



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,

Ingyen Jogtár

Ingyen Cégtár

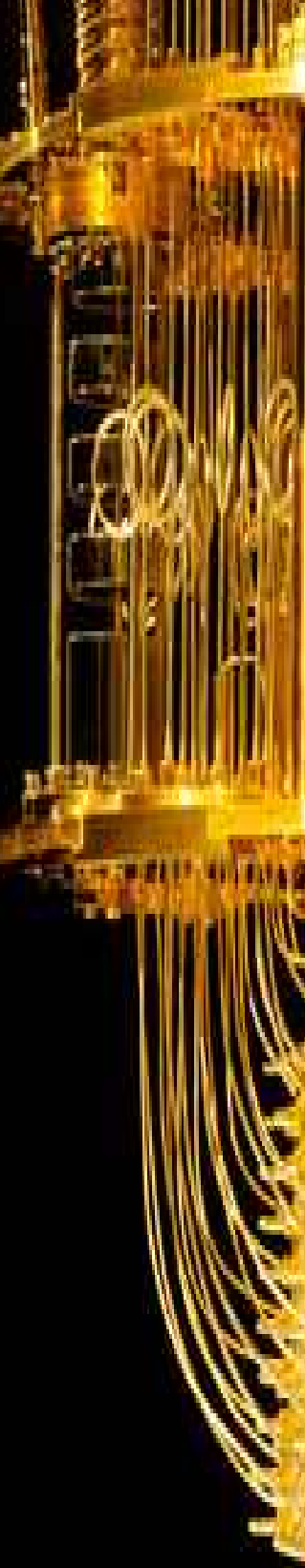


Hagyományos gép

- 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 :-)

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 Schrodinger equation).

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

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



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

Tárgy: Bankszámla számának változása

Tisztelt Partnerünk,

Értesítjük Önöket, hogy cégünk pénzügyi adatai megváltoztak.
Új bankszámlánkat a Budapest Bank Zrt.nél vezetjük, az új számlaszámunk Budapest Bank: 10102543.
Kérjük, hogy az új bankszámla számot rögzítsék.
Ezen a felelős 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: „Üdvözlétem. 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 fizetett a bűnözőknek, miután a zsarolóvírussal fertőzték meg a rendszerét titkosítással is túsul ejtett információk között a hallgatók adatai szerepeltek.

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

...ak el több svájci egyetem alkalmazottainak bérét – írja az M...
...ájci lapra hivatkozva. **Martina Weiss**, a svájci rektori konferen...




haveibeenpwned.com/PwnedWebsites

Have I Been Pwned: Pwned websites

2/3 egyezés Tartalmazza adobe Kész

[Permalink](#)

Adobe




In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Breach date: 4 October 2013
Date added to HIBP: 4 December 2013
Compromised accounts: 152,445,165
Compromised data: Email addresses, Password hints, Passwords, Usernames

[Permalink](#)

Adult FriendFinder (2015)



In May 2015, the adult hookup site Adult FriendFinder was hacked and nearly 4 million records dumped publicly. The data dump included extremely sensitive personal information about individuals and their relationship statuses and sexual preferences combined with personally identifiable information.

Breach date: 21 May 2015
Date added to HIBP: 22 May 2015
Compromised accounts: 3,867,997
Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Races, Relationship statuses, Sexual orientations, Spoken languages, Usernames

[Permalink](#)

Menü megjelenítése

<https://havibeenpwned.com>

575

pwned websites

11,733,674,867

pwned accounts

114,169

pastes

208,000,875

paste accounts



Jelszavak feltörése brute force technikával

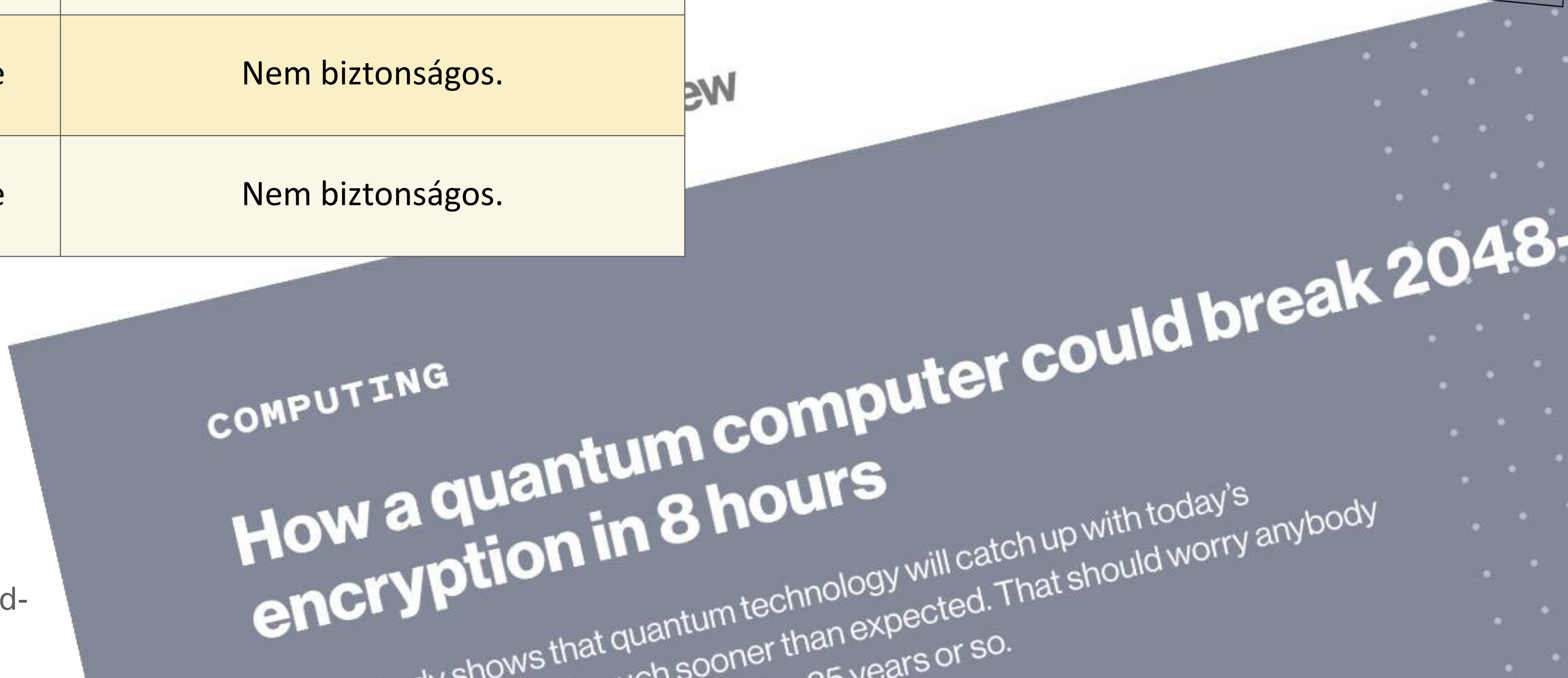
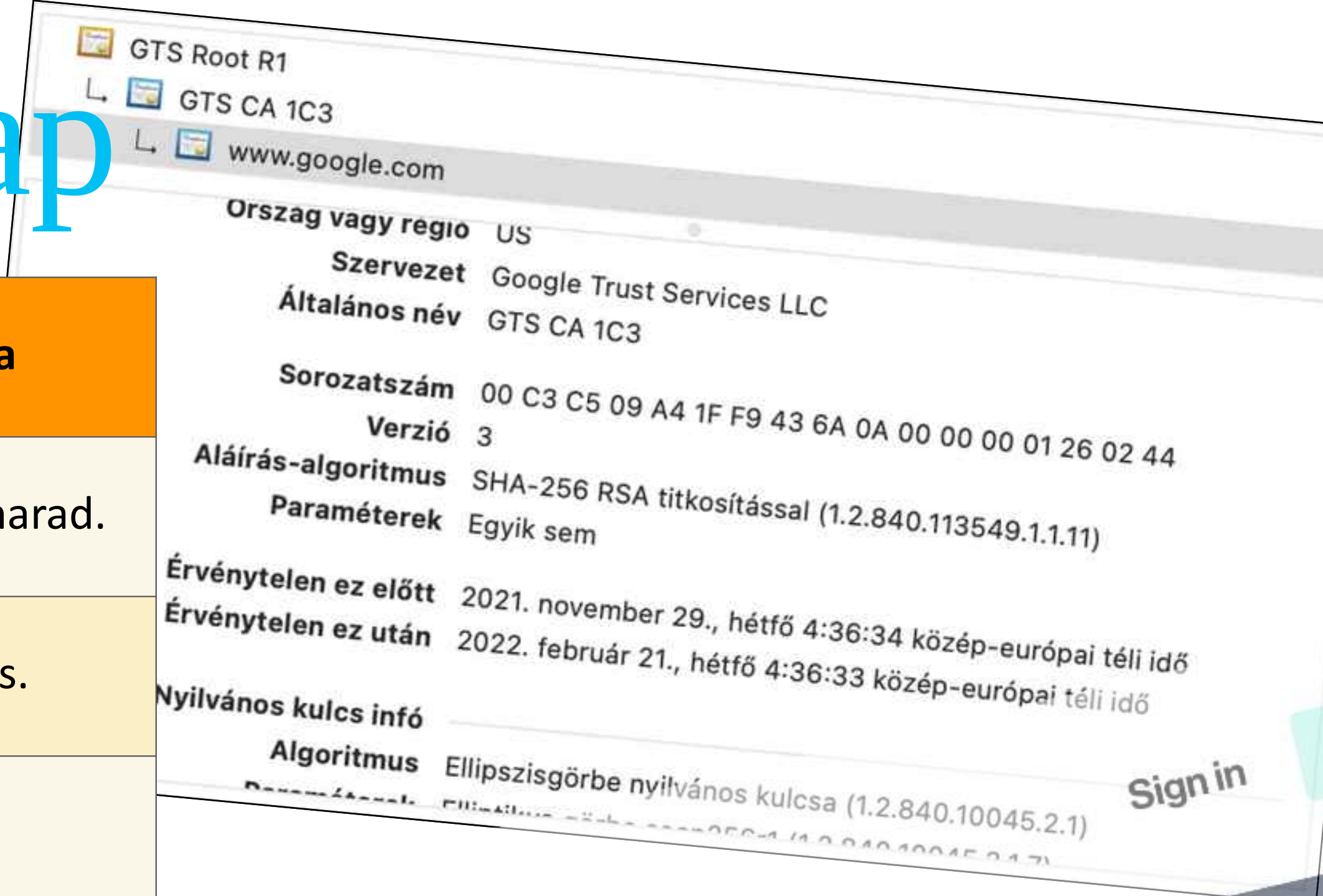
2650 db. NTLM		4	5	6	7	8	9
Futási idő	Alapértelmezett maszk	0 mp	0 mp	0 mp	23 mp	18 perc 35 mp	12 óra 41 perc
666, 25%	Teljes ASCII névtér	0 mp	3 mp	2 perc 14 mp	3 óra 39 perc	Várhatóan 15 nap	Nem kezdtük el
	Saját maszk 1	0 mp	2 mp	5 mp	2 perc 34 mp	1 óra 54 perc	3 nap 5 óra
	Saját maszk 2	0 mp	0 mp	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

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

470, 21%

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.

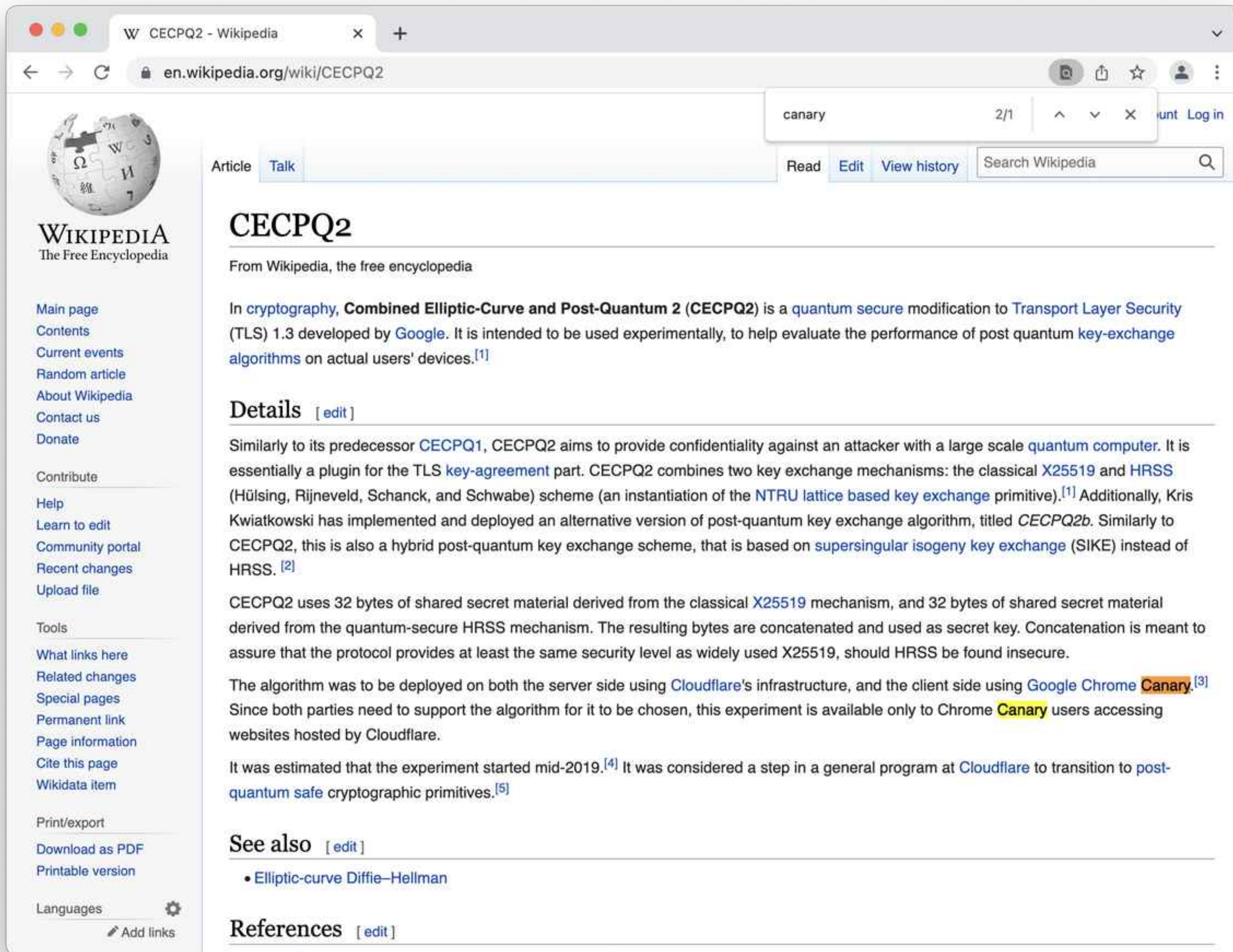
It's Time for TLS 1.0 and 1.1 to Die



The screenshot shows the NIST CSRC website page for Post-Quantum Cryptography (PQC) Round 2 Submissions. The page includes a navigation bar with the NIST logo, a search bar, and a CSRC menu. Below the navigation bar, there are tabs for 'PROJECTS' and 'POST-QUANTUM CRYPTOGRAPHY'. The main content area features a 'Post-Quantum Cryptography PQC' section with social media icons and a 'PROJECT LINKS' section containing links for Overview, FAQs, News & Updates, Events, Publications, and Presentations. The 'Round 2 Submissions' section provides instructions on how to submit comments and includes a disclaimer. At the bottom, there is a table titled 'Public-key Encryption and Key-establishment Algorithms' with columns for Algorithm, Algorithm Information, Submitters, and Comments. The table lists the BIKE algorithm with links to Zip File (77MB) and IP Statements, and lists submitters: Nicolas Aragon, Paulo Barreto, Slim Bettaieb, and Loic Bidoux.

Algorithm	Algorithm Information	Submitters	Comments
BIKE	Zip File (77MB) IP Statements	Nicolas Aragon Paulo Barreto Slim Bettaieb	Submit Comment View Comments

Egy példa: Google Canary



The image shows a screenshot of a web browser displaying the Wikipedia article for CECPQ2. The browser's address bar shows the URL 'en.wikipedia.org/wiki/CECPQ2'. The article title is 'CECPQ2' and it is categorized under 'Article' and 'Talk'. The main text of the article describes CECPQ2 as a quantum secure modification to Transport Layer Security (TLS) 1.3 developed by Google. It mentions that CECPQ2 combines two key exchange mechanisms: the classical X25519 and HRSS (Hülsing, Rijnveld, Schanck, and Schwabe) scheme. The article also notes that CECPQ2 uses 32 bytes of shared secret material derived from the classical X25519 mechanism and 32 bytes of shared secret material derived from the quantum-secure HRSS mechanism. The article is dated mid-2019 and is considered a step in a general program at Cloudflare to transition to post-quantum safe cryptographic primitives.

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Current events
Random article
About Wikipedia
Contact us
Donate

Contribute
Help
Learn to edit
Community portal
Recent changes
Upload file

Tools
What links here
Related changes
Special pages
Permanent link
Page information
Cite this page
Wikidata item

Print/export
Download as PDF
Printable version

Languages
Add links

CECPQ2

From Wikipedia, the free encyclopedia

In **cryptology**, **Combined Elliptic-Curve and Post-Quantum 2 (CECPQ2)** is a **quantum secure** modification to Transport Layer Security (TLS) 1.3 developed by **Google**. It is intended to be used experimentally, to help evaluate the performance of post quantum **key-exchange algorithms** on actual users' devices.^[1]

Details [edit]

Similarly to its predecessor **CECPQ1**, CECPQ2 aims to provide confidentiality against an attacker with a large scale **quantum computer**. It is essentially a plugin for the TLS **key-agreement** part. CECPQ2 combines two key exchange mechanisms: the classical **X25519** and HRSS (Hülsing, Rijnveld, Schanck, and Schwabe) scheme (an instantiation of the **NTRU lattice based key exchange** primitive).^[1] Additionally, Kris Kwiatkowski has implemented and deployed an alternative version of post-quantum key exchange algorithm, titled **CECPQ2b**. Similarly to CECPQ2, this is also a hybrid post-quantum key exchange scheme, that is based on **supersingular isogeny key exchange** (SIKE) instead of HRSS.^[2]

CECPQ2 uses 32 bytes of shared secret material derived from the classical **X25519** mechanism, and 32 bytes of shared secret material derived from the quantum-secure HRSS mechanism. The resulting bytes are concatenated and used as secret key. Concatenation is meant to assure that the protocol provides at least the same security level as widely used X25519, should HRSS be found insecure.

The algorithm was to be deployed on both the server side using **Cloudflare's** infrastructure, and the client side using **Google Chrome Canary**.^[3] Since both parties need to support the algorithm for it to be chosen, this experiment is available only to Chrome **Canary** users accessing websites hosted by Cloudflare.

It was estimated that the experiment started mid-2019.^[4] It was considered a step in a general program at **Cloudflare** to transition to **post-quantum safe cryptographic primitives**.^[5]

See also [edit]

- Elliptic-curve Diffie–Hellman

References [edit]

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