Michał Pilarski
Wydział Matematyki, Informatyki i Mechaniki UW

Komputery kwantowe za x lat

Komputery kwantowe są jednym z najbardziej interesujących wynalazków przyszłości. Pomimo swojego potencjału komputery kwantowe jeszcze nie mają wystarczającej mocy obliczeniowej w postaci ilości kubitów oraz są wysoce podatne na błędy spowodowane dekoherencją, przez co jeszcze nie są stosowane na dużą skalę. Obecne prace nad komputerami kwantowymi przypominają początki rozwoju klasycznych komputerów, więc jeśli ich postęp będzie podążał w tempie porównywalnym do prawa Moore'a, w najbliższych dekadach powstaną znacznie bardziej niezawodne komputery kwantowe o większej mocy obliczeniowej. Taki postęp umożliwiłby praktyczne zastosowanie ich na dużą skalę.

Jednym z najbardziej znanych zastosowań komputerów kwantowych jest szybka faktoryzacja dużych liczb przy użyciu algorytmu Shora. Implementacja takiego algorytmu na odpowiednio wydajnym komputerze kwantowym pozwoliłaby na złamanie szyfrów opartych na kryptografii asymetrycznej (np. algorytmu RSA), których bezpieczeństwo jest oparte na trudności faktoryzacji iloczynów dużych liczb pierwszych. W wielu popularnonaukowych opisach, komputery kwantowe zdolne do łamania szyfrów są opisywane jako bezpośrednie zagrożenie dla bezpieczeństwa cyfrowego świata, ponieważ nagle wiele wrażliwych danych, w tym wykorzystywanych przez banki i rządy państw, przestanie być bezpiecznych. Jednakże, już w obecnych czasach są prowadzone działania mające na celu zapobiec temu zagrożeniu. Odpowiedzią na to jest kryptografia postkwantowa (*PQC - Post Quantum Cryptography*), która zajmuje się opracowaniem rozwiązań odpornych na dotychczas znane metody ataków wykorzystujących komputery kwantowe[1]. Amerykańska agencja NIST (*National Institute of Standards and Technology*) w sierpniu 2024 r.[2] ogłosiła pierwszy zbiór algorytmów kryptografii postkwantowej, które już w najbliższych latach będą powszechnie stosowane do szyfrowania danych. Z tego powodu, komputery kwantowe przyszłości nie będą stanowiły tak dużego zagrożenia dla bezpieczeństwa, jak to jest obecnie często przedstawiane w opinii publicznej.

Wraz ze wzrostem wydajności i bezawaryjności komputerów kwantowych, nastąpi wzrost zainteresowania użyciem tej technologii do obliczeń. W bliskiej przyszłości najwięksi gracze na rynku komputerów kwantowych (m.in. Google, IBM, Microsoft)[3] zaczną oferować dostęp do mocy obliczeniowej nowych kwantowych komputerów szerokiej grupie klientów - nie tylko instytucjom badawczym i dużym przedsiębiorstwom, ale również małym start-upom i entuzjastom. Dzięki wprowadzeniu takiej usługi, liderzy rynku będą mogli odzyskać część kosztów poniesionych na utworzenie tej technologii oraz sfinansować jej dalszy rozwój. Taka usługa funkcjonowałaby w podobnym modelu jak obecnie można wynajmować serwery ze specjalistycznymi GPU do trenowania AI. Usługa ta umożliwiłaby dostęp do kwantowej mocy obliczeniowej instytucjom, których nie stać na zbudowanie i utrzymanie swojej własnej platformy obliczeniowej. Szeroki dostęp do wyżej wspomnianych zasobów pozwoli na przeprowadzenie symulacji procesów fizycznych i chemicznych na większą skalę, dzięki czemu

[1] Mielczarek J., Pierwsze standardy kryptografii postkwantowej, https://nauka.uj.edu.pl/aktualnosci/-/journal_content/56_INSTANCE_Sz8leL0jYQen/74541952/151477525, (01.01.2025).
[2] NIST Releases First 3 Finalized Post-Quantum Encryption Standards, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards , (01.01.2025).
[3] Wszyscy wymienieni liderzy już podjęli kroki w celu utworzenia takiej usługi, a IBM już ją oferuje za kwotę 96$ za minutę obliczeń, https://www.ibm.com/quantum/pricing, (01.01.2025).

będzie możliwe opracowanie nowych materiałów i leków. Znaczne poszerzenie grona użytkowników komputerów kwantowych pozwoli na dalszy rozwój informatyki kwantowej oraz odkrycie nowych praktycznych zastosowań, o których nikt jeszcze nie myśli.

W zakresie indywidualnego odbiorcy, marzeniem wielu entuzjastów gatunku science fiction byłoby posiadanie własnego komputera kwantowego w swoim własnym domu. Jednakże, prawdopodobnie w przyszłości nie powstaną osobiste komputery kwantowe, ponieważ takie rozwiązanie byłoby skomplikowane technicznie ze względu na problematyczny rozmiar, utrzymanie niskiej temperatury, odporności na czynniki zewnętrzne itp. Ponadto, klasyczne komputery osobiste, które są znacznie tańsze niż ich kwantowy odpowiednik, w zupełności wystarczają do zastosowań domowych i rozrywkowych. Co prawda, dokładnie tak samo myślano o klasycznych komputerach, mających obecnie wiele nowych zastosowań, o których nikt wcześniej nie myślał.

Podsumowując, pomimo braku obecności komputerów kwantowych w domach, odegrają one ważną rolę w życiu codziennym, dzięki postępowi nauki i nowo odkrytym materiałom, których odkrycie nie byłoby możliwe bez komputerów kwantowych. Komputery kwantowe obecnie budzą wiele obaw związanych z bezpieczeństwem danych, jednakże ten problem może zostać rozwiązany dzięki pracy kryptologów, którzy wdrożą skuteczne algorytmy PQC przed stworzeniem komputerów kwantowych zdolnych zagrozić kryptografii asymetrycznej.