Kiss Károly

Közeleg a kvantum-kompjúterek korszaka

Az SNDL és a poszt-kvantum kriptográfia[1]

Szakértők szerint a kvantum-kompjúterek 2030-ra lesznek üzemképesek, ami azt jelenti, hogy akkortól kezdve e gépek képesek lesznek minden kódolást megfejteni. A kíbertér bűnözői és adattolvajai erre szisztematikusan készülnek: gyűjtik és lopják az adatokat, hogy majd annak idején a kvantumkompjúterekkel megfejtsék. Ez nevezik SNDL-nek: store now, decript later – gyűjtsd be most és fejtsd meg később.)

A hivatalos oldal erre pedig kvantum-rezisztens kriptográfiai módszerek kidolgozásával készül: PQC, post quantum criptography.

A feladat hihetetlenül nagy. 2030-ra több, mint 20 milliárd eszköz védelmét kell megoldani: minden mobiltelefonét, laptopét, ipad-ét, szerverét, weboldalét, mobil-applikációét. Plusz mindazokat a rendszereket is fel kell majd frissíteni, melyeket autókba, hajókba, repülőgépekbe és az operációs infrastruktúrába építettek be.

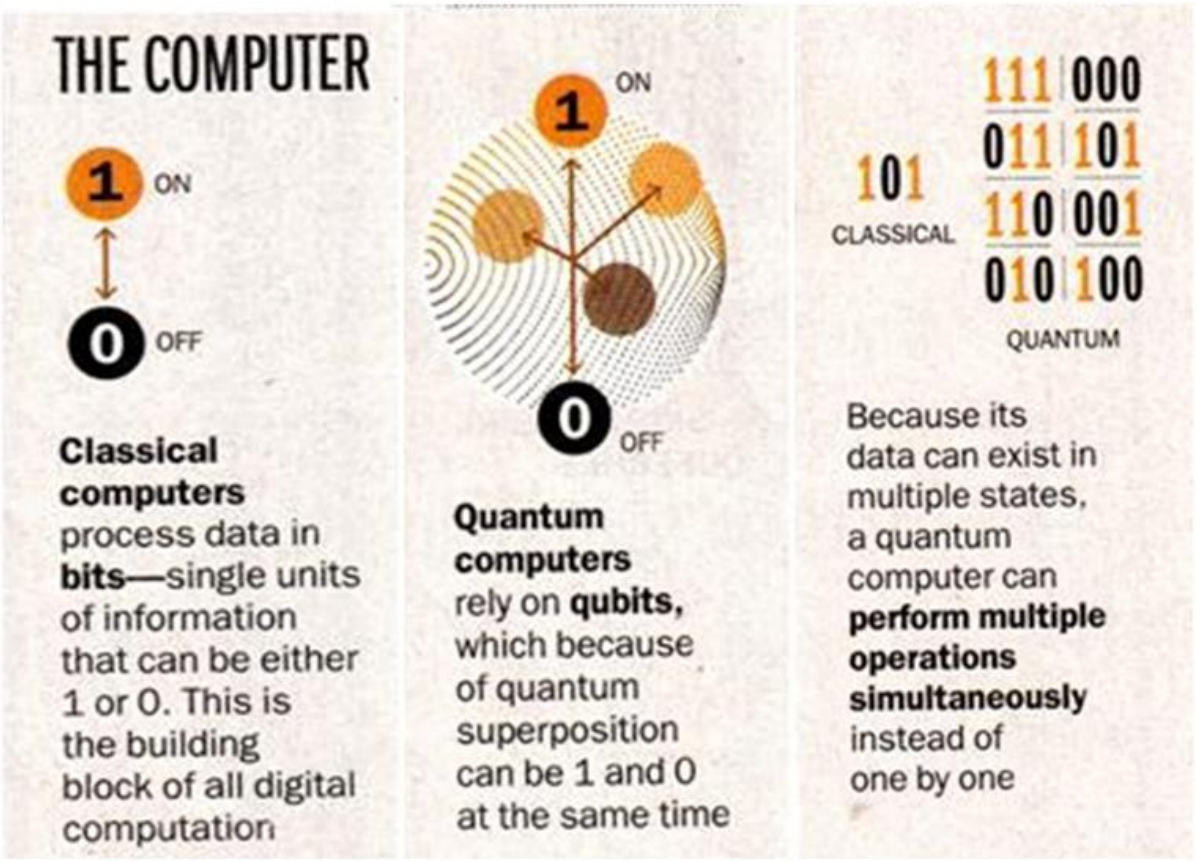
Működési elv

Ez az, amit egyszerű halandók nem érthetnek meg (beleértve e sorok íróját is, aki amatőr a témában). A kvantumfizika alapja a szuperpozíció és a kvantumos összefonódás. E fogalmak az elektronok helyzetére és viszonyára vonatkoznak, melyek bonyolult kémiai reakciók során szinte átláthatatlanok. E pozíciók megszámlálhatatlan sokasága és variációja ad lehetőséget a bitek elhelyezésének és az azokkal való műveleteknek.[2] „A kvantum kompjúterek a kvantumfizika vad, valószínűségi, egyidejűleg itt és ott furcsaságait titkokat feltörő eleganciává varázsolják.”[3]

A tradicionális kompjúterek működése a bináris biteken alapul, melyek az 1 vagy a 0 állapotában létezhetnek, és ezt használják fel az információ feldolgozására. A qubit-ek, a quantum számítás alapjai parányi szubatomi részecskék, melyek egyidejűleg mindkét állapotban létezhetnek. „Ez az ugrás a duálistól a multivariáns adatfeldolgozásig exponenciálisan megnöveli a számítási kapacitást.”[4] A kvantum-kompjúter jobban tükrözi a természetben lejátszódó folyamatokat, jobban megfelel azoknak. A molekulák atomokból

[1] The Economist: The World Ahead 2023**.**
[2] Egy ehhez képest kevésbé bonyolult módja az információtárolásnak és a számításnak, amikor a DNS génjeit használják fel ugyanerre a célra. (De mint elméleti lehetőség, szóba került az elektronok spin-jének a felhasználása is információtárolás céljából.)
[3] The Economist July 16th 2022.
[4] Time February 13d 2023, 2030 / Technology.

állnak, melyeket elektronok kapcsolnak össze, és ez elektronok egyszerre részei mindegyik atomnak. Az a mód, ahogy az elektronok egyszerre részei két atomnak, reprezentálja a kvantumkompjúter működési elvét. Az ötletet Richard Feynman egy 1981-ben tett kijelentésére vezetik vissza, miszerint „ha a természetet utánozni akarjuk, akkor azt kvantum-mechanikusan kell tenni”.[5]



Az IBM újra az élvonalban

Az IBM-nek több, mint 60 működő kvantumkompjútere van, és ez több, mint a világ összes többi ilyen eszköze együttvéve. Az utóbbi években az IBM lemaradt az Apple és a Microsoft mögött a felhőtechnikában, és nem ragadta meg a mesterséges intelligencia fejlesztésében rejlő lehetőségeket. De a kvantumkompjúterekkel most újból az élvonalban van. Legújabb fejlesztése a 433 qubites Osprey chip, a világ legnagyobb teljesítményű kvantum processzora, melynek a sebessége – ha hagyományos bitekben fejeznénk ki – messze meghaladná az ismert Univerzumban található összes atom számát.[6] (Az IBM tervei közt szerepel egy 1.121 qubites chip megépítése az idén, majd 2025-ben a 4.000 qubites sebesség túlszárnyalása, „moduláris kvantum áramkörök” létrehozásával.

[5] The Economist September 26th 2020.
[6] Time February 13d, 2023, 2030 / Techology (Őszintén szólva fogalmam sincs, a számítási sebesség hogyan fejezhető ki az atomok számával. KK)

Mire használható?

Amit régóta tudunk; hogy a kvantumkompjúterek megjelenése után nem lesz biztonsági kód, amit ne tudnának feltörni. De mi másra használhatók? A szó szoros értelmében mindenre, ahol nagy adathalmazra támaszkodva optimalizálni kell. A világtengereket átszelő tankerek útjának optimalizálására, annak eldöntésére, hogy egy intenzív osztály betegei közül melyik szorul a legsürgősebb ápolásra, új anyagok létrehozására az atomi szintű vegyi folyamatok ismeretének felhasználásával, a mesterséges intelligencia ellenőrzésére, az önvezető autók és repülő drónok algoritmusának a tökéletesítésére, alapkezelő vállalatok működtetésére, valutaspekulációra, a MI egy újfajta „deep learning"-jének a kialakítására, adatfeldolgozáásra, a járművek hosszadalmas tervezési folyamatának a lerövidítésére, ipari kísérletek eredményének a megelőlegezésére, stb. stb. „Ez a technológia a soron következő ipari forradalom."[7]

Első látásra úgy tűnik, hogy a kvantum-kompjúterek hasonló feladatok ellátására lesznek képesek, mint a mesterséges intelligencia: bonyolult szellemi feladatok megoldására.

Fejlesztési kiadások

2020-ban globálisan 412 millió dollár állt az iparág rendelkezésére. 2027-ben becslések szerint 8,6 md dollárral rendelkezik majd a szektor. Ma már 17 országnak van kvantum-stratégiája, és négy továbbiban kidolgozás alatt áll. A '80-as évek közepe óta Kína – becslések szerint – 25 milliárd dollárt (!) fordított kvantumszámítási kutatásokra. (2021-ben még a kínaiak álltak az élen 56 qubites számítógépükkel.) Ötéves tervükben e fejlesztések prioritást élveznek.

Az amerikai kormány e területet a gazdaságra és a nemzetbiztonságra nézve súlyos veszélyeket hordozónak tekinti és minden kormányzati szinten kiemelten kezeli. Becslések szerint Amerikának 1 billió (ezer milliárd) dollár nagyságrendű összeget kellene fordítania a jövendő „kvantum-fenyegetés" elhárítására. A program a Manhattan tervet idézi.

A World Economic Forum szerint 2022-ben a világ több, mint 30 md dollárt költött kvantum-fejlesztésre; ennek durván a felét a kínaiak, a negyedét az EU, Amerika pedig 1,2 milliárdot (szemben a szükségesnek tartott ezer milliárddal).

Kína gazdasági helyzetét évek óta tanulmányozom, igyekszem lépést tartani az ottani fejleményekkel. Az általános szakmai felfogással szemben – miszerint Kína a gazdaságban és a tudományban megközelíti Amerikát, de hátrányának ledolgozása még jó ideig eltart – az a véleményem, hogy az utólérés és a lehagyás sokkal hamarabb be fog következni a vártnál. Ennek beszédes bizonyítéka a most tárgyalt téma.

[7] Uott.

Kíber-biztonság

Ma gyakorlatilag a nagy nemzetközi platformok és okostelefon-szolgáltatók által alkalmazott kíber-biztonság az RSA rendszeren alapul (Asymmetric Criptography Algorithm). Egy mai átlagos kompjúternek évmilliárdokra lenne szüksége, hogy e kódokat feltörje. Egy gyors kvantumkompjúternek ehhez csak néhány órára lenne szüksége. Kínai kompjútertudósok tavaly év végén azt jelentették, hogy egy 372 qubites kvantumkompjúterrel sikerült feltörniük az RSA rendszert.

Az új technológia egy új elemet is visz a kompjúterizáció világába: ***bizalom*** szükségeltetik hozzá! A hagyományos kompjútereink által produkált eredményeknek ugyanis még kézi számítással utána tudunk járni. A kvantumkompjúterek korában erre már nem lesz lehetőség, hinni kell az eredményben.

Bp, 2023 május

Források:

Time, February 13, 2023. 2030 / Technology: The Quantum Leap (Leslie Dickstein)
The Economist: The World Ahead 2023
The Economist July 16th 2022: Cryptography. Post-quantum solace.
The Economist September 26th 2020. Quantum computing. From cloisters to the cloud.
Asbóth János: Szuper a pozíció. Magyar Nemzet 2023 márc. 25. (Eötvös Z.)