URZĄD OCHRONY DANYCH OSOBOWYCH

Ministerstwo Cyfryzacji

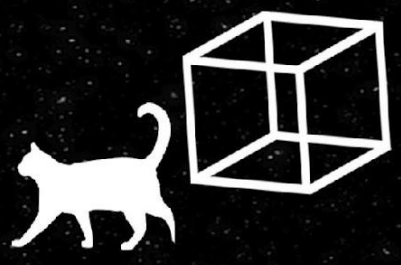
Materiały pokonferencyjne

autorstwa uczestników konferencji naukowej:

„Człowiek w postkwantowej rzeczywistości”

AI LAW TECH

GRAI



Redaktor prowadzący:

Jakub Groszkowski

Opracowanie redakcyjne:

Natalia Misiuk

Balbina Hermanowicz

Autorstwo poszczególnych rozdziałów:

dr hab. Paweł Przybyłowicz, prof. AGH

r.pr. Maciej Gawroński
GP Partners

dr Anna Kamińska
Creotech Instruments S.A.

dr Piotr Biskupski
IBM

Urząd Ochrony Danych Osobowych

ul. Stawki 2,

00-193 Warszawa

SPIS TREŚCI

WSTĘP

Obecnie jesteśmy świadkami dynamicznego rozwoju technologii kwantowych, które niewątpliwie mają potencjał zrewolucjonizowania wielu dziedzin i problemów, przed którymi stoimy dzisiaj. Mogą jednak stanowić również zagrożenie dla cyberbezpieczeństwa, dlatego musimy być przygotowani na radzenie sobie ze wszystkimi możliwymi konsekwencjami.

Prezentujemy Państwu materiały będące podsumowaniem konferencji naukowej pt. „Człowiek w postkwantowej rzeczywistości", podczas której prelegenci przybliżyli temat technologii kwantowej, odpowiadając m.in. na pytanie czy zagraża ona cyberbezpieczeństwu i w jaki sposób wpłynie na ochronę danych osobowych. Wydarzenie było doskonałą okazją, aby dowiedzieć się w jaki sposób można zapewnić bezpieczeństwo i poufność przetwarzanych danych przy jej wykorzystaniu.

W materiałach zostały przedstawione m.in. główne przewidywane zastosowania komputerów kwantowych oraz postęp i wyzwania związane z ich budową. Poruszono również kwestię kwantowej sztucznej inteligencji, odnosząc się do możliwości jakie niesie za sobą rozwój takiej technologii. Eksperci wskazali również zagrożenia, które mogą osłabiać prywatność i ochronę danych osobowych.

Szanowni Państwo,

z przyjemnością oddaję w Państwa ręce publikację będącą podsumowaniem konferencji naukowej „Człowiek w postkwantowej rzeczywistości" organizowanej przez Urząd Ochrony Danych Osobowych przy współpracy z Kancelarią Prezesa Rady Ministrów. Z satysfakcją odnotowuję fakt, że wydarzenie było miejscem interesujących dyskusji, wymiany poglądów i doświadczeń, które znajdują odzwierciedlenie w tej publikacji.

Słowa podziękowania kieruję w stronę Autorów zaangażowanych w powstanie wartościowych materiałów pokonferencyjnych „Człowiek w postkwantowej rzeczywistości", które stanowią cenne źródło informacji na temat technologii postkwantowej oraz jej wpływu na życie człowieka.

Jestem przekonany, że publikacja będzie dla Państwa cennym uzupełnieniem wiedzy przekazanej podczas konferencji i przyczyni się do lepszego, praktycznego zrozumienia istoty problematyki oraz podniesienia świadomości na temat szans i wyzwań dotyczących komputerów kwantowych.

Jan Nowak

Prezes Urzędu Ochrony Danych Osobowych

Czym jest technologia kwantowa?

Autor: Dr hab. Paweł Przybyłowicz, prof. AGH
AGH

„Technologia jest zmienną niezależną cywilizacji”

Stanisław Lem

Początki komputerów kwantowych sięgają przełomu lat 50 i 60 XX wieku. Podczas wykładu „Tam na dole jest jeszcze dużo miejsca” Richard Feynman przedstawił główne idee leżące u podstaw obliczeń i technologii kwantowej. Zasugerował również możliwość konstrukcji nano-urządzeń (robotów) oraz jednostek obliczeniowych opartych na prawach mechaniki kwantowej. Urządzenia tego typu mogły by symulować zjawiska fizyki kwantowej w czasie rzeczywistym *in silico*. Od czasu wspomnianego wykładu nastąpił znaczny postęp (zarówno teoretyczny jak i praktyczny) w zakresie rzeczywistej realizacji i zastosowania technologii kwantowych.

Na potrzeby niniejszej prezentacji przyjmijmy następującą roboczą definicję technologii kwantowej:

„Technologia kwantowa (TK) jest to klasa technologii, która działa z wykorzystaniem zasad mechaniki kwantowej (fizyki cząstek subatomowych), w tym: splątania kwantowego, superpozycji kwantowej, pomiaru kwantowego.”

Poniżej zostały wypisane główne kamienie milowe jakie zostały osiągnięte w ciągu ostatnich czterdziestu lat w temacie obliczeń kwantowych. M.in.:

- w latach 80-tych powstały główne podstawy teoretyczne obliczeń kwantowych, wykorzystujące właśnie stany splątane, superpozycje, bramki kwantowe oraz pomiar kwantowy do przeprowadzania obliczeń;

- w latach 90-tych pojawiły się dwa główne (także obecnie) algorytmy kwantowe tj algorytm Shor'a (94') oraz Grover'a (96') – algorytmy te są dwoma głównymi przykładami na to jak bardzo komputery kwantowe mogą przyśpieszyć obliczenia w porównaniu do komputerów klasycznych;

- w 1998 roku zaprezentowano pierwszą rzeczywistą realizację prostego komputera kwantowego opartego na 2 kubitach;

- od roku 2016 widać stały postęp technologiczny i konstrukcyjny. Mianowicie firma IBM uruchomiła platformę Quantum Experience[1] dającą dostęp do ich komputerów kwantowych. Warto podkreślić, że dla celów niekomercyjnych i edukacyjnych dostęp ten jest darmowy. Dzięki temu obecnie każdy zainteresowany tematem może rozpocząć przygodę z obliczeniami kwantowymi.

W kontekście powyższych informacji można zadać następujące pytania:

- Czy technologia kwantowa to kolejny **gamechanger**?
- Czy obecnie mamy do czynienia z **pełnoprawną technologią kwantową**?
- Czy nasza rzeczywistość jest jeszcze **prekwantowa**, czy już **postkwantowa**?

Główny postęp jaki się zrealizował w dziedzinie komputerów kwantowych dotyczy liczby jednocześnie przetwarzanych kubitów. Kubit jest to kwantowa jednostka informacji[2]. Na komputerze klasycznym taką jednostką jest dobrze znany bit: 0 lub 1 (prawda/fałsz, jest prąd/brak prądu etc.). W przypadku kwantowym okazuje się, że kubit, oprócz dwóch stanów klasycznych 0 i 1, może przyjmować każdy z

[1] https://quantum-computing.ibm.com/

[2] C. Bernhardt, Obliczenia kwantowe dla każdego, PWN, 2020

kontinuum stanów pomiędzy stanami klasycznymi – stan kubitu jest tzw. superpozycją stanów klasycznych. Tym samym komputer kwantowy ma dostęp nieskończenie większej liczby stanów niż komputer klasyczny. Dzięki temu możliwe jest (przynajmniej teoretycznie) przeprowadzenie niektórych obliczeń na komputerze kwantowym wykładniczo szybciej niż na komputerze klasycznym. Zostało to udowodnione m.in. dla algorytmu Shora[3]. To przyśpieszenie jest również głównym źródłem emocji i zainteresowania komputerami kwantowymi.

Peter Shor udowodnił w 1994 roku, że konstruując odpowiedni obwód kwantowy można bardzo szybko przeprowadzić faktoryzację wielkich liczb naturalnych na iloczyn liczb pierwszych. Z jednej strony jest to fantastyczny wynik teoretyczny (nieznane są bowiem szybkie algorytmy klasyczne dla tego problemu), z drugiej jednak strony wynik ten zachwiał wiarą w bezpieczeństwo powszechnie używanych algorytmów opartych na tzw. kodowaniu asymetrycznym do których należy np. bardzo dobrze znany algorytm RSA. Na razie szyfry RSA wydają się względnie bezpieczne, gdyż wydaje się, że do ich złamania potrzeba komputera kwantowego operującego na tysiącach kubitów, podczas gdy obecne komputery kwantowe mają dostęp do setek kubitów. Do tego dochodzą główne problemy konstrukcyjne związane m.in. z utrzymaniem kubitów w odpowiednich stanach i odizolowania ich od jakichkolwiek wpływów zewnętrznych. Nie ma ponadto na razie żadnego konsensusu w dziedzinie technologii budowy komputera kwantowego i badane są różne podejścia, np.:

- topologiczne komputery kwantowe

- kropki kwantowe

- komputery kwantowe oparte na nanoprzewodnikach, atomowych kondensatach Einsteina-Bosega, kropkach kwantowych.

[3] J-P. Aumasson, Nowoczesna kryptografia – praktyczne wprowadzenie do szyfrowania, PWN, 2018

Należy jednak pamiętać, że postęp technologiczny cały czas następuje i niektóre prognozy mówią, że w ciągu 3 do 10 lat powstaną skalowalne komputery kwantowe zdolne do złamania obecnych szyfrów asymetrycznych. Mamy więc jeszcze trochę czasu na opracowanie odpowiednich systemów zabezpieczeń i algorytmów kryptografii postkwantowej. Należy również dodać, że szyfrowanie symetryczne (po odpowiednim zwiększeniu liczby bitów potrzebnych do szyfrowania) pozostaną bezpieczne nawet po pojawieniu się komputerów kwantowych. Obecnie natomiast już działają maszyny dedykowane specjalnym zadaniom, np. optymalizacyjnym. Do tego służą komputery firmy D-Wave[4] , które, operując na 5000 kubitach, są dedykowane do szybkiego wykonywania algorytmu kwantowego wyżarzania. Inne obszary jakie z pewnością ulegną zmianie po pojawieniu się komputerów kwantowych to:

- finanse i bankowość (już wspomniane wyżej cyberbezpieczeńswo ale również pojawi się możliwość przyśpieszenia wykonywania symulacji Monte Carlo, które służą do wyceny instrumentów pochodnych);

- Blockchain i kryptowaluty (teoretycznie jest możliwe załamanie zabezpieczeń łańcucha bloków za pomocą dostatecznie potężnego komputera kwantowego);

- Medycyna (za pomocą komputera kwantowego będzie można badać własności nowych cząsteczek chemicznych bez konieczności wykonywania drogich testów laboratoryjnych)

- Sztuczna inteligencja (dzięki komputerom kwantowym będzie można trenować szybciej sieci neuronowe a także przetwarzać więcej danych podczas treningu. Obecnie można już próbować wykorzystać do tego celu komputer D-Wave.)

[4] https://www.dwavesys.com/

Zmianie i dopasowaniu, jak to już się dzieje w przypadku sztucznej inteligencji, będzie również będzie musiało ulec prawo – nowe przepisy będą regulować sposób i możliwy zakres użycia komputerów kwantowych m.in. w takich wrażliwych obszarach jak cyberbezpieczeństwo, przetwarzanie danych wrażliwych itp.

Wracając do trzech zadanych powyżej pytań wydaje się, że ewidentnie komputer kwantowy będzie kolejnym 'gamechangerem' na zawsze zmieniającym (tak jak internet, sztuczna inteligencja, energia jądrowa) naszą egzystencję jako ludzkości. Co prawda nie mamy jeszcze do czynienia z rzeczywistością postkwantową (komputer kwantowy operujący setkami tysięcy kubitów jeszcze się nie pojawił), jednakże prawie codziennie pojawiają się nowinki w temacie budowy komputerów kwantowych. Możemy się więc spodziewać w miarę rychłego pojawienia pełnoprawnych (w swej kwantowej istocie) komputerów opartych na prawach mechaniki kwantowej.

Prywatność a komputery kwantowe

Autor: r. pr. Maciej Gawroński
GP Partner

Thou shalt not make a machine in the likeness of a human mind.
[Nie będziesz czynił maszyny na podobieństwo ludzkiego umysłu]
Pomarańczowa Biblia Katolicka, Frank Herbert, cykl Diuna

Piszę ten tekst w przededniu uwolnienia Chat GPT-4 ale już po doniesieniach o wybrykach i potencjale nowego Bing[5]. Czynienie teraz przewidywań co do rozwoju i wpływu technologii komputerów kwantowych na prywatność jest zadaniem niewdzięcznym i przerażającym.

Zadanie jest niewdzięczne, bo czynienie prognoz krótkoterminowych na temat skutków przełomowych technologii rzadko wychodzi dobrze. Zadanie jest też przerażające, bo do głowy, napakowanej nie tylko literaturą SF ale i świadomością potencjału i słabości informatyki ale także świadomością tego, że korporacje i światowi decydenci żyją w świecie braku odpowiedzialności za swoje decyzje, przychodzą gównie przykłady przerażające.

Jestem wielkim miłośnikiem literatury fantastyczno-naukowej (hard science-fiction, nie mylić z fantasy). „Cyberiadę"[6] Lema przeczytałem mając 10 lat a „Dialogi" mając 14 lat[7]. Jednak w kontekście komputerów kwantowych, a

[5] Doniesienia o potencjale wydają się nieco przesadzone. Wprawdzie sam spytałem Bing wyłącznie o Billa Gatesa, więc może to nie być doświadczenie reprezentantywne.

[6] Znalezioną na półce u dziadka, pod Tarnowem. Wydanie I z 1967 roku.

[7] Gdy w 2008 roku zakładałem kancelarię Bird & Bird w Warszawie, zastanawiałem się, co takiego dobrze zilustrowałoby połączenie tradycji, technologicznego charakteru i naszej polskości. Długo to nie trwało, bo natychmiast przyszły mi do głowy ilustracje Daniela Mroza do „Cyberiady" Stanisława Lema. Dzięki operatywności naszego ówczesnego managera Pawła Dudka, udało nam

szczególnie kwantowej sztucznej inteligencji do głowy przychodzi mi najbardziej „Neuromancer". Williama Gibsona[8] i świat cyberpunku, gdzie cyberprzestrzeń jest dość anarchistyczną areną walki „wszystkich ze wszystkimi".

Dla potrzeb oceny relacji między technologią kwantową a naszą prywatnością przyjmuję oczywiście założenie, że jest to technologia działająca. Czytam[9], że wyzwaniem jest obsługa błędów i zapewnienie stałości i powtarzalności wyników obliczeń komputerów kwantowych. Ale zapewne problemy te zostaną pokonane. Liczyć natomiast, że rozwój komputerów kwantowych zostanie powstrzymany przez technologiczny rozwód USA i Chin, to jak liczyć na trzecią wojnę światową. Więc pomińmy.

Kwantowa sztuczna inteligencja. Największą dostrzegalną (przynajmniej przeze mnie) szansą i wyzwaniem dotyczącym komputerów kwantowych jest właśnie połączenie technologii AI z technologią kwantową[10]. Sztuczna inteligencja z dostępem do wszystkich zasobów informacyjnych internetu i wszechpotężną mocą obliczeniową będzie w stanie przewidywać i kontrolować wszystkie jednostki ludzkie w czasie rzeczywistym. Proszę sobie wyobrazić bezwzględne stosowanie prawa przez każdego cały czas lub, jeszcze gorzej – stuprocentową odpowiedzialność za każde naruszenie prawa. W takim świecie nie dałoby się żyć.

---

się skontaktować z córką Pana Daniela Mroza, Panią Łucją Mróz-Raynoch. Pani Łucja zgodziła się, abyśmy korzystali z ilustracji do Cyberiady. Gdy później przeszedłem na chwilę do kancelarii Maruta Wachta a potem otworzyłem kancelarię Gawroński & Partners (obecnie GP Partners), roboty Daniela Mroza i Stanisława Lema szły za mną.

[8] Chat GPT-3 podpowiada trylogię Hyperion Dana Simmonsa, ale takich AI jak tam, to jednak na razie nie przewiduję. Taktownie, ani Chat GPT-3 ani ja, nie będziemy nawiązywać do Terminatora ani gry Mass Effect.

[9] Czytam też np. o memristorach i o ich kwantowych wersjach 😅.

[10] Nie będę tu rozważał sytuacji, że powstanie sztuczna świadomość …albo urodzi się nowy malutki wszechświat.

Przewidywalność. Problem jest praktyczny i filozoficzny. Problem praktyczny polega na tym, że obecnie jesteśmy w pełni identyfikowalni, namierzalni, monitorowalni i …przewidywalni. Żadne czipowanie nie jest już do tego potrzebne. W zasadzie nie ma prywatności. Tym bardziej regulacja ingerencji w naszą prywatność, możliwości odwoływania się od decyzji względem nas, które mogą być zautomatyzowane i natychmiast wykonywane, ma znaczenie fundamentalne. Problem filozoficzny to cienka i nieostra granica między determinizmem (czyli przewidywalnością naszego zachowania) a wolną wolą. Problem ten staje się problemem prawnym – czy możemy ponosić konsekwencje zdarzeń, które jeszcze nie nastąpiły? To płynne przejście w świat znany z „Raportu mniejszości". Kwantowa sztuczna inteligencja prawdopodobnie będzie mogła typować przestępstwa, których się dopuścimy. Albo dopuścilibyśmy, gdyby prokuratura nas prewencyjnie nie osadziła w areszcie. Nawet obecnie przecież prokuratura poświęca wielkie środki, aby na pewno przypisać winę osobom, które już uwięziła. Pełnej inwigilacji i windykacji przysłużyć się może także kolejna przewidywana zaleta kwantowej sztucznej inteligencji – integracja baz danych a także zdolność do wykrywania wzorców w wielkich zbiorach danych (choć to też wielka szansa).

Inwigilacja i manipulacja. Komputery kwantowe a szczególnie kwantowa sztuczna inteligencja da potężne narzędzia rządom, organizacjom i osobom, które będą do niej miały dostęp przeciwko tzw. zwykłemu obywatelowi. W mniej lub bardziej brutalny sposób będzie można kontrolować i kompromitować przeciwników. Pytanie, kto będzie kontrolował tych, którzy taki dostęp będą posiadali. Z tej perspektywy nieco chocholi taniec uprawiany przez USA, Komisję Europejską, TSUE i Maxa Schremsa nabiera jednak istotnej głębi.

Cybersecurity. Klasycznym wyzwaniem ery postkwantowej jest z kolei brak odporności obecnych algorytmów szyfrujących na brutalne przełamanie (czyli sprawdzenie wszystkich możliwości). NIST pracuje nad nowymi algorytmami,

odpornymi na komputery kwantowe. Zobaczymy, co z tego wyjdzie. Z tej perspektywy niezwykle istotne jest pytanie, kto będzie miał dostęp do komputerów kwantowych. W świecie o niskim i niejasnym poziomie cyberbezpieczeństwa można sobie wyobrazić chaos i zniszczenie, jakie wyrządziłoby dostanie się do tej technologii przez niektóre kraje lub organizacje przestępcze. Natomiast w każdym świecie możliwość przełamanie aktualnej kryptografii daje dodatkową możliwość inwigilacji służbom wywiadowczym państw wiodących w wyścigu technologicznym.

Deep fake. Problem doskonałych podróbek osób staje się realny na naszych oczach i bez komputerów kwantowych. Jak odróżniać prawdę od fałszu, jak bronić się np. przed podłożeniem naszej twarzy do filmu pornograficznego (co już się dzieje) i jak wierzyć cyfrowym obrazom – z tym zapewne będziemy mierzyć się coraz bardziej. Wydaje się oczywiste, że komputery kwantowe będą zdolne do idealnego symulowania ludzi i innych obiektów.

Szanse. Oprócz tych wyzwań oczywiście technologia kwantowa daje przede wszystkim wielkie szanse. Kto by nie chciał mieć takiego asystenta jak Jarvis Tony'ego Starka (ale aby nie Ultron). Może na przykład, mimo tego że istnieją lekarze i przemysł farmaceutyczny, uda się stworzyć medycynę osobistą oraz postęp w naukach medycznych ruszy z miejsca? Sztuczna inteligencja radzi sobie dobrze z wychwytywaniem wzorców (pattern recognition). Kwantowa sztuczna inteligencja ma sobie radzić z tym o kilka wielkości lepiej[11]. Komputery kwantowe zapewne umożliwią też dalszy postęp w nauce, mechanice, fizyce, astronomii, wspomnianej już medycynie, w naukach społecznych etc etc.

[11] Ta użyteczność KSI/QAI rodzi oczywiście ów posthumanistyczny problem zbędności takiej masy ludzkiej, o której pisze niesławny popularyzator transhumanizmu Youval Harrari. Tyle że on tego problemu nie wymyślił. Automatyzacja procesów intelektualnych i fizycznych zabierze pracę wielu ludziom. Ale może równocześnie da inną w zamian? Lekarze na przykład mogą zacząć korzystać z KSI zamiast kontestować Dr Google.

Technologię kwantową można też stosować do zapewnienia prywatności komunikacji, dzięki zjawisku splątania kwantowego. I to podobno już się udaje. Miałem nadzieję, że dzięki temu komunikacja „przejdzie w nadświetlną". Ale podobno jednak i w ten sposób przełamać prędkości światła się nie da.

Wracając na podwórko prywatności, może kwantowa sztuczna inteligencja okaże się panaceum na nietransparentność „konwencjonalnej" sztucznej inteligencji? Czyli będzie w stanie wyjaśnić decyzje swoje jak i decyzje owej konwencjonalnej AI. To odpowiedziałoby na realne i regulacyjne zagadnienie, o którym napisałem odrębny artykuł, który ukaże się w materiałach poseminaryjnych webinaru „Projektowanie systemów SI zgodnych z RODO" zorganizowanego przez Urząd Ochrony Danych Osobowych we współpracy z Kancelarią Prezesa Rady Ministrów.

Kwantowy deep fake może mieć także znakomity użytek w przemyśle rozrywkowym. Będziemy mogli oglądać już nieżyjących aktorów (podobno, nie czekając na komputery kwantowe, ktoś scastingował już Jamesa Deana) a jeśli aktorzy wirtualni zastąpią tych żywych, ileż celebryckich „mądrości" mogłyby oszczędzić nam media głównego nurtu.

Wreszcie, w kwantowej sztucznej inteligencji dostrzegam szczególny potencjał dla Polski, polskich przedsiębiorców i szerzej, polskich podatników. Jest bowiem szansa, że wreszcie pojawi się ktoś, kto rozezna się w Polskim Ładzie.

Co robić? Regulacje

Odpowiedzią na zagrożenia związane z technologią quantum computing musi być rozwój istniejących oraz tworzenie nowych regulacji a w ramach tych regulacji także systemów wzajemnej kontroli. Obecnie jesteśmy na etapie badania zagadnienia i poszukiwania praktycznych narzędzi i rozwiązań, które mogły by służyć za podwalinę przyszłego prawa. Pojawiają się głosy, kiedyś niesłychane, żeby najpierw regulować a później się zastanawiać, aby nie wpaść w

opóźnienie, jak to się (według autorów artykułu w przypisie) stało z regulacją sztucznej inteligencji[12].

Regulacje powinny uwzględniać to, że poziom zagrożenia jest zależny od dostępności komputerów kwantowych. Dlatego, ewentualne obowiązki i sankcje należy dopasować do podmiotu zobowiązanego. Karać można firmy, ale nie jest to już tak oczywiste w przypadku organów państwa korzystających z technologii kwantowych. Nie uda się objąć regulacją tzw. „bad actors" stosujących narzędzia kwantowe do nieuczciwych i przestępnych celów. Tu szczególną rolę będzie pełnić postkwantowe cyberbezpieczeństwo oraz zdolność do odstraszania w cyberprzestrzeni.

A dlaczego regulacje? Moją chyba najbardziej ulubioną sceną filmową jest monolog Jokera w filmie Christophera Nolana „Mroczny Rycerz". Gdy pod koniec filmu Batman ratuje Jokera łapiąc go na linkę i wciąga go za nogę na wysokość swojej twarzy, Joker zaczyna mówić wisząc do góry nogami i wtedy kamera odwraca się o 180%. Joker mówi Batmanowi, że go nie zabije, bo jest z nim za dużo radości. Ale przede wszystkim mówi: „To się dzieje, gdy niepowstrzymana siła napotyka na niewzruszony obiekt" [*This is what happens when an unstoppable force meets an immovable object*]. Joker ma na myśli swoje zderzenie z Batmanem. Ale ja widzę tu analogię do zderzenia technologii z przepisami. Technologia jest niepowstrzymaną siłą, przepisy są niewzruszonym obiektem. Jeśli się zderzą, technologia może opłynąć przepisy. Ale może też tak się stać, że przepisy, par excellence, uregulują technologię.

Komputery kwantowe a RODO?

12

https://foreignpolicy.com/2022/08/21/quantum-computing-artificial-intelligence-ai-technology-regulation/

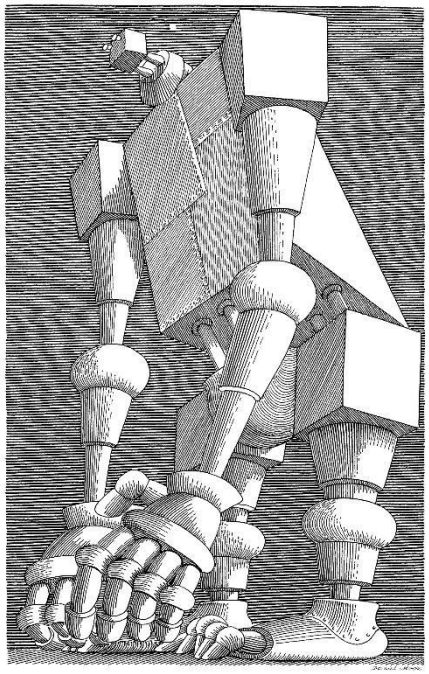
Zastosowanie technologii kwantowej można skutecznie wpisać w obecny system regulacji RODO. Z perspektywy przepisów o ochronie danych osobowych szczególnie istotne będą następujące kwestie:

- kto będzie odpowiedzialny za korzystanie z technologii kwantowej? Kto będzie administratorem, a kto podmiotem przetwarzającym w kontekście operacji przetwarzania danych z zastosowaniem komputerów kwantowych;
- jak do przetwarzania danych za pomocą technologii kwantowej mają się ogólne zasady ochrony danych – np. zasada ograniczenia celu przetwarzania, zasada minimalizacji, zasada przejrzystości lub zasada rozliczalności;
- czy regulacje ochrony danych są wystarczająco neutralne technologicznie, aby poradzić sobie z nadejściem ery postkwantowej;
- jak zapewnić podmiotom danych indywidualną kontrolę nad danymi osobowymi, przetwarzanymi za pomocą technologii kwantowych? W jaki sposób realizować prawa podmiotów danych;
- czy planowany przez projekt Rozporządzenia UE o sztucznej inteligencji system certyfikacyjny i zarządzania ryzykiem sztucznej inteligencji będzie chronił dostawców i użytkowników technologii, czy społeczeństwo, czy zasady przetwarzania danych określone RODO zostaną utrzymane, czy rozwodnione, jak to się stało w trakcie tak zwanej pandemii i jak w pewnym zakresie zostało to zaprojektowane w projekcie Rozporządzenia.

To tylko niektóre z pytań, na które będzie trzeba udzielić odpowiedzi w związku z rozwojem i rozpowszechnieniem technologii komputerów kwantowych.

Wyzwania związane z komputerami kwantowymi i kwantową sztuczną inteligencją na polu prywatności, wolności i dostępu do informacji (o ile nie

dojdzie do uzyskania przez samoświadomości przez AI) sprowadzają się na końcu do tego, jaki z niej użytek uczynią rządy i korporacje. Pomny doświadczeń ostatnich trzech lat jak i całego XX wieku, w komputerach kwantowych boję się najbardziej ludzi o małym rozumku lub wielkim ego, którzy dostaną do rąk kolejne potężne narzędzia do wymuszania swojej woli. I niech to zilustruje obrazek mistrza Daniela Mroza zaczerpnięty z „Cyberiady" Lema.



Na zakończenie

Gdy poprosiłem Chat GPT-3 o cytat z Diuny odpowiedni na motto artykułu, ale nie podpowiadając, że już taki mam, GPT-3 zaproponował mi „Litanię przeciw strachowi" Bene Gesserit:

> *Strach jest umysłem zabójcy. Strach jest małą śmiercią, która prowadzi do całkowitego unicestwienia. Stawię czoła mojemu strachowi. Pozwolę mu przejść przez mnie i kiedy odejdzie, odwrócę się i spojrzę na jego ślad. Tam, gdzie strach przeszedł, nic już nie będzie.*

Czyżby sztuczna inteligencja sugerowała, że nasze obawy są rzeczywiste ale powinniśmy zachować zimną krew?

Postęp i wyzwania związane z budową komputerów kwantowych

Autor: dr Anna Kamińska
Creotech Instruments S.A.

Działanie komputerów kwantowych opiera się na zjawiskach fizycznych na poziomie właściwości i oddziaływań pojedynczych atomów, jonów, cząstek czy nano-obwodów elektrycznych. Budowa komputerów kwantowych jest więc dużym wyzwaniem. Warto zdawać sobie sprawę, że istniejące obecnie komputery kwantowe są na bardzo niskim poziomie gotowości technologicznej i daleko im do demonstracji pełni możliwości docelowych maszyn, które mamy nadzieję zbudować. W szczególności, rozważane są jeszcze liczne podejścia technologiczne do budowy procesorów kwantowych, opierające się na różnych typach kwantowych bitów – kubitów. Główne rozwijane obecnie rodzaje kubitów to:

- Kubity nadprzewodzące, bazujące na miniaturowych obwodach elektrycznych
- Spułapkowane jony
- Zimne atomy
- Fotony
- Defekty w diamencie
- Kubity krzemowe (bazujące na kropkach kwantowych lub defektach)
- Kubity topologiczne.

Rozwijane są również różne rodzaje komputerów kwantowych:

- Uniwersalne, bazujące na zestawie bramek pozwalających na implementację dowolnych algorytmów

- Specyficzne dla konkretnego zastosowania (np. Boson Sampling)
- Symulatory
- Quantum annealer – wyżarzacze kwantowe, tworzone na potrzeby rozwiązywania problemów optymalizacyjnych mapowanych bezpośrednio na kubity, bazujące na poszukiwaniu minimum energetycznego

Najbardziej intensywne prace odbywają się w kierunku uniwersalnych komputerów kwantowych, czyli takich, które wspierają pełen zestaw podstawowych operacji logicznych – bramek kwantowych – pozwalający na wykonanie dowolnego algorytmu. Komputery takie mają bardzo duży potencjał przełomowych zastosowań w przyszłości. Główne przewidywane zastosowania obejmują usprawnienie rozwiązywania problemów optymalizacyjnych, Monte Carlo oraz machine learning, a także generację liczb losowych. Przy odpowiednio dużej dostępnej ilości kubitów, zaimplementowanej korekcji błędów, odpowiedniej szybkości wykonywania bramek oraz „czasie życia" procesora przewiduje się uzyskanie możliwości rozwiązywania problemów niedostępnych dla nawet największych istniejących obecnie superkomputerów. Wśród najczęściej wymienianych obszarów zastosowań znajdują się m.in. optymalizacja procesu produkcji nawozów azotowych, wsparcie projektowania lepszych baterii, materiałów i leków, a także zastosowania w sektorze finansowym w optymalizacji portfela i predykcjach finansowych. Warto też pamiętać o możliwym zastosowaniu komputerów kwantowych w łamaniu protokołów bezpiecznej komunikacji, np. RSA. W najbliższym czasie niedoskonałe komputery kwantowe będą służyć zapewne jako narzędzie naukowe oraz platforma do rozwijania nowych algorytmów obliczeniowych. Pomimo, że ogłoszone zostało już jakiś czas temu osiągnięcie tzw. "quantum supremacy", czyli przewagi komputera kwantowego nad klasycznym (na 54 kubitowym procesorze Sycamore Google), nie wykazano jeszcze żadnej przewagi komputerów kwantowych w jakichkolwiek praktycznie „użytecznych" zastosowaniach – komercyjnych bądź́ naukowych...

Niewykluczone, że w najbliższej przyszłości najszybciej zastosowanie znajdą inne typy procesorów kwantowych, zbudowane na potrzeby rozwiązywania tylko konkretnego typu problemów. Szczególnie obiecującym przykładem są symulatory kwantowe, na których strukturze próbuje się odwzorować właściwości kwantowe cząsteczek i lepiej zrozumieć efekty kwantowe. Takie symulatory jako narzędzia badawcze kwantowego „świata" mogą pomóc w rozwoju nowych materiałów lub leków, a także przyczynić się do postępu w chemii, biologii i medycynie.

Jeśli chodzi o rozwój uniwersalnych komputerów kwantowych, można powiedzieć, że jesteśmy na etapie pierwszych niedoskonałych prototypów takich urządzeń, o bardzo ograniczonych możliwościach. Główne problemy obecnych komputerów kwantowych są następujące:

- Mała ilość kubitów – największym komercyjnie dostępnym procesorem (na początku 2023) roku jest Eagle firmy IBM, bazujący na nadprzewodzących kubitach, z 127 kubitami. Firma ta przewiduje osiągnięcie ~1000 kubitów w 2023 roku.
- Ograniczony czas koherencji kubitów, co przy braku „podręcznej" pamięci kwantowej ogranicza dostępny czas wykonywania operacji na procesorze kwantowym. Obecnie najdłuższy czas koherencji liczony w setkach sekund mają komputery bazujące na spułapkowanych jonach. Procesory bazujące na nadprzewodzących kubitach mają czas koherencji rzędu 10-100 mikrosekund.
- Błędy – każda operacja w procesorze kwantowym (przygotowanie stanów, wykonanie bramki kwantowej, odczyt) obarczona jest zauważalnym błędem, typowo od jednego do kilku procent. Najlepszej „jakości" są obecnie bramki w komputerach bazujących na spułapkowanych jonach, gdzie można uzyskać błędy na poziomie ułamków procenta. Tymniemniej,

wraz z długością algorytmu, błędy się kumulują, a obecne komputery kwantowe są jeszcze zbyt niedoskonałe by móc wdrożyć na nich algorytmy korekcji błędów.

Na obecnym etapie rozwoju komputerów kwantowych o bardzo ograniczonych możliwościach stosuje się tzw. podejście NISQ (Noisy Intermediate-Scale Quantum Computing), które skupia się na maksymalnym wykorzystaniu małych procesorów („Intermediate-Scale": 50-100 kubitów) bez korekcji błędów („Noisy"). Podejście to oparte jest o wykorzystanie krótkich algorytmów kwantowych (na tyle krótkich, by błędy nie zniszczyły kompletnie wiarygodności końcowego wyniku), dopasowanych do konkretnych zastosowań. Obiecującą ścieżką rozwoju są algorytmy hybrydowe, w których komputer kwantowy stosowany jest jako koprocesor dla komputera klasycznego, a algorytm wykonywany jest w pętli „sprzężenia zwrotnego" między procesorem klasycznym a kwantowym. Pozwoli to potencjalnie na wykorzystanie przewag komputera kwantowego tam, gdzie jest to wykonalne przy użyciu krótkich algorytmów, przy wsparciu komputera klasycznego.

Aby zrozumieć lepiej, dlaczego budowa komputerów kwantowych jest w praktyce tak trudna, warto rozważyć konkretny przykład jednej z wiodących technologii kubitów. Tutaj skupimy się na komputerze kwantowym opartym na spułapkowanych jonach. Kubity w takim komputerze bazują na stanach kwantowych jonów, które utrzymywane są w próżni, w polu elektrycznym w pułapce jonowej (najczęściej stosowana jest pułapka Paula). Zaletą takiego wyboru kubitów jest najdłuższy osiągalny obecnie czas koherencji, niski poziom błędów w porównaniu do innych technologii oraz łatwość uzyskiwania stanów splątanych – w szczególności w komputerach tego typu można z reguły wykonywać bramki dwu- i wielokubitowe pomiędzy dowolnie wybranymi kubitami, co jest niemożliwe w obecnych komputerach z kubitami

nadprzewodzącymi. Dodatkową zaletą komputerów opartych o spułapkowane jony jest możliwość wykorzystania niektórych technologii opracowanych na potrzeby zegarów atomowych oraz możliwa praca w temperaturze pokojowej. Wadą tego podejścia technologicznego jest relatywnie długi (w porównaniu do innych typów procesorów), mikrosekundowy czas wykonywania bramek czy odczytu oraz konieczność wykorzystywania różnych typów komponentów, zarówno elektronicznych, jak i optoelektronicznych i optycznych, przy budowie procesora. Komercyjnie dostępne komputery kwantowe bazujące na spułapkowanych jonach oferowane są m.in. przez IonQ (USA), 23 kubity, Quantinuum (Honeywell + Cambridge Quantum, USA+UK), 20-kubitów, AQT (Austria), 20-kubitów.

Komputer kwantowy bazujący na jonach, oprócz wspomnianej wcześniej pułapki jonowej w komorze próżniowej, wykorzystuje duży zestaw laserów stosowanych w procesie chłodzenia i pułapkowania jonów, a także w trakcie wykonywania bramek kwantowych i odczytu stanu kubitów. Do odczytu stanu kubitów dodatkowo potrzebne są dedykowane detektory, najczęściej używana jest w tej funkcji specjalistyczna kamera. W pracy komputera często stosuje się również pole magnetyczne. Ciekawym i ważnym do zrozumienia praktycznych wyzwań w budowie komputerów kwantowych aspektem jest to, że komputer kwantowy bazujący na spułapkowanych jonach wymaga dużej ilości zaawansowanej klasycznej elektroniki do sterowania wszystkimi wymienionymi powyżej elementami procesora kwantowego uraz do kontroli i utrzymywania optymalnych warunków pracy. Kontrola pułapki jonowej, stabilizacja, modulacja i kontrola laserów, tworzenie i modyfikacja sekwencji impulsów laserowych, odczytów kamery i zmiany parametrów pułapki – wszystko to wykonywane jest za pomocą specjalistycznej elektroniki. W związku z tak różnorodnymi wymaganiami sprzętowymi, budowa komputerów kwantowych jest ciekawym

wyzwaniem inżynieryjnym. Główne obecne wymagania względem elektroniki dla komputerów bazujących na spułapkowanych jonach są następujące:

- Szybka reakcja systemu kontrolnego (mikrosekundy)
- Precyzyjna synchronizacja czasu (nanosekundy)
- Niski poziom szumów i zakłóceń
- Obsługa dużej ilości sygnałów jednocześnie.

W związku ze zidentyfikowaną potrzebą przeniesienia kontroli procesora kwantowego na ultra-szybkie procesory FPGA oraz moduły obsługujące liczne sygnały analogowe i cyfrowe, kilka lat temu powstał nadal rozwijający się otwarty ekosystem sprzętowo-programistyczny Sinara / ARTIQ. Był on inicjatywą dużej grupy instytutów badawczych. Oprogramowanie opracowane zostało przez firmy Quartiq i M-Labs, natomiast prawie wszystkie projekty elektroniki tego ekosystemu wykonane były w Polsce, przez inżynierów z Politechniki Warszawskiej oraz firmy Creotech Instruments S.A.

W najbliższej przyszłości czekają nas kolejne liczne wyzwania związane z budową coraz lepszych komputerów kwantowych. Niezbędna jest:

- Lepsza integracja elektroniki z procesorem kwantowym w celu skrócenia czasu reakcji systemu kontroli kubitów
- Dla komputerów opartych na jonach - implementacja elementów elektroniki kontrolnej przy samej pułapce jonowej, w próżni i – docelowo - niskiej temperaturze
- Lepsze zrozumienie źródeł zakłóceń i maksymalna ich eliminacja
- Zwiększenie ilości kubitów – wdrożenie nowych rodzajów pułapek jonowych, skalowalna obsługa coraz większej liczby sygnałów
- Implementacja protokołów korekcji błędów

- Integracja komputerów kwantowych z klasycznymi superkomputerami (algorytmy hybrydowe)
- Wdrożenie pamięci kwantowych.

Pomimo licznych wyzwań, istnieje ugruntowana koncepcja ścieżki technologicznej, która powinna pozwolić w najbliższych latach znacząco zwiększyć liczbę kubitów w komputerach kwantowych i docelowo pozwolić na implementację algorytmów korekcji błędów. W programie naukowym Komisji Europejskiej, w ramach tzw. Quantum Flagship, zakłada się zbudowanie procesora 100-kubitowego w 2025 roku, a następnie 1000-kubitowego do roku 2029. Warto wspomnieć, że w projekcie na budowę „dużego" komputera kwantowego opartego na spułapkowanych jonach, od strony elektroniki kontrolnej, bierze udział polskie przedsiębiorstwo Creotech Instruments S.A. Na gruncie polskim, w Poznaniu, w Poznańskim Centrum Superkomputerowo-Sieciowym afiliowanym przy Instytucie Chemii Bioorganicznej PAN, umieszczony zostanie w ramach programu EuroHPC JU 20-kubitowy komputer kwantowy i nastąpi jego integracja z lokalnym superkomputerem. Z zasobów komputera kwantowego będzie można powszechnie korzystać w celach naukowych, aby rozwijać umiejętności posługiwania się tymi nowymi maszynami oraz tworzyć nowe algorytmy.

IBM Quantum Computing – przyszłość, możliwości, bezpieczeństwo

Autor: dr Piotr Biskupski
IBM

Świat nowoczesnego przetwarzania danych bardzo mocno skupia się w ostatnim czasie na doniesieniach o budowie nowych komputerów kwantowych, o zwiększeniu ich dostępności dla wszystkich chętnych. Jednakże zbudowanie urządzenia, które będzie potrafiło uchwycić całe piękno fenomenów mechaniki kwantowej okazuje się jednym z najtrudniejszych problemów naszych czasów – a wręcz wydaje się niemożliwe. Nie powstrzymuje to jednak firm, których celem jest zmiana paradygmatu obliczeniowego i wprowadzenie komputerów kwantowych do użytku codziennego, tak wszyscy chcą zbudować największy możliwy superkomputer kwantowy. W przyszłości komputer ten pozwoli wypełnić lukę tam, gdzie klasyczne komputery nie są w stanie osiągnąć odpowiedniej szybkości przetwarzania, a przez to ograniczają możliwość rozwoju rewolucyjnego podejścia do obliczeń w różnych gałęziach przemysłu powstrzymując rewolucje w prowadzeniu biznesu.

Firma IBM niedawno ogłosiła najnowszy plan rozwoju, który przeniesie nas z czasu zaszumionych, niewielkich urządzeń do systemów w których będziemy wykorzystać potencjał drzemiący w ponad milionie kubitów. Zespoły IBM Research pracują aktualnie nad procesorami skalowalnymi procesorami, w których w 2023 dostępne będzie ponad tysiąc nadprzewodnikowych qubitów, nazwa kodowa IBM Quantum Condor, który będzie początkiem rewolucji związane z ze skalowaniem QPU.

Jednakże aby móc zbudować jeszcze większe systemy (o wiele większe niż IBM Quantum Condor należy zbudować największą komorę chłodzącą na świecie. Co warto podkreślić systemy te będą ogólnodostępne w ramach IBM Cloud czyli

maszyny te nadal będzie można programować przy użyciu pakietu oprogramowania IBM Quantum Experience oraz Qiskit.

Zespół IBM Quantum buduje kolejne kwantowe procesory, które wykorzystują fenomeny mechaniki kwantowej w których reprezentujemy dane przy użyciu elektronicznych stanów kwantowych sztucznych atomów znanych jako nadprzewodnikowe kubity transmonowe, które są połączone i kontrolowane przez sekwencje impulsów mikrofalowych. W wyniku oddziaływania z zewnętrznym światem qubity szybko tracą informację o swoich stanach kwantowych. Dlatego też największym wyzwaniem stojącym dziś przed zespołami budującymi takie procesowy jest znalezienie sposobu sterowania dużymi systemami tych qubitów przez odpowiednio długi czas z jednoczesnym ograniczeniem błędów. Pozwoli to w przyszłości uruchomić złożone układy kwantowe wymagane przez przyszłe aplikacje kwantowe.

IBM bada nadprzewodnikowe qubity od połowy lat 2000., zwiększając czas koherencji i zmniejszając liczbę błędów. Na początku 2010 roku uruchomiono pierwsze urządzenia wielokanałowe. Ciągłe udoskonalenia i postępy na każdym poziomie systemu od qubitów do kompilatora pozwoliły nam na umieszczenie pierwszego komputera kwantowego w chmurze w 2016 roku. Obecnie utrzymujemy ponad dwadzieścia cztery stabilne systemy w chmurze IBM Cloud dostępne nie tylko dla naszych klientów, ale również dla ogółu. W ramach tych systemów możliwe są eksperymenty na 5-kwubitowych procesory IBM Quantum Canary i 27-kwubitowych procesory IBM Quantum Falcon.

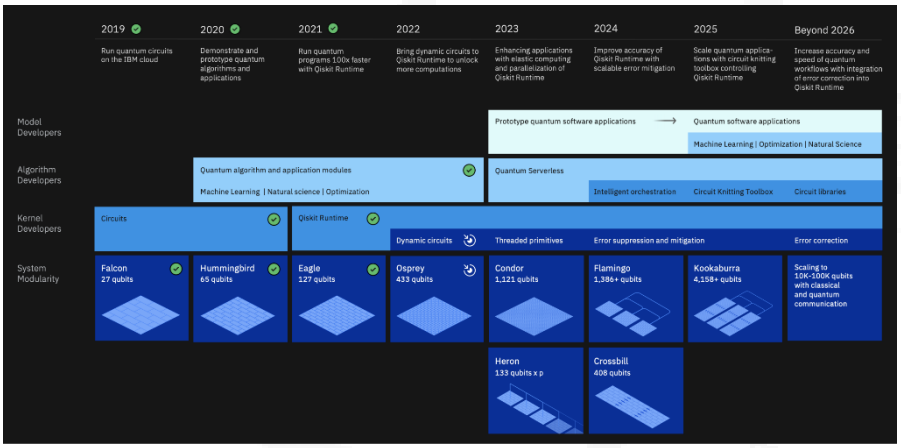
Co istotne niedawno na jednym z naszych układów udało się osiągnąć wystarczająco długi układ kwantowy, aby zadeklarować kwantowy wolumen 64. Udało się to osiągnąć dzięki wprowadzeniu ulepszeń kompilatora i udoskonaleniu kalibracji bramek przy jednoczesnej redukcji szumów

Równolegle do naszych wysiłków zmierzających do ulepszenia dostępnych w chmurze IBM urządzeń, firma IBM skupia się na stworzeniu coraz większych skalowalnych urządzeń. W tym miesiącu członkowie sieci IBM Quantum Network zostali zaskoczeni, gdyż po cichu udostępniliśmy nasz 65-qubitowy procesor IBM Quantum Hummingbird. Urządzenie to posiada funkcję multipleksowania odczytu 8:1, co oznacza, że łączymy sygnały odczytowe z ośmiu qubitów w jeden, zmniejszając całkowitą ilość okablowania i komponentów potrzebnych do odczytu i poprawiając naszą zdolność do skalowania, zachowując jednocześnie wszystkie wysokowydajne funkcje z procesorów generacji Falcon. Znacznie skróciliśmy czas opóźnienia przetwarzania sygnału w powiązanym systemie sterowania w ramach przygotowań do nadchodzących możliwości systemu sprzężenia zwrotnego i zasilania, gdzie będziemy w stanie kontrolować qubity w oparciu o klasyczne warunki podczas pracy układu kwantowego.

Jak już zostało to niedawno ogłoszone w przyszłym roku zadebiutujemy naszym 127-kubitowym procesorem IBM Quantum Eagle. Eagle posiada kilka ulepszeń, które mają na celu przekroczenie 100-qubitowej granicy. Co najważniejsze nie jest to tylko osiągnięcie tej liczby kubitów ale również kolejne techniczne zmiany mające na celu zwiększenie gęstości sygnałów a co za tym idzie zwiększenie upakowania układu z jednoczesnym zmniejszeniem ilości błędów.

Zasady projektowania ustalone dla mniejszych procesorów kwantowych firmy IBM są bazą dla zaprojektowanego systemu którego dostępność planuje się na 2022 rok. Nazwa kodowa systemu brzmi IBM Quantum Osprey 433-qubit. System będzie wykorzystywał ulepszony system chłodzenia, oraz architekturę bazująca na ograniczeniu błędów wynikających ze zbyt dużej ilości kubitów.

W 2023 roku planowany jest debiut systemu zbudowanego z 1,121-kubitów, procesorem IBM Quantum Condor. Według mnie Condor będzie punktem zwrotnym w QC i potencjalnie może prowadzić do osiągnięcia przewagi obliczeniowej Quantum Advantages – i niektóre problemy będziemy mogli rozwiązać wydajniej na komputerze kwantowym niż na najlepszych superkomputerach na świecie.



Ciekawostka :

W tym roku zespół IBM uruchomił superchłodziarkę o wielkości około 3x2 metry o nazwie kodowej "Goldeneye", czyli wielokrotnie większą niż jakakolwiek obecnie dostępna na rynku. Zespół IBM Research zaprojektował tę chłodziarkę z myślą o systemie z ponad milionem kubitów pozwalającym na intranetowe połączenie z innymi procesorami i stworzenie klastra obliczeniowego, który pozwoli zmienić całkowicie nasze podejście do obliczeń.

Sama mapa drogowa i osiągnięcie w 2023 roku ponad 1000 qubitów jest bardzo ambitna, uznano jednak , że nie tylko zwiększanie ilości kubitów pozwolić może na osiągniecie przewagi obliczeniowej, dlatego warto zauważyć pięć elementów które pozwolić mogą na tak dynamiczne zwiększenie mocy.

Upubliczniając swoją mapę drogową, IBM zobowiązuje się do spełnienia szeregu agresywnych benchmarków, które pomogą firmie utrzymać pozycję lidera w dziedzinie obliczeń kwantowych i wprowadzić klientów na drogę do przełomowych osiągnięć.

IBM Quantum Safe Cryptography - CRYSTALS

Jako pionier technologiczny IBM Research, firma oferuje wsparcie kryptografii odpornej na ataki z wykorzystaniem technologii kwantowej. Co najważniejsze jest to ogólnodostępne w ramach chmury obliczeniowej, która pozwala na zarządzanie kluczami i transakcjami aplikacjach w IBM Cloud®. Pokazuje to najbardziej holistyczne w branży podejście do zabezpieczania danych za pomocą opracowanych w ramach IBM Research algorytmów kryptografii kwantowej Cryptographic Suite for Algebraic Lattices" (CRYSTALS), który obejmuje dwa prymitywy kryptograficzne: Kyber, bezpieczny mechanizm enkapsulacji klucza (KEM) IND-CCA2; oraz Dilithium, silnie bezpieczny algorytm podpisu cyfrowego EUF-CMA. Oba algorytmy są oparte na trudnych problemach na kratach modułowych, są zaprojektowane tak, aby wytrzymać ataki przeprowadzane z wykorzystaniem komputerów kwantowych i zostały zgłoszone do projektu NIST dotyczącego kryptografii postkwantowej.

Nowe możliwości obejmują:

- Wsparcie dla kryptografii bezpiecznej kwantowo: Dzięki wykorzystaniu otwartych standardów i technologii open source usługa ta udoskonala standardy wykorzystywane do przesyłania danych między przedsiębiorstwem a chmurą, pomagając

zabezpieczyć dane dzięki zastosowaniu algorytm bezpiecznego kwantowo.

- Rozszerzone usługi IBM Cloud Hyper Protect Crypto: Dostępne są nowe możliwości zwiększania prywatności danych w aplikacjach chmurowych, w których dane przesyłane przez sieć do aplikacji chmurowych oraz wrażliwe elementy danych, takie jak numery kart kredytowych, są przechowywane w bazie danych, która może być szyfrowana na poziomie aplikacji - wspierane przez najwyższy w branży poziom ochrony szyfrowania kluczy kryptograficznych z możliwością "Keep Your Own Key" (KYOK).
- Szyfrowanie Homomorficzne - FHE to nowa i zaawansowana technologia szyfrowania, która pozwala na zachowanie poufności danych nawet podczas ich przetwarzania, potencjalnie wypełniając tę krytyczną lukę w obecnie stosowanych rozwiązaniach chmurowych.

Zwiększając swoje zaangażowanie w kwestie bezpieczeństwa i zgodności, IBM kontynuuje współpracę z partnerami branżowymi w celu osiągnięcia dalszych kroków w inicjatywach standaryzacyjnych. Na przykład najlepsze praktyki w zakresie bezpieczeństwa w chmurze IBM są obecnie dostępne jako wzorzec Center for Internet Security (CIS) Foundations dla IBM Cloud, a kryptografowie z IBM Research mają kluczowy wkład w algorytmy QSC, które znalazły się na krótkiej liście w Narodowym Instytucie Standardów i Technologii (NIST).