さて今回、量子スプレマシーが起きる前に量子オモラシ―が起きてしまったわけですが、このようなことを起こさないためにはジョンマルチネスはどうすべきだったのか、ここで検証してみましょう。

まず、ジョンマルチネスは密閉された自宅にこもり、自宅からグーグルラボにある５３量子ビットマシンにリモートアクセスしてブラインド量子計算[Broadbent et al. FOCS 2009]を行うべきでした。ブラインド量子計算プロトコルを使えば、計算内容を誰にも知られることなく量子計算が実現できます（情報理論的安全性）。ただ、ブラインド量子計算の場合必要なキュービット数は数百、数千に増えてしまいますので、５３量子ビットなんてけちなことをいわずに数百、数千量子ビットをどーんと使いましょう。さらに、グーグルラボからジョンマルチネスの密閉された自宅まで量子ビットを送る際のデコヒーレンスに対処するために、量子誤り訂正符号が必要となります。量子誤り訂正はたしか、スプレマシーの次の NISQ のさらにその次だったはずですがその辺も細かいことは気にせず、量子誤り訂正符号をばんばん使っていきましょう。密閉された自宅の中で、飛んでくる数千の量子ビットをひとつづつちまちま一人で測定しているジョンマルチネスの姿を思い浮かべるとちょっとじわじわくるものがあります。

今回の論文ではスパコンによる古典シミュレーションも目玉の一つです。それには HE を使いましょう。待遇に不満を持つポスドクが、ラボにある５３量子ビットマシンを使って攻撃してくるかもしれないので量子耐性のあるものが望ましいです。

最後に、ジョンマルチネスは密閉された自宅ですべての結果を一人で decrypt し、一人で論文を執筆します。論文ができたら Nature に投稿しましょう。査読者がオモラシ―するかもしれないので、査読者に内容を知られてはいけません。ここで zero-knowledge[Goldwasser et al. SIAM J. Comput. 1989]が使えるはずです。ある量子回路（の古典的記述）が与えられたときそれがスプレマシーを示す（つまり YES インスタンス）ならば、ある多項式長の論文（witness）が存在して、古典多項式時間査読者は確率 1 で論文を受理（accept）します。一方、もしスプレマシーを示さない（つまり NO インスタンス）ならば、どんな多項式長論文をもってきても古典多項式時間査読者は論文を受理しません（reject）。つまり、量子回路がスプレマシーを示すか否かという判定問題は in NP です。（注：査読者はある確率で判断を間違えるので、より正確には in MA）。NP は zero-knowledge を持つので、ジョンマルチネスは論文の内容を査読者に知られることなく論文を受理させることが可能です。査読者が量子計算機を使ってアタックしてくる可能性もありますが、量子アタックに対する Zero-knowledge は Watrous により証明されています[Watrous, SIAM J. Comput. 2009]。量子スプレマシーの検証には、量子論文と量子査読者が必要かもしれませんが、その場合は、QMA が zero-knowledge を持つことを使えば OK です[Broadbent et al. FOCS 2016]。