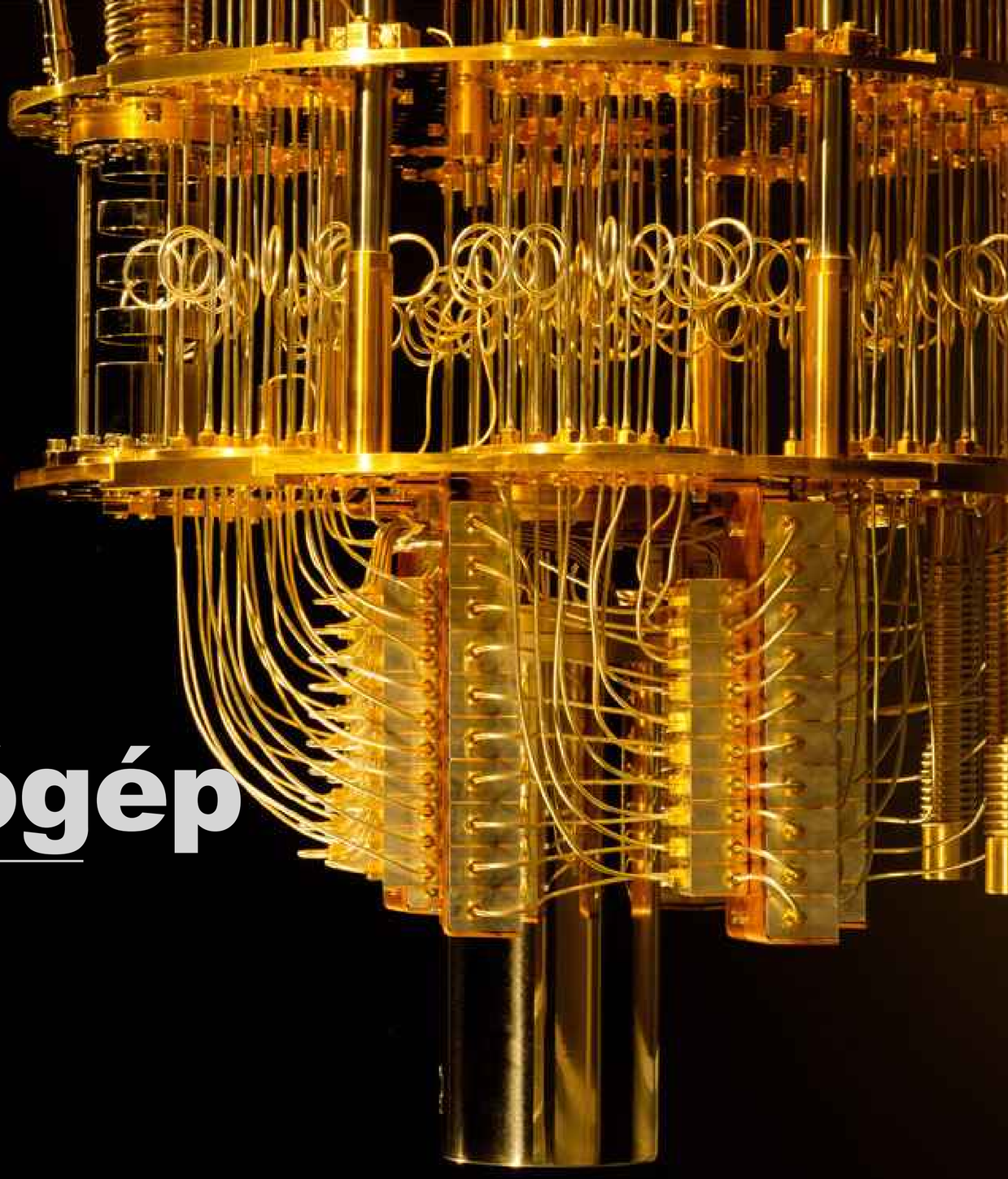


Kvantumszámítógép

Áldás vagy átok?

Koczka Ferenc, Eszterházy Károly Katolikus Egyetem,
koczka.ferenc@uni-eszterhazy.hu

III/B. FEJEZET *

A POSZT-KVANTUMTITKOSÍTÁS ALKALMAZÁSÁNAK SZABÁLYAI *

12/F. * A poszt-kvantumtitkosítás alkalmazásra kötelezett szervezet védelme

22/F. § * A poszt-kvantumtitkosítás alkalmazásra kötelezett szervezet a jogszabályban meghatározott feladatainak ellátása körében köteles a fizikailag elkülönített helyszínei közötti kormányzati célú hálózaton, továbbá a publikus internet felületen zajló, az elektronikus hírközlési törvény szerinti szolgáltató igénybevételével vagy egyéb információs társadalommal összefüggő szolgáltatás igénybevétele esetén poszt-kvantumtitkosítás alkalmazást annak kiépítéséhez az alkalmazás nyújtására jogosult, nyilvántartásba vett szervezettől beszerezni, és a kezelésében álló hálózatain a védelmet kialakítani, annak érdekében, hogy az elektronikus úton történő információáramlás a kvantumszámítógép okozta kibertámadás ellen biztosított legyen.

12/G. * A poszt-kvantumtitkosítás alkalmazást nyújtó szervezetre vonatkozó feltételek

22/G. § * (1) Kizárólag olyan szervezet nyújthat poszt-kvantumtitkosítás alkalmazást a poszt-kvantumtitkosításra kötelezett szervezet számára (a továbbiakban: poszt-kvantumtitkosítás alkalmazást nyújtó szervezet), amely

a) nemzetbiztonsági kockázatot nem jelent és

b) a 22/H. § szerinti követelményeknek megfelel.

(2) Az (1) bekezdésben foglaltak alapján a tanúsítási eljárásban történő részvételre kizárólag olyan gazdasági szereplő jelentkezhet, amely

Hagyományos gép

- Kettes számrendszer (nullák és egyesek)
- Memóriában tárolt program és adatok
- Soros utasítás-végrehajtás
- Univerzális használhatóság
- Kiforrott technika

Kvantum-számítógép

- 50 éves múlt, emulátorok
- Bonyolult, különböző fizikai háttér
- Abszolút nulla fok közeli működés
- Nem csak nullák és egyesek vannak, qubit
- Az eredmény is csak egy valószínűség
- Kiolvasási problémák (quantum measurement)
- Új algoritmusok, pl. shore
- Csak speciális feladatokra használható

Kvantum számítások és algoritmusok

- Különleges számítási teljesítmény
- Meglevő titkosítási eljárások feltörése
- Kriptovaluták
- Speciális anyagok kifejlesztése
- Qubitek száma (IBM: 127)
- 2 qubites házi kvantumgép

Kvantum Internet

- Kvantum kriptográfia a titkosításhoz és az illetéktelen hozzáférés észleléséhez.
- Bohr-Einstein vita.

Teleportálás, féreglyukak :-)

QUANTUM FRONTIERS
REPORT ON COMMUNITY INPUT TO THE NATION'S STRATEGY FOR QUANTUM INFORMATION SCIENCE

https://www.quantum.gov/wp-content/uploads/2020/10/QuantumFrontiers.pdf

b. Expanding the Limits of Physical Theory

"[T]he field should think carefully about which key, longstanding questions in physics could be solved using quantum technology." – *RFI response*

Research in QIS has begun to shed light on other interwoven areas of physics and other scientific fields. For example, research on entanglement can address fundamental questions about the emergence of spacetime, entropy of black holes, correspondence with wormholes, and the foundations of thermodynamics. Research areas described in workshop reports and RFI responses include: how quantum computational analysis of quantum walks can extend scattering theory; how quantum error correction codes and multipartite entanglement can inform searches for new phases of matter and topological states; and how the anti-de Sitter/conformal field theory (AdS/CFT) correspondence and associated dictionary for translating results can be used to inform quantum gravity theory, and explore properties of gauge theories at strong coupling where perturbative analysis is not possible. Furthermore, quantum networks and computers can test quantum mechanics in new regimes by exploring fundamental limits for coherence and entanglement. QIS can help explore the question, "What credible deviations from conventional quantum theory are experimentally testable?" (e.g., gravitationally induced decoherence, spontaneous wavefunction collapse models, or nonlinear corrections to the Schroedinger equation).

Stratégiai cél

A kvantumtechnológiai kutatásra fordított éves kiadások becslése (mE)
Cél: a kvantumfölény elérése

1,500	WORLD
550	EUROPEAN UNION*
360	UNITED STATES
220	CHINA
120	GERMANY
105	BRITAIN
100	CANADA
75	AUSTRALIA
67	SWITZERLAND
63	JAPAN
52	FRANCE
44	SINGAPORE
36	ITALY
35	AUSTRIA
30	RUSSIA
27	NETHERLANDS
25	SPAIN
22	DENMARK
15	SWEDEN
13	SOUTH KOREA
12	FINLAND
12	POLAND

Source: McKinsey

*Combined estimated budget for EU countries

SDA Informatika

Eszterházy Károly Egyetem
Pénzügyi osztály részére
Eszterházy tér 1.
3300 Eger

Tárgy: Bankszámla számának változása

Tisztelt Partnerünk,

Értesítjük Önöket, hogy cégünk pénzintézeti sz
megváltozik.
Új bankszámlánkat a Budapest Bank Zrt. nél vez
Bankszámlaszámunk Budapest Bank: 10102543

Kérjük, hogy az új bankszámla számot rögzítsék
már az új számlaszámra teljesítsék.

Terem a Tanítók szíves tudomásulvételét.

Belföld | Debrecen

Kibervédelem: a Debreceni Egyetemet is érte dzsihadista hackertámadás

...járta be a Pannon Egyetem informatikai rendszerét

Írta: Dajkó Pál Forrás: IT café

2009-02-27 15:30

A napokban egy újabb adatbiztonsági **incidensre derült fény**, mely újra a Pannon Egyetemet érinti, s bár teljes pontossággal még nem lehet megállapítani, hogy mi is történt, most igyekszünk összefoglalni az eddigi tényeket.

Az Ismeretlen Hacker jelentkezik

Február 23-án egy ismeretlen (a továbbiakban: hacker) körlevelet küldött a magyar sajtó jó néhány szereplőjének, így az *IT café*-nak is, mely a következőképpen kezdődött: *„Üdvözletem. Csatolva a Pannon Egyetem neptunkódjainak és jelszavainak egy része, diákoké, tanároké(!)"*. A levél mellékletében két táblázat szerepelt: az egyikben 27 tanár, a másikban 500 hallgató adatai szerepeltek. A tanári táblázat volt a teljesebb, itt a Neptun-kód (azonosító) mellett szerepelt többek között egy jelszó, az e-mail cím és a teljes név. A hallgatói táblázatban a Neptun-kód mellett többek között (körülbelül az esetek felében, harmadában) szerepelt egy jelszó, mindenkinél a születési dátum és az e-mail cím.

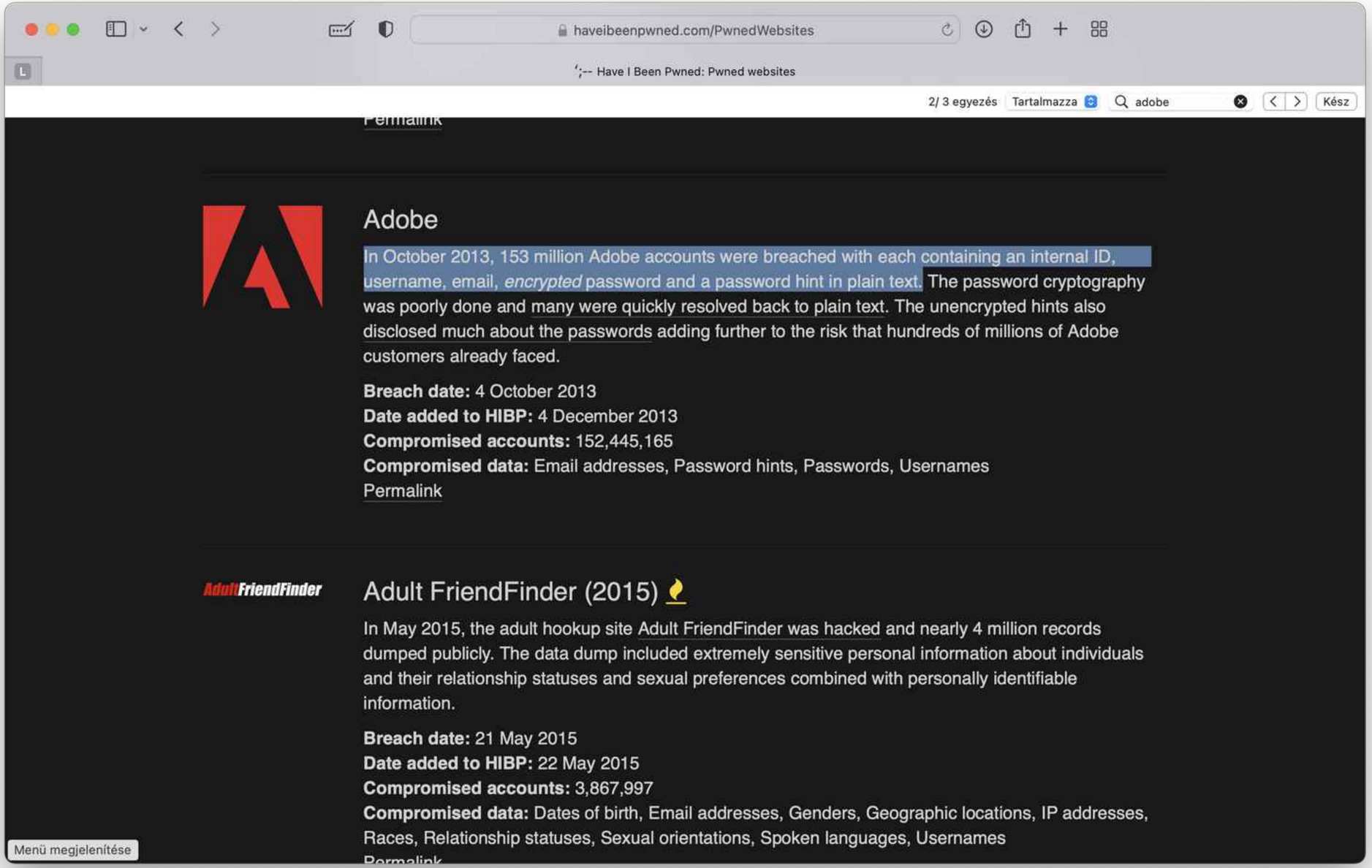
Tessék, itt a kért 135 millió

2020. augusztus 24. 12:53 - Csizmazia Darab István [Rambo]

135 millió forintnak megfelelő (457 ezer dollár) összeget f
bűnözőknek, miután a zsarolóvírussal fertőzték meg a re
titkosítással is túszul ejtett információk között a hallgat

...ák el több svájci egyetem alkalmazottainak bérét – írja az M
...ájci lapra hivatkozva. **Martina Weiss**, a svájci rektori konferen
...int az eset több felsőoktatási intézmény érintett.

A hackerek adathalász módszerekkel kicsalt személyes információk felhasználásával tették rá a kezü
fizetésére.



https://havibeenpwned.com

575	11,733,674,867	114,169	208,000,875
pwned websites	pwned accounts	pastes	paste accounts

Jelszavak feltörése brute force technikával

666, 25%

2650 db. NTLM		4	5	6	7	8	9
Futási idő	**Alapértelmezett maszk**	0 mp	0 mp	0 mp	23 mp	18 perc 35 mp	12 óra 41 perc
	Teljes ASCII névtér	0 mp	3 mp	2 perc 14 mp	3 óra 39 perc	Várhatóan 15 nap	Nem kezdtük el
	Saját maszk 1	0 mp	2 mp	5 mp	2 perc 34 mp	1 óra 54 perc	3 nap 5 óra
	Saját maszk 2	0 mp	0 mp	19 mp	5 perc 40 mp	4 óra 8 perc	Kb 1 hét lenne
	Saját maszk 3	0 mp	1 mp	19 mp	3 perc 13 mp	2 óra 18 perc	3 nap 21 óra
Találatok száma	**Alapértelmezett maszk**	2	11	26	25	186	117
	Teljes ASCII névtér	2	11	28	26	-	-
	Saját maszk 1	2	10	27	24	25	13
	Saját maszk 2	2	11	28	25	435	-
	Saját maszk 3	2	11	28	25	435	154

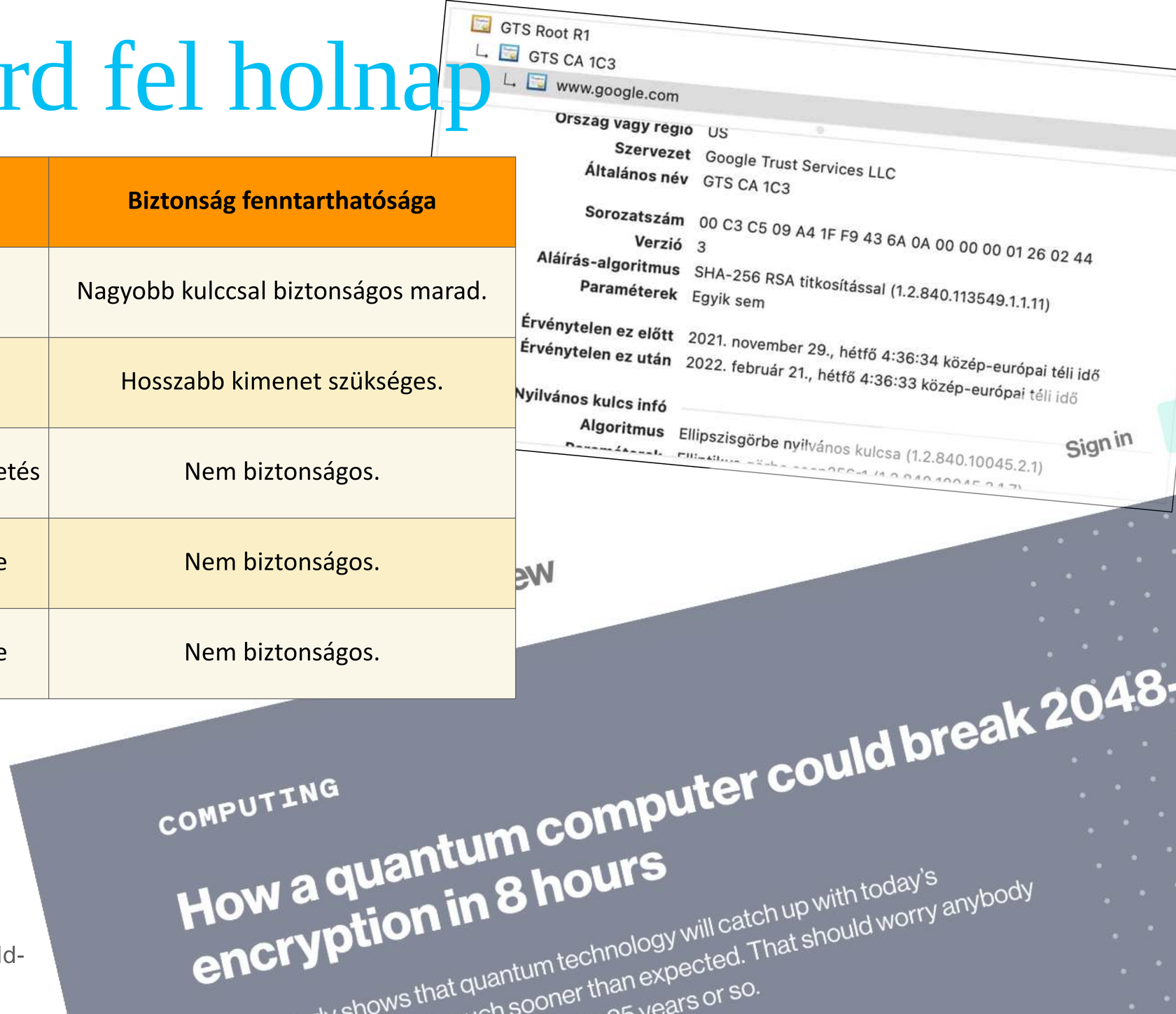
470, 21%

2194 db. SHA1	4	5	6	7	8
Kombinációk száma	2,40E+07	1,68E+09	1,18E+11	1,02E+12	4,18E+13
Futási idő	0 másodperc	2 másodperc	1 perc 6 mp	10 perc 55 mp	7 óra 24 perc
Találatok száma	2	11	21	22	414

Mérések megvalósítása: Vertike László, Eszterházy Károly Egyetem

Lopd el ma, törd fel holnap

Algoritmus	Alkalmazási terület	Biztonság fenntarthatósága
AES	Titkosítás	Nagyobb kulccsal biztonságos marad.
SHA-2, SHA3	Lenyomatképzés	Hosszabb kimenet szükséges.
RSA	Digitális aláírás, kulcs egyeztetés	Nem biztonságos.
ECDSA, ECDH	Digitális aláírás, kulcscsere	Nem biztonságos.
DSA	Digitális aláírás, kulcscsere	Nem biztonságos.

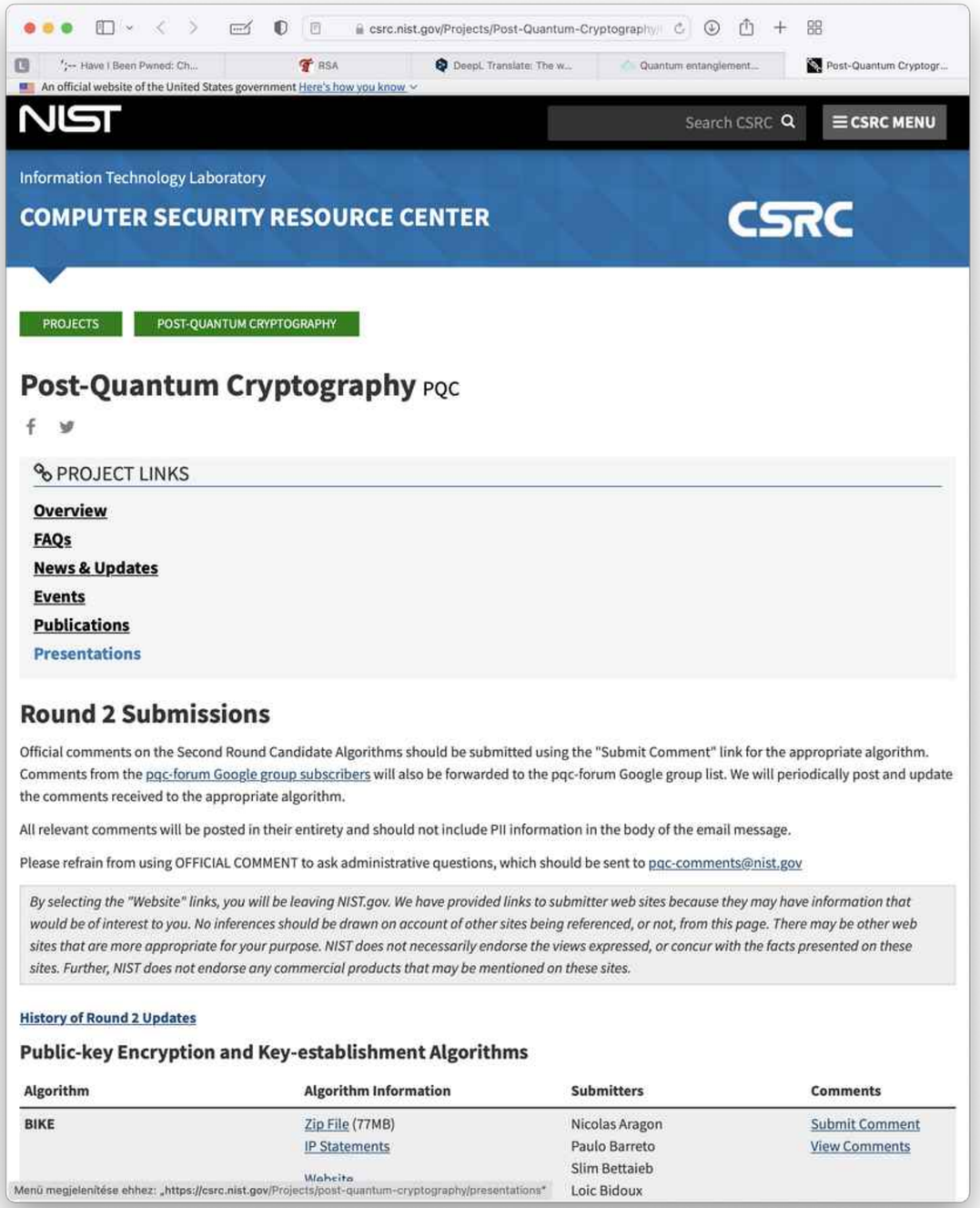


https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/

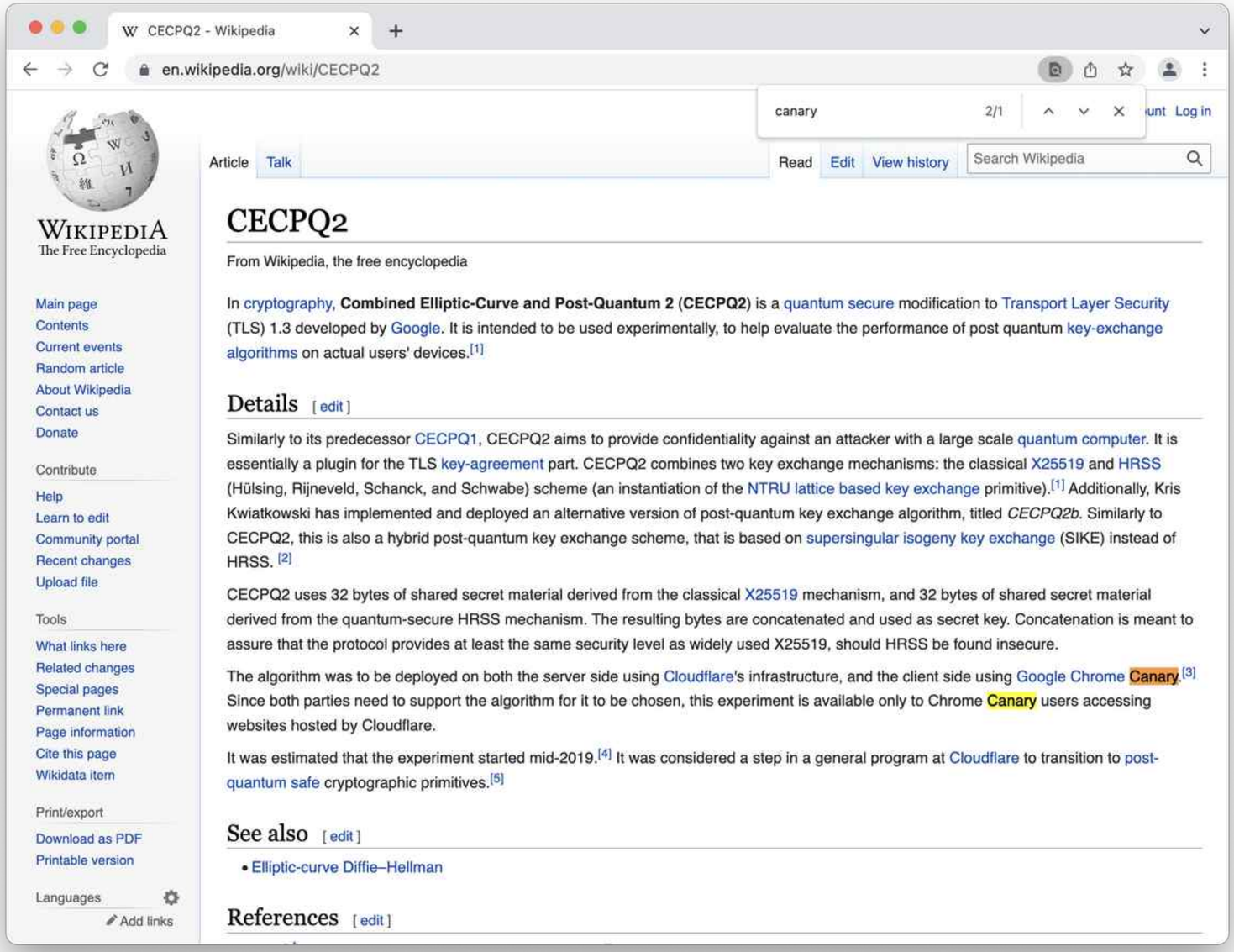
Cserélhető algoritmusok

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions

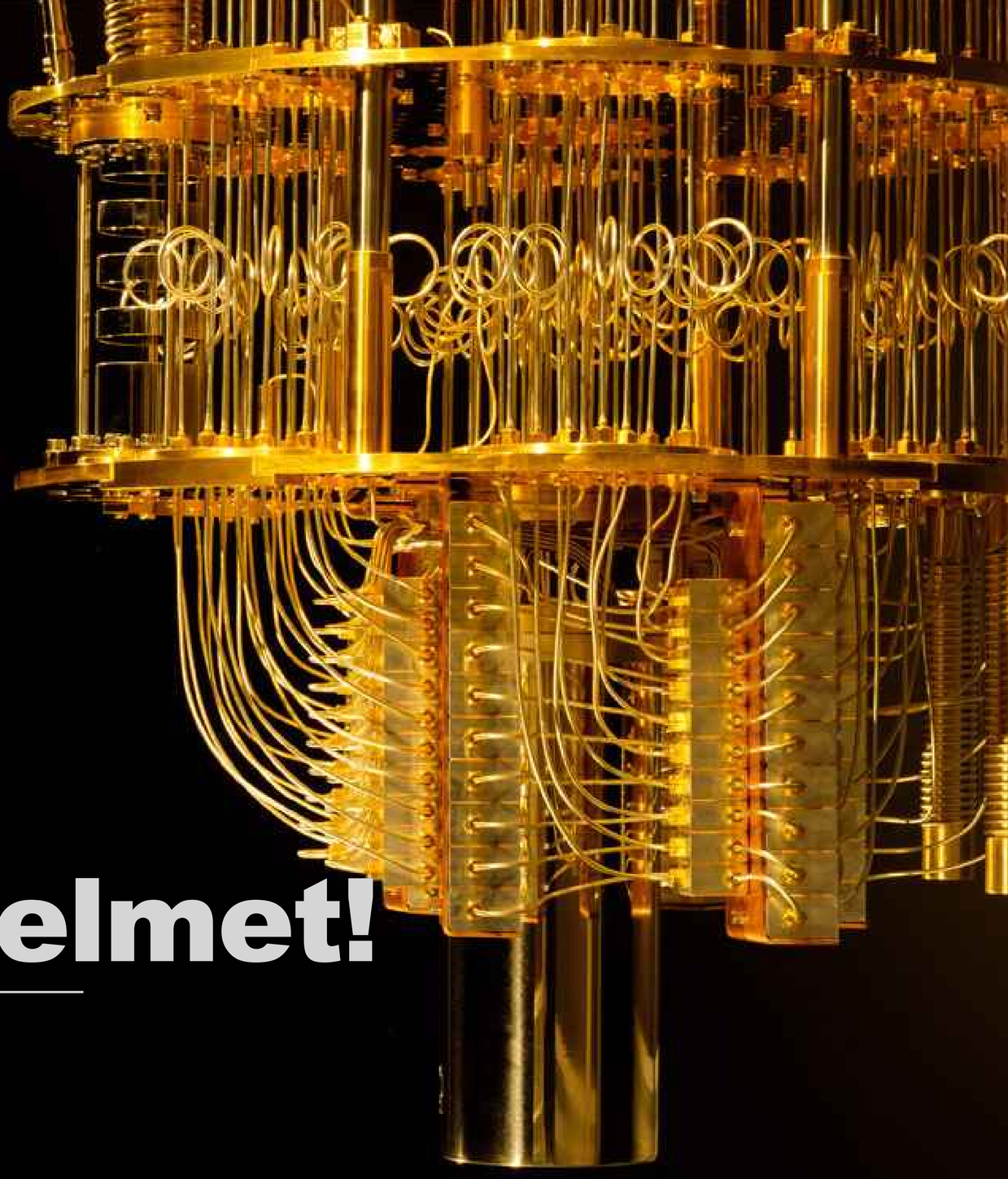
- Régi algoritmusok kicserélése.
- A rendszereinknek cserélhető algoritmusokat kell alkalmazniuk.
- Az MD5 példája.
- Jelenleg is folyik a quantum-safe algoritmusok fejlesztése.
- A nyilvános kulcsú titkosítás helyettesítése.
- A digitális aláírás helyettesítése.
- A NIST pályázata.



Egy példa: Google Canary



Google is working on safeguarding Chrome against the potential threat of quantum computers, the company announced today. It's doing so by implementing post-quantum cryptography in an experimental version of the browser. While there exist hardware defenses against the vastly superior computing power of quantum machines, **Google is using a new so-called post-quantum key-exchange algorithm.** This software, is enabled in Chrome Canary, a kind of testing ground for new browser technology, on only a small number of connections between the browser and Google servers.



Köszönöm a figyelmet!

Koczka Ferenc, Eszterházy Károly Katolikus Egyetem,
koczka.ferenc@uni-eszterhazy.hu