

Napadi kvantnim računalima

Pregled osnovnih pojmove napada
kvantnim računalima, kvantne i
postkvantne kriptografije

Kvantna mehanika – osnovni pojmovi

- Disclaimer: predavač nije fizičar i nema pojma o kvantnoj mehanici 😞
- Superpozicija (*superposition*)
 - Sustav može biti istovremeno u više stanja
 - Kvantni bit (*qubit*): $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
- Kvantno sprezanje (*entanglement*)
 - Dva ili više qubita mogu biti spregnuti tako su im stanja međuvisna
 - *Sustav od dva qubita*: $\alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$
- Kvantna vrata
 - Rade na kvantnim bitovima
 - Npr. X vrata: $X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$.

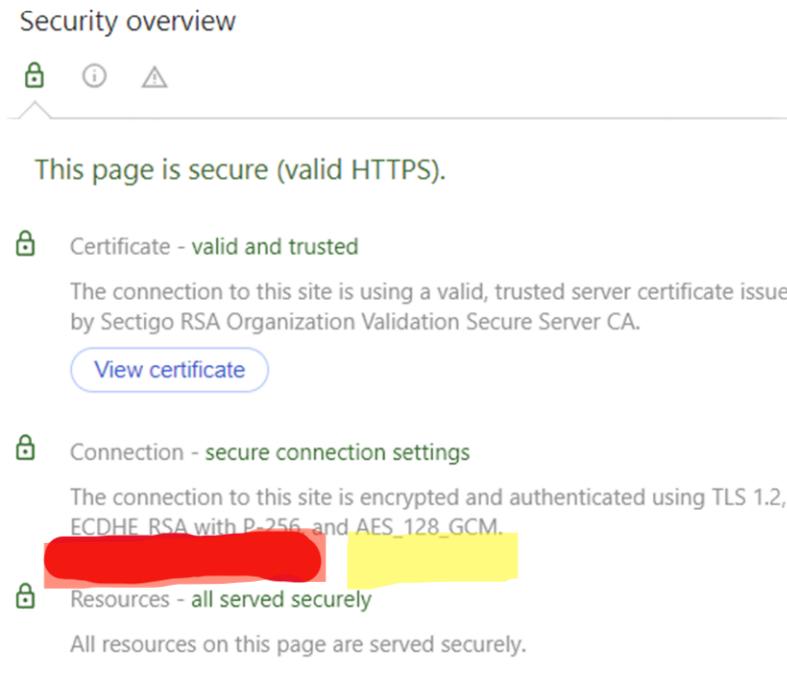
Kvantna računala

- Kvantni sklopovi
 - Grade se od kvantnih vrata
 - Mogu sve što i „obični“ logički sklopovi (ali ne direktno)
- Kvantni paralelizam (puno, puno pojednostavljeno)
 - Klasični algoritam: pokreni algoritam za jedan ulaz
 - Kvantni algoritam: stanje je superpozicija svih mogućih ulaza, pokreni algoritam i izračunaj izlaz za sve moguće ulaze, odaberi željeni izlaz
- Teškoće
 - Ne možemo očitati stanje cijelog spregnutog sustava
 - *No cloning theorem* – nemoguće je kopirati kvantne bitove

Napadi na kriptografiju kvantnim računalima

- Peter Shor (1997). „Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”
 - RSA, Diffie-Hellman i povezane sheme su potpuno razbijene.
- Lov K. Grover (1998). „A framework for fast quantum mechanical algorithms”
 - Napad u $2^{n/2}$ koraka na bilo koju blok šifru s veličinom ključa n
- Obrane
 - Simetrična kriptografija: veći ključevi (npr. 256 umjesto 128 bitova)
 - Asimetrična kriptografija: novi algoritmi, procesi standardizacije u tijeku

Osnovni kriptografski algoritmi – napadi



Simetrični algoritmi – smanjena razina sigurnosti!

- Simetrične šifre
- Kriptografske funkcije sažetka
- Kodovi za integritet poruke

Asimetrični algoritmi – potpuno razbijeni

- Asimetrične šifre
- Digitalni potpisi
- Diffie-Hellmanova razmjena ključeva

Koliko je opasna ova prijetnja?

- Mišljenja variraju između:
 - Napadi kvantnim računalima su novi izmišljeni Y2K problem!
 - Kinezi već razbijaju kriptografiju kvantnim računalima.
- Ozbiljne institucije smatraju:
 - Praktični napada kvantnim računalima mogući u narednim desetljećima.
 - Potrebno je već danas krenuti s procesima prelaska na post-kvantne algoritme.

Quantum supremacy

- Nije svako „kvantno računalo“ pogodno za napade na kriptografske algoritme!
- Već postoje demonstracije kvantnih računala koja **određene specifične probleme** mogu riješiti brže nego klasična računala.
- Arute, F., et al. (2019). "Quantum supremacy using a programmable superconducting processor." *Nature*, 574(7779), 505-510. DOI: 10.1038/s41586-019-1666-5.
 - 53-qubitno kvantno računalo
 - Problem: „sampling the output of a pseudo-random quantum circuit“
 - Kvantno računalo: 200 sekundi – klasično superračunalo trebalo 10000 godina

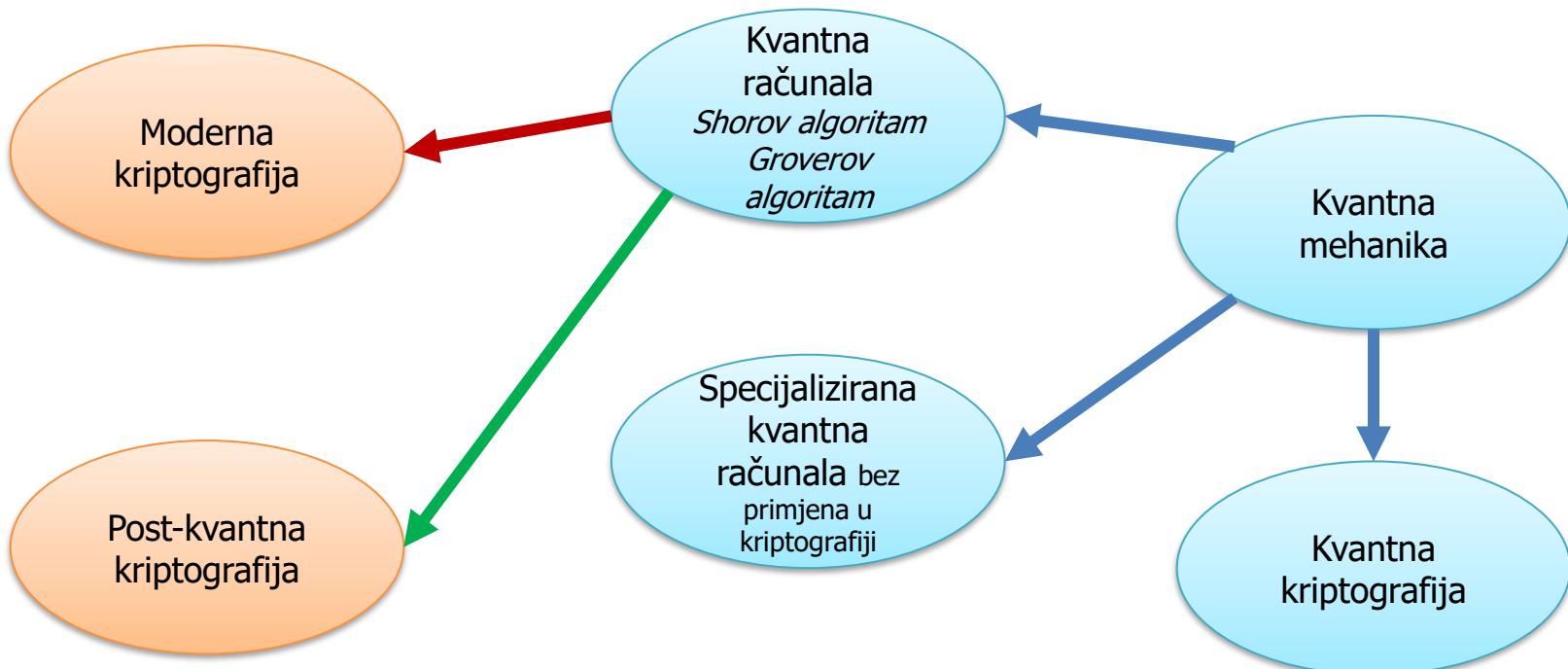
Post-kvantna kriptografija

- Algoritmi koji su (vjerujemo) otporni na napade kvantnim računalima
- Algoritmi su namijenjeni običnim, klasičnim, računalima.
- Tri klase:
 - Zasnovani na hash funkcijama
 - Zasnovani na rešetkama
 - Zasnovani na izogenijama
- Aktivno područje znanstvenog istraživanja
- Postupci standardizacije u tijeku
- Upitna sigurnost!

Kvantna kriptografija – *Quantum Key Distribution*

- Sigurna razmjena ključeva temeljena na principima kvantne mehanike
- Nije zasnovana na kvantnim računalima!
- Primjer: BB84 protokol
 - Ideja: Ako Alice i Bob uspješno završe protokol mora biti da nitko nije kopirao (mjerio) kvantne bitove koje su razmijenili jer bi mjerjenje narušilo uspješno izvođenje protokola.
- Nedostaci:
 - Specijalizirana oprema
 - Potrebna direktna veza između sudionika

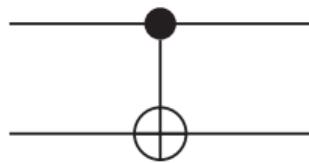
Mapa osnovnih pojmoveva



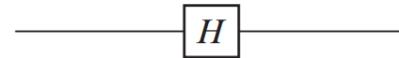
Podsjetnik – osnovni pojmovi

- Superpozicija (*superposition*)
 - Sustav može biti istovremeno u više stanja
 - Kvantni bit (*qubit*): $\alpha_0|0\rangle + \alpha_1|1\rangle$
- Kvantno sprezanje (*entanglement*)
 - Dva ili više qubita mogu biti spregnuti tako su im stanja međuvisna
 - *Sustav od dva qubita*: $\alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$
- Kvantna vrata
 - Rade na kvantnim bitovima
 - Npr. X vrata: $X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$.

Kvantna vrata – primjeri



Hadamardova vrata



CNOT

Input	Output
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$

$$H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Kvantna vrata – ograničenja

- Funkcija koju računaju kvantna vrata mora biti:
 - *linear operator* na prostoru kvantnog stanja, što više *unitarni operator*
 - *Invertibilna*
- Nemoguće kopiranje qbitova!
- Jedna posljedica: Nije moguće direktno implementirati I vrata jer se gubi informacija.

Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

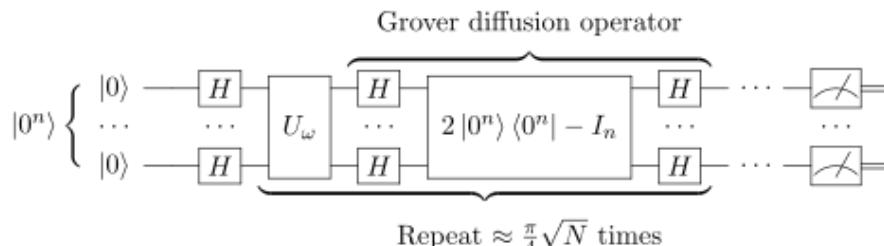
Nestrukturirano pretraživanje

- Problem nestruktuiranog pretraživanja:
 - Zadana je funkcija $f: \{1, \dots, N\} \rightarrow \{0, 1\}$
 - Za samo jedan ulaz x vrijedi $f(x) = 1$
 - Potrebno je pronaći x sa što manje evaluacija funkcije f
 - Funkcija f je crna kutija, možemo je evaluirati ali ne znamo kako radi iznutra
- Klasično računalo treba $O(N)$ koraka

1	2	3	4	...	x	...	N-2	N-1	N
0	0	0	0	...	1	...	0	0	0

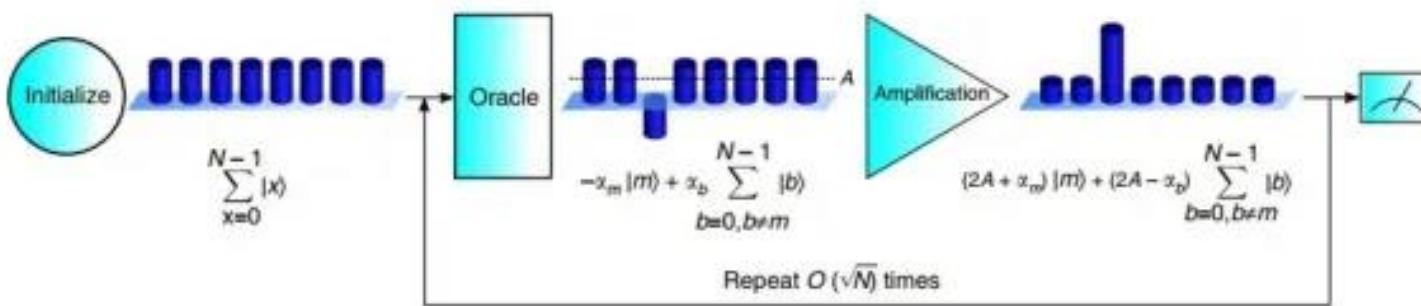
Groverov algoritam

- Lov K. Grover (1998). „A framework for fast quantum mechanical algorithms“
- Kvantni sklop za nestrukturirano pretraživanje
 - Radi u $O(\sqrt{N})$ koraka!
 - Pronalazi x s velikom vjerojatnošću.



wikipedia.org

Groverov algoritam – koraci



Demystifying Grover's Algorithm: a way quantum computing can serve power and energy applications, March 27, 2023 Abhishek Jadhav

Groverov algoritam – posljedice

- Brute-force napad na simetrične kriptosustave je problem nestrukturiranog pretraživanja!
 - $c = AES(k, m)$
 - $f(k) = AES(k, m) == c?$
- Ključ veličine n bitova se može pronaći u $2^{n/2}$ koraka!

Traženje perioda

- Problem traženja perioda:
 - Zadana je funkcija $f: \mathbb{Z}_N \rightarrow S$
 - Funkcija je periodička s periodom π ako vrijedi $f(x + \pi) = f(x)$ za svaki x
 - Potrebno je pronaći najmanji period sa što manje evaluacija funkcije f
 - Funkcija f je crna kutija, možemo je evaluirati ali ne znamo kako radi iznutra
- Klasično računalo treba $O(N)$ koraka

0	1	2	3	2	5	6	7	8	...
1	5	3	1	5	3	1	5	3	...

Shorov algoritam

- Peter Shor (1997). „Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”
- Pronalazi period funkcije u $O(\log^2 N)$ koraka
 - Zasnovan na kvantnoj Fourierovoj transformaciji.
- Problem faktoriziranja brojeva se može efikasno (i klasično) svesti na problem traženja perioda!
- Problem diskretnog logaritma se može efikasno (i klasično) svesti na problem traženja perioda!

Napadi kvantnim računalima – posljedice

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	-----	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Chen, Lily, et al. *Report on post-quantum cryptography*. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, NIST, 2016.

Napadi „kvantnim računalima” u praksi

- 2001 – faktoriziran broj 15
 - Vandersypen, Lieven MK, et al. "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance." *Nature* 414.6866 (2001): 883-887.
- 2012 – faktoriziran broj 15
 - Martin-Lopez, Enrique, et al. "Experimental realization of Shor's quantum factoring algorithm using qubit recycling." *Nature photonics* 6.11 (2012): 773-776.
- 2012 – faktoriziran broj 21
 - Lucero, Erik, et al. "Computing prime factors with a Josephson phase qubit quantum processor." *Nature Physics* 8.10 (2012): 719-723.

Cilj!

Public-Key: (4096 bit)

Modulus:

```
00:b4:73:d2:d6:65:d3:02:ef:58:3a:f4:82:82:d3:  
a7:eo:8a:60:b2:3a:f5:b1:65:38:a7:24:0e:21:6b:  
7d:ea:9:a0:9d:33:a2:74:cd:ae:91:ba:94:b5:cc:6:  
80:b5:71:df:48:71:ca:75:4b:a7:bf:ff:26:eb:84:  
fe:fb:9:72:16:c8:c2:7e:86:d4:bf:af:ee:63:35:b9:  
c0:e4:da:05:4f:b8:48:9e:22:28:ff:55:05:23:6b:  
81:4e:b3:17:11:2c:2a:25:1f:4:e1:df:61:c8:3c:  
f2:56:69:d0:55:7d:96:10:b2:a8:7:b5:90:5b:a6:  
5e:53:8b:41:e3:c7:87:c7:31:bd:34:39:ec:19:21:  
d9:80:c4:e8:0d:db:da:03:0c:00:f4:aa:b5:82:06:  
25:0c:c5:d9:1a:62:9d:fd:0a:49:05:fc:1c:be:93:  
46:fc:ce:89:91:ff:cd:cc:5f:48:5f:dc:38:0d:75:  
6f:d2:2d:ab:cc:22:12:78:88:12:1f:fe:0:d5:4e:77:  
bc:2c:89:4d:76:7a:88:9b:5d:07:da:b3:67:98:1:  
39:ce:7a:46:ab:cf:f6:7d:57:25:13:fa:84:c4:03:  
70:af:0c:76:0c:d2:40:24:7c:59:df:77:37:59:50:  
b1:25:46:4e:42:1d:08:22:09:72:55:c4:42:ea:6f:  
6f:65:59:d4:4e:e0:3d:a3:ab:70:7:c6:69:09:30:55:  
76:62:89:f3:6f:d2:0:a6:b3:6e:19:3d:96:86:7a:  
66:94:cd:f2:cc:7a:f0:07:08:b3:69:ae:1b:ff:1c:  
71:18:a2:44:f9:db:d6:0d:84:10:81:74:49:61:62:  
d7:10:f0:01:a6:45:c0:b5:d0:52:f4:51:86:3d:e2:  
f7:16:29:5a:fa:4a:9e:27:4b:8e:46:f1:72:3e:a7:  
f5:a4:0c:e0:0b:17:9a:22:ff:f9:7:ea:ab:35:8e:01:  
84:d5:75:93:7f:e6:75:a8:7a:64:de:62:3a:02:47:  
1:a:0:23:c4:4c:3f:d0:dc:4e:33:7:6c:bb:fa:f6:  
18:10:2b:34:30:5f:c7:33:50:99:02:e9:b1:59:46:  
55:65:a6:ba:4:83:18:8b:cd:1:f1:ca:18:e2:d9:  
20:e6:b7:84:87:1f:0b:56:7c:4d:31:54:26:f2:99:  
56:c8:a6:59:a6:85:33:f2:90:cc:28:5a:c8:6c:a4:  
cb:a6:47:46:4:9a:55:39:84:64:8d:77:e7:0a:3d:  
c3:d0:12:f7:76:a8:cc:1c:b3:1f:58:85:3a:4:36:  
8:dec:9a:ec:0:e:7:1:c9:9f:4f:fb:d0:7a:07:0c:  
c6:05:b0:ab:8d:ba:72:5d:4e:23:d9:6f:0c:5c:f8:  
a6:72:d1
```

Exponent: 65537 (0x10001)

Što kažu vjerodostojni izvori?

- National Institute of Standards and Technology (NIST) – **20 godina**
 - Chen, Lily, et al. Report on post-quantum cryptography. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, NIST, 2016
- The European Union Agency for Cybersecurity (ENISA) – **ne znamo, ali želimo biti spremni**
 - POST-QUANTUM CRYPTOGRAPHY, Current state and quantum mitigation, MAY 2021, v2
- Bundesamt für Sicherheit in der Informationstechnik (BSI) – **10-20 godina**
 - Studie: Entwicklungsstand Quantencomputer Version 2.0, Datum, 13.11.2023

Teško je pronaći potpuno objektivne izvore!

Research suggests that by 2026, there is a 1 in 7 chance that quantum computers will break the most used cryptographic systems, which will go as high as 50% by 2031.¹ However, research published² in early 2023 by Chinese scholars suggests that it could happen even before.

A quantum cybersecurity agenda for Europe. Governing the transition to post-quantum cryptography, Andrea García Rodríguez, Publisher European Policy Centre

The question of when a large-scale quantum computer will be built is complicated and contentious. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge. Some experts even predict that within the next 20 or so years, sufficiently large quantum computers will be built to break essentially all public key schemes currently in use [2]. It has taken almost 20 years to deploy our modern public key cryptography infrastructure. It will take significant effort to ensure a smooth and secure migration from the current widely used cryptosystems to their quantum computing resistant counterparts. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.

Chen, Lily, et al. *Report on post-quantum cryptography*. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, NIST, 2016.

I have estimated a one in seven chance that some of the fundamental public-key cryptography tools upon which we rely today will be broken by 2026 and a 50% chance by 2031. [1,2] Although the quantum attacks are happening yet, critical decisions need to be taken *today* in order to be able to respond to these threats in the future, and organizations are already being differentiated by how well they can articulate their readiness.

Mosca, Michele (2016), Quantum Computing: A New Threat to Cybersecurity. Global Risk Institute.



evolutionQ provides scalable defense-in-depth with PQC and QKD software solutions for resilience and quantum-safe security.

OUR STORY

About evolutionQ

evolutionQ was co-founded by leading quantum-safe cryptography experts, Dr. Michele Mosca, Dr. Norbert Lütkenhaus, and Dr. David Jao.

Zdrava doza skepticizma

- Sasvim je moguće da su praktični napadi kvantnim računalima
jako jako daleko!
- Postoje puno ozbiljniji sigurnosni problemi kojima bi trebalo
posvetiti više pažnje!

On the Heffalump Threat

Peter Gutmann

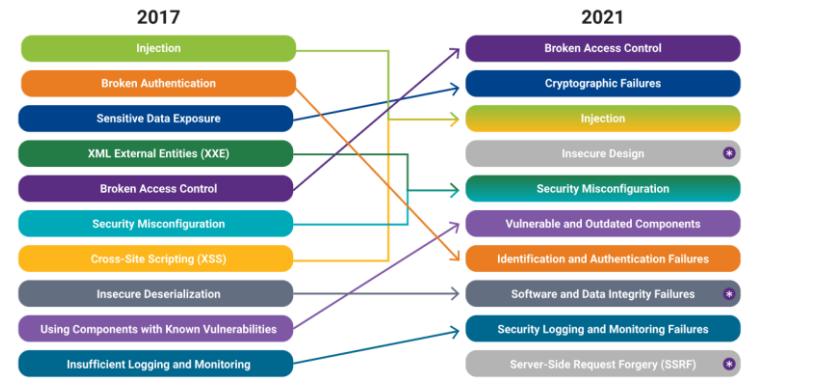
University of Auckland

pgut001@cs.auckland.ac.nz

Abstract

Over the last few years a new type of attack has been receiving a lot of attention. Unfortunately the technical details can be quite confusing to laypeople. This paper explains it in easy-to-understand terms.

<https://www.cs.auckland.ac.nz/~pgut001/>



<https://www.synopsys.com/glossary/what-is-owasp-top-10.html>

Proliferacija post-kvantnih rješenja!

- Oprez: vrlo popularno područje za znanstvena istraživanja i komercijalne proizvode upitne kvalitete!

The collage consists of three separate journal article covers:

- drones** journal cover:
 - Article title: A Quantum-Resistant Identity Authentication and Key Agreement Scheme for UAV Networks Based on Kyber Algorithm
 - Authors: Tao Xia ^{1,*†}, Menglin Wang ^{1,*}, Jun He ^{1,†}, Gang Yan
 - Keywords: Security and Communication Networks
 - Notes: ¹ College of Information at Wuhan 430000, China; ² School of Information Sec Correspondence: sttao@163.com; Tel.: +86-153-1484-2578 ([†] These authors contributed equally to this work.)
- MDPI** journal cover:
 - Article title: Post-Quantum Secure Identity-Based Random Integer Lattices for IoT-enabled AI Applications
 - Authors: Dharminder Dharminder, Ashok Kumar Das , Sourav Saha, Basudeb Bera, Athanasios V. Vasilakos
 - Notes: First published: 06 July 2022 | <https://doi.org/10.1155/2022/5498058> | Citations: 3
 - Academic Editor: Wenbo Shi
- Security and Communication Networks** journal cover:
 - Article title: Post QUANTUM LATTICE-BASED SECURE FRAMEWORK USING AGGREGATE SIGNATURE FOR AMBIENT INTELLIGENCE ASSISTED BLOCKCHAIN-BASED IoT APPLICATIONS
 - Authors: Prithwi Bagchi, Basudeb Bera, Ashok Kumar Das, Sachin Shetty, Pandi Vijayakumar, and Marimuthu Karuppiah

Regulativa (EU)

- (3) The future potential development of quantum computers capable of breaking today's encryption makes it necessary for Europe to look for stronger safeguards, ensuring the protection of sensitive communications and the long-term integrity of confidential information, i.e., by switching to Post-Quantum Cryptography as swiftly as possible. This new type of cryptography will remove the known vulnerabilities of current asymmetric cryptography and enhance the robustness against the threats posed by the malicious use of quantum computers.

- (5) Member States should consider migrating their current digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography as soon as possible, inducing a fundamental shift in cryptographic algorithms, protocols and systems. As highlighted in the Commission's recent White Paper "How to master Europe's digital infrastructure needs", this requires a coordinated effort involving government agencies, standardization bodies, industry stakeholders, researchers and cybersecurity professionals.

EUROPEAN COMMISSION RECOMMENDATION of 11.4.2024 on a
Coordinated Implementation Roadmap for the transition to Post-
Quantum Cryptography

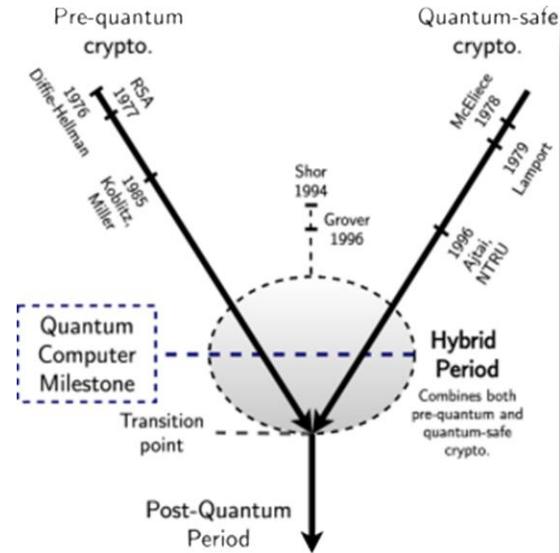
Napadač iz budućnosti!

- Problem: današnji kriptirani podaci mogu biti dekriptirani u budućnosti kada kvantna računala postanu dostupna i praktična!
 - *Store now – decrypt later* napad
- Potreba za zaštitom post-kvantnim algoritmima postoji već danas!
- Napad nije primjenjiv na sve kriptografske ključeve/algoritme/sustave.
 - Npr. kompromis FINA CA privatnog ključa



Hibridna faza

- Prijelazna faza u kojoj se kombiniraju klasični kriptografski algoritmi i post-kvantni algoritmi
 - Jednostavni primjer: dvostruka enkripcija
- Omogućuje postupni prijelaz na sigurnije kriptografske algoritme
- Smanjuje rizik od neočekivanih slabosti u novim algoritmima



A. Giron, R. Custodio, and F. Rodríguez-Henríquez.
Post-quantum hybrid key exchange: a systematic
mapping study. *Journal of Cryptographic Engineering*,
13 (1):71–88, 2023.

Post-kvantna kriptografija

Cilj

- Tražimo post-kvantne inačice asimetričnih algoritama!
 - Asimetrične šifre
 - Digitalni potpisi
 - Diffie-Hellmanova razmjena ključeva
- Novi pojam – *key encapsulation mechanism*
 - Zamjena za asimetričnu šifru
- Novi pojam – *key exchange mechanism*
 - Zamjena za Diffie-Hellmanovu razmjenu ključeva

Sustav enkapsulacije ključa (KEM)

Asimetrična enkripcija

- Trojka *efikasnih* algoritama G , E i D
 - G – algoritam koji generira par ključeva pk, sk
 - $E(m, pk)$ – algoritam enkripcije
 - $D(c, sk)$ – algoritam dekripcije

Sustav enkapsulacije ključa

- Trojka *efikasnih* algoritama G , E i D
 - G – algoritam koji generira par ključeva pk, sk
 - $E(pk)$ – algoritam enkapsulacije koji generira skriveni tekst c i k
 - $D(c, sk)$ – algoritam dekapsulacije
- Vrijedi $D(c, sk) = k$

NIST Standardizacija – kratki pregled

- 2016 – poziv za prijedloge za algoritme asimetrične kriptografije
- 2022 – objavljeni kandidati za standarizaciju
 - Key encapsulation mechanisms: CRYSTALS-Kyber
 - Digitalni potpis: CRYSTALS-Dilithium, Falcon, SPHINCS+
 - Kandidati: BIKE, SIKE, Classic McEliece, HQC
- 2023 – SIKE potpuno razbijen (Castryck and Decru)

NIST Standardizacija – epilog

- FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard, August 13, 2024
 - ML-KEM
 - Zasnovan na jednoj od inačica CRYSTALS-KYBER KEM prijedloga
- FIPS 204: Module-Lattice-Based Digital Signature Standard, August 13, 2024
 - ML-DSA
 - Zasnovan na jednoj od inačica CRYSTALS-DILITHIUM prijedloga
- FIPS 205, Stateless Hash-Based Digital Signature Standard, August 13, 2024
 - SLH-DSA
 - Zasnovan na SPHINCS+ prijedlogu

ML-KEM veličina ključa i razina sigurnosti

ML-KEM comes equipped with three parameter sets:

- ML-KEM-512 (security category 1)
- ML-KEM-768 (security category 3)
- ML-KEM-1024 (security category 5)

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

Table 3. Sizes (in bytes) of keys and ciphertexts of ML-KEM

	encapsulation key	decapsulation key	ciphertext	shared secret key
ML-KEM-512	800	1632	768	32
ML-KEM-768	1184	2400	1088	32
ML-KEM-1024	1568	3168	1568	32

Performance

Algorithm	Public key (bytes)	Ciphertext (bytes)	Key gen. (ms)	Encaps. (ms)	Decaps. (ms)
ECDH NIST P-256	64	64	0.072	0.072	0.072
SIKE p434	330	346	13.763	22.120	23.734
Kyber512-90s	800	736	0.007	0.009	0.006
FrodoKEM-640-AES	9,616	9,720	1.929	1.048	1.064

Table 1: Key exchange algorithm communication size and runtime

Algorithm	Public key (bytes)	Signature (bytes)	Sign (ms)	Verify (ms)
ECDSA NIST P-256	64	64	0.031	0.096
Dilithium2	1,184	2,044	0.050	0.036
qTESLA-P-I	14,880	2,592	1.055	0.312
Picnic-L1-FS	33	34,036	3.429	2.584

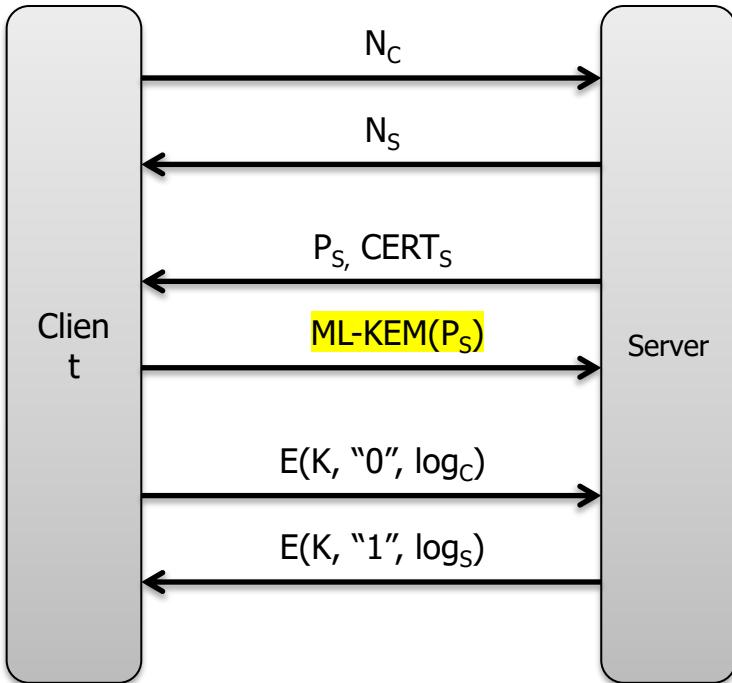
Table 2: Signature scheme communication size and runtime

Paquin, Christian, Douglas Stebila, and Goutam Tamvada. "Benchmarking post-quantum cryptography in TLS." *Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings 11*. Springer International Publishing, 2020.

Post-kvantna kriptografija

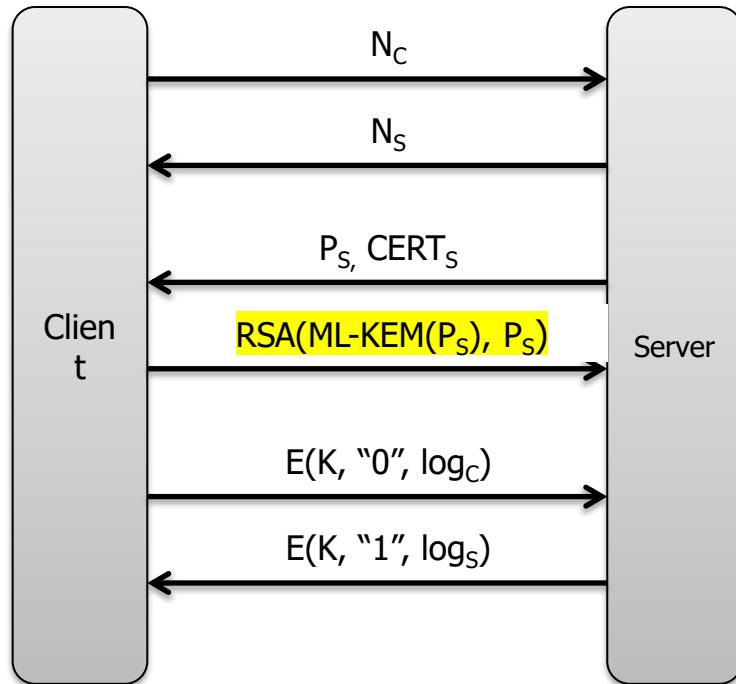
- Zamjena za klasične asimetrične algoritme!
- Standardi postoje, ali treba proći 10-20 godina prije nego što ćemo ih smatrati sigurnima.
- Veći ključevi i slabije performanse za istu razinu sigurnosti (na klasičnim računalima) u usporedbi s asimetričnim algoritmima koje zamjenjuju.
- Još nemamo post-kvantnu varijantu Diffie-Hellmanove zamjene ključeva – potrebno je redizajnirati neke protokole i sustave.

Zadatak – PQ TLS – V1



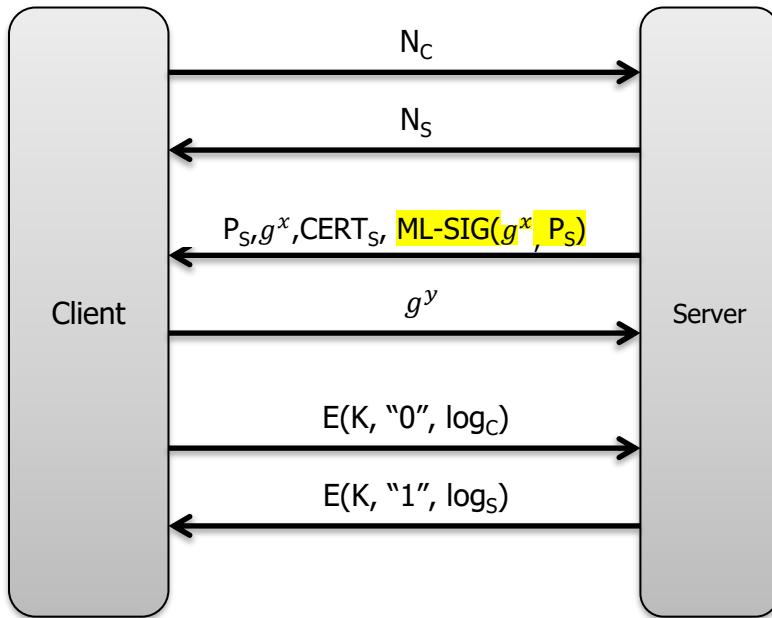
- Obzirom da nemam zamjene za post-
kvantni Diffie-Hellman
biram RSA varijantu i
prelazim na KEM!
- Prednosti i mane?

Zadatak – PQ TLS – V2



- Od viška glava ne boli?
- Prednosti i mane?

Zadatak – PQ TLS – V3



- Prednosti i mane?