古典通信による量子インターネット

2020 年 3 月 29 日

アリスが、次のような量子デバイスを持っているとします。このデバイスには二つのボタンがあり、一つのボタンには X、もう一つのボタンには Z と書かれています。ボタン Z を押すと、$|0\rangle$ か $|1\rangle$ のどちらかが確率 $1/2$ でデバイスから吐き出されます。一方で、ボタン X を押すと、$|+\rangle = |0\rangle + |1\rangle$ か $|-\rangle = |0\rangle - |1\rangle$ のどちらかが確率 $1/2$ でデバイスから吐き出されます。吐き出された量子状態は遠くにいるボブのもとに送られます。このデバイスは、また、4 つの状態 $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ （BB84 状態といいます）のうちどの状態を出したかという古典情報を（古典のインクで）記した（古典の）紙も吐き出します。この紙はアリスが外部に漏れないように大事にとっておきます。

ボブのもとには 4 つの状態 $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ のどれかが届くわけですが、量子力学の原理によると、ボブはどの状態が届いたのか完璧に知ることはできないし、届いた状態と全く同じコピーを作ることもできません。このような量子的性質をうまく使うことにより、量子鍵配送（QKD) や、量子マネー、量子計算の検証 [1, 2, 3]、ブラインド量子計算 [4] といった様々な量子暗号タスクが可能になります。

つまり、アリスが自分で BB84 状態をつくり、それをボブに送ることができれば、いろいろな量子暗号タスクが可能となるのです。

最近、「耐量子暗号を使うことにより、アリスを古典にして、かつ量子通信路を古典通信路に置き換えても同じことができる」ということを示す研究がいろいろなされています。[1]つまり、古典計算機しかもっていないアリスが、量子計算機を持っているボブと古典メッセージをやり取りすることにより、ボブに BB84 状態を作らせることができ、しかも、あたかもアリスが自分で作ってボブに送ったかのような状況にできるのです。（つまり例えばボブは自分でどういう状態を作ったのか分からないし、作った状態のコピーもできないような状況。）

これは一見すると非常に不思議です。なぜならば、アリスがボブと古典通信しかしないとすると、ボブは自分の作った状態について完全な古典情報を持っているはずです。ですからボブは同じ状態のコピーも何個も作れるでしょう。

[1] これはわかりやすさのためにあえて大雑把にいいました。実際は厳密に同じものではありません。

ポイントとなるのは、耐量子暗号を使うことによりボブにある制限を課すことができるという点です。これを理解するために、最もシンプルな次の例を考えてみましょう。ある関数 $f : \{0,1\}^n \to \{0,1\}^m$ があり、2-to-1 で、さらに claw-free という性質を持つとします。Claw-free とはどういうものかというと、$f(x_0) = f(x_1)$ なるペア (x_0, x_1) を見つけるのは量子計算機でも効率的にはできない、というものです。アリスはまずボブに f を送ります。ボブは

$$|\psi\rangle \equiv \sum_x |x\rangle \otimes |f(x)\rangle$$

という状態を作ります。そして第二レジスターを測定して測定結果 $y \in \{0,1\}^m$ を得ると、測定後の状態は

$$|\psi_y\rangle \equiv (|x_0\rangle + |x_1\rangle) \otimes |y\rangle$$

となります。ただし $x_0, x_1 \in \{0,1\}^n$ は y の preimage、つまり $f(x_0) = f(x_1) = y$ なる (x_0, x_1)。

ボブは状態 $|\psi_y\rangle$ のコピーを（量子計算機で効率的な時間で）作ることはできません。なぜならば、もし $|\psi_y\rangle^{\otimes k}$ が作れたとすると、それらを測定すれば、(x_0, x_1) の両方を知ることができますがそれは f の claw-free という性質に反します。（もし一つの $|\psi_y\rangle$ しかないときは、測定したら x_0 か x_1 のどちらかしか出なくて、測定で状態は $|x_0\rangle$ か $|x_1\rangle$ のどちらかに収縮するので、ボブは x_0 と x_1 の両方を知ることはできない。）つまり、完全に古典通信だけでボブにコピーできない量子状態を作らせることができました。

これは最もシンプルな例ですが、もっと複雑なプロトコルを考えると、古典アリスが古典通信だけで、あたかもボブに BB84 状態をアリスが送ったかのようにすることができたり、それを使って量子計算の検証やブラインド量子計算をすることが可能です。詳しい内容に興味のある人は論文 [5, 6, 7, 8, 9] を参照してください。

アリスが自分で BB84 状態を作ってボブに送ることにより量子暗号タスクをやる場合のメリットは、情報理論的安全性が達成できることです。つまり、攻撃者が無限の計算能力を持っていても安全、ということです。また、ボブはフルの量子計算機を持っていなくても、簡単な量子的操作だけでよい場合が多いです。例えば QKD だとボブは量子ビットを測定するだけです。デメリットは量子状態を遠くまで送る必要があるのと、アリスも量子デバイスを必要とする点です。

一方で、耐量子暗号を使ってやる場合のメリットはアリスが完全に古典になり、また量子通信路が必要なく、今ある古典通信路がそのまま使える点です。デメリットは安全性が計算量的になることです。つまり、もし攻撃者の計算能力が超強力だったり、安全だと思っていた耐量子暗号が破れてしまったりするともうダメです。さらに、単に BB84 状態をつくるためだけに、ボ

ブは $|\psi\rangle$ を作るといった複雑な量子計算をしないといけなくなるので、ボブの負担が大きなものになります。

現在、より巨大な量子計算機を実現しようと皆が頑張っていますが、大きな量子計算機の応用先の一つとして、「量子通信路を古典通信路に置き換えることができる」というのがあるというのは面白いですね。

参考文献

[1] J. F. Fitzsimons, M. Hajdušek, and T. Morimae, Phys. Rev. Lett. **120**, 040501 (2018).

[2] T. Morimae, arXiv:2003.10712

[3] J. F. Fitzsimons and E. Kashefi, Phys. Rev. A **96**, 012303 (2017).

[4] A. Broadbent, J. F. Fitzsimons, and E. Kashefi, FOCS 2009; arXiv:0807.4154

[5] U. Mahadev, FOCS 2018; arXiv:1804.01082

[6] A. Gheorghiu and T. Vidick, FOCS 2019; arXiv:1904.06320

[7] T. Vidick, Bull. Amer. Math. Soc. **57**, 39-76 (2020).

[8] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick, FOCS 2018; arXiv:1804.00640

[9] T. Metger and T. Vidick, arXiv:2001.09161