

Quantum computing and key impacts on digital security

Marco Brenner

IBM Quantum Senior Ambassador
Quantum Safe Transformation
Office of the IBM CISO

IBM **Research**





IBM Research Europe Zurich Research Lab



130+
H2020 Collaborations



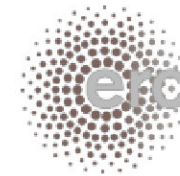
500+
Collaborations with SMEs,
Enterprises and Universities



26
Swiss National Science
Foundation Projects



45+
Nationalities



12
European Research Council
Grants



4
Nobel Laureates

Bring useful quantum
computing to the world

Make the world
quantum safe

Quantum computing is available and in use

Compute resources | IBM Quantum Platform

Search by name

QPU name	Region	Programmable qubits	Physical qubits	Status	Pending jobs	Type	2Q error (best)	2Q error (layered)
ibm_phoenix	us-east	120	458	Online Maintenance: 10/27	0	Nighthawk r2	8.207E-4	2.748E-3
ibm_miami	us-east	120	338	Online	0	Nighthawk r1	8.583E-4	9.256E-3
ibm_boston	us-east	156	332	Online Maintenance: 10/22	328	Heron r3	5.217E-4	2.254E-3
ibm_kingston	us-east	156	332	Online Maintenance: 10/20	2	Heron r2	8.216E-4	3.239E-3
ibm_pittsburgh	us-east	156	332	Online Maintenance: 10/26	8	Heron r3	6.256E-4	3.338E-3
ibm_fez	us-east	156	332	Online Maintenance: 10/14	2	Heron r2	1.323E-3	5.566E-3
ibm_marrakesh	us-east	156	332	Online Maintenance: 10/19	2	Heron r2	1.155E-3	4.624E-3
ibm_berlin	eu-de	120	338	Online Maintenance: 10/15	1	Nighthawk r1	6.326E-4	4.519E-3
ibm_aachen	eu-de	156	332	Online Maintenance: 10/21	2	Heron r3	6.427E-4	3.541E-3

IBM demonstrates world's first known quantum advantage

Who we are | Investors | News and views | Careers | Online banking

IBM and U.S. Department of Commerce Announce America's First Purpose-Built Quantum Foundry, Supported by Proposed \$1 Billion CHIPS Award

Powered by quantum workloads

May 21, 2023

CSCS
Centro Svizzero di Calcolo Scientifico
Swiss National Supercomputing Centre

ETH zürich

USER DOCUMENTATION

1 / 3

ETH Zurich to host a new IBM quantum computer

10.09.2026

Switzerland is to host one of the world's most advanced quantum computers from IBM. The new system is intended to...

MORE

MORE INSIGHTS

... can be broken by a sufficiently powerful quantum computer

- the integer factorization problem,
- the discrete logarithm problem
- the elliptic-curve discrete logarithm problem

- Digital signatures
- Key exchange (establishment of a common symmetric key)

Challenge:
find prime factors

Computation time

$$= p * q$$

Most powerful computer today:
millions of years

Shor's Quantum Algorithm (1994): Some hours

Quantum algorithms affect current cryptography differently

Name	function	pre-quantum security level	post-quantum security level
Symmetric cryptography			
AES-128 [1]	block cipher	128	64 (Grover)
AES-256 [1]	block cipher	256	128 (Grover)
Salsa20 [2]	stream cipher	256	128 (Grover)
GMAC [3]	MAC	128	128 (no impact)
Poly1305 [4]	MAC	128	128 (no impact)
SHA-256 [5]	hash function	256	128 (Grover)
SHA-3 [6]	hash function	256	128 (Grover)
Public-key cryptography			
RSA-3072 [7]	encryption	128	broken (Shor)
RSA-3072 [7]	signature	128	broken (Shor)
DH-3072 [8]	key exchange	128	broken (Shor)
DSA-3072 [9, 10]	signature	128	broken (Shor)
256-bit ECDH [11, 12, 13]	key exchange	128	broken (Shor)
256-bit ECDSA [14, 15]	signature	128	broken (Shor)

Security (theoretically) “halved”

Security broken

Quantum Algorithms

Grover’s algorithm

Quadratic improvement in brute-force attacks on symmetric encryption schemes like AES., however, full size implementations considered impractical or highly inefficient for a long time*

Shor’s algorithm

Exponential improvement in attacks on asymmetric encryption schemes like RSA, ECC, ElGamal.

* <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar3.ipd.pdf>

What do we need asymmetric cryptography for?

Confidentiality

To protect information from being disclosed to unauthorized entities.

Authentication

To identify the entities involved in a communication or transaction.

Integrity

To ensure communication is not changed between entities.

Nonrepudiation

To ensure that authorship or receipt of a message can not be disputed.

This type of cryptography provides the foundation for trust in our digital activities, services, business models and ecosystems.

Powerful quantum computers remove the basis of trust from all these digital activities, services, business models and ecosystems.

Cryptography is everywhere

Cryptography touches every corner of the digital world

Internet

Domain Name Service(DNS), Hyper-text Transfer Protocol (HTTP), Telnet, File-Transfer Protocol (FTP)

Digital Signatures

eIDAS – PDF Advanced Electronic Signature – (PAdES), Advanced Electronic Signatures (AES), ...

Critical Infrastructure

Code updates, Control systems, Car systems,...

Financial Systems

Payment Systems: (EMV, CHAPS, Fedwire, Target2, EURO1, ...), SWIFT, Settlement Systems, ...

Blockchain

Wallets, Transactions, Authentication

Enterprise

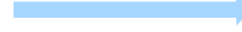
EMAIL – PGP, Identity Management PKI/LDAP/.., Virus scanning patterns, PKI Services, Bespoke applications, ...

Upgrading digital infrastructure takes a long time

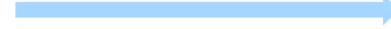
Passports – 10 years from issue



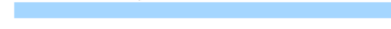
Road Vehicles – 15-20 Years



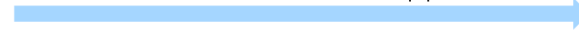
Critical Infrastructure – 25-30 Years



Aircrafts / Trains – 25-30 Years



(Some) Critical Mainframe Applications – 50 Years



Data needs to stay secure for a long time

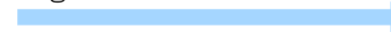
HIPAA – 6 years from its last use, Securities exchange act



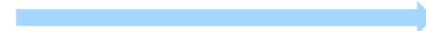
Tax Records – 7-10 Years in most countries, Sarbanes Oxley



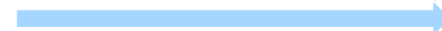
Legitimate Interest under GDPR – 20+ years



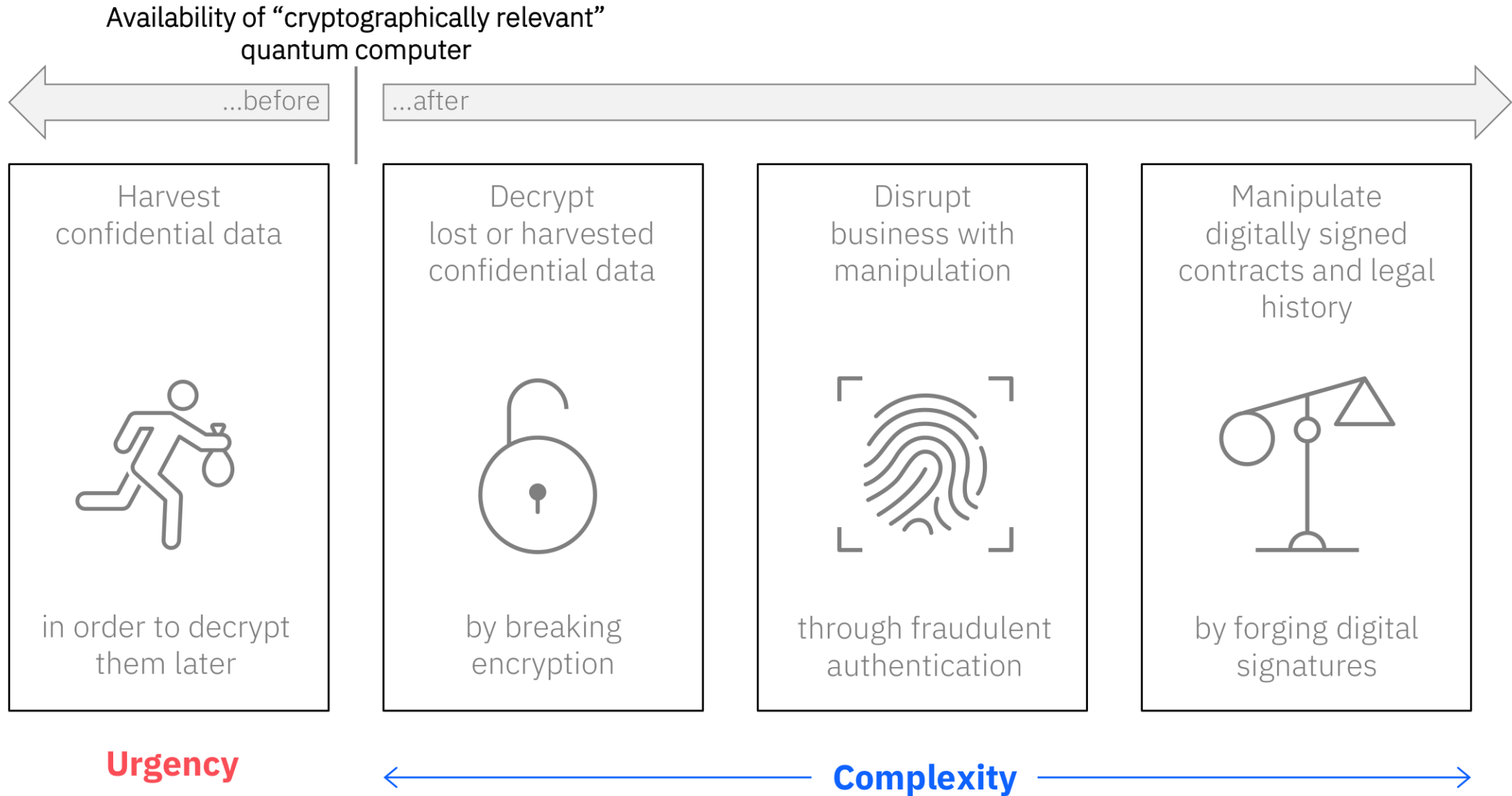
Guide 0068 - Clinical Trials – 25 Years



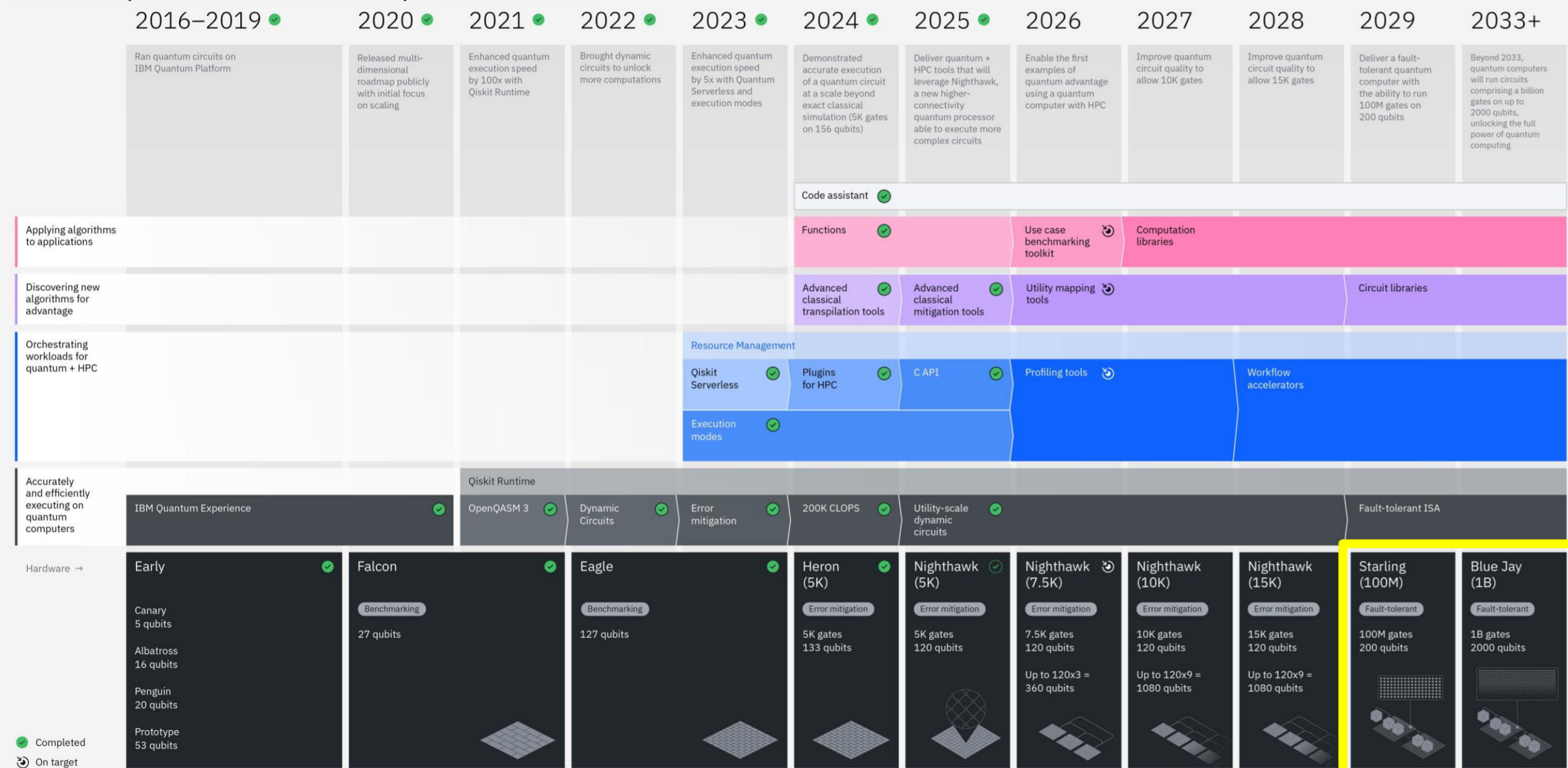
Toxic Substances Control Act / Occupational Safety and Health Act



What will a cyber criminal be able to do?

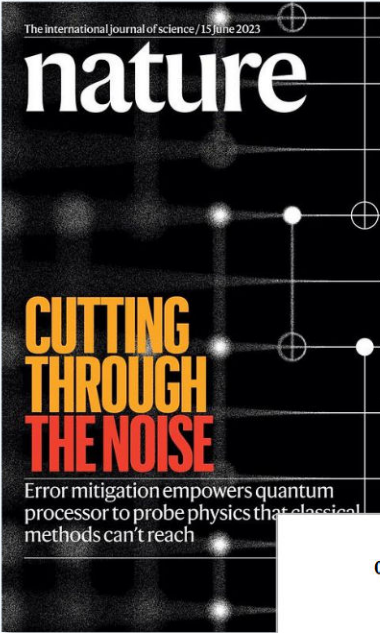


Development Roadmap



Completed
On target

Progress happens in leaps...



Quantum error correction below the surface code threshold

Google Quantum AI and Collaborators
(Dated: August 27, 2024)

Quantum error correction [1–4] provides a path to reach practical quantum computing by combining multiple physical qubits into a logical qubit, where the logical error rate is suppressed exponentially as more qubits are added. However, this exponential suppression only occurs if the physical error rate is below a critical threshold. In this work, we present two surface code memories operating below this threshold: a distance-7 code and a distance-5 code integrated with a real-time decoder. The logical error rate of our larger quantum memory is suppressed by a factor of $\Lambda = 2.14 \pm 0.02$ when increasing the code distance by two, culminating in a 101-qubit distance-7 code with $0.143\% \pm 0.003\%$ error per cycle of error correction. This logical memory is also beyond break-even, exceeding its best physical qubit's lifetime by a factor of 2.4 ± 0.3 . We maintain below-threshold performance

Space-Efficient and Noise-Robust Quantum Factoring

Seyoon Ragavan
MIT
sragavan@mit.edu

Vinod Vaikunta
MIT
vinodv@mit.edu

June 27, 2024

Abstract

An Efficient Quantum Factoring Algorithm

Oded Rogov*

Abstract

ers can be factorized by independently running a quantum circuit 4 times, and then using polynomial-time classical post-processing.

Google The Keyword

INNOVATION & AI > TECHNOLOGY > SAFETY & SECURITY

Quantum frontiers may be closer than they appear

Mar 25, 2026 · 2 min read

We're setting a timeline for post-quantum cryptography migration to 2029.

Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations

Ryan Babbush,^{1,*} Adam Zalcman,^{1,†} Craig Gidney,^{1,‡} Michael Broughton,¹ Tanuj Khattar,¹ Hartmut Neven,¹ Thiago Bergamaschi,^{1,2} Justin Drake,³ and Dan Boneh⁴

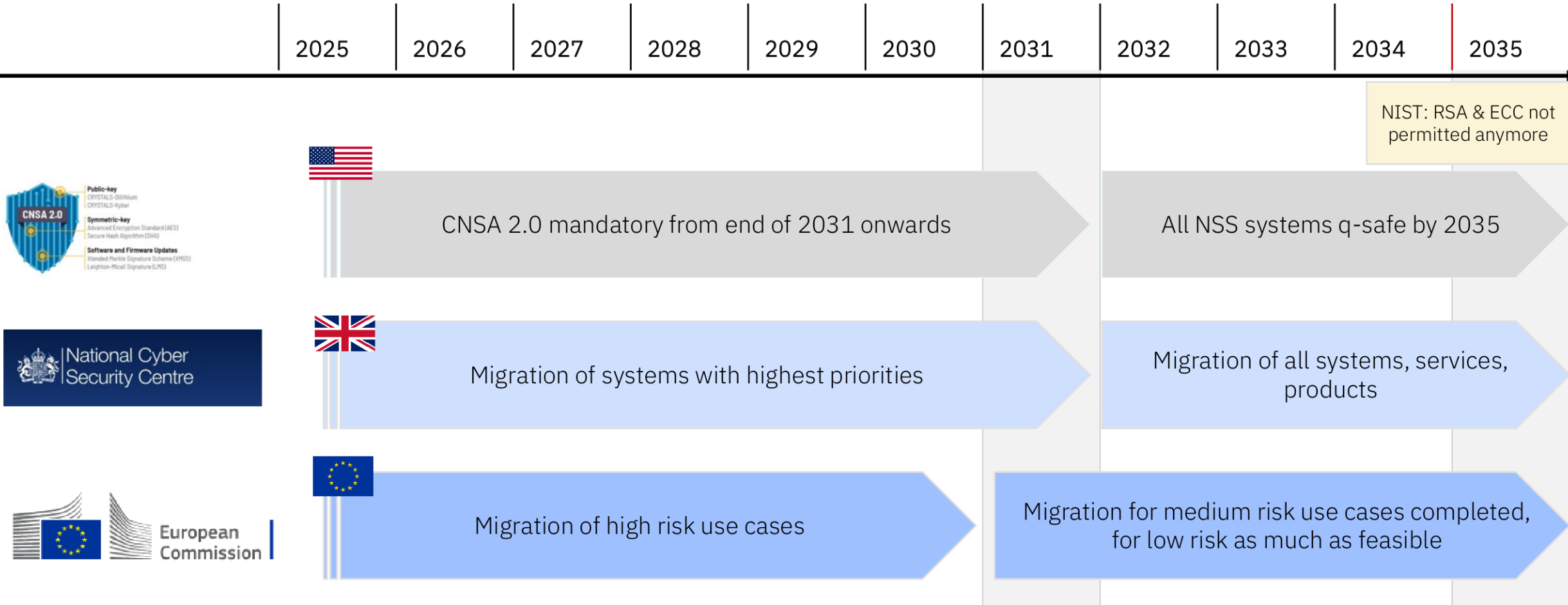
¹Google Quantum AI, Santa Barbara, CA 93111, United States
²Department of Computer Science, University of California Berkeley, Berkeley, CA 94720, United States
³Ethereum Foundation, Zeughausgasse 7a, 6300 Zug, Switzerland
⁴Department of Computer Science, Stanford University, Stanford, CA 94305, United States
(Dated: March 30, 2026)

Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits

Madelyn Cain^{1,*†}, Qian Xu^{1,2,*†}, Robbie King¹, Lewis R.B. Picard¹, Harry Levine^{1,3}, Manuel Endres^{1,2}, John Preskill^{1,2}, Hsin-Yuan Huang^{1,2}, Dolev Bluvstein^{1,2,§}

¹Oratomic, Pasadena, California 91125, USA
²California Institute of Technology, Pasadena, California 91125, USA
³Department of Physics, University of California, Berkeley, California 94720, USA
[†]mcain@oratomic.com, [†]qxu@oratomic.com, [§]dbluvstein@oratomic.com
*These authors contributed equally
(Dated: March 31, 2026)

Global recommendations and converging milestones 2030-2035



https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF
<https://www.ncsc.gov.uk/guidance/pqc-migration-timelines>
<https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>

...what about Switzerland?

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

Rolf Oppliger, NCSC
(mit Unterstützung von FUB Kryptologie)

24. Februar 2016
14. August 2020 (aktualisiert)

Technologiebetrachtung

Quantencomputer und Post-Quanten-Kryptografie

Swiss Banking
QuantumBasel

Action Plan to a Quantum-Safe Financial Future

A Pathway 2035

March 2025

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DOPS
Office fédéral de la cybersécurité OFCS

16 mai 2024

Considérations technologiques

Ordinateur quantique et cryptographie post-quantique

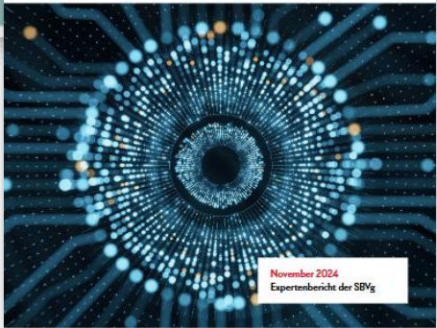
1 Introduction

Pas plus tard qu'en 2019, dans la revue scientifique *Nature*, Google a annoncé avoir atteint la suprématie quantique¹. Les médias parlent également beaucoup d'informatique quantique, des dangers et des menaces qui en découlent pour les procédés actuels et de la nécessité de pouvoir utiliser la cryptographie en toute sécurité, y compris face aux ordinateurs quantiques. Parfois, cet écho médiatique fait aussi naître de grandes incertitudes et craintes concernant les limites de la cryptographie. Le présent guide s'attache donc à décrire brièvement les caractéristiques d'un ordinateur quantique, les problèmes qu'il pose pour la sécurité de certaines techniques, le concept de cryptographie post-quantique (CPQ) et les domaines où il faut intervenir.

Swiss Banking
QuantumBasel

Quantum Computing in Banking

Funktionsweise, Anwendungsfelder und Handlungsempfehlungen für Schweizer Banken



November 2024
Expertenbericht der SBVG

finma

Bewilligung Überwachung Durchsetzung Dokumentation FINMA

FINMA Public

Home » News » FINMA-Aufsichtsmitteilung zu Quantum Computing

FINMA-Aufsichtsmitteilung zu Quantum Computing

09. Juli 2026 Medienmitteilung 2026

Die Eidgenössische Finanzmarktaufsicht FINMA veröffentlicht ihre Aufsichtsmitteilung zu den Risiken des Quantum Computing. Massnahmen zur Risikoprüfung und -minderung.

202628 | Cybersicherheit und U X

www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20263628

PARLNET KONTAKT LEICHTE SPRACHE DE FR IT RM EN

ORGANE RATSBEREIB ÜBER DAS PARLAMENT SERVICES INTERNATIONALES

HOME RATSBEREIB SUCHE CURIA VISTA

GESCHÄFT ABONNIEREN

26.3628 MOTION

Cybersicherheit und digitale Souveränität. Eine nationale Roadmap für den Übergang zur Post-Quanten-Kryptografie in der Schweiz

Eingereicht von:



JUILLARD CHARLES
Die Mitte Fraktion, Die Mitte, EVP, Die Mitte

Einreichungsdatum:

11.06.2025

Eingereicht im:

Ständerat

Stand der Beratungen:

In Kommission des Nationalrats

GESCHÄFT DRUCKEN

WEITERFÜHRENDE UNTERLAGEN

AMTLICHES BULLETIN

INFORMATIONEN ZUM VERFAHREN BEI MOTIONEN

<https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/technologiebetrachtung.html>
<https://www.sif.admin.ch/dam/de/sd-web/5jN0vjz3EBDI/Action%20Plan%20to%20a%20Quantum-Safe%20Financial%20Future.pdf>
<https://www.swissbanking.ch/Resources/Persistent/2/8/0/e/280e835f95ee449a7306046260cb6b0bbd0736b2/Expert%20report%20for%20Quantum%20Computing%20in%20Banking.pdf>
<https://www.finma.ch/de/news/2026/07/20260709-mm-am-05-26/>
<https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20263628>

IBM Research / IBM Corporation © 2026

44

Conclusions

Organizations should

- Put quantum safe **on the agenda**
- Appoint and **empower** internal roles to drive **related activities**
- **Keep track** of (Quantum) technology progress and **adjust plans** where necessary
- **Share** key insights and recommendations **across organizations**

Industry associations should

- Establish **competency groups** and provide **guidance** to industry
- Prepare and share solution templates for members within the industry
- Provide platform to **exchange** insights, experience and **best practices**
- Stay aligned and **interact with government and regulatory bodies** regarding industry implications

Government bodies should consider to

- Provide **ongoing information and detailed guidance** to organizations and industry associations
- Issue regulations to **support consistency and interoperability**
- Foster **exchange of insights and experience** between industries
- **Expedite** certification of industry **relevant technology products**

The time to act is **now**

