On Bin Kübit İnternet Güvenliğini Ortadan Kaldırabilir

Mahir E. Ocak

Son bilimsel çalışmalar, kuantum bilgisayarların internet güvenliğini ortadan kaldırmasının geçmişte tahmin edilenden çok daha az sayıda kübitle mümkün olabileceğini gösteriyor.

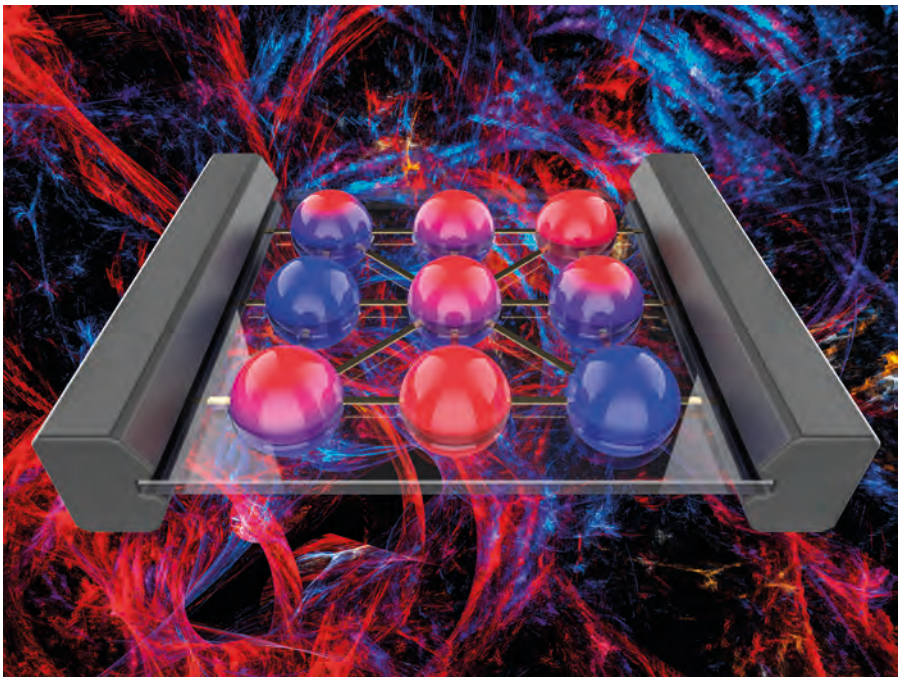
Güçlü kuantum bilgisayarların klasik bilgisayarlardan çok daha kısa süre içinde çözebileceği matematik problemlerinin bazılarından günümüzde internet güvenliğini sağlamak için yararlanıyor. Geçmişte kuantum bilgisayarların internet güvenliğini tehdit etmeye başlamasının ancak milyonlarca kuantum bit (kübit) içeren sistemlerin geliştirilmesiyle mümkün olabileceği düşünülüyordu. Ancak son araştırmalar özellikle kuantum hata düzeltme konusunda yaşanan gelişmeler sebebiyle bu sayının on binlere kadar düşebileceğini gösteriyor.

Bir grup araştırmacının yaptığı hesaplara göre 9.988 kübit içeren bir sistem, eliptik eğri kriptografisiyle şifrelenmiş metinleri yaklaşık 1.000 günde çözebilir. Kübitlerin sayısı 26.000'e çıktığındaysa bu süre bir güne kadar düşüyor. Söz konusu RSA-2048 algoritması olduğundaysa bir başka araştırma, bilgileri 10 günde deşifre etmek için gereken kübitlerin sayısının yaklaşık 100.000 olduğunu gösteriyor. Google Quantum AI araştırmacılarının yaptığı çalışmalar ise 500.000 fiziksel kübite sahip bir kuantum bilgisayarın birkaç dakika içinde kripto paraların güvenliğini tehdit edebileceğini gösteriyor.

Son çalışmalardaki daha düşük tahminler, kuantum hata düzeltmesi konusunda yaşanan gelişmelerden kaynaklanıyor. Kuantum bilgisayarları meydana getiren kübitler hataya açıktır. İşlemleri hatalardan arındırmak için, genellikle, çok sayıda hataya açık "fiziksel kübit" bir araya getirilerek hatasız işlem yapabilen "mantık kübitleri" oluşturulur. Bir kuantum bilgisayarın ne kadar az sayıda kübitle ne kadar çok işlem yapabileceği, bir mantık kübiti elde etmek için gereken fiziksel kübitlerin sayısına bağlı olarak değişir.

Geçmişte tahmin edilenden çok daha az sayıda kübit ile internet güvenliğinin ortadan kaldırılabileceğini gösteren son çalışmalar doğal olarak internet güvenliğini sağlayan algoritmaların güncellenmesine olan ihtiyacın zannedilenden daha acil olduğuna da işaret ediyor. ■

https://arxiv.org/abs/2603.28627v1
https://arxiv.org/abs/2602.11457
https://quantumai.google/static/site-assets/downloads/cryptocurrency-whitepaper.pdf



Laguna Design / SPL