量子コンピューターを使って新元号を知らずに済ます方法

新元号を知りたくない理論物理学者がいるとします。（仮に T さんとしましょう。）彼は大学事務にとある書類を提出しないといけませんが、その書類には新元号を記入する欄があります。さて、彼はこの難局をどうやって乗り越えたらよいのでしょうか？実は量子コンピューターを使えばこの問題を解決することができます[1]。

今、新元号を x とし、書類に新元号を記入するという作業は f(x)を計算するということであらわします。（f は高々量子計算機で多項式時間で計算できる関数。）T さんは協力してくれる学生の A さんに頼んで、P|x>を作って送ってもらいます。ここで、|x>は x をエンコードした量子状態、P はランダムなパウリ演算子とする。計算基底にランダムパウリ(実質 X のみ)をかけるだけなので、A さんの負担はそんなにありません。ランダムパウリにより one-time pad 化されているため、T さんは P|x>から x の情報を得ることはできません。次に、T さんは P|x>をグラフ状態に CZ ゲートを使ってつなげます。CZ はパウリと交換するので、|x>がグラフ状態とくっついたものにパウリが乗った状態が生成されます。ＣＺでグラフ状態とくっつける操作で情報が漏れることはありません。（one-time pad は任意のＣＰＴＰに対し安全。）T さんは 1 量子ビットづつ A さんに送り、A さんはそれを測定していきます。最終的に、T さんのもとには P'U|x>＝P'|f(x)>という状態が生成されます。（P'はあるパウリ演算子、U は f を計算するユニタリ。）この状態も one-time pad 化されているので、T さんは情報を得ることはできません。T さんはこの状態を事務に提出します。事務は A さんから P'を教えてもらえば、|f(x)>を複合することができます。（A さんは P から P'を求める必要がありますが、これは Parity-L の能力で可能。）このようにして、T さんは無事、新元号を知ることなく書類を事務に提出することができました。ちなみに、T さんが正しいグラフ状態を作らない可能性がありますが、A さんは状態のスタビライザーをランダムにチェックすることにより、T さんの量子計算の正しさを検証することもできます[2,3]。ノイズで量子計算にエラーが起こるかも、と心配するかもしれませんが、誤り訂正が使えます。A さんが送る状態は古典状態なので簡単に誤り訂正符号でエンコードできますし、あるいは、 f の回路に x 自体も hard-wired してしまえば、A さんは何も送る必要がありません。さらに、ＸＺ測定でユニバーサルなリソース状態[4]を使うことにより、ＣＳＳコードで簡単にファールトトレラントにできます。T さんは量子コンピューターを買う必要がありますが、それはしかたないでしょう。A さんは量子ビットを測定するデバイスが必要となります。学生にそんな負担を強いるのはよろしくないと考えるならば、安全性は計算量的になりますが、[5]を使うことにより、完全古典の A さんでも同じ目的を達成することができます。

[1] TM and Fujii, PRA(R)87, 050301 (2013)

[2] Hayashi and TM, PRL 115, 220502 (2015)
[3] TM, Nagaj, and Schuch, PRA93, 022326 (2016)
[4] Takeuchi, TM, and Hayashi, arXiv:1809.07552
[5] Mahadev, arXiv:1708.02130