り 2 番目のレジスターを測定する。測定結果が y だとすると、測定後の状態は $(|x_0\rangle + |x_1\rangle) \otimes |y\rangle$ になる。ただし x_0, x_1 は $f(x_0) = f(x_1) = y$ を満たすビット列。この状態 $|x_0\rangle + |x_1\rangle$ のコピーを（多項式時間で）作ることは不可能である。なぜならもしできたら claw が得られてしまう[12]。

7.3 Noisy trapdoor claw-free functions

LWE から、Noisy trapdoor claw-free function (NTCF) f という特殊な 2-to-1 関数を作ることができる [25]。これは、claw-free つまり、$f(x_0) = f(x_1)$ なる x_0, x_1 を求めるのは難しい、という性質をもつ。さらに、trapdoor という特殊な秘密の鍵を持っている場合は、claw (x_0, x_1) が簡単に求まる、という性質も持つ。そして、f はさらに、adaptive hardcore bit property という非常に面白い性質を持つ。これは、次のような性質である。まず、$\sum_x |x\rangle|0..0\rangle$ を作り、$f(x)$ をコヒーレントに計算する。つまり、$\sum_x |x\rangle|f(x)\rangle$ を作る。そして、第二レジスターを測定して、y という結果を得たとしよう。すると測定後の状態は $(|x_0\rangle + |x_1\rangle) \otimes |y\rangle$ となる。ここで、(x_0, x_1) は $f(x_0) = f(x_1) = y$ を満たすものである。この第一レジスターを計算基底で測定すると当然、x_0 か x_1 をそれぞれ確率 1/2 で得る。一方で、Hadamard 基底で測定すると簡単に確かめられるように、$d \cdot (x_0 \oplus x_1) = 0$ なる d を得る。adaptive hardcore bit property というのは、x_0 か x_1 のどちらか一方と、d を同時に得ることは不可能、という性質である。

7.4 Proof of quantumness

NTCF の応用例として、proof of quantumness[25] というものがある。ボブは古典ではない、つまり量子的な操作ができると主張しており、アリスはそれを確かめたい。ただし、アリスは完全に古典の操作しかできず、アリスとボブの間の通信も古典通信のみである。アリスはボブが量子的な能力を持つことを確認できるだろうか？次のようにすればよい。

1. アリスは NTCF 関数 f を一つ選んでボブに送る。
2. ボブは $\sum_x |x\rangle|f(x)\rangle$ を作り第二レジスターを測定する。測定結果を y とする。ボブはアリスに測定結果 y を送る。測定後の状態は $(|x_0\rangle + |x_1\rangle)|y\rangle$ となる。ここで $f(x_0) = f(x_1) = y$ である。
3. アリスはランダムにビット $c \in \{0, 1\}$ を選びボブに送る。

[12] 一つ目の $|x_0\rangle + |x_1\rangle$ を計算基底で測定すると 1/2 の確率で x_0 か x_1 が出る。もう一つの $|x_0\rangle + |x_1\rangle$ も計算基底で測定すると 1/2 の確率で x_0 か x_1 が出るので、確率 1/2 で (x_0, x_1) が得られる。

4. もし $c=0$ なら、ボブは第一レジスターを計算基底で測定する。x_0 か x_1 を確率 1/2 で得る。x_b を得たとしよう。ただし $b \in \{0,1\}$。ボブは x_b をアリスに送る。

5. もし $c=1$ なら、ボブは第一レジスターを Hadamard 基底で測定する。$d \cdot (x_0 \oplus x_1) = 0$ なる d を得る。ボブは d をアリスに送る。

6. アリスはボブから正しいものが届いているかチェックする。つまり、$c=0$ の時は、$f(x_b)=y$ になっているかチェックし、$c=1$ の時は $d \cdot (x_0 \oplus x_1) = 0$ になっているかチェックする。もし届いていたらボブは確かに量子であると結論づける。もしそうでないならボブは古典であると結論づける。

もしボブが本当に量子であるなら、上記の操作を行うことにより、ボブは、アリスに確率 1 で認めさせることができる。一方で、ボブは本当は古典なのに、量子であると偽っているとしよう。そして、それにも関わらず、ボブは高い確率でどちらの c に対しても正しい返事ができると仮定しよう。すると、f の adaptive hardcore bit property が破れることが示せる。したがって、LWE が量子では難しいことを仮定するならば、古典のボブはアリスを騙すことは不可能であることが分かる。

古典のボブが高い確率でどちらの c に対しても正しい返事ができるならば f の adaptive hardcore bit property が破れることは rewinding というテクニックにより示せる。ボブは古典アルゴリズムなので、逆戻しが可能である。（アルゴリズムを動作させるための入力と乱数を固定することで、ステップ 2 までの状況を再現（巻き戻すことが）できる。）そこで、まずボブを c をもらう直前までシミュレートする。そして $c=0$ をボブに入れると、ボブは $f(x_b)=y$ を満たす x_b を高い確率で吐き出す。その後、ボブを逆戻しして、$c=0$ をもらう直前まで巻き戻す。そして今度はボブに $c=1$ を入れると、ボブは高い確率で正しい d を出す。そうすると、x_b と d を同時に得ることができてしまっているので f の adaptive hardcore bit property に反する。

7.5 Semi-quantum money

NTCF の他の応用に、semi-quantum money[26] がある。これは、銀行は古典で利用者は量子という設定の量子マネーである。上記の proof of quantumness において、アリスが銀行、ボブが利用者という設定である。量子マネーは $\bigotimes_{j=1}^{n}(|x_0^j\rangle + |x_1^j\rangle)$ である。ただし、$f(x_0^j) = f(x_1^j) = y_j$。ボブが正しい量子マネーを持っていることを検証するには、ボブにランダムに選んだビット列 $c=(c_1,c_2,...,c_n) \in \{0,1\}^n$ を送る。ボブは $c_j=0$ なら x_b^j を、$c_j=1$ なら d_j を返さなければならない。これが量子マネーとして使える理由は、検証に 2 回通ることができないからである。（同じお金で 2 重に支払いができてしまうと大変である！）一度検証が終わって、もう一度検証をするときは前と

は異なるランダムビット列 $c' = (c'_1, ..., c'_n)$ が送られてくるが、高い確率で、$c_j \neq c'_j$ なる j が存在し、その j については adaptive hardcore bit property より、もはや正しい結果を返すことができない。

7.6 量子計算の古典検証

Mahadev は NTCF をさらに拡張し、LWE 仮定のもとで f と計算量的に区別がつかない関数 g を導入し、それを用いて量子計算の古典検証を実現した [18]。詳細は非常に複雑であるのでここでは説明できないが、直観的には、post hoc 検証プロトコル [17] をベースにしている。この post hoc 検証プロトコルにおいては、証明者（サーバ）は検証者（クライアント）に history state と呼ばれるある種の量子状態を送る。検証者はランダムに選んだ量子ビットを計算基底もしくは Hadamard 基底で測定するだけで任意の量子計算の検証が可能である。Mahadev の検証プロトコルにおいては、証明者に history state を測定させる。邪悪な証明者はもちろん正しい測定を行うとは限らないが、f と g をうまく使うことにより、あるテストにパスしたら、証明者はなんらかの状態を計算基底か Hadamard 基底で測定していることが保証されるため、もともとの post hoc 検証プロトコルの安全性から、こちらの安全性もいえる。

7.7 Classical channel certified deletion

関数 f と g を使うテクニックは、古典通信のみによる certified deletion にも利用できる [14]。Broadbent-Islam の certified deletion では、BB84 状態を準備して送る必要があったが、その代わりに、BB84 状態の計算基底の状態を g に、Hadamard 基底の状態を f に対応させることにより、certified deletion を実現する。

7.8 One-shot signature

Tokenized signature は、状態 $|A\rangle$ がちゃんと作られているという設定であった。論文 [27] において、状態が必ずしも正しく作られるとは限らない設定での「一回しか使えない量子はんこ」が提案された。f をある関数とし、oracle として公開されているとしよう。署名したい人は、$\sum_x |x\rangle|f(x)\rangle$ を作り、第二レジスターを測定する。測定結果 y は署名を検証する公開鍵である。測定後の状態は $\sum_{x:f(x)=y} |x\rangle$ になる。メッセージ 0 を署名したい場合は、Grover のアルゴリズムを使い $\sum_{x:f(x)=y} |x\rangle$ を $\sum_{x:f(x)=y,x|_1=0} |x\rangle$ にする。ここで、$x|_1$ は x の 1 番目のビットである。この状態を測定すると、$f(x) = y$ かつ $x|_1 = 0$ なる x を得るが、それをメッセージ 0 の署名とする。これが valid な署名であることは公開されている情報のみから誰でもチェックできる（$f(x) = y$ かつ

$x|_1 = 0$ であることを確かめればよい)。メッセージ 1 を署名したい場合は、同様にして、Grover のアルゴリズムを使い $\sum_{x:f(x)=y} |x\rangle$ を $\sum_{x:f(x)=y,x|_1=1} |x\rangle$ にして、測定結果を署名とすればよい。これが one-shot signature である直観的な理由は、一度 $\sum_{x:f(x)=y,x|_1=0} |x\rangle$ を測定して測定結果を得てしまうと、状態が壊れてしまい、もはや $\sum_{x:f(x)=y,x|_1=1} |x\rangle$ が作れないからである。関数 f は oracle として与えられているが、これを indistinguishability obfuscation あるいは耐量子の標準的な仮定に置き換えることができるかどうかは未解決の問題である。

7.9 Quantum fully homomorphic encryption

古典通信のみで、任意の量子計算をサーバに秘密に委託できるだろうか？Mahadev は LWE を使うとそれが可能であることを示した [19]。アイデア自体は非常にシンプルである。ユニバーサル量子計算はクリフォードと、非クリフォードゲート何か一つ（例えばトフォリ）で可能である。量子状態はランダムなパウリ X, Z を作用させることにより情報理論的に暗号化できる（量子 one-time pad)。クライアントは入力 $|\psi\rangle$ を暗号化したもの $X^x Z^z |\psi\rangle$ をサーバーに送る。また、量子 one-time pad の鍵を古典の homomorphic encryption で暗号化したもの $ct_{x,z}$ も一緒に送る。サーバーは量子 one-time pad で暗号化された状態に量子ゲートを作用させていく。クリフォードゲートの場合は、単にパウリの X, Z が変化するだけなのでその変化を $ct_{x,z}$ に対し homomorphic に計算すればよい。トフォリゲートの場合は、パウリとは単純には交換せず、場合により $CNOT$ が出てくるためそれをキャンセルする必要がある。Mahadev は、LWE を用いて、$X^x Z^z |\psi\rangle$ と $ct_{x,z}$ と ct_s から、$X^{x'} Z^{z'} CNOT^s |\psi\rangle$ と $ct_{x',z'}$ を作る方法を提案した。これにより、ユニバーサル量子計算が homomorphic に可能になる。

8 他の量子暗号プリミティブ

今回はスペースの都合上触れられなかったが、今回紹介した以外にも様々な面白い量子暗号プリミティブがある。例えば quantum copy protection[24, 31, 32]、unclonable encryption[34]、unclonable decryption key[30]、quantum lightning[22]、quantum garbled circuit[33]、QFHE を使って古典通信のみでコピーできない状態を作る方法 [35] などである。興味のある方は論文を見ていただきたい。

9 Minicrypt と cryptomania

Impagliazzo の 5 つの世界というものがある。これは、有名な未解決問題 P = NP? に関連するものであり、我々の世界は 5 つの異なるありえる世界のうちどれなのか分からないというものである。例えば、P = NP が成り立つ世界（algorithmica）や、P ≠ NP だけど NP 問題は平均的には簡単な世界（heuristica）、NP 問題は平均的にも難しいけど一方向性関数は存在しない世界（pessiland）などがある。あとの二つは minicrypt と cryptomania というものであり、前者は一方向性関数が存在する世界であり、後者はさらに公開鍵暗号といったようなもっと強いものが存在する世界である。計算量的暗号が可能である世界がこのように 2 つの世界に分けられている理由は、多くの暗号プリミティブが一方向性関数と等価であることが知られている一方で、いくつかのプリミティブは一方向性関数からは作れなさそうだということを示唆する結果が得られているからである。例えば、疑似乱数生成器、コミットメント、署名などは一方向性関数と等価であることが分かっている。（一方向性関数から署名を作る方法は最初の方で説明した。）コミットメントというのは将棋の封じ手のようなものである。つまり、A さんはコミットした内容を後で変更できないし、B さんはコミットされた中身を見ることはできない、というものである。このように、一方向性関数と等価になるものたちが住む世界が minicrypt である。

一方で、公開鍵暗号、鍵交換、oblivious transfer、multi-party computation などは一方向性関数からは作ることができないだろうということを示唆する結果が得られており、一方向性関数よりももっと強い仮定が必要だろうと信じられている。このようなものたちが住む世界が cryptmania である。

古典の暗号の世界はこのような分類になっているのだが、量子が入ってくると（つまり量子状態を送受信できたり量子計算ができたりすると）だいぶ様子が違ってくる。最初のほうでも述べたように、まず鍵配送は計算量的仮定なしで可能となる。また、oblivious transfer や multi-party computation は（耐量子）一方向性関数のみから構成できることが知られている [5, 6]。

最近、[7, 8] において、コミットメントや署名も一方向性関数無しで作れる可能性を示唆する結果が得られた[13]。（[5, 6] と組み合わせると、multi-party computation も一方向性関数無しでも構成可能であることまで言える。）疑似ランダム量子状態という概念が [28] において提案されており、[29] において疑似ランダム量子状態は一方向性関数が無くても存在しうるという結果が得られた[14]。[7, 8] では、疑似ランダム量子状態からコミットメントや署名を構成できることが示された。したがって、コミットメントや署名も一方向性関数なしでも構成可能であることが示唆される。古典の世界では一方向性関数

[13]ただし署名は使い捨て署名である。

[14]正確には、BQP=QMA だけど疑似ランダム量子状態は存在するような量子オラクルが示された。BQP=QMA なら BQP が NP を含むので全ての（耐量子）古典暗号は量子計算機で破られることになる。

が最もエッセンシャルであることは良く知られているが、量子の世界では全くちがうことが起こっているというのはとても面白い。

この話は暗号だけでなく計算量理論の視点からも面白い示唆を与える。疑似ランダム量子状態やそれに基づく量子暗号プリミティブが、全ての耐量子古典暗号が破られても生き残る理由は、攻撃者が量子状態を受け取るためである。従来の計算量理論はたとえ量子のクラス（BQP や QMA など）であっても、入力は古典のビット列であった。そのため、そのような古典の計算量クラスで崩壊が起こっても、量子状態を入力とする問題には必ずしも影響があるわけでは無いのである。量子状態を入力としたり、量子状態や量子演算を実現する、という問題に対する計算量理論は、最近数本の面白い論文 [36, 37] がでているがまだほとんど全く研究がなされておらず、今後の展開が待たれる。

10 謝辞

量子暗号の研究に関して共同研究を行っていただいている NTT の西巻陵氏と山川高志氏、私の学生の廣岡大河氏に感謝いたします。特に、山川氏には暗号理論について多くのことを教えていただき大変勉強になりました。

参考文献

[1] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information.

[2] 森前智行、量子計算理論、森北出版

[3] M. Zhandry, How to record quantum queries, and applications to quantum indifferentiability. CRYPTO 2019.

[4] T. Yamakawa and M. Zhandry, Classical vs Quantum Random Oracles. EUROCRYPT 2021.

[5] A. B. Grilo, H. Lin, F. Song, and V. Vaikuntanathan, Oblivious Transfer is in MiniQCrypt. EUROCRYPT 2021.

[6] J. Bartusek, A. Coladangelo, D. Khurana, and F. Ma, One-Way Functions Imply Secure Computation in a Quantum World. CRYPTO 2021.

[7] T. Morimae and T. Yamakawa, Quantum commitments and signatures without one-way functions, arXiv:2112.06369

[8] P. Ananth, L. Qian, and H. Yuen, Cryptography from pseudorandom quantum states, arXiv:2112.10020

[9] D. Unruh, Revocable quantum time-released encryption. Journal of the ACM 62, 1-76 (2015).

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

[11] A. Lutomirski, An online attack against Wiesner's quantum money. arXiv:1010.0256

[12] S. Aaronson. Quantum copy-protection and quantum money. Proceedings of IEEE Conference on Computational Complexity, pages 229-242, 2009.

[13] A. Broadbent and R. Islam, Quantum encryption with certified deletion. TCC 2020.

[14] T. Hiroka, T. Morimae, R. Nishimaki, and T. Yamakawa, Quantum Encryption with Certified Deletion, Revisited: Public Key, Attribute-Based, and Classical Communication. Asiacrypt 2021.

[15] A. Broadbent, J. F. Fitzsimons, and E. Kashefi, Universal blind quantum computation. FOCS 2009.

[16] M. Hayashi and T. Morimae, Verifiable measurement-only blind quantum computing with stabilizer testing, Phys. Rev. Lett. 115, 220502 (2015).

[17] J. F. Fitzsimons, M. Hadjusek, and T. Morimae, Post hoc verification of quantum computation. Phys. Rev. Lett. 120, 040501 (2018).

[18] U. Mahadev, Classical verification of quantum computations. FOCS 2018.

[19] U. Mahadev, Classical homomorphic encryption for quantum circuits. FOCS 2018.

[20] S. Aaronson and P. Christiano, Quantum money from hidden subspaces. STOC 2012.

[21] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. Journal of the ACM, 59(2):6, 2012.

[22] M. Zhandry, Quantum Lightning Never Strikes the Same State Twice. Advances in Cryptology - EUROCRYPT 2019.

[23] S. Ben-David and O. Sattath, Quantum tokens for digital signatures. arXiv:1609.09047

[24] A. Coladangelo, J. Lui, Q. Liu, and M. Zhandry, Hidden cosets and applications to unclonable cryptography. CRYPTO 2021.

[25] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick, A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device. FOCS 2018.

[26] R. Radian and O. Sattath, AFT'19: Proceedings of the 1st ACM Conference on Advances in Financial Technologies 2019 Pages 132-146. arXiv:1908.08889

[27] R. Amos, M. Georgiou, A. Kiayias, and M. Zhandry, One-shot signatures and applications to hybrid quantum/classical authentication. STOC 2020.

[28] Z. Ji, Y.-K. Liu, and F. Song, Pseudorandom quantum states. CRYPTO 2018.

[29] W. Kretschmer, Quantum pseudorandomness and classical complexity. The 16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021).

[30] M. Georgiou and M. Zhandry, Unclonable Decryption Keys. IACR eprint:2020/877

[31] S. Aaronson, J. Liu, Q. Liu, M. Zhandry, and R. Zhang, New approaches for quantum copy-protection. CRYPTO 2021.

[32] A. Coladangelo, C. Majenz, and A. Poremba, Quantum copy-protection of compute-and-compare programs in the quantum random oracle model. arXiv:2009.13865

[33] Z. Brakerski and H. Yuen, Quantum Garbled Circuits, arXiv:2006.01085

[34] A. Broadbent and S. Lord, Uncloneable Quantum Encryption via Oracles, arXiv:1903.00130

[35] O. Shmueli, Public-Key Quantum Money with a Classical Bank, IACR eprint:2021/1427

[36] G. Rosenthal and H. Yuen, Interactive Proofs for Synthesizing Quantum States and Unitaries, arXiv:2108.07192

[37] S. Irani, A. Natarajan, C. Nirkhe, S. Rao, and H. Yuen, Quantum search-to-decision reductions and the state synthesis problem, arXiv:2111.02999