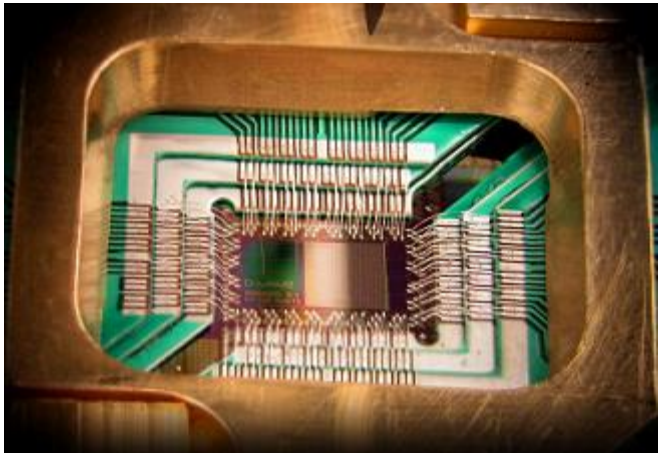
E-GROUP
SOFTWARE & BEYOND

Post-Quantum Cryptography

avagy mire számíthatunk a NIST PQC döntése után?



Szabó Áron
(aron.szabo@egroup.hu)

Budapest
2022-06-30

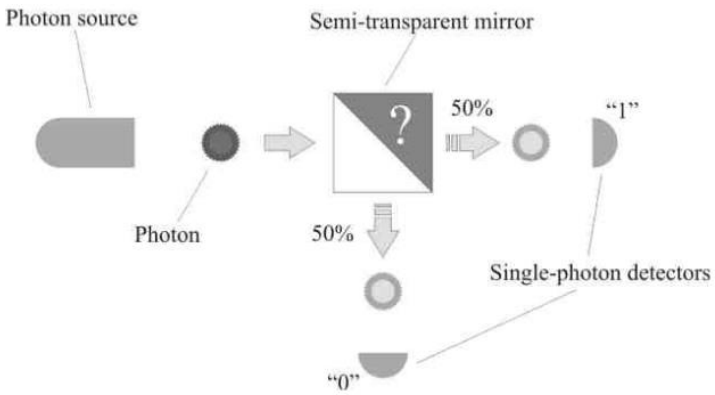
Mik a területek?

A “quantum-safe cryptography” megvalósítható

- kvantummechanikai eszközökkel: “quantum cryptography”
  pl. “Quantum Key Distribution” (QKD) BB84 protokoll révén kerül egyeztetésre az adatot rejtjelező “one-time pad” vagy AES szimmetrikus kulcs az SSL/TLS handshake során RSA vagy Diffie-Hellman helyett (kábelen, 60-90 km-es szakaszokkal “szobahőmérsékleten”, 200 km-es szakaszokkal 3 Kelvin fokon)

- hagyományos eszközökkel: “post-quantum cryptography”
  pl. “code-based” vagy “lattice-based” aszimmetrikus algoritmus révén kerül egyeztetésre az adatot rejtjelező AES szimmetrikus kulcs az SSL/TLS handshake során RSA vagy Diffie-Hellman helyett

A “quantum-safe cryptography” területén az olyan kvantumszámítógépek érdekesek, amik a Shor algoritmus és Grover algoritmus futtatására képesek, illetve az olyan véletlenszám-generátorok hasznosak, amelyek Hadamard-transzformáción alapulnak.



Mik a vélelmek és félelmek?

Ha ma kell valamit aláírnom/hitelesítenem 10 évre, akkor mit használjak?

Az adatok, dokumentumok (felül)hitelesítésére még van időnk az utolsó előtti pillanatig, elég akkor egy "quantum-safe" algoritmuson alapuló pl. archív időbélyeget beszerezni. Ezzel biztosíthatjuk a hitelesség folytonosságát.

Ha ma kell valamit rejtjeleznem/titkosítanom 10 évre, akkor mit használjak?

A bizalmasság biztosításával már rég elkéstünk...
(WikiLeaks várható)

2009. évi CLV. törvény a minősített adat védelméről

5. § (6) Az érvényességi idő:
a) „Szigorúan titkos!" és „Titkos!" minősítési szintű adat esetén legfeljebb 30 év,
b) „Bizalmas!" minősítési szintű adat esetén legfeljebb 20 év,
c) „Korlátozott terjesztésű!" minősítési szintű adat esetén legfeljebb 10 év lehet.

Mik a tervek?

Ha a közeli jövőben kell valamit rejtjeleznem/titkosítanom, akkor mit használjak?

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (2022-07-01)

1. § (1) E törvény alkalmazásában
49. poszt-kvantumtitkosítás:
[...] kvantumszámítógép által megvalósított támadás ellen [...] megoldást nyújtó titkosítás, amely során a két végpont közötti kommunikáció felhasználásával, az adatátvitellel megosztott kulcsot hoz létre a két végfelhasználó között [...];

1. § (1) E törvény alkalmazásában
50. poszt-kvantumtitkosítás alkalmazásra kötelezett szervezet:
[...]
a) a kormányzati célú hálózatokról szóló kormányrendelet szerinti igénybevételre kötelezett szervezet,
b) a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény szerinti bank, valamint
c) [...] közműszolgáltató és [...] közszolgáltatást nyújtó szervezet.

Mik a fejlemények?

E-GROUP
SOFTWARE & BEYOND

2020-07-22 - NIST PQC Round 3 Finalists

	Public-Key Encryption Key-Encapsulation Mechanism		Digital Signature	
	Finalist	**Alternate**	**Finalist**	**Alternate**
code-based	Classic McEliece	BIKE HQC		
lattice-based	CRYSTAL-KYBER NTRU SABER	FrodoKEM NTRU Prime	CRYSTAL-DILITHIUM FALCON	
isogeny-based		SIKE		
multivariate			Rainbow	GeMSS
zero-knowledge				Picnic
hash-based				SPHINCS+

Mik a fejlemények?

E-GROUP
SOFTWARE & BEYOND

2022-04-19 - NIST PQC Winners (???)

dustin...@nist.gov Apr 19, 2022, 10:09:39 PM

to pqc-forum, dustin...@nist.gov

Everybody,

We appreciate your patience. The announcement of the algorithms we will standardize is still coming very soon. This is a major milestone of our project, and the delay is not due to technical considerations but is due to some legal and procedural steps that are taking more time than we anticipated. Again, thank you for your patience.

The PQC team

dustin...@nist.gov Jun 28, 2022, 5:42:57 PM (15 hours ago)

to bongh...@gmail.com, pqc-forum, SH

We've been asked for an update on where things stand with our announcement.

We know the delay is frustrating, and we are also very eager for it to happen. We want to emphasize that no technical issues are behind the delay in the announcement. There are still some legal and procedural steps being taken care of, and while we remain hopeful that we'll be able to announce very soon, the remaining steps are out of our hands. So, we cannot provide more tangible information on when the announcement will come.

We do have some information we can share. Our next NIST PQC Standardization Conference will be held Nov 29 – Dec 1, 2022. As NIST is not yet welcoming visitors, the conference will be held virtually. We will shortly send out a Call for Papers with more information.

Dustin Moody

NIST PQC team

Mik a fejlemények?

E-GROUP
SOFTWARE & BEYOND

2022-04-19 - NIST PQC Winners (???)

crypto libraries
CA
HW eszközök
tanúsítások
...

https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

Timeline

**This is a tentative timeline, provided for information, and subject to change.*

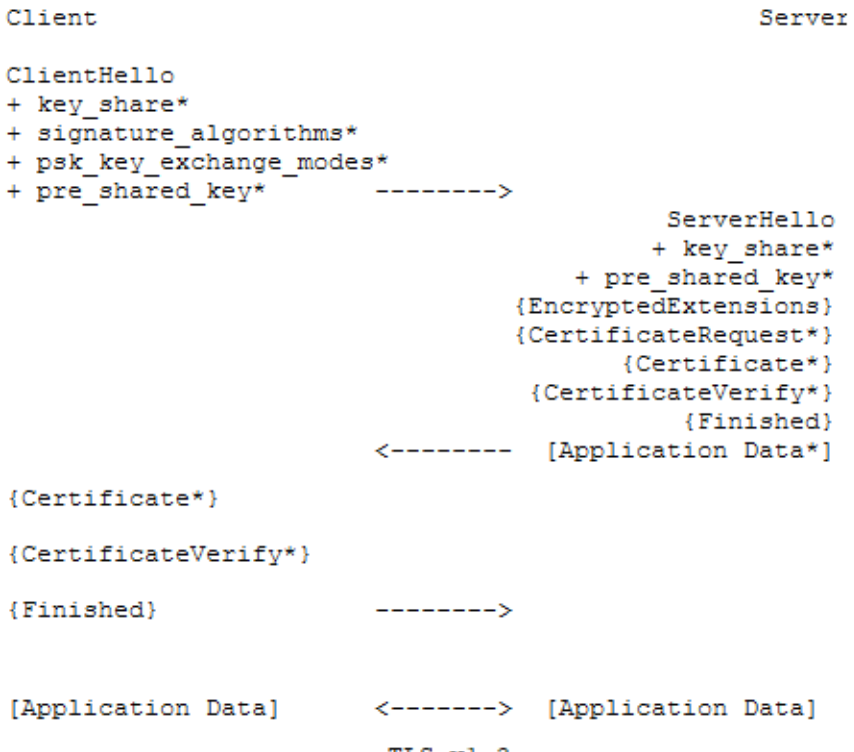
Date	
Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: *Announcement and outline of NIST's Call for Submissions (Fall 2016)*, *Dustin Moody*
April 28, 2016	NIST releases NISTIR 8105, Report on Post-Quantum Cryptography
Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Dec 4, 2017	NIST Presentation at AsiaCrypt 2017: *The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition"*, *Dustin Moody*
Dec 21, 2017	Round 1 algorithms announced (69 submissions accepted as "complete and proper")
Apr 11, 2018	NIST Presentation at PQCrypto 2018: *Let's Get Ready to Rumble - The NIST PQC "Competition"*, *Dustin Moody*
April 11-13, 2018	First PQC Standardization Conference - Submitter's Presentations
January 30, 2019	Second Round Candidates announced (26 algorithms)
March 15, 2019	Deadline for updated submission packages for the Second Round
May 8-10, 2019	NIST Presentation at PQCrypto 2019: Round 2 of the NIST PQC "Competition" - What was NIST Thinking? (Spring 2019), *Dustin Moody*
August 22-24, 2019	Second PQC Standardization Conference
July 22, 2020	Third Round Candidates announced (7 Finalists and 8 Alternates)
October 1, 2020	Deadline for updated submission packages for the Third Round
2022/2024	Draft Standards Available

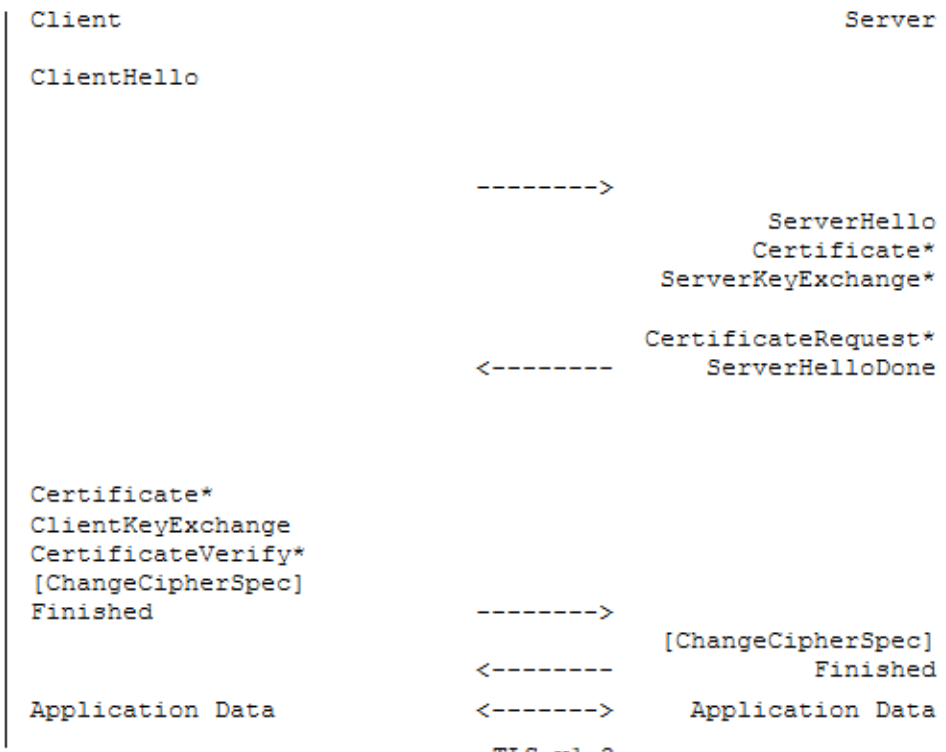
Mik a teendők?

2018-08-10 – SSL/TLS v1.3 vs. SSL/TLS v1.2

“long-term” RSA helyett “ephemeral” Diffie-Hellman kulcsegyeztetés

Perfect Forward Secrecy





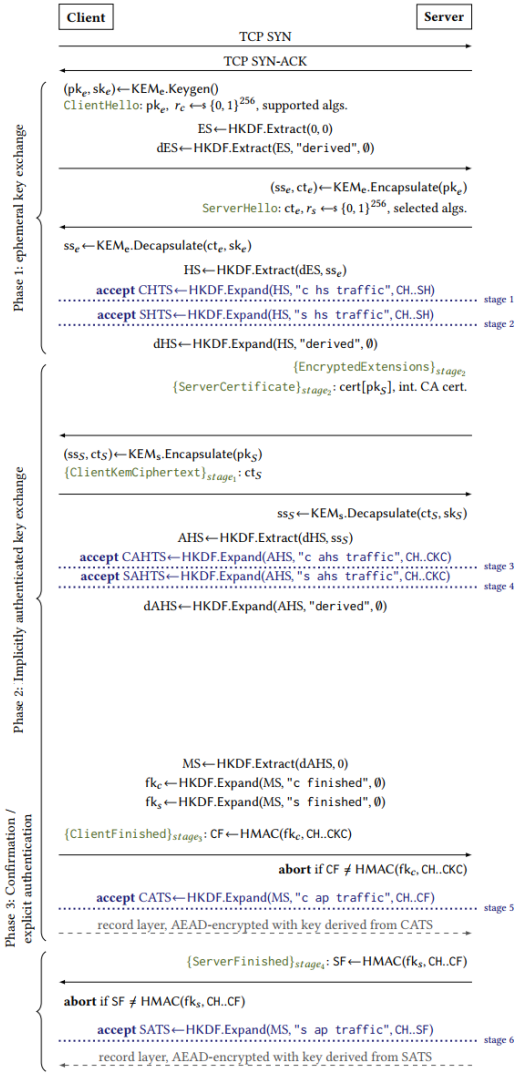
Mik a teendők?

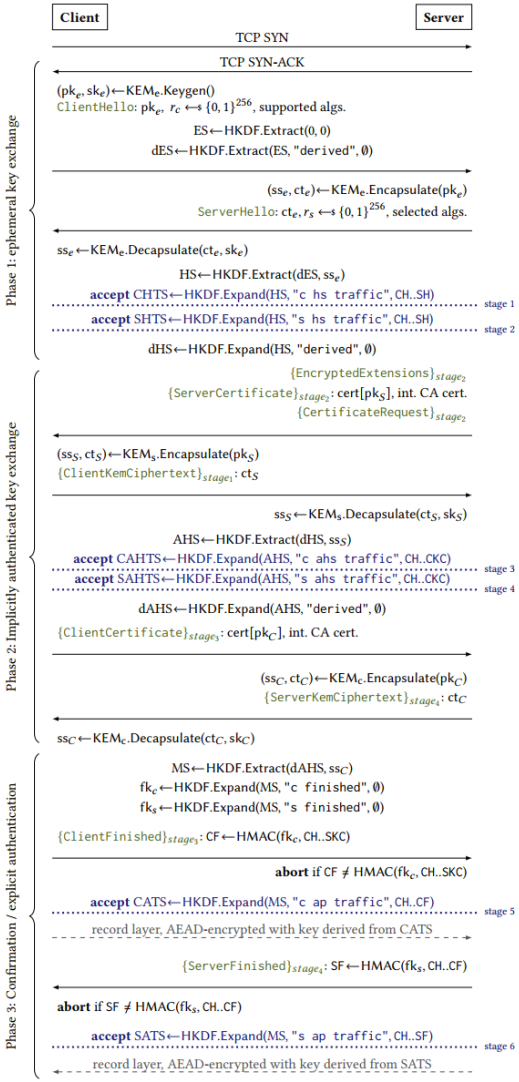
E-GROUP
SOFTWARE & BEYOND

2020-11-09 - SSL/TLS v1.3

KEMTLS

Peter Schwabe
Douglas Steblia
Thom Wiggers



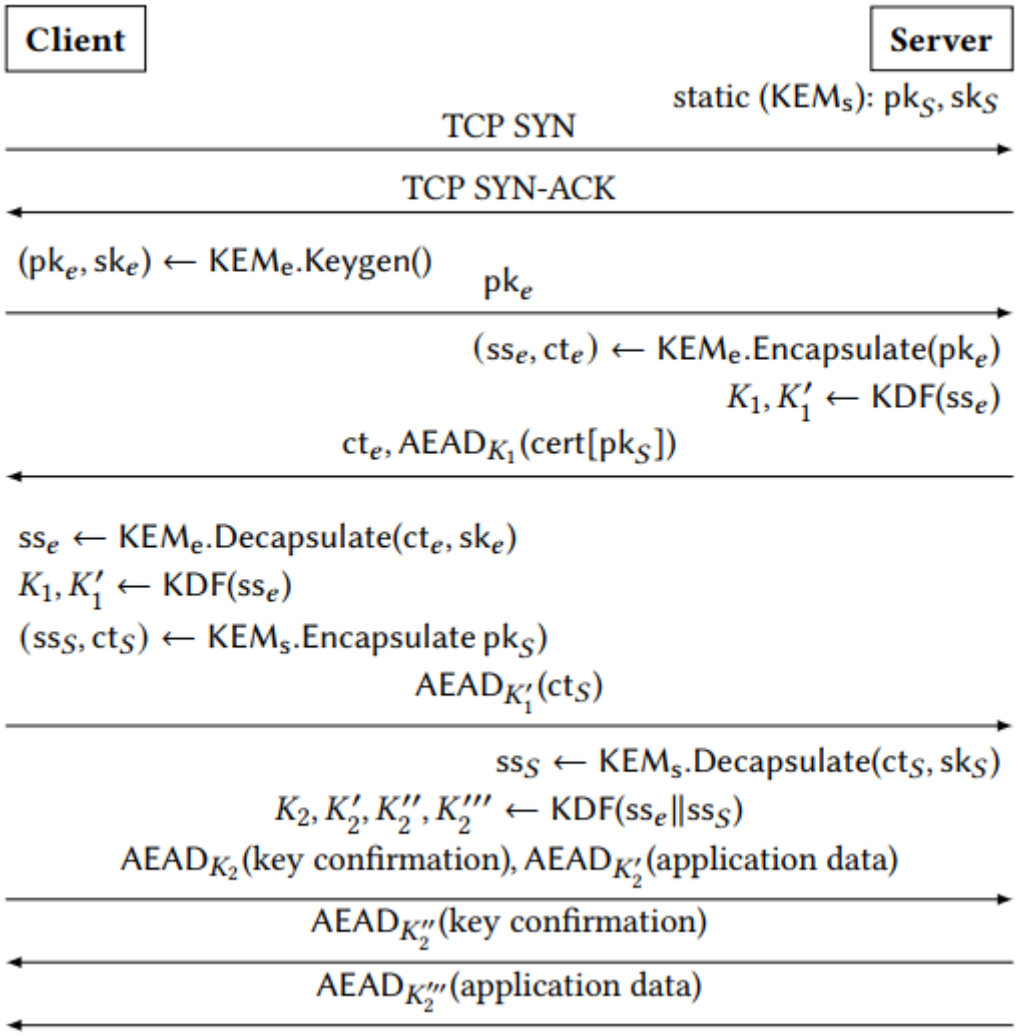


Mik a teendők?

E-GROUP
SOFTWARE & BEYOND

2020-11-09 – SSL/TLS v1.3

pk - public key
sk - secret key
ss - shared secret
ct - ciphertext
K - key space

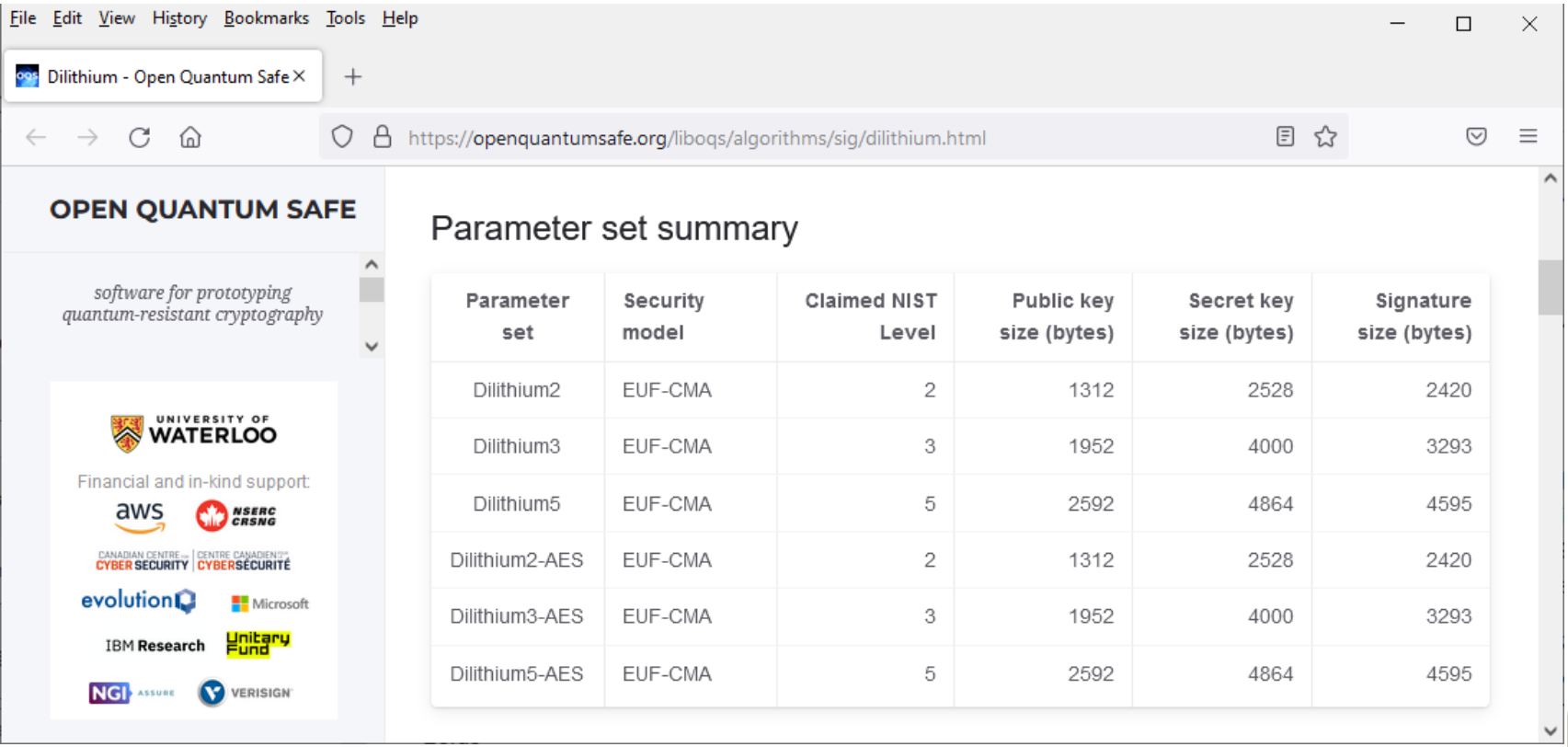


Mik a teendők?

E-GROUP
SOFTWARE & BEYOND

2022-???-??? – A méretproblémák (ld. RSA vs. ECDSA @ IoT) itt is megjelennek.

1977	RSA	(2048)	“quantum-safe”: no	signature size:	2 048 bit
2005	ECDSA	(P-256)	“quantum-safe”: no	signature size:	512 bit
2017	Dilithium	(2592)	“quantum-safe”: yes	signature size:	36 760 bit
=>	NIST PQC Round 4 Digital Signature				



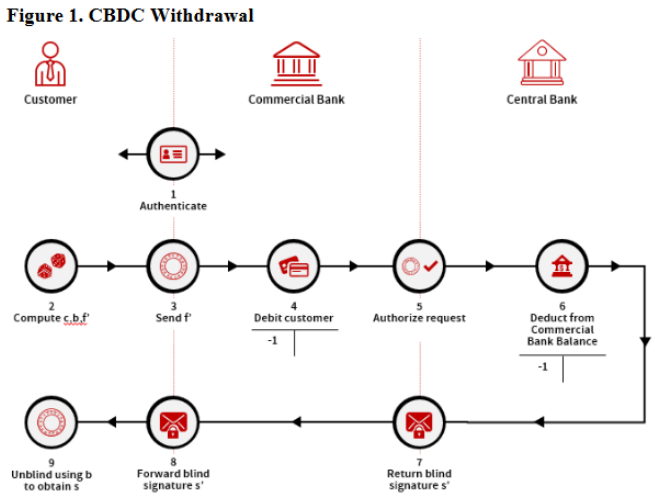
Parameter set	Security model	Claimed NIST Level	Public key size (bytes)	Secret key size (bytes)	Signature size (bytes)
Dilithium2	EUF-CMA	2	1312	2528	2420
Dilithium3	EUF-CMA	3	1952	4000	3293
Dilithium5	EUF-CMA	5	2592	4864	4595
Dilithium2-AES	EUF-CMA	2	1312	2528	2420
Dilithium3-AES	EUF-CMA	3	1952	4000	3293
Dilithium5-AES	EUF-CMA	5	2592	4864	4595

Mik a teendők?

2022-???-??? – vak aláírás, homomorf rejtjelezés

vak aláírás (mindegyiknél lehetséges)

- CBDC (Central Bank Digital Currency)
  David Chaum, Swiss National Bank



homomorf rejtjelezés (csak “lattice-based” jó, “code-based” nem)

- e-voting
  érzékeny választási adatok, rejtjelezett szavazatok összeszámlálása
- e-health
  érzékeny egészségügyi adatokkal végzett statisztikai számítások
- federated learning
  érzékeny adatokon végzett algoritmus-tanítás

  algoritmushoz megy az adat, ahol a tanítás történik
  algoritmus megy az adathoz, ahol a tanítás történik
  algoritmus és adat megy a 3rd party szolgáltatáshoz, ahol a tanítás történik

Mik a teendők?

E-GROUP
SOFTWARE & BEYOND

A biztonságos technológiaváltáshoz mély ismeretszerzés szükséges!

Az RSA-ról elliptikus görbékre való váltásnál még napjainkban is előjönnek súlyos hibák a .NET (Microsoft, 2020-01-14) és Java (Oracle, 2022-04-19) rendszereinél:

- CVE-2020-0601
  Microsoft nem ellenőrizte az elliptikus görbék “G generator/base point” értékét
- CVE-2022-21449
  Oracle nem ellenőrizte a NULL értékű elliptikus görbés aláírásokat

A “quantum-safe” SIKE rejtjelezőt is még meg kell tanulni biztonságosan használni, hogy pl. a teljesítményingadozások megfigyelésével (“side-channel attack”) se derüljenek ki a kriptográfiai kulcsok, mint a Hertzbleed (2022-06-15) támadásnál a

- CVE-2022-24436
  Intel
- CVE-2022-23823
  AMD

processzorok esetében.

Ezek alapján nemzetbiztonsági szempontból (is) fontos, hogy a “quantum-safe” algoritmusokra való váltást megelőzze egy alapos felkészülés, matematikai és informatikai kódaudit, üzleti igényekhez való igazítás.

Köszönöm a figyelmet!

E-GROUP
SOFTWARE & BEYOND

Szabó Áron
(aron.szabo@egroup.hu)