

Kwantowa apokalipsa nadchodzi i może być nieunikniona

28 stycznia 2022

Eksperci ostrzegają, że komputery kwantowe mogą przewyższyć konwencjonalne metody szyfrowania. Byłaby to zła wiadomość dla ludzkości, ponieważ stanęlibyśmy przed groźbą zdarzenia, które naukowcy nazywają „apokalipsą kwantową”.

Głównym zagrożeniem dla ludzkości nie są anonimowi hakerzy, a światowe mocarstwa. Kraje takie jak USA, Chiny, Rosja i Wielka Brytania, inwestują ogromne sumy pieniędzy w rozwój superszybkich komputerów kwantowych w celu uzyskania strategicznej przewagi w cybersferze.

Tak duże koszty są zrozumiałe, ponieważ obliczenia kwantowe są drogie, pracochłonne, nie mówiąc o tym, że generują duże ilości ciepła, które musi być odprowadzane.

Aby poprawnie zrozumieć skalę zagrożenia, należy mieć świadomość tego, że WSZYSTKO co robimy dzisiaj przez Internet jest zaszyfrowane. Łamanie najbardziej skomplikowanych szyfrów z użyciem dzisiejszych komputerów zajęłoby setki lat. Wraz z pojawieniem się komputerów kwantowych proces ten będzie można skrócić do kilku sekund. Jeśli taka technologia wpadnie w niepowołane ręce, właściciel takiej maszyny będzie mógł oczyszczać konta bankowe, całkowicie zamykać rządowe systemy obronne i przełamywać wszelkie cyfrowe zabezpieczenia (wliczając w to portfele kryptowalutowe).

Komputery kwantowe łamiące każdy rodzaj szyfrowania to zagrożenie na miarę cyfrowej bomby atomowej. Giganci technologiczni, tacy jak Google, Microsoft, IBM i Intel, mają nadzieję wyprzedzić konkurencję, zapewniając kwantową ochronę poufnych danych. Przypomina to nieco budowę kwantowego bunkra, który ochrania nasze dane. Jest to de facto jedyny dostępny sposób na przeciwdziałanie takim atakom. Lekkim pocieszeniem

może być fakt, że według badaczy do kwantowej apokalipsy nie dojdzie jeszcze przez wiele lat.

Autorstwo: M@tis

Źródło: ZmianyNaZiemi.pl