NSA buduje komputer kwantowy

4 stycznia 2014

W ramach projektu „Penetrating Hard Targets” NSA buduje „kryptologicznie użyteczny komputer kwantowy”. „The Washington Post”, powołując się na dokumenty udostępnione przez Edwarda Snowdena twierdzi, że na wspomniany projekt przeznaczono 79,7 miliona dolarów. Budowa kwantowego komputera zdolnego do złamania niemal każdego szyfru to tylko jedna z części projektu.

Eksperci od dawna zastanawiają się, czy NSA nie jest bliższa zbudowania kwantowego komputera niż ktokolwiek inny. Jednak z ujawnionych przez Snowdena dokumentów wynika podobno, że Agencja nie prowadzi bardziej zaawansowanych prac. „Wydaje się mało prawdopodobne, by NSA w jakimś znaczącym stopniu wyprzedzała resztę świata i zdołała utrzymać to w tajemnicy” – mówi profesor Scott Aaronson z MIT-u. Podobno sama NSA uważa, że idzie łeb w łeb z laboratoriami finansowanymi przez UE czy rząd Szwajcarii. Nikt jednak nie jest bliski jakiegoś znaczącego przełomu. Z takim poglądem zgadza się profesor Seth Lloyd, specjalista ds. mechaniki kwantowej z MIT-u.

NSA pracuje nad kwantowym komputerem nie tylko dlatego, że chce podsłuchiwać innych, ale również dlatego, iż obawia się, że sama może zostać podsłuchana jeśli ktoś wybuduje kwantowy komputer szybciej. W jednym z ujawnionych przez Snowdena dokumentów czytamy, że „zastosowanie technologii kwantowych do tworzenia algorytmów wpłynie dramatycznie zarówno ma możliwość ochrony tajemnic rządowych USA jak i na możliwość śledzenia komunikacji innych rządów”.

Jeszcze przed 10 laty mówiono, że pierwszy duży komputer kwantowy może powstać w ciągu 10-100 lat, przed pięcioma laty eksperci zaczęli twierdzić, iż na taką maszynę trzeba będzie poczekać około 20 lat.

Kanadyjska firma D-Wave Systems od 2009 roku chwali się, że wyprodukowała komputer kwantowy. W 2011 roku jedną z takich maszyn kupił Lockheed Martin, a w 2012 roku sprzedała taką maszynę Google'owi, NASA i Universities Space Research Association, które założyły Kwantowe Laboratorium Sztucznej Inteligencji.

Jednak, jak zauważa profesor Matthew Green z Uniwersytetu Johnsa Hopkinsa, „nawet jeśli wszystko, co mówią o swoim komputerze jest prawdziwe, to nie można na nim uruchomić algorytmu Shora". W 1994 roku Peter Shor z Bell Laboratories zaprezentował kwantowy algorytm rozkładu wielkich liczb na liczby pierwsze. Rozłożenie szyfru, czyli liczby naturalnej składającej się z wielu cyfr, na liczby pierwsze, oznacza jego złamanie. Shor wykazał, że komputery kwantowe – w przeciwieństwie do komputerów tradycyjnych – byłyby w stanie błyskawicznie dokonać takiej operacji. Maszyna D-Wave nie była budowana z myślą o uruchomieniu na niej algorytmu Shora, zatem nie nadaje się do łamania szyfrów.

Jeśli chcielibyśmy porównać zaawansowanie prac nad kwantowym komputerem do komputera tradycyjnego, należałoby stwierdzić, że ludzkość nie wynalazła jeszcze abakusa. Z dokumentów NSA wynika, że Agencja miała nadzieję, iż do września 2013 roku uda jej się kontrolować dwa kwantowe bity (kubity). Do łamania szyfrów potrzebne zaś będą setki lub tysiące kubitów.

Autor: Mariusz Błoński
Na podstawie: The Washington Post
Źródło: Kopalnia Wiedzy