COSIC

KU LEUVEN

The Quantum Threat and Post-Quantum Cryptography

Bart Preneel
COSIC KU Leuven
Bart.Preneel(at)esat.kuleuven.be @bpreneel1
SecAppDev – 4 June 2025

1

1

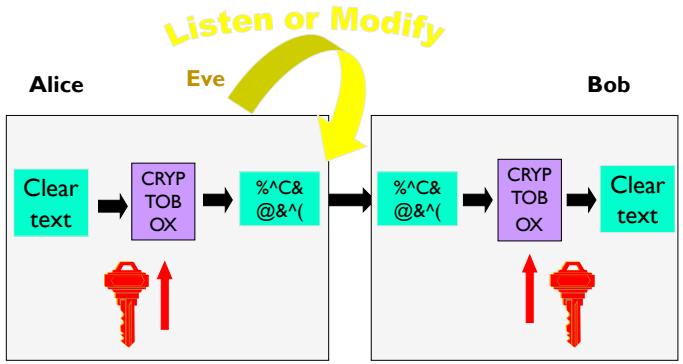
Outline

- Cryptography
- The Quantum Threat
- Post-Quantum cryptography
- QKD

2

2

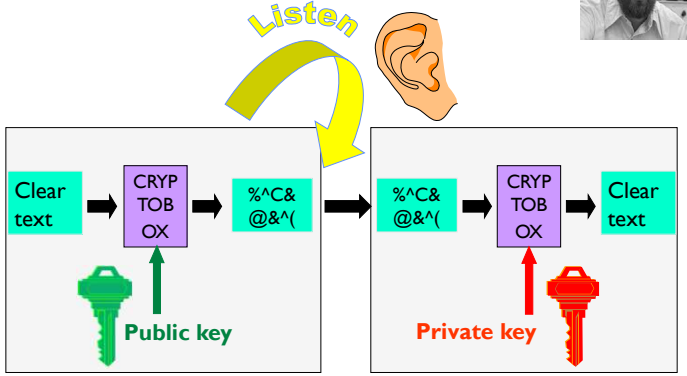
Cryptology: principle



3

3

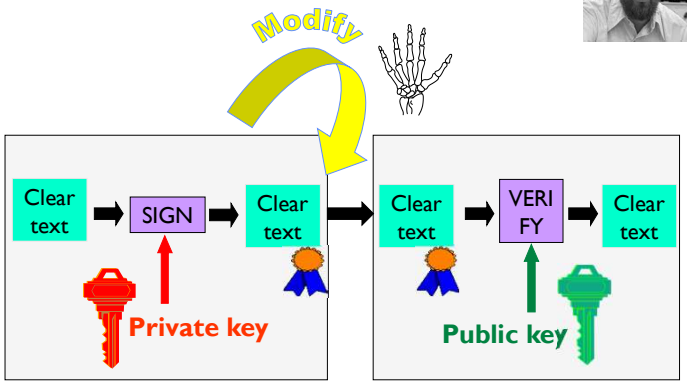
Public key cryptology: encryption



4

4

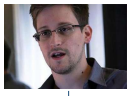
Public key cryptology: digital signature



5

5

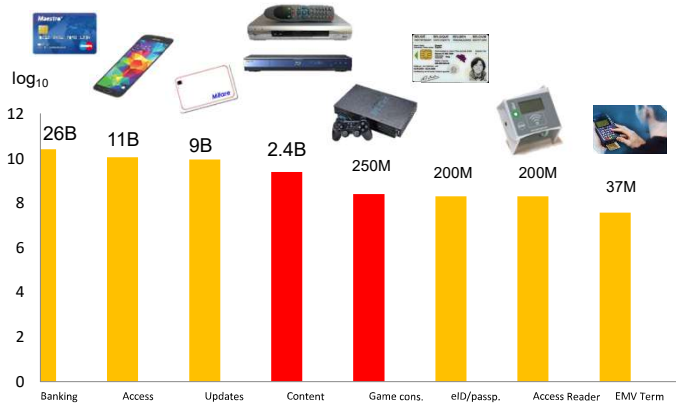
Cryptography Timeline



6

6

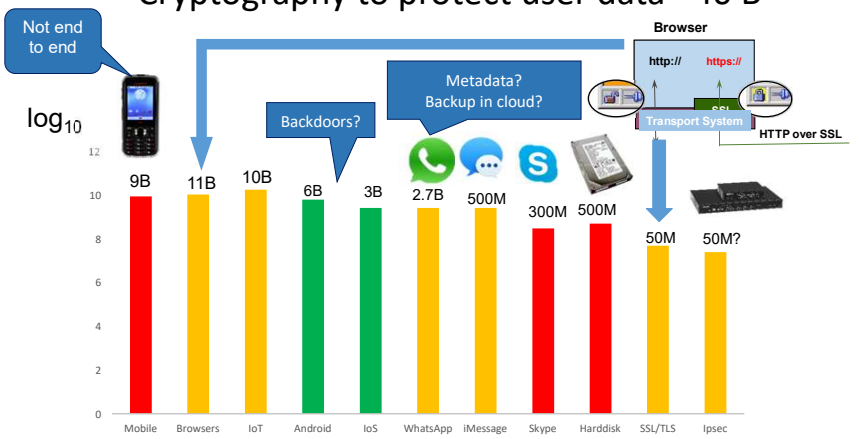
Cryptography to protect industry ~50 B



7

7

Cryptography to protect user data ~40 B



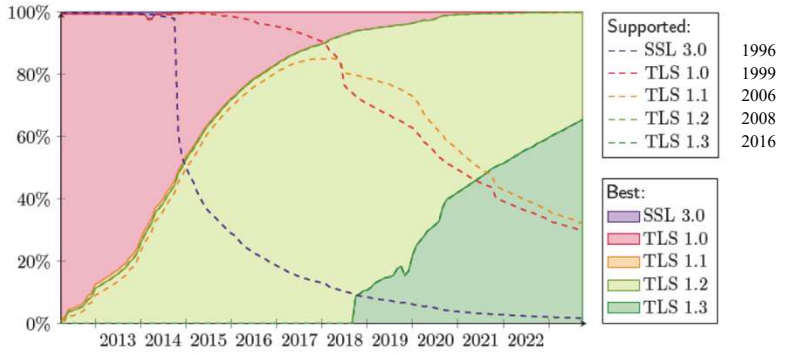
8

8

Public-key cryptography deployments ~ 60 B

9

TLS migration on top 150K websites



Source: https://www.ssllabs.com/ssl-pulse/

10

10

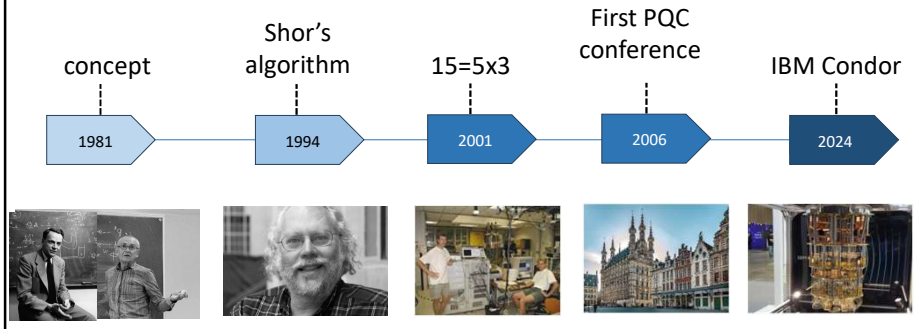
Outline

- Cryptography
- The Quantum Threat
- Post-Quantum cryptography
- QKD
- Computing on Encrypted Data

11

11

Timeline



12

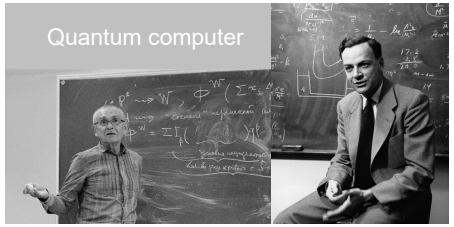
12

The advent of quantum computers

Yuri Manin 1980

Richard Feynman 1981

Exponential parallelism based on entanglement and superposition



Jan. 2014: NSA has spent $85M on research to build a quantum computer

[McKinsey'24] China has spent $14B on quantum technologies (or is it $4B?) versus $3.7B by the US

13

13

If a large quantum computer can be built

public-key cryptography algorithms have to be replaced [Shor'94]

RSA, Diffie-Hellman (including elliptic curves)

Breaking RSA-2048 requires 4096 ideal qubits (< 1 million physical qubits) https://arxiv.org/abs/2505.15917

symmetric crypto: key sizes: x2 [Grover'96]

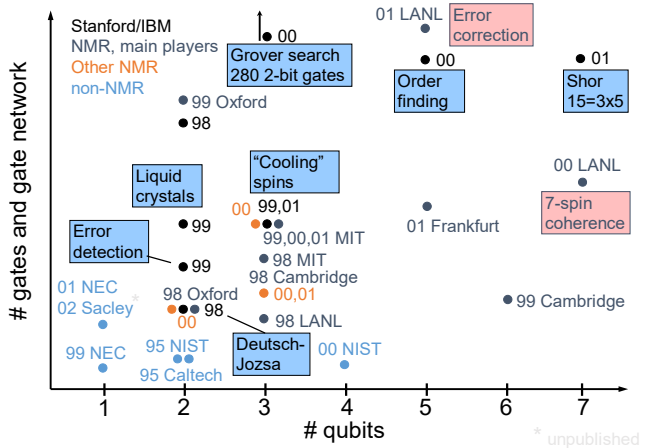
but huge devices needed; serial algorithm

Sam Jacques (CHES'24): don't worry
https://www.youtube.com/watch?v=eB4po9Br1YY

14

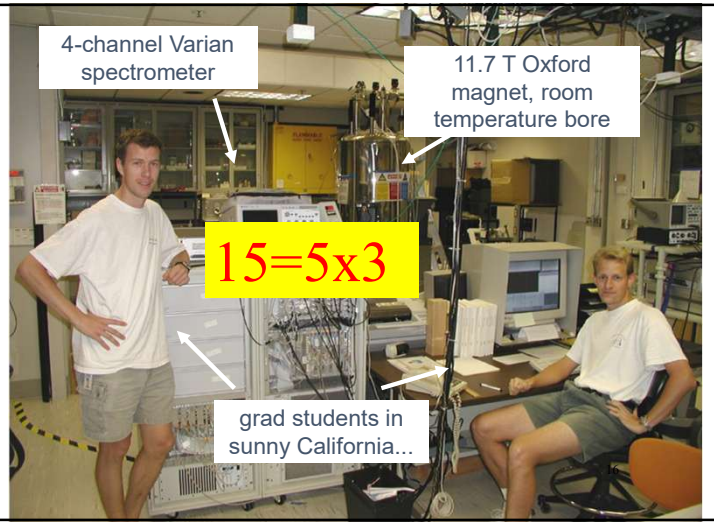
14

State of the art in coherent qubit control ('01)



15

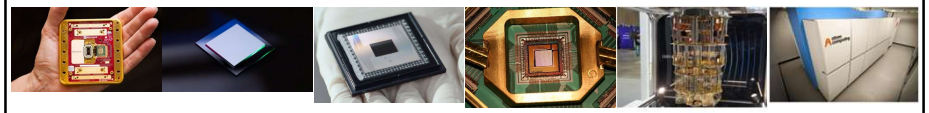
15



16

Quantum computers get names

Microsoft	Amazon	Google	Chinese Academy of Sciences and QuantumCTek	IBM	Atom
Majorana 1	Ocelot	Willow	Tianyan	Condor	
8 qubits	9 qubits	105 qubits	504 qubits	1121 qubits	1180 qubits

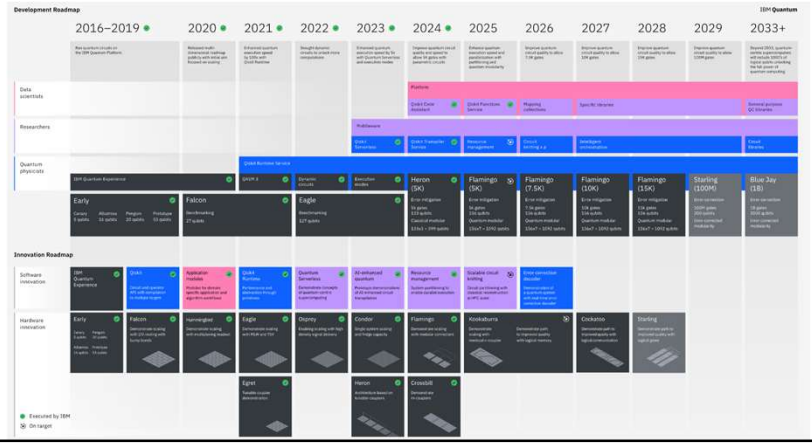


Kookabura
4158 qubits
(announced)

17

17

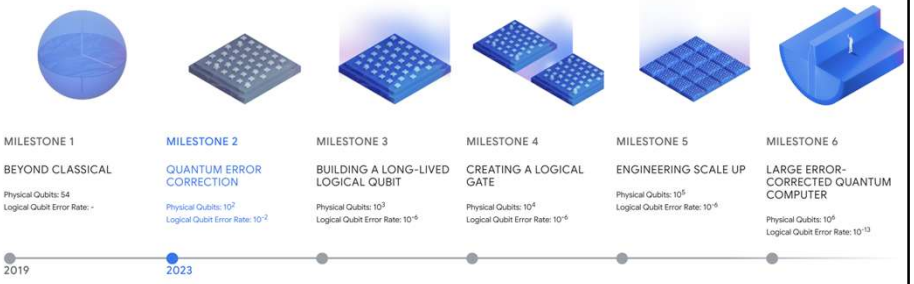
IBM Roadmap (Nov. ’24)



18

18

Google Roadmap (2025)



Source: https://quantumai.google/roadmap

19

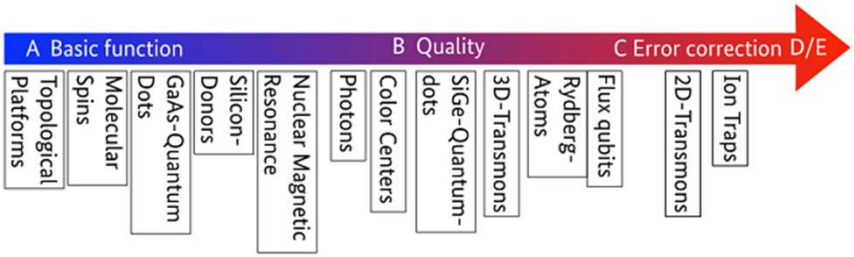
19

What does BSI say?

https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Entwicklungsstand-Quantencomputer/entwicklungsstand-quantencomputer.html

20

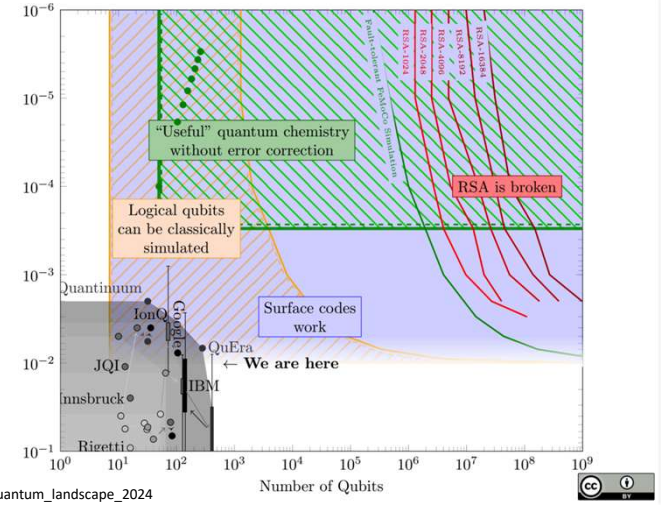
BSI Assessment of technologies



BSI: we estimate at the conservative end that it will take 16 years to build a Cryptographically Relevant Quantum Computer (CRQC)

Source: Federal Office for Information Security

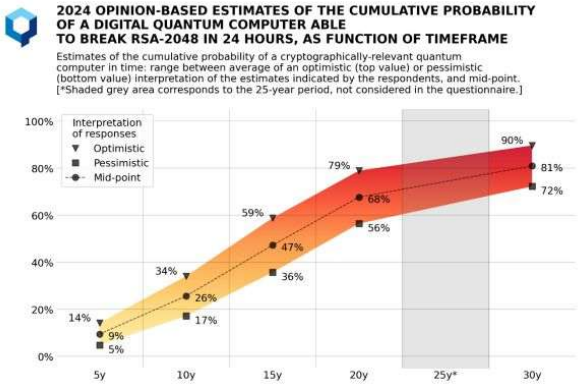
21



https://sam-jaques.appspot.com/quantum_landscape_2024

22

What do "the experts" say? (2024)



Source: EvolutionQ

23

What do some other experts say?

The Register

You can cross 'Quantum computers to smash crypto' off your list of existential fears for 30 years

RSA's Adi Shamir thinks we're safe for a generation, but more gnarly keys are still a good idea

Iain Thomson Wed 26 Apr 2023 06:28 UTC

RSA CONFERENCE Adi Shamir, the cryptographer whose surname is the "S" in "RSA", thinks folks need to stop worrying about quantum computing breaking encryption algorithms.

Speaking on the annual cryptographers' panel at the RSA Conference in San Francisco this week, he opined that in the 1990s he saw three big issues appear on the security industry's radar: AI, cryptography, and quantum computing. Two out of three had delivered, he said, and quantum computing has yet to show promise and won't for decades to come.

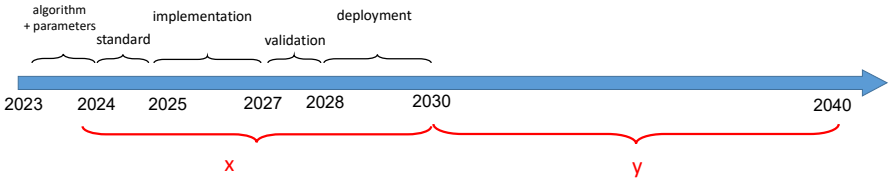
24

When to switch to post-quantum cryptography? [Mosca]

Q = #years until first large quantum computer
x = #years it takes to switch (3-12 years)
y = #years data needs to be confidential (10 years)

For digital signatures, y ≈ 0

Need to start switching in the year 2025 + Q – x – y
e.g. Q = 15, x=5, y=10: today!



25

Outline

- Cryptography
- The Quantum Threat
- Post-Quantum cryptography
- QKD

26

26

NIST Post-Quantum Competition (2016-2026)

https://en.wikipedia.org/wiki/Post-Quantum_Cryptography_Standardization
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

Encryption: KYBER
Digital signatures: Dilithium, Falcon, SPHINCS+ (hash-based signature)

	Signatures	Encryption/KEM	TOTAL
Lattice	4/3/2/2	24/9/3/1	28/12/5/3
Code	5/0/0/0	19/7/1/0	24/7/1/0
Multivariate	7/4/1/0	6/0/0/0	13/4/1/0
Hash	4/1/0/1	0/0/0/0	4/1/0/1
Other	3/1/0/0	10/1/0/0	13/2/0/0
TOTAL	23/9/3/3	59/17/4/1	82/26/7/4

IETF (independent of NIST): 2 hash-based signatures
- RFC 8554 Leighton-Micali signatures
- RFC 8391 XMSS eXtended Merkle signatures

27

27

COSIC breaks two finalists

A New Attack Easily Knocked Out a Potential Encryption Algorithm

SIKE was a contender for post-quantum-computing encryption. It took researchers an hour and a single PC to break it.

Wouter Castryck, Thomas Decru
Microsoft bounty of 50.000$

Paper 2022/214

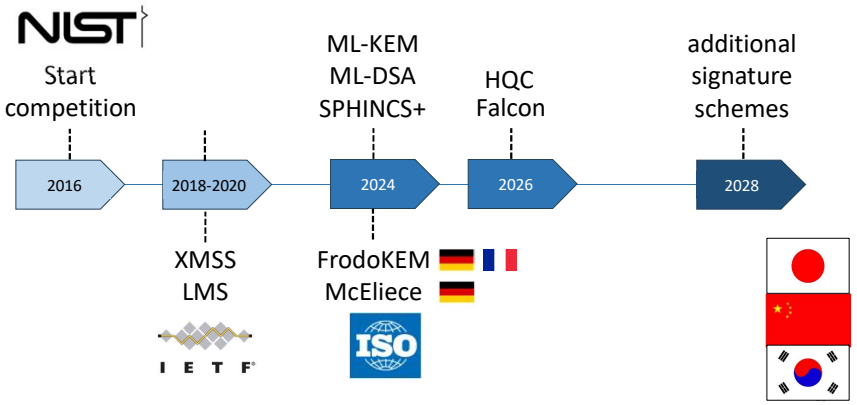
Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

28

28

Timeline standardization



29

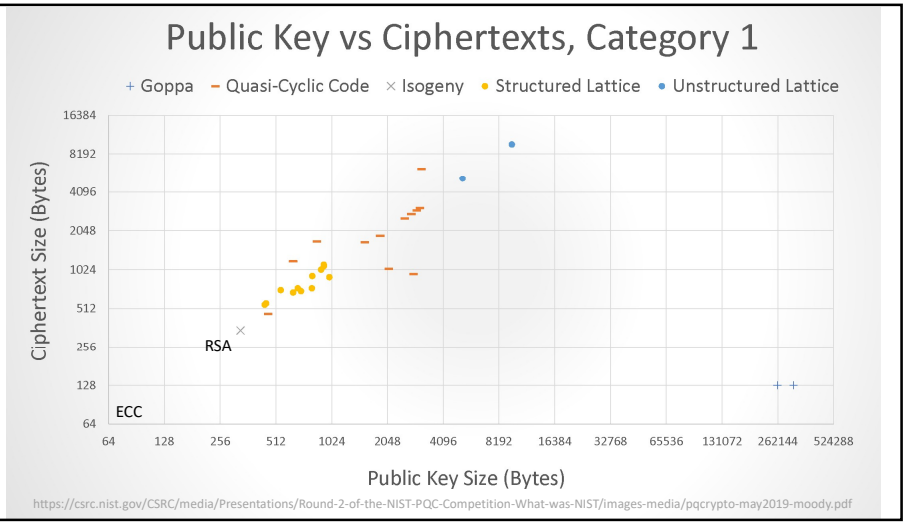
New scheme: larger sizes but not slower

- Key agreement/encryption:
  - key size + ciphertext x3..x15
  - Encryption: 2x slower than RSA, 5x faster than ECC
  - Decryption faster
- Signatures
  - Public key + signature x15..x30
  - Signing faster
  - Verification: comparable to faster

30

30

Public Key vs Ciphertexts, Category 1



31

Digital Signature comparison

source: Signature Zoo (Tom Wiggers)

Scheme	Security	Public key + signature (byte)	Sign + Verify (relative to Dilithium)
ECC (Ed25519)	X	96	0.73
Factoring (RSA)	X	528	40.2
Lattice (ML-DSA)	OK	2733	1.00
Symmetric (LMS) (3)	OK	1160	5.65
Lattice (Falcon 512)	Maybe	1563	1.85
Code (CROSS)	?	7994	27.5
MPC (Ryde) (5)	?	7532	27.5
VOLE (FAEST)	?	5728	12
Lattice (HAWK)	?	1579	0.73
Isogeny (SQISIGN)	?	241	8950
Multivariate (~~SNOVA~~) (8)	?	1264	1.15

32

32

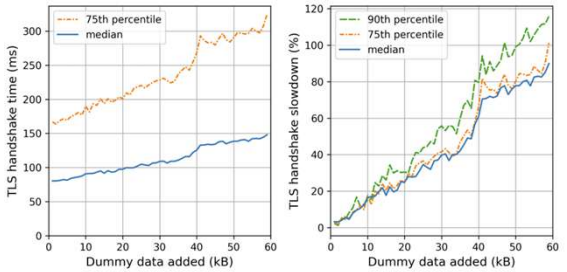
Challenges: technical

- Larger keys/ciphertexts/signatures:
- Most robust schemes have worse performance: hash-based signature and Classic McEliece
- Lattice based schemes: ML-KEM, ML-DSA, Falcon
  - Good performance
  - Some uncertainty about parameters for structured lattices
  - Decryption failure, floating point, noise sampling
- Side channel resistance: KyberSlash, KEM in Fujisaki-Okamoto mode: FO-calyps [Azouaoui et al., Surviving the FO-CALYPS: Securing PQC Implementations in Practice, RWC'22]

33

33

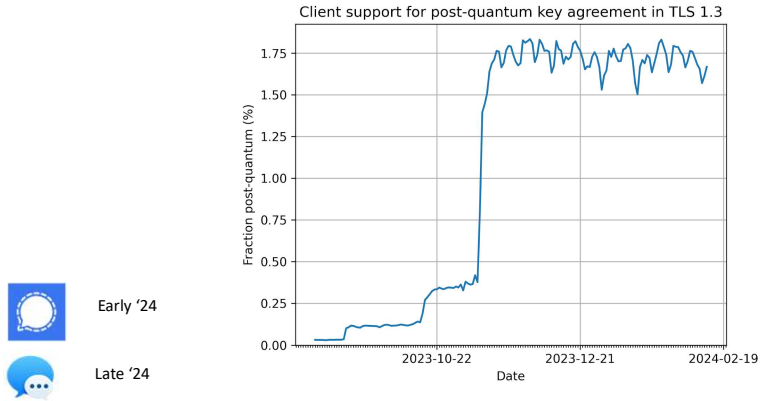
TLS slowdown (source: Cloudflare)



Performance when artificially inflating certificate chain size to simulate post-quantum certificates.

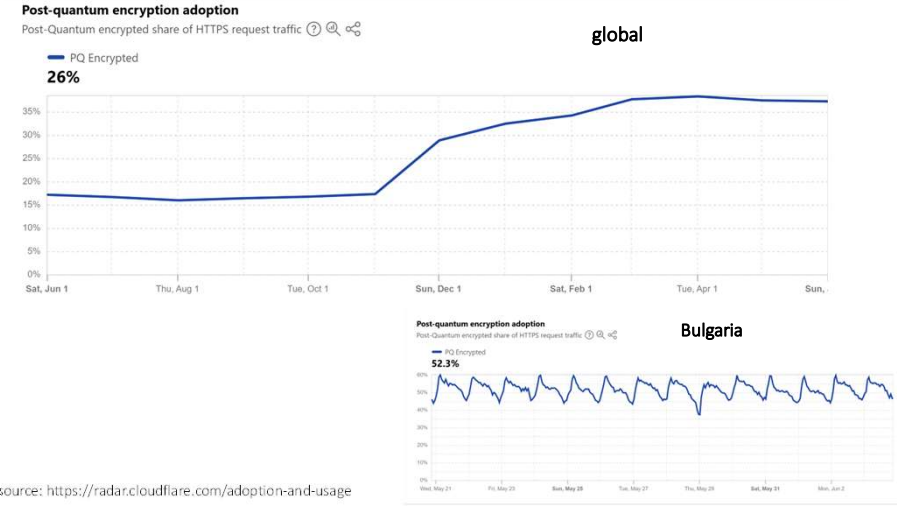
34

34



35

35



36

How to continue?

- Pre-Quantum era
  - RSA / ECC
- Hybrid era
  - RSA / ECC + Post-Quantum
- Post-Quantum Era
  - Once confidence in post-quantum is high enough

	OR: gradual transition	AND: no gradual transition
Digital signature	Ok	Long term secure
Public key encryption	No long term security	Long term secure

Migration 60 billion libraries and applications in billions of devices

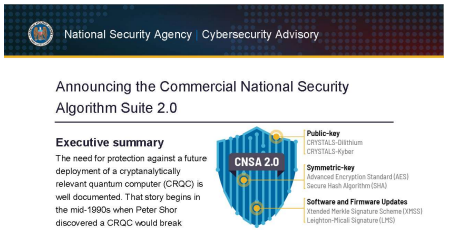
37

37

What did the NSA say in Sept.'22?

https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

AES-256, SHA-384, SHA-512
LMS/XMSS
CRYSTALS-Kyber, CRYSTALS-Dilithium level V



		2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Software/firmware signing	transition			Support and prefer						Exclusive		
Networking (VPN/routers)												
Web browsers/servers												
Operating systems												
Niche (IoT, PKI)												
Custom applications & legacy	No hybrid mode!									Update/replace		

38

What did the NIST propose in Nov.'24?

https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

	Security level	2025-2030	2031 - 2034	2035-
RSA-2048, DH, MQV	112		Deprecated	Disallowed
ECDSA, ECDH, MQC	112			
RSA-3072, DH, MQV	128			
ECDSA, ECDH, EdDSA	128			
PQC or **Hybrid**	128-256			

39

What did the White House say (17 Jan.'25)?

https://www.govinfo.gov/content/pkg/FR-2025-01-17/pdf/2025-01470.pdf

Presidential Documents

Executive Order 14144 of January 16, 2025

Strengthening and Promoting Innovation in the Nation's Cybersecurity

- Secure BGP, DNS
- Encrypt email
- End to end encryption of voice and video conferencing
- TLS 1.3
- Agencies shall implement PQC key establishment or hybrid key establishment including a PQC algorithm **as soon as practicable** upon support being provided by network security products and services already deployed in their network architectures

40

What did the EU say? (Apr.'24)

https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

This Commission Recommendation encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, to ensure a coordinated and synchronised transition among the different Member States and their public sectors.

Call by 18 EU Member States (Nov'24)

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf

Roadmap for Member States by 2026

Projects: PQCSA and PiQASO

41

European Cybersecurity Certification Group: Agreed Cryptographic Mechanisms (v2.0 April 2025)

https://certification.enisa.europa.eu/document/download/a845662b-aee0-484e-9191-890c4cfa7aaa_en?filename=ECCG%20Agreed%20Cryptographic%20Mechanisms%20version%202.pdf

- **Good:** Adds lattice-based schemes Frodo-KEM and ML-KEM in hybrid mode
- **Bad:** Phasing out RSA-2048 (up to RSA-2999) for encryption by the end of 2025!
- **Ugly:** transparent process for public review is missing

42

42

OWASP Top 10

https://www.owasp.org/Top10

1. Broken access control
2. Cryptographic failures (Data Breach)
3. Injection
4. Insecure design
5. Security misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data integrity failures
9. Security logging and monitoring failures
10. Server-side request forgery

→

No Encryption
Weak Algorithms
Default Keys
Cryptographic Usage
Certificate management
Security Configuration
Use of Randomness
……

43

43

OWASP Top 10

https://www.owasp.org/Top10

1. Broken access control
2. Cryptographic failures (Data Breach)
3. Injection
4. Insecure design
5. Security misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data integrity failures
9. Security logging and monitoring failures
10. Server-side request forgery

All rely on public key cryptography!

44

44

PQC: A huge software migration project: slow, expensive and complex does not bring in new revenue

- Risk-based analysis (cannot do all)
- Crypto-inventory is first step but extremely complex – most organizations depend on suppliers who will not move synchronously
- Gradations of complexity – 10-year agenda
  - Relatively easy: messaging, network security (TLS, SSH) underway
  - Difficult: digital signatures for secure boot/update
  - Hard: PKI e.g. middleboxes and clients break when certificate chains grow by 10kB/30kB
  - Hard: platforms
- End-game should be crypto-agility

45

45

Cryptographic governance

- Understanding where crypto is being used by building an **Inventory**:
- **Monitoring** crypto is being used
- **Auditing** that crypto is being used in accordance with a specific standard, regulations or policy
- The **enforcement** of minimum security policy for crypto usage
- Policy for **migration** to new generations of cryptography
- Policy for the **retirement** of older cryptography
- Managing cryptography used in **supply chains**, provided by third parties
- Policy to **consolidate** and **simplify** an enterprise crypto landscape
- Guidance on how applications should consume cryptography to allow simpler migration of cryptographic (**cryptographic agility**):
- Lack of **strategic interlock** with new application and application migration
- Guidance on **deployment models** for hybrid cloud platforms

Source: IBM Quantum

46

46

Outline

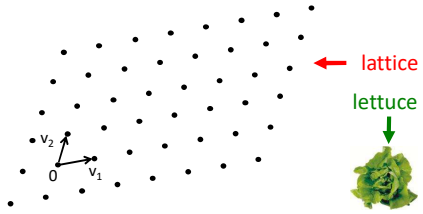
- Cryptography
- The Quantum Threat
- Post-Quantum cryptography
- QKD

47

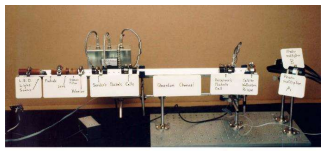
47

Post-quantum Cryptography ≠ Quantum Key Distribution

Find new cryptographic algorithms that resist attacks on quantum computers



Use quantum physics to agree on secret keys



Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

Sender's side produces very faint green light pulses of 4 different polarizations.

Quantum channel is an empty space about 30 cm long. There is no Eavesdropper, but if there were she would be detected.

Calcite prism separates polarizations. Photomultiplier tubes detect single photons.

48

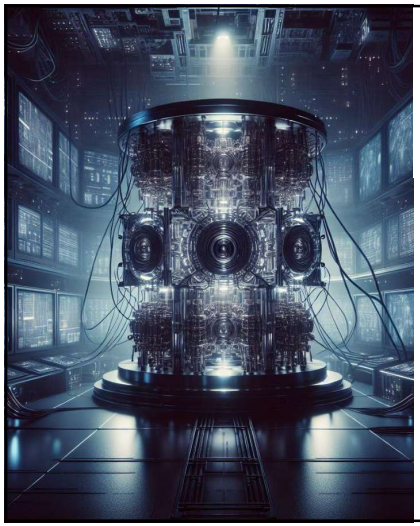
QKD strategic research and industry agenda 2030

quantum communication lacks quantitative data
(TRLs, bit rates, distances, energy, cost, market sizes)
https://qt.eu/about-quantum-flagship/strategic-research-and-industry-agenda-2030

- Mostly point to point
  - distance constraints
  - trusted relay nodes needed (repeaters at low TRL)
- Need secret key pre-distribution for entity authentication
- Slow performance – always combined with AES-256
- Very complex systems are expensive to certify
- No full EU supply chain
- Business model?
- Quantum internet = beyond 2040

49

49



Conclusion

- We do not know for sure if or when a quantum computer will break RSA & ECC
- But there seems to be a consensus that we can't take the risk
- Need to move:
  - risk-based approach
  - crypto-agility
  - EU-level strategy
- Quantum computers will bring many cool applications
- QKD is only for niche

50

50

Bart Preneel

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE: homes.esat.kuleuven.be/~preneel/
EMAIL: Bart.Preneel@esat.kuleuven.be
MASTODON: bpreneel@infosec.exchange
TWITTER: @bpreneel1
TELEPHONE: +32 16 321148

KU LEUVEN

COSIC

51

Links

NIST
- https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-postquantum-cryptographic-algorithms

GSMA
- https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/
- https://www.gsma.com/newsroom/wp-content/uploads/PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf
- https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/

SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Jan '20
- https://sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf (EU level Common Criteria agreement)

BSI
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.html

Canada
- https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf

Australia
- https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography

52

52