17 stycznia 2022

Systemy kwantowe w chmurze do dyspozycji WAT

Badania nad bezpieczeństwem algorytmów kryptograficznych z wykorzystaniem symulatorów kwantowych, usługi, oprogramowania i narzędzi w chmurze w ramach programu grantowego Amazon Web Services Cloud Credit for Research poprowadzi zespół dr.inż. Krzysztofa Kanciaka z Wydziału Cybernetyki WAT.

Projekty badawcze z wykorzystaniem Amazon Braket – usług obliczeń kwantowych udostępnianych przez Amazon Web Services (AWS) w chmurze rozpoczęły dwa zespoły akademickie: Wydziału Cybernetyki Wojskowej Akademii Technicznej w Warszawie oraz Centrum Fizyki Teoretycznej PAN . Oba projekty, zdaniem przedstawicieli Amazon Web Services, przyczynią się do lepszego zrozumienia technologii obliczeń kwantowych i jej zastosowań w świecie akademickim i biznesowym.

ZABEZPIECZENIE SZYFRÓW

Kredyty w ramach programu AWS Cloud Credit for Research otrzymał zespół zajmujący się zastosowaniami komputerów kwantowych do zabezpieczenia kryptograficznego powszechnych szyfrów. Naukowcy pod kierunkiem naukowym dr. inż. Krzysztofa Kanciaka zamierzają wdrożyć oparte na algorytmie podejście Grovera do znalezienia tajnego klucza na sprzęcie kwantowym dostępnym za pośrednictwem Amazon Braket.

Jak wyjaśnia dr inż. Kanciak, komputery kwantowe oparte na zjawisku „kwantowego wyżarzania” oraz oparte o pułapki jonowe świadczone są przez Amazon jako usługa. Doktoranci Szkoły Doktorskiej WAT mogą w ten sposób prowadzić badania nad bezpieczeństwem algorytmów kryptograficznych i w praktyczny sposób „przez palce” budować doświadczenie z zupełnie nową formą prowadzenia obliczeń.

„Ataki kwantowe na stosowane dziś powszechnie algorytmy kryptograficzne są mniej złożone obliczeniowo, w szczególności problemy matematyczne jak faktoryzacja czy logarytm dyskretny w kwantowym modelu obliczeniowym mają złożoność wielomianową. Czy komputer kwantowy z odpowiednio długim dla przeprowadzenia tych ataków rejestrem kubitów powstanie w najbliższych latach? A może już powstał? Trudno powiedzieć. Z pewnością prowadzenie badań naukowych w tym obszarze ma znaczenie dla rozwoju kryptografii oraz bezpieczeństwa państwa" - mówi dr inż. Krzysztof Kanciak.

ŁAGODZENIE SZUMU POMIAROWEGO

Naukowcy z Centrum Fizyki Teoretycznej PAN za pomocą eksperymentów prowadzonych z pomocą platformy AWS będą badali szum pomiarowy na złożonych urządzeniach kwantowych.

„Błędy przy pomiarze są jednym z głównych efektów utrudniających działanie współczesnych komputerów kwantowych. Sytuacja komplikuje się w przypadku układów wieloqubitowych, dla których już sam opis błędów stanowi wyzwanie dla komputerów klasycznych" – wyjaśnia prof. Michał Oszmaniec z CFT PAN. Naukowcy zaproponowali uproszczony model szumu i planują go wykorzystać do zredukowania wpływu błędów na działanie algorytmów kwantowych.

Zespół Quantin Research Group prof. Oszmańca zajmuje się zarówno teoretycznymi, jak i stosowanymi aspektami obliczeń kwantowych i realizuje cele naukowe w zakresie charakteryzacji i łagodzenia błędów w krótkoterminowych komputerach kwantowych.

OBLICZENIA KWANTOWE W CHMURZE

Komputery kwantowe to systemy, który działanie jest oparte na fizyce kwantowej. Zwykłe komputery operują na bitach, mogących przyjmować wartość „0" albo „1". Natomiast podstawą działania kwantowych komputerów są kubity (czyli bity kwantowe) przyjmujące tzw. superpozycję, w której „0" i „1" występują w tym samym czasie.

„Komputery kwantowe będą w stanie rozwiązać wiele problemów, które są obecnie poza zasięgiem klasycznych maszyn obliczeniowych. Ma to szczególne znaczenie dla społeczności naukowej. Jednocześnie oczywistym wyzwaniem pozostaje dostępność komputerów kwantowych. Tutaj naturalną odpowiedzią jest udostępnianie tych systemów w formie usług chmurowych" – wyjaśnia Dariusz Matczak z Amazon Web Services. Dodaje, że firma zapewni publiczny dostęp do jednostki przetwarzania kwantowego (QPU) z Oxford Quantum Circuits (OQC) i rozszerzy dostępność tej usługi w Europie.

Systemy kwantowe oraz inne usługi AWS są dostępne dla wszystkich pracowników naukowych i studentów, prowadzących projekty badawcze. Polscy naukowcy mogą ubiegać się o granty w ramach programu AWS Cloud Credit for Research na stronie aws.amazon.com/government-education/research-and-technical-computing/cloud-credit-for-research

red. Karolina Duszczyk

Źródło: Amazon, Krzysztof Kanciak