Technologie kwantowe, a cyberbezpieczeństwo

Technologie kwantowe stanowią potencjalne zagrożenie dla cyberbezpieczeństwa, a z drugiej strony dają narzędzie dla jego wzmocnienia. Rozwój technologii kwantowych na nowo ustali więc zasady bezpieczeństwa w cyberprzestrzeni.
Jednym z najważniejszych filarów bezpieczeństwa w cyberprzestrzeni jest kryptografia. Dzięki kryptografii możliwe jest m.in. robienie zakupów online czy korzystanie z bankowości elektronicznej.
Z punktu widzenia Państwa, kryptografia to kluczowy element tarczy chroniącej przed cyberatakami na strategiczne komponenty (zarówno infrastrukturę fizyczną, jak i zasoby cyfrowe) oraz narzędzie umożliwiające wymianę i przechowywanie informacji niejawnej, o podstawowym znaczeniu dla interesu i bezpieczeństwa Państwa.
Technologie kwantowe wykorzystują zjawiska fizyczne w skali atomowej i subatomowej. Najmniejsze cząstki materii, takie jak fotony czy elektrony zachowują się według zupełnie innych zasad niż obiekty, które możemy dostrzec gołym okiem. Fizycy od mniej więcej stu lat opracowują skomplikowane teorie i wzory składające się na mechanikę kwantową, niezwykle skomplikowaną dziedzinę fizyki.
- Jeśli myślisz, że rozumiesz mechanikę kwantową, nie rozumiesz mechaniki kwantowej, twierdził wybitny fizyk Richard Feynman.
I rzeczywiście wiele uznanych teorii na temat cząstek elementarnych wciąż jest kwestionowanych, a specjaliści z tej dziedziny nieustannie się spierają. Nie oznacza to jednak, że odkryć mechaniki kwantowej nie da się zastosować w praktyce. Obecnie coraz szybciej rozwijają się kwantowe technologie obliczeniowe, komunikacyjne i detekcyjne. W najbliższej przyszłości staną się one bardziej dostępne i zmienią nasze życie. Według analityków MarketsandMarkets, wartość rynku obliczeń kwantowych osiągnie do 2026 roku pułap niemal 1,8 mld dol.

Jak działają komputery kwantowe
Naukowcy już dawno doszli do wniosku, że specyficzne właściwości cząstek elementarnych można wykorzystać do zbudowania komputera zupełnie nowego typu
Kubity, czyli kwantowe bityumożliwiają komputerom kwantowym wykonywanie wielu obliczeń w tym samym czasie, co potencjalnie prowadzi do ogromnego wzrostu mocy obliczeniowej w porównaniu z komputerami klasycznymi. W przypadku niektórych rodzajów obliczeń oznacza to przyspieszenie tempa rozwiązania problemów matematycznych z wielu dziesiątek, setek a nawet milionów lat do zaledwie kilku minut!

Wpływ na cyberbezpieczeństwo
Ogromna moc obliczeniowa komputerów kwantowych stawia pod znakiem zapytania bezpieczeństwo zaszyfrowanych informacji. Wiele spośród obecnie stosowanych systemów kryptograficznych straci rację bytu, skoro ktoś dysponujący komputerem kwantowym będzie w stanie złamać je w oka mgnieniu.
Z drugiej zaś strony, technologie kwantowe dostarczają zupełnie nowych rozwiązań kryptograficznych, które mogą pozwolić osiągnąć poziom bezpieczeństwa niedostępny z wykorzystaniem kryptografii klasycznej. Duże nadzieje wiązane są z tzw. komunikacją kwantową, polegającą na przesyłaniu informacji bezpośrednio w formie kubitu. Próba przejęcia informacji przez hakera automatycznie doprowadzi do wyjścia cząsteczki ze stanu superpozycji i zniszczenia informacji.

Jak się bronić przed kwantami
Aktualnie rozwój komputerów kwantowych znajduje się na początkowym, eksperymentalnym etapie. Ich budowa wiąże się z wieloma wyzwaniami technologicznymi, m.in. kubity działają poprawnie tylko w ekstremalnie niskich temperaturach i przez krótki, ograniczony czas. Można jednak spodziewać się przyspieszenia tempa rozwoju tych technologii, zwłaszcza że pierwszy komercyjny komputer kwantowy, należący do Google, działa już od 2019 r.
Odpowiedzią na zagrożenia cyberbezpieczeństwa ze strony komputerów kwantowych jest opracowanie nowych sposobów szyfrowania danych, które są odporne na analizę kwantową. Od 2016 r. nad wdrożeniem nowych standardów pracuje amerykański Narodowy Instytut Standaryzacji i Technologii.

Wygląda na to, że odpowiednie procedury bezpieczeństwa będą gotowe, zanim dostęp hakerów do komputerów kwantowych stanie się realnym zagrożeniem. Ze względu na wysokie koszty i poważne wyzwania technologiczne jeszcze przez długi czas będą one w wyłącznej gestii rządów państw i największych korporacji.

Program sektorowy „Bankowcy dla Edukacji" to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę www.bde.wib.org.pl

BANKOWCY
DLA EDUKACJI
program sektorowy