Informatyka kwantowa – szansa, zagrożenie, niespełniona obietnica?

Czy informatyka kwantowa jest Świętym Graalem cyfryzacji, ślepą ścieżką ewolucji technologicznej, a może puszką Pandory, która zniszczy znany nam świat? Znani eksperci informatyki kwantowej – prof. Jacek Cichoń i prof. Mirosław Kutyłowski – przedstawili perspektywy rozwoju tej technologii podczas sympozjum towarzyszącego wręczeniu nagród w konkursie PTI na najlepsze prace magisterskie.

Nakłady na rozwój informatyki kwantowej wynoszą w skali świata miliardy dolarów. Szacuje się, że do tej pory globalnie przeznaczono na rozwój tej technologii aż 35,5 miliarda dolarów.

Kryterium opłacalności i wydajności

Czy efekty tych inwestycji są satysfakcjonujące, innymi słowy – czy otrzymano zwrot z tak gigantycznych środ-

ków? Obecnie odpowiedź na to pytanie brzmi – nie. Wygląda na to, że informatyka kwantowa stworzyła bańkę spekulacyjną, podobnie jak kryptowaluty. Póki co zyski firm z informatyki kwantowej są małe i pochodzą głównie ze szkoleń oferowanych instytucjom rozważającym zakup technologii kwantowej[1].

Jednym z ważniejszych argumentów zwolenników rozwoju informatyki kwantowej jest to, że może ona pomóc nam poradzić sobie z przetwarzaniem ogromnych ilości danych, którymi dysponujemy (Big Data). Przechowywanie tych danych generuje obecnie bardzo wysokie koszty. Tymczasem – jak wskazuje prof. Jacek Cichoń – istnieją już obecnie algorytmy klasyczne, które pozwalają znacznie zredukować ilość przetwarzanych danych kosztem niewielkiego spadku pewności predykcji. To tak zwane probabilistyczne szkice danych – obliczenia wykonywane są na próbce danych, a nie na całym ich zbiorze. Jeśli założymy, że pełen zestaw danych sprzedaży w dużej firmie zajmuje 300 GB, to probablistyczny szkic zajmuje zaledwie 10 GB (zapewniając dokładność rzędu 95%). Biznes powinien więc przekierować inwestycje płynące do wielkich hurtowni danych na opracowanie odpowiednich metod obliczeniowych.

Komputery kwantowe miały służyć także do modelowania związków chemicznych, co pozwoliłoby na szybsze odkrywanie leków i szczepionek. Była to obietnica rewolucji w medycynie i skokowego wzrostu skuteczności leczenia. Okazało się, że w najbardziej elementarnym zadaniu – szacowaniu energii stanu podstawowego układu chemicznego – nie udało się udowodnić przewagi komputerów kwantowych nad tradycyjnymi obliczeniami. Przygotowanie systemu kwantowego (do każdego eksperymentu osobno) jest tak trudne i długotrwałe, że niweluje zysk z szybkości obliczeń kwantowych.[2]

Kryterium bezpieczeństwa

Jeśli jednak udałoby się wdrożyć komputery kwantowe, to algorytm Shora stanowiłby ogromne zagrożenie dla działających obecnie systemów zabezpieczeń, opartych na wykorzystaniu kluczy prywatnych i publicznych. Faktoryzacja liczb RSA czy też obliczanie dyskretnego logarytmu pozwoliłoby poznać klucz prywatny i tym samym uczynić większość obecnie stosowanych schematów bezużetycznymi. Zastosowanie algorytmu Shora – jak wskazał prof. Kutyłowski – spowodowałoby więc złamanie systemów typu blockchain, podpisów elektronicznych, protokołów https, rozliczeń międzybankowych oraz problemy z automatyczną aktualizacją oprogramowania.

> *Z punktu widzenia etycznego ogromne nakłady na informatykę kwantową można by porównać do inwestycji w stworzenie nowego, śmiertelnego wirusa. Pytanie strategiczne i etyczne brzmi: czy powinno się inwestować pieniądze w opracowanie bardzo niebezpiecznego rozwiązania, czy może w przygotowanie antidotum?*

Obecnie nakłady na informatykę kwantową są ogromne, a środki na obronę przed potencjalnie groźnym jej wykorzystaniem – znikome.

Bezpieczeństwo w sytuacji ataku z wykorzystaniem komputerów kwantowych mogą zapewnić algorytmy postkwantowe. Trwają nad nimi już prace, ale wiele kwestii wymaga pilnego rozwiązania. Algorytmy tego typu są bardzo złożone, klucze prywatne i publiczne zajmują dużo miejsca na serwerach, co w praktyce biznesowej jest zdecydowanie źle widziane. Nowe algorytmy są jeszcze niedojrzałe, może być w nich sporo błędów wieku dziecięcego (mimo że niektóre z nich są pokłosiem dosyć starych idei, poprzednio zarzuconych ze względu na wydajność algorytmów). Trzeba ponadto sprawdzić, czy nie są podatne na ataki bocznym kanałem (ataki bazujące na dodatkowych informacjach o systemie, takich jak charakterystyka konsumpcji energii). Nowe rozwiązania powinny być odporne na złośliwą implementację czy celowe osłabienia systemu kryptograficznego. Im dłuższy i bardziej skomplikowany algorytm – tym ryzyko tego typu problemów wzrasta.

Wydaje się, że wbrew obietnicom i rozlicznym publikacjom popularnonaukowym informatyka kwantowa jak na razie nie oferuje cudownych rozwiązań, które pozwoliłyby na kolejny skok cywilizacyjny. Może okazać się ślepą odnogą rewolucji cyfrowej lub ogromnym zagrożeniem. Czy przewróci nasz świat do góry nogami, czy może nie zmieni nic – przekonamy się zapewne już za kilka lat.

Paulina Giersz

1 Gourianov N. (2022) The quantum computing buble, *Financial Times*, https://www.ft.com/content/6d2e34ab-f9fd--4041-8a96-91802bab7765

2 Lee S. i inni (2022) Is there evidence for exponential quantum advantage in quantum chemistry? *Chemical Physics*, https://www.researchgate.net/publication/362467917_Is_there_evidence_for_exponential_quantum_advantage_in_quantum_chemistry