Nagy Zoltán András

KVANTUMSZÁMÍTÓGÉPEK ÉS A KIBERBIZTONSÁG
BEVEZETÉS A KVANTUMVILÁGBA

A számítástechnikai rendszerek és az ott kezelt adatok védelme elvitathatatlanul napjaink egyik legfontosabb feladata, követelménye. Az információ ellen irányuló támadások megelőzéséhez az informatikai rendszer magas fokú fizikai, személyi, logikai védelme mellett a támadások felismerése és az azokra adott válaszlépések azonnalisága is elvárt követelmény.[1]

A KIBERBIZTONSÁGOT FENYEGETŐ „HAGYOMÁNYOS" VESZÉLYEKRŐL

Az informatikai és az információvédelem folyamatos fejlesztése, ideértve a fizikai, logikai, humán védelmet egyaránt, az egyre kiterjedtebb és szofisztikáltabb támadások miatt elvitathatalanul szükséges. Lássunk néhány már ismert támadási formát! Ilyen az informatikai rendszerhez többféle technikával végrehajtható jogosulatlan hozzáférés (*hacking*, azaz „elektronikus betörés"), amely fenyegeti a rendszer működését, így például kódtörő programokkal vagy *brute force*-szal (nyers erővel – a jelszó próbálgatásaival).

A *social engineering* körébe tartozik a színlelt vagy valódi bizalmi, érzelmi viszony kihasználásával történő adatszerzés, a másik személy jelszavainak,

[1] Megkülönböztetünk informatikai és információ-, ezen belül adatvédelmet. Az informatikai védelem az abban kezelt adatok/információk védelmén túl az erre szolgáló technikai rendszer védelmét jelenti. Ennek részei az informatikai hálózatok, eszközök (számítógépek, perifériák, ezek mobil formában is stb.). A védelem alappillérei a fizikai, személyi, logikai. Az információvédelem azon adatokra terjed ki, amelyek valamilyen tartalommal rendelkeznek, és tartalmukat írásban, kép-, videófelvételen rögzítették, továbbá szóban közölve kommunikációs, informatikai és egyéb elektronikus rendszerekben, vagy bármilyen más módon kezelnek. Az információvédelmen belül az adatvédelem a személyes adatok védelmére szűkül.

DOI: https://doi.org/10.36250/01279_38 · ORCID: https://orcid.org/0000-0002-6888-9059

azonosítóinak, bankszámlaszámainak, PIN-kódjainak megismerése. Egyre elterjedtebb a semmiféle technikai tudást nem igénylő, viszont ötletességet kívánó, különféle céllal és tartalommal elküldött megtévesztő elektronikus levél:

- hamis, nem létező e-mail-címről vagy a valódi e-mail-címről, de nem a tulajdonostól származó, jellemzően megtévesztő tartalommal a felhasználó adatait célozzák meg, vagy zaklató, fenyegető, zsaroló stb. üzenetet küldenek;
- a szigonyozó levelek *(spear fishing)* azon célzott felhasználókat „szigonyozzák", akik a vállalkozásról, intézményről stb. érzékeny adatokkal (pénzügyi, személyzeti, fejlesztési stb.) rendelkeznek, azokkal dolgoznak;
- befektetésre, pénzutalásra felhívó csalárd e-mailek (*Business E-mail Compromise*, BEC);
- a legkülönfélébb tartalommal érkezhetnek olyan csalárd e-mailek, amelyek színlelik a munkahelyi vezetőt vagy főhatóságot (CEO-levelek);
- a vállalati/intézményi magasabb vezetőkhöz csalási célzattal küldött e-mailek *(whaling)* befektetést kínálnak, banki ajánlatot tesznek, számlavezető bank váltását javasolják.

Intézményeket, vállalkozásokat veszélyeztető támadástípus a terheléses (túlterheléses) támadás, továbbá az ezzel történő fenyegetés, zsarolás. E támadásfajta végrehajtásához egy botnet- (a *robot network* rövidítése) vírusra van szükség, amely a vírus által megfertőzött számítógépeket egy hálózatba köti össze. Ezzel a hálózatot irányító az „uralma alatt" levő számítógépekkel egy időben rengeteg kérést küld a megcélzott szerverek felé. Ezt a hívásmennyiséget a szerver nem képes kezelni, ami a szerver lelassulásához, elérhetetlenségéhez vezet. A túlterheléses támadással való fenyegetés alkalmas váltságdíj követelésére is. Más a motivációja az úgynevezett „cselédbosszúként" *(maid revenge)* emlegetett támadásnak, amikor az elégedetlen, kollégáival konfliktusba került, elbocsátott dolgozó bosszúból támadja volt munkahelyét, vagy kiszolgáltatja az általa ismert jelszavakat, egyéb információkat.

Természetesen a humán, a logikai és a fizikai védelem is része az informatikai rendszer általános védelmének, amelyek önmagukban biztonságtechnikai kérdések. A számítástechnikai rendszereket potenciálisan veszélyeztető támadások számbavétele szinte lehetetlen.

ÚJ VESZÉLYFORRÁS

Míg a kvantumfizika[2] 125 évre, addig a kvantumszámítógép megépítésének története mindössze néhány évtizedre tekint vissza. Szemben Newton klasszikus mechanikai axiómáival, Maxwell elektrodinamikai törvényével vagy Einstein relativitáselméletével, a kvantumfizikára vonatkozó, pláne azt összegző elmélet, tan nem fűzhető egyetlen tudós nevéhez sem. Matematikusok és fizikusok munkájának köszönhetően lépésről lépésre körvonalazódtak a kvantumvilágra vonatkozó megállapítások, megközelítések. E helyütt összefoglalóan, több forrásból építkezve tekintjük át azokat a történéseket, elméleteket, amelyek a kvantumvilághoz kapcsolódnak.[3]

A kvantumelméletet Max Planckkal szokták kezdeni, de magunk visszalépünk néhány évet. Henri Becquerel hívta fel a figyelmet az atomokat alkotó részecskék rejtélyére, amikor felfedezte az atomok spontán és kiszámíthatatlan sugárzását 1897-ben. Ezért a felfedezésért 1903-ban megosztott fizikai Nobel-díjat kapott Pierre és Marie Curie-vel. Madame Curie volt az, aki bebizonyította, hogy ez a sugárzás nem kémiai folyamat eredménye, hanem az atomban rejlő tulajdonság.

Visszatérve a fő mederhez Max Planck a 20. század fordulóján tartott előadásában felvetette, hogy az energia kvantált,[4] vagyis nem folyamatos, hanem diszkrét egységekben vagy „kvantumokban" jelenik meg. Planck elismerte, hogy a folyamatot maga sem értette meg.[5]

Tudósok tucatjai eredtek az atomi világ rejtélyének nyomába. Albert Einstein, Niels Bohr, Ernst Rutherford, Werner Heisenberg, Max Born, Erwin Schrödinger és mások megalkották a kvantumfizika alapvető elveit, szabályait, amelyek ismeretében egy olyan fantasztikus világba érkezünk, amelyben jórészt felednünk kell a newtoni fizika évszázados tanításait, törvényeit. Az atomok és

[2] Néhány leegyszerűsített definíció:
Kvantumfizika: a fizika azon ága, amely a mikroszkopikus világ viselkedését vizsgálja, írja le, szemben a newtoni törvényekkel, amelyek a makrovilág törvényszerűségeit írják le.
Kvantummechanika: a kvantumfizika matematikai leírása és törvényei, alapvető egyenlete: Schrödinger-egyenlet. Kísérleti eredményeken alapul.
Kvantumtechnológia: a kvantummechanika alkalmazása gyakorlati eszközökben és/vagy rendszerekben; alkalmazott tudomány, egyben a mérnöki fejlesztések területe.

[3] Sakurai–Napolitano 2010: 66; *Britannica Hungarica* 2013: 171; Zubairy 2020: 230; Rockenbauer 2020: 79; Chakraborty 2022: 18.

[4] A probléma lényege: miért melegít a villanykörte? Kvantálás: a folyamatnak, minőségnek stb. mennyiségi mutatókkal értelmezése; diszkrét: nem folyamatos, szakaszos.

[5] Geszty 2007: 15–46.

részecskék viselkedése nem írható le a makrovilágra alkalmazható klasszikus fizika törvényeivel (Newton, Maxwell stb.), a mikrovilágban a kvantummechanika szabályai érvényesek.

Mielőtt rátérnénk azon kvantummechanikai alapokra, amelyek a kvantumszámítógép létrehozásához szükségesek, idézzük ide a kiváló tudós, Richard Feynman véleményét a kvantumvilágról:

> „azt hiszem, nyugodtan állíthatom, hogy a kvantummechanikát senki sem érti. Ezért ne vegyék ezt az előadást túlságosan komolyan, s ne érezzék úgy, hogy meg kell érteniük valamilyen modellel mindazt, amiről beszélni fogok: inkább engedjék el magukat, s élvezzék gondtalanul, amit hallani fognak! El fogom mondani, hogy viselkedik a természet. Ha csak elfogadják, hogy ez lehetséges, máris gyönyörűségesnek és elbájolónak fogják találni."[6]

Nézzünk néhány meghökkentő tételt:

- Míg a makrovilágban egy objektum, tárgy egy adott időpillanatban csak egy konkrét állapotban, helyen létezik, addig a kvantumrészecskék egyszerre több állapotban lehetnek (van és nincs állapotban vannak egyszerre), és meghatározatlan helyen, ugyanis a kvantumrészecske helyzetét és impulzusát nem lehet egyidejűleg tetszőleges pontossággal meghatározni (Heisenberg határozatlansági tétele).
- A hullámrészecskének kettős jellemzője van, az elektronok hullámként és részecskeként is viselkedhetnek, a megfigyelés módjától függően.
- Két vagy több kvantumrészecske úgy kapcsolódhat össze, hogy állapotuk összefügg, földrajzi távolságtól függetlenül. Einstein „kísérteties kapcsolatnak" *(Spukhafte Fernwirkung, Spooky Connection)* nevezte ezt az összefüggést. Már születtek rá magyarázatok, de még vitatott a folyamat.
- A kvantummechanika nem determinisztikus, hanem csak valószínűségi hullámfüggvényként írható fel (Schrödinger tétele). Emlékezzünk a „Schrödinger macskája" elvi kísérletre (él vagy sem a dobozban a macska, mielőtt kinyitjuk a dobozt), amely a valóságban soha nem történt meg.

Heisenberg határozatlansági felfogásával szemben Einstein hittel vallotta, hogy Isten nem játszik kockajátékot, ez ellentmond a determinisztikus fizika

[6] Feynman 2005: 149.

törvényeinek. Egy másik kiváló tudós, Niels Bohr azzal vágott vissza, hogy „ne mond meg Istennek, hogy mit tegyen".

Tudomásul kell vennünk, hogy az atomi világban nem érvényesülnek a makrofizika törvényei. A természet a meghatározó, „ő az úr", és a természetben jellemzően a véletlenszerűség a törvény. Ennek elfogadásával közel kerülhetünk a világegyetem vagy saját sorsunk véletlenjeinek megértéséhez (születésünktől életünk különböző fázisain át a szakma, házasságtárs stb. választásáig stb.). Az, hogy a véletlen által adatott helyzettel hogyan él az emberiség vagy mi magunk, az már a mi jó vagy rossz döntésünk. Elismerve, hogy lehetnek a véletlenszerűséget másképp, mással, a transzcendenciával magyarázó („az alkotó pihen" – Madách) vagy éppen ezzel ellentétes vélemények, érvek.

Térjünk vissza a technológiai fejlődéshez! Az 1980-as években Richard Feynman egyik előadásában azon töprengett, hogyan lehet a kvantummechanikát szimulálni. Elegendő a mai számítógépek továbbfejlesztett változata, vagy egy új technológiában kell gondolkodnunk? David Deutsch és Józsa Richárd létrehozta az első kvantumalgoritmust, amellyel bizonyította a kvantumszámítás előnyeit. Lov Grover kvantumalgoritmusa a kvantumszámítógépek gyors keresési képességeit mutatta meg. Építőelemenként készült el a kvantumszámítógép elméleti modellje, majd a legnagyobb cégek, egyetemek nekifogtak a kvantumszámítógépek létrehozásának.

MIÉRT VESZÉLYES A KIBERBIZTONSÁGRA A KVANTUMSZÁMÍTÓGÉP?

A jelenleg használt számítógépek „lelke" a szilíciumalapú chip. Ma ezek a chipek miniatürizálásuk folytán a mobileszközök részei. A mai chipekre tranzisztorok tucatjait – a szó szoros értelmében – nyomtatják, avagy másik megoldásként a chipek méreteit csökkentik. Napjaink „világcsúcstartója" a 2 nanométer méretű chip.[7] Napjainkban a laptopokban, notebookokban, asztali számítógépekben multi-chip modulokat látunk, amelyek egyetlen „tokban" több chipet tartalmaznak. Az eszközök miniatürizálásának mindig van és lesz fizikai korlátja. Új utat kellett keresni az információk tárolására és feldolgozására.

7 IBM [é. n.].

Kezdjük onnan, hogy a hagyományos számítógép alapegysége az „1" *vagy* „0" jelpár, azaz van töltés vagy nincs töltés (nyitva vagy zárva vannak a tranzisztorok a chipeken). A kvantumszámítógép egészen más elvek szerint épül fel. Szintén a bit elnevezését alapul véve a kvantumkomputerek alapegysége a kvantumbit, röviden qubit. A *szuperpozíció* alapján a kvantumszámítógép alapegysége „1" *és* „0". Ez a kettősség csak akkor bomlik fel, és lesz „1" vagy „0", ha megmérjük, megtapasztaljuk, megnézzük a jelpárt (visszatérve a feldobott pénzérme hasonlatához: leesik a pénzérme, és vagy fej, vagy írás).[8] A qubit alapját kétállapotú kvantumrendszerek alkotják, ilyen például az elektron spinje, amely egyszerre lehet „fel" és „le" állapotban, vagy másik példaként a foton polarizációja lehet vízszintes és lehet függőleges stb.

A *kvantum-összefonódás* adja azt a lehetőséget, hogy a kvantumszámítógépek párhuzamosan sok-sok számítást képesek végezni egy időben. Egy qubit két műveletet, két qubit négy műveletet, három qubit nyolc műveletet egyszerre, azaz a kvantumalgoritmusok exponenciálisan gyorsabban képesek információt feldolgozni, mint a leggyorsabb klasszikus számítógépek.

Elképzelhetetlen, hogy százas vagy ezres nagyságú qubittal mennyi információval és milyen idő alatt végezhetők el műveletek. 2019-ben a Google be is jelentette az úgynevezett kvantumfölényt *(Quantum Supremacy),* amely azt jelenti, hogy a kvantumszámítógépek egy-egy műveletben már felülmúlják a hagyományos számítógépeket.[9] Ez a számítási kapacitás alkalmas hatalmas mennyiségű adathalmazok *(Big Data)* áttekintésére, azokkal statisztikai összefüggések és egyéb matematikai műveletek végzésére.

A kvantumszámítógépek megjelenése jelentős kihívásokat és potenciális veszélyeket hozhat a jelenlegi kiberbiztonsági rendszerek számára. Ez elsősorban annak köszönhető, hogy a kvantumtechnológia radikálisan más számítási módszereket alkalmaz, amelyek a jelenlegi kriptográfiai protokollok hatékonyságát veszélyeztethetik. A mai modern számítástechnikai rendszer az RSA-, az ECC- vagy a Diffie–Hellman-protokollokon alapszik.[10] Ezek a rendszerek a hagyományos számítógépek számára rendkívül nehezen feltörhetők, mert

8 Képzeljünk el egy nem igazán helyénvaló analógiát, de a bizonytalanságot talán elénk vetíti a valós térben! Dobjunk fel egy pénzérmét, ami pörög-pörög-pörög. A pörgése pillanatában nem tudjuk, hogy „fej" vagy „írás" lesz. Csak amikor az érme leesik a földre, és megnézzük, megtapasztaljuk, akkor derül ki a számunkra, hogy „fej" vagy „írás" lett-e.

9 Hughes et al. 2021: 90; Rincon 2019.

10 Lunde 2009: 274–275.

hatalmas számítási kapacitást igényelnek. Ma az egyik leggyakoribb titkosítás, amely védi számítógépünket, az RSA-titkosítás, amely egy saját kulcsból és egy nyilvános kulcsból álló protokoll, amely – véletlenül generált – jellemzően prímszámokkal végzett sok-sok műveletből áll össze. Amit a saját kulcs kódol, az a nyilvános kulccsal dekódolható, és *vice versa*. A bonyolult többlépcsős matematikai művelet teszi biztonságossá az RSA-kódolást.

Úgy tűnik, hogy a kvantumszámítógépek képesek feltörni a hagyományos számítógépekben alkalmazott titkosításokat. Peter Shor brit matematikus kvantumalgoritmusa képes visszafejteni a nagy számokat, ezzel pedig a titkosítási módszerek sebezhetővé válnak. A ma általános szimmetrikus titkosítás (amikor a küldő és a fogadó ugyanazt a kulcsot használja a titkosításhoz és annak felfedéséhez) is veszélybe kerülhet a Grover-algoritmus miatt. Ez az algoritmus a szimmetrikus kulcsok feltörését lehetővé teszi, ami a mai számítógépekkel csak rendkívül hosszú idő alatt sikerülhet.

A kvantumszámítógépek alkalmazásának a lehetősége, híre az adatlopások új célját vetítette előre: *Harvest now, decrypt later,* azaz szerezd meg most, és fejtsd meg később.[11] Az elkövetők, bár most még nem tudják visszafejteni a megszerzett adatállományokat, e-maileket stb., ha szert tesznek akár egy nagyobb tudású számítógépre, akár egy kvantumszámítógépre, akkor az adatok titkosításait később fel tudják törni. Mielőtt feltennénk azt a kérdést, hogy mi az értelme egy ilyen támadásnak, egy szóval felelek: a múlt. Intézmények, cégek, személyek története, múltja. Cégek, intézmények keletkezése, története vagy magánszemélyek pénzügyi helyzete, egészségi állapota, korábbi politikai tényked ése, mind-mind értékes információ lehet a jövőben.

Ha egy számítástechnikai rendszer védtelenné válik, nincs akadálya a különböző támadások végrehajtásának:

- az adatokban, programokban kárt okozó *malware*-ek (akár egy zsarolóvírus) feltölthetők;
- a rendszerben kezelt adatok „ellophatók" (azaz lemásolhatók);
- az adatok vagy programok manipulálhatók (adatok részlegesen vagy teljesen felülírhatók, részlegesen vagy teljesen törölhetők (billentyűzettel vagy malware-ek által is);

[11] Europol 2023.

- a rendszer vagy egyes elemei működése akadályozható (például a program valamely funkciójának kikapcsolása), a rendszer teljesen vagy részlegesen leállítható;
- a rendszerben folyó kommunikáció lehallgatható, a kommunikáció rögzíthető stb.

Milyen megoldások tűnnek alkalmazhatónak (egyelőre)?

- Posztkvantum-kriptográfia: a mai titkosítási protokollok folyamatos fejlesztése. Olyan titkosítási módszerek fejlesztése, amelyek ellenállnak a kvantumszámítógépek támadásainak.
- Hibrid titkosítás: a jelenlegi és a posztkvantum-algoritmusok együttes használata, hogy a biztonság folyamatos legyen az átmeneti időszakban.
- Kvantumtitkosítás: olyan technológia, amely a kvantumfizika törvényeit használja a biztonságos kommunikációhoz. Ez garantálja, hogy a kommunikációt nem lehet lehallgatni a kvantummechanika alapvető elvei miatt.

ÖSSZEGZÉS

Jelenleg a kvantumszámítógépek még nem elég fejlettek ahhoz, hogy valós fenyegetést jelentsenek a széles körben alkalmazott titkosítási rendszerekre. Azonban a technológia gyors fejlődése miatt a nem túl távoli jövőben elérhetik azt a szintet, amikor már veszélyt jelentenek a jelenlegi titkosítási rendszerekre.

Felhívjuk a figyelmet arra, hogy tovább fognak mélyülni azok a technológiai, gazdasági és társadalmi szakadékok, amelyek a kvantumtechnológiát alkalmazó országok, országon belül társadalmi csoportok, illetve az e technológiát nem értők, nem használók között lesznek. Fel kell rá készülni az oktatási rendszerünk minden szintjén tananyagokban, az egyetemistákat, hazai kutatókat hozzá kell engedni a nagy európai, amerikai oktatási-kutatási programokhoz.

Hazánkban a kiberbiztonságról szóló 2024. évi LXIX. törvény már foglalkozik a kvantumtámadások jövőbeni veszélyével, a posztkvantum-védekezéssel, ami nagyon helyes, de ezt a folyamatot fel kell gyorsítani. Nem véletlen, hogy az Egyesült Nemzetek Szervezete 2025-öt a kvantumtudomány nemzetközi évének nyilvánította, felhívva a problémára figyelmet.

IRODALOMJEGYZÉK

Britannica Hungarica (2013). Budapest: Kossuth.

Chakraborty, Utpal (2022): *Quantum Computing and Future.* Noida: BPB Publications.

European Space Agency (2014): *Max Planck: Originator of Quantum Theory.* Online: www.esa.int/Science_Exploration/Space_Science/Planck/Max_Planck_Originator_of_quantum_theory

Europol (2023): *Internet Organised Crime Threat Assessment (IOCTA) 2023.* Online: www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023

Feynman, Richard (2005): *A fizikai törvények jellege.* Ford. Gajzágó Éva. Budapest: Akkord.

Geszty Tamás (2007): *Kvantummechanika.* Budapest: Typotex.

Griffiths, David (2005): *Introduction to Quantum Mechanics.* Uppes Saddle River, NJ: Pearson Education.

Hughes, Ciaran et al. (2021): *Quantum Computing for the Quantum Curious?* Cham: Springer. Online: https://doi.org/10.1007/978-3-030-61601-4

IBM [é. n.]: *Advanced Logic Technology at 2nm Node.* Online: https://research.ibm.com/projects/advanced-logic-technology-at-2nm-node

Lunde, Paul (2009): *Kódok, szimbólumok, titkos nyelvek, rejtjelek.* Ford. Béresi Csilla. Budapest: Kossuth.

Rincon, Paul (2019): Google Claims „Quantum Supremacy" for Computer. *BBC,* 2019. október 23. Online: www.bbc.com/news/science-environment-50154993

Rockenbauer Antal (2020): *Útikalauz a fizikához Newtontól Higgsig.* Budapest: Scolar.

Sakurai, Jun John – Napolitano, Jim (2010): *Modern Quantum Mechanics.* London: Pearson Education.

Zubairy, M. Suhail (2020): *Quantum Mechanics for Beginners.* Oxford: Oxford University Press. Online: https://doi.org/10.1093/oso/9780198854227.001.0001