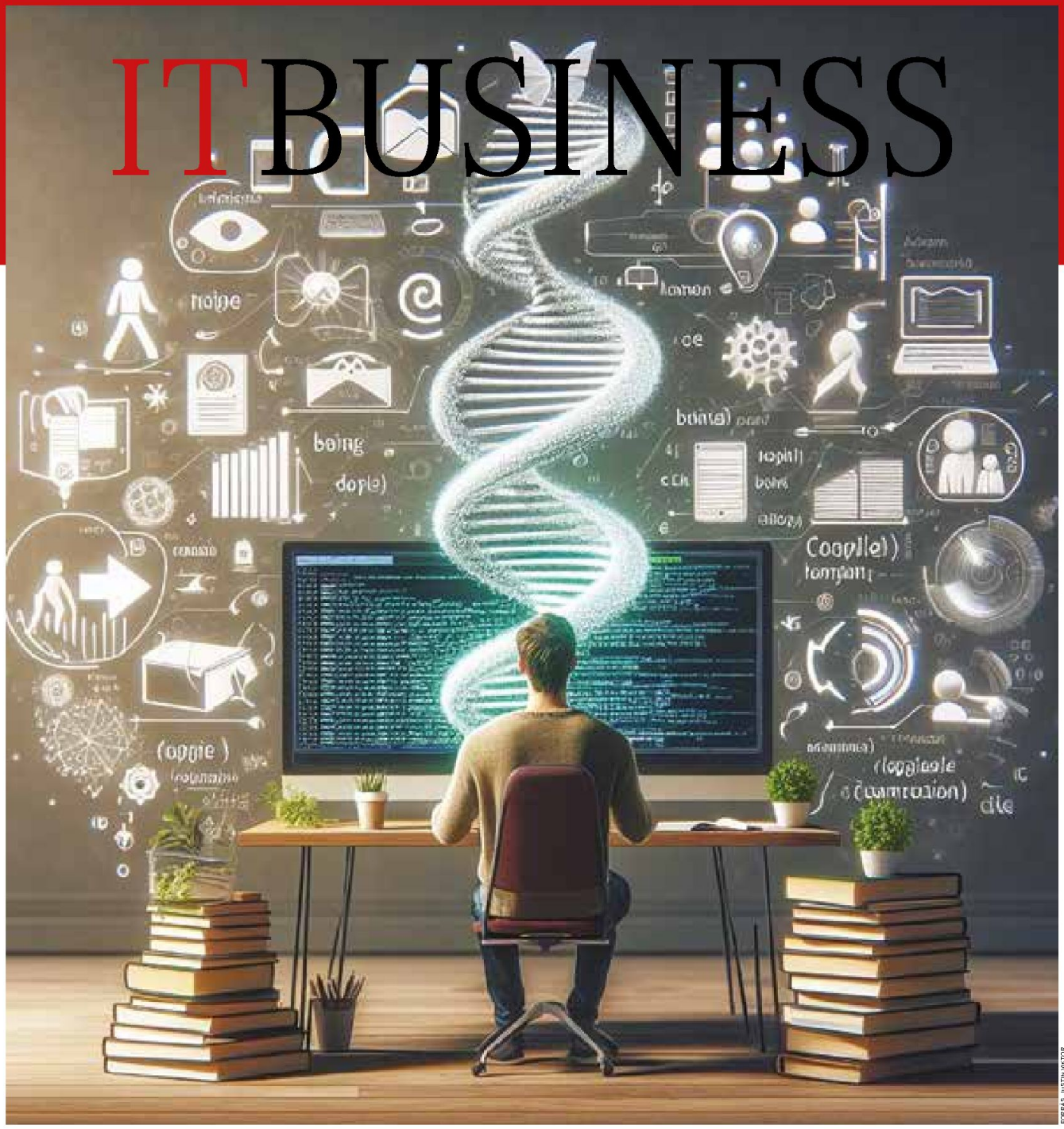
informatikáról üzleti döntéshozóknak XXII. évfolyam 3. szám 2024. március 5. Ára: 3990 Ft www.itbusiness.hu

IT BUSINESS



FORRÁS: JUSTIN VIKTOR

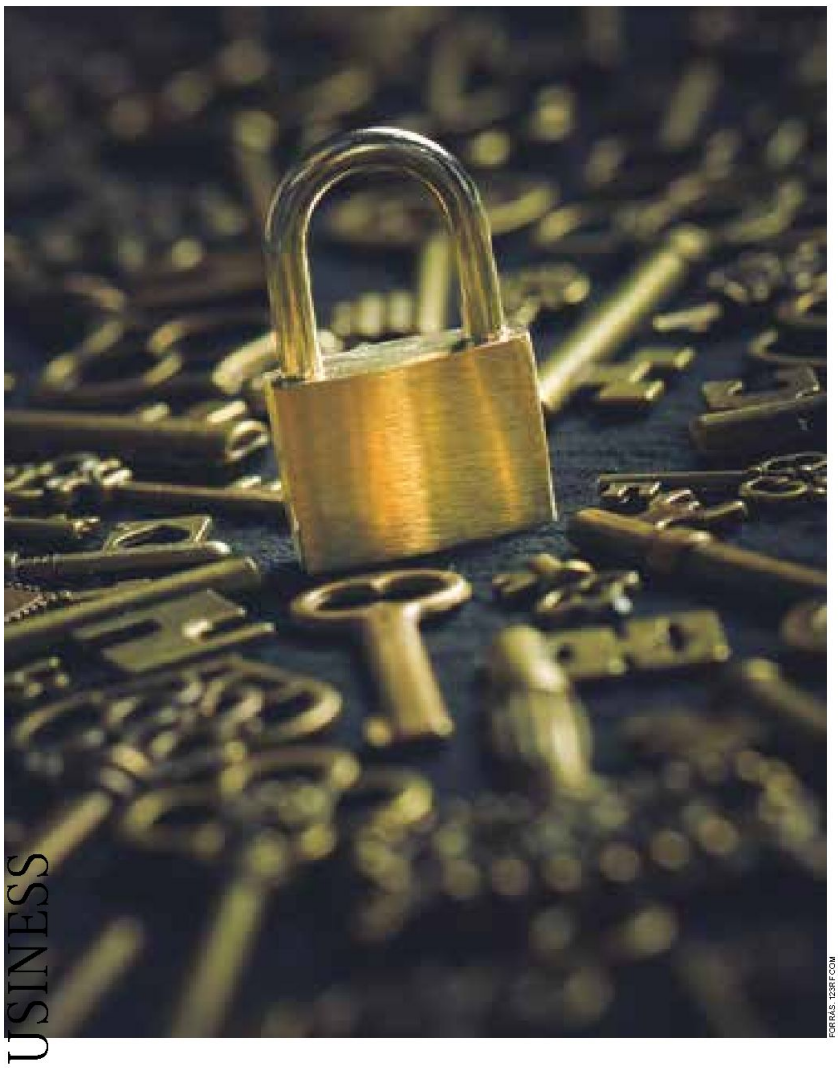
EGY SZINTTEL FELJEBB: A FEJLŐDÉST KELL FEJLESZTENI

MI LESZ VELED, SZOFTVER?

TUDÓSKLUB VITATJA MEG A POSZTKVANTUM CSÚCSKRIPTOGRÁFIÁT

Amit csak a megoldhatatlan képes megoldani

Budapesten járt *Jintai Ding* professzor, a kínai Csinghua Egyetem posztkvantum kriptográfiával foglalkozó kutatója. Itteni előadásáról és kutatási területeiről beszélgettünk két hazai, kvantumkriptográfiával foglalkozó tudóssal, *Buttyán Levente* egyetemi tanárral, a BME CrySyS Adat- és Rendszerbiztonsági Laboratóriumának (CrySyS Lab) vezetőjével, és *Nagy Gábor Péterrel,* a Szegedi Tudományegyetem Bolyai Intézetének matematikus egyetemi tanárával.



FORRÁS: 123RF.COM

Jintai Ding professzor európai útja során először Lengyelországba látogatott, de kíváncsi volt Budapestre is, ezért hozzánk is elutazott, ahol a Rényi Intézetben és a BME-n is előadást tartott. Buttyán Levente örömmel segített a tanulmányait és kutatásait korábban az USA-ban végző, ma a Cincinnati Egyetem professzoraként is dolgozó matematikus és kriptográfus kínai kutató nálunk töltött idejének megszervezésében.

Veszélyes számítógépek jönnek

A kvantumkomputerek potenciális veszélyt jelentenek a ma használt kriptográfiai eljárásokra, és 2016-17 óta az amerikai kormányzat tudatosan készül is a váltásra, amelynek során lecserélik majd az internetes kommunikációban jelenleg használt protokollokat kvantumállókra – ismertette Buttyán Levente. Beszámolt arról is, hogy a National Institute of Standards and Technology (NIST), az amerikai szabványügyi szervezet folyamatosan különböző versenyeket ír ki az új megoldások keresésére, és ezeken vár javaslatokat a szükséges titkosítási eljárásokra.

A kriptográfiai eljárások fontos osztályát képezik az úgynevezett digitális aláírások is, ezen a területen a legfrissebb fejlemények a posztkvantum digitális aláírásokhoz kapcsolódnak. 2023 közepén járt le egy nagy NIST-pályázat határideje, amelyre rengeteg ilyen javaslat érkezett, maga Ding professzor is több területen részt vett a munkában, ő maga is tett javaslatokat kollégáival mind a titkosítási protokollokra, mind az új digitális aláírásokra. Munkájuk során ők is aktívan próbálják megkeresni a protokollok gyenge pontjait.

Ding professzor előadásaiból kiderült, hogy nagyon erős elméleti matematikai háttér kell ezeknek a protokolloknak a megértéséhez, vizsgálatához. „Emellett mély programozási tudás, és a különböző eszközök fizikai ismerete is szükséges, tehát az elméleti matematikustól kezdve a villamosmérnökökig sokan vesznek részt ezekben a munkákban", vette át a szót Nagy Gábor matematikus. A nagy országok kormányai komolyan veszik


FORRÁS: CRYSYS LAB

BUTTYÁN LEVENTE, BME CRYSYS LAB


FORRÁS: CINCINATTI EDU

JINTAI DING, CSINGHUA EGYETEM


FORRÁS: SZTE BÓLYAI INTÉZET

NAGY GÁBOR PÉTER, SZTE BÓLYAI INTÉZET

a posztkvantum világ veszélyeit, és valójában nem is lehet tudni, hogy melyik ország hol tart ma a csúcskategóriás kvantumkomputerek fejlesztésében. Valószínűleg az első időkben nem is fogják a nagy kormányok az orrunkra kötni, hogy éppen milyen titkosítási eljárást tudnak hatékonyan feltörni. „Viszont várható, hogy néhány éven belül eljön az a pillanat, amikor a nagy kommunikációs rendszereket megpróbálják átállítani az új típusú, posztkvantum eljárásokra", mondta Nagy Gábor.

Nem feltétlenül kell megvárnunk azt, amíg egy igazán ütőképes kvantumszámítógépet megépít valaki, a probléma már ma is itt van. „A bonyodalom abban áll, hogy ha valamit szeretnénk titkosítani, mondjuk 20 vagy 30 évre, és 15 éven belül létrejön egy nagy kapacitású kvantumszámítógép, akkor annak birtokosai dekódolhatják majd a titkosított anyagokat", hívta fel a figyelmet Buttyán Levente. Hozzátette, nem biztos, hogy ezeket a számítógépeket a közeljövőben megépítik, vagy olyan méretskálát érnek el, amely kriptográfiai szempontból a gyakorlatban is veszélyessé teszi őket. De ha ma hosszú távon használható rejtjelezést szeretnénk kifejleszteni, akkor el kell gondolkodni azon, hogy hogyan cseréljük le a jelenlegi algoritmusainkat.

Sebezhető algoritmusok

Visszatérve az izgalmas előadásra, Buttyán Levente elmondta, hogy Jintai Ding professzor részt vett több, a NIST által kiírt versenyen, amelyeken javaslatokat vártak az új titkosítási algoritmusokra. Nagyon sok javaslat érkezett, és több körben ezekből próbálták kiválasztani azokat, amelyek alkalmasak a szabványosításra. Végül az egyik kiválasztott algoritmusnak Ding professzor volt a szerzője, de a beadott egyéb javaslatok kriptográfiai elemzésében is részt vett. Az ilyen elemzések során időben kiderülhet, ha valamelyik megoldás túl gyenge lenne, a professzor segítségével sebezhetőségeket is azonosítottak a mások által beadott algoritmusokban.

Tavaly tehát a NIST már győzteseket is hirdetett, és az ő algoritmusaikat el is kezdték szabványosítani. Az egyik ilyen figyelemreméltó algoritmus a „Kyber" nevű titkosítási eljárás volt, amely egy kulcsbefoglaló eljárás (key encapsulation mechanism, KEM), és Ding professzor neve ott szerepel a létrehozói között. Más algoritmusok feltörői között is szerepelt: Jingtai Ding a terület egyik jelentős tudósa.

A megoldhatatlan problémák óriási haszna

„Engem magával ragadott az a lendület, amelyet ő képvisel az egész ügy fontossága szempontjából", mondta el Nagy Gábor. A Rényi Intézetben matematikusoknak tartott előadásában Ding professzor világossá tette, hogy a szóban forgó kriptográfiai eljárások biztonságát egyrészt matematikai, elméleti módszerekkel is alá kell támasztani, ugyanakkor ez egy gyakorlati tudomány. „Tehát hiába alkotunk kitűnő elméleti okfejtéseket arra, hogy egy adott eljárás biztonságos, ha valaki talál egy trükköt, és feltöri vele, akkor azt félre is tehetjük, onnantól haszontalan, fel van törve. Ding professzor rávilágított, hogy a gyakorlat a mérvadó ezen a területen", mondta el Nagy Gábor.

„Ha valahol, itt biztosan összeér az elmélet és a gyakorlat, és nem működik egyik sem a másik nélkül", húzta alá Buttyán Levente. „Én azt emelném ki, amikor Ding professzor elmesélt egy problémát, amelyen sokat dolgozott, mivel meg akart oldani a segítségével egy feladatot, de nem igazán akart sikerülni a dolog. Öt évig próbálkoztak a doktoranduszával, míg végül talált egy szakmai újságcikket 1923-ból – tehát egy nagyon régi cikket – amelyet elolvasva rájött, hogy nincs is megoldás arra a problémára, amelyen gondolkozott. Ilyen dolgok bizony előfordulnak egy kutató életében, hogy gondolkodunk, és aztán kiderül, hogy valójában nincs is megoldás, és mindez néha egy 100 éves cikkből kell, hogy kiderüljön", vélekedett Buttyán Levente.

A professzor ezzel együtt mégis azt emelte ki, hogy később ez az öt év hasznosnak bizonyult, mert egy másik, igen makacs probléma megoldása során felhasználhatta ezt az öt évnyi tapasztalatot. „Szerintem ez nagyon érdekes és tanulságos anekdota a kutatóknak, főleg a fiataloknak arról, hogy mi minden előfordulhat a munkánk során", zárta gondolatait Buttyán Levente.

Justin Viktor