報道関係者各位

令和6年2月5日

コンピューター部門

最近は量子コンピューターの普及を鑑みて今現在の公開暗号が破られてしまう恐れがあることから対策を練りサーバーの運営管理に活かしているのですが、それには秘訣があります。

量子コンピューターの性質上、今迄安全だった公開鍵暗号方式がショアのアルゴリズムにより破られてしまう可能性があるので早期に対応が必要である。

公開鍵暗号方式は素数を基にした計算式からなるので数学の論理上、大きな素数を求めるのには天文学的な時間が今の計算機では掛かる。それが、１９９４年にMITの数学教授であるピーターショアが大きな数の素因数を生成する為の量子アルゴリズムを考案し、量子コンピューターを使う事で現在の公開鍵基盤が脅威に晒されてしまうことを防ぐのを狙いとしたものである。

この知恵を活かせばコストを対してかけずにショアのアルゴリズムでの公開鍵基盤が破られても通常どうりサーバの運営管理が行えるはずである。

組織概要

KUMO
所在地 奈良県天理市嘉幡町372
会長 橋本 健二
TEL 0743-64-3170
URL [https://kumo.site](https://kumo.site/)

問い合わせ先
担当 玉和道
TEL 070-3771-8527
E-mail code\_xyz-kumo@yahoo.co.jp