Quantum computing and key impacts on digital security

Marco Brenner IBM Research



IBM Quantum



IBM Research Europe-Zurich



130+ H2020 Collaborations

ې د ک 500+ Collaborations with SMEs, Enterprises and Universities

ENSINE 26 Swiss National Science Foundation Projects



45+ Nationalities

12



European Research Council Grants



4 Nobel Laureates

With a focused research on AI, Hybrid Cloud, Quantum, Science



IBM Research / IBM Corporation © 2024

Our mission

Bring useful quantum computing to the world Make the world quantum safe

IBM Cloud quantum services

☐		\sim
\leftarrow \rightarrow C \textcircled{a} \bigcirc A $\overrightarrow{\ }$ https:	//quantum. ibm.com /services/resources	67% ☆ 🛛 🖄 Ξ
IBM Quantum Platform Dashboard Functions Compute	resources Workloads	۹ 🕲 🗄
Quantum processing units Access IBM quantum processing units (QPUs) via one of our access plan	18.	
(i) Looking to test your code before running on QPUs? Explore debuted and the second secon	ıgging tools and local simulators. Learn more $ ightarrow$	
QPUs you do not have access to with any instance appear with a lock icon below.		30 Card 🗐 Table
Q Search by QPU name		All QPUs (11) \lor 1
ibm_fez OPU status OPU status Online Processor type Heron r2 Oubits 20 Error (best/layered) CLOPS 156 3.40e-3/4.53e-3 28K	bim_torino OPU status Online Processor type Heron r1 Oubits 20 Error (best/layered) CLOPS 133 1.18e-3/1.28e-2 30K	ibm_sherbrooke Image: Constraint of the segment of
bim_quebec OPU status Online Processor type Eagle r3 Qubits 20 Error (hest/layered) LOPS 127 2.37e-3/1.80e-2 32K	B ibm_kawasaki QPU status • Online Processor type Eagle r3 Qubits 20 form fbert/layered) CLOPS 127 3.29e-3/1.93e-2 29K	ibm_kyiv QPU status • Online Processor type Eagle r3 Qubits 20 Error (bert/layered) CLOPS 127 N/A/1.99e-2 30K
ibm_brisbane OPU status • Online Processor type Eagle r3 Oubits 20 Error (hest/layreed) CLOPS 127 3.23e-3/2.06e-2 30K	A ibm_brussels OPU status • Online Processor type Eagle r3 Qubits 20 frort dest[laypreck] CLOPS 127 2.65e-3/2.12e-2 37K	A ibm_rensselaer OPU status • Online Processor type Eagle r3 Qubits 20 Error (best/layered) CLOPS 127 3.00e-3/2.12e-2 32K
ibm_nazca OPU status • Online Processor type Eagle r3 Oubits 20 Error (hest/layered) CLOPS 127 4.26e-3/3.12e-2 29K	A ibm_strasbourg Image: Constraint of the status OPU status • Online Processor type Eagle r3 Qubits 20 form then(layared) CLOPS 127 3.07e-3/3.28e-2 37K	



Why Quantum ?

IBM Quantum



5/*'Ž+/'Ž&.'*&'Žž*+ž`*+/I'IŽflŽ+*#'X`#**ž`*#'Y'`&\$', ,*ž%/**'')&_#/\$*'fi&)'.Žž`Ž'./w-/'_`)/#O'*`)*

Digital security is based on mathematical problems

Current popular cryptographic algorithms rely on one of three hard mathematical problems:

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

Used mainly for:

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

Challenge: find prime factors

Computation time

232278756443554916483436144302814961299403168472741726378629 043050821809225325073582179649272923967859532854739028287315 490064402564114268108868740578441743673658232286043895597927 09805944636540646316777 4970594635540646316777 4970594635540646316777 49705946355534624 43743658643499508 87405757920599 8740371337996855534624 6312330141103519407212 458567407248316849708228 03970194588404522985355437.00479372510824571915521143930 659330867582930373

Factorization

= p * q

Most powerful computer today: millions of years

D Ž & Qwantum Algorithm: Some hours

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 can not be disputed.





/ 🔲	
	\Box
\sim	



Our digital infrastructure depends on cryptography to provide the foundation for trusting digital ecosystems.

What will attackers be able to do?



Development Roadmap

IBM Quantum / © 2024 IBM Corporation

	2016-2019 🛛	2020 🥑	2021 🤗	2022 🥝	2023 🤗	2024	2025	2026+	2027	2028	2029	2033+
	Run quantum circuits on the IBM Quantum Platform	Release multi- dimensional roadmap publicly with initial aim focused on scaling	Enhancing quantum execution speed by 100x with Qiskit Runtime	Bring dynamic circuits to unlock more computations	Enhancing quantum execution speed by 5x with quantum serverless and Execution modes	Improving quantum circuit quality and speed to allow 5K gates with parametric circuits	Enhancing quantum circuit quality to allow 7.5K gates	Improving quantum circuits quality to allow 7.5K gates	Improving quantum circuits quality to allow 10K gates	Improving quantum circuits quality to allow 15K gates	Improving quantum circuits quality to allow 100M gates	Beyond 2033, quantum-centric supercomputers will include 1000's of logica qubits unlocking the ful power of quantum computing
Data Scientist						Platform						
						Code assist 🥹	Functions	Mapping Collections	Specific Libraries			General purpose QC libraries
Researchers					Middleware	iddleware						
					Quantum 🕑 Serverless	Transpiler 👌 Service	Resource Management	Circuit Knitting x P	Intelligent Orchestration		Circuit libraries	
Quantum			Oiskit Runtime									
Physicist												
Physicist	IBM Quantum Experience	ø	QASM3 🥥	Dynamic 🥝 circuits	Execution 🥝 Modes	Heron [©] (5K)	Flamingo (5K)	Flamingo (7.5K)	Flamingo (10K)	Flamingo (15K)	Starling (100M)	Bluejay (1B)
Physicist	IBM Quantum Experience	✓ Falcon	QASM3 📀	Dynamic circuits Eagle	Execution Ø Modes	Heron (5K) Error Mitigation	Flamingo (5K) Error Mitigation	Flamingo (7.5K) Error Mitigation	Flamingo (10K) Error Mitigation	Flamingo (15K) Error Mitigation	Starling (100M) Error correction	Bluejay (1B) Error correction
Physicist	IBM Quantum Experience	✓ Falcon Benchmarking	QASM3 ©	Dynamic circuits Eagle Benchmarking	Execution 🔗 Modes	Heron (5K) Error Mitigation 5k gates 133 qubits	Flamingo (5K) Error Mitigation 5k gates 156 qubits	Flamingo (7.5K) Error Mitigation 7.5k gates 156 qubits	Flamingo (10K) Error Mitigation 10k gates 156 qubits	Flamingo (15K) Error Mitigation 15k gates 156 qubits	Starling (100M) Error correction 100M gates 200 qubits	Bluejay (1B) Error correction 1B gates 2000 qubits
Physicist	IBM Quantum Experience	Falcon Benchmarking 27 qubits	QASM3 📀	Dynamic circuits Eagle Benchmarking 127 qubits	Execution Modes	Heron (5K) Error Mitigation 5k gates 133 qubits Classical modular Up to 133x3 = 399 qubits	Flamingo (5K) Error Mitigation 5k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Flamingo (7.5K) Error Mitigation 7.5k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Flamingo (10K) Error Mitigation 10k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Flamingo (15K) Error Mitigation 15k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Starling (100M) Error correction 100M gates 200 qubits Error corrected modularity	Bluejay (1B) Error correction 1B gates 2000 qubits Error corrected modularity
Physicist	IBM Quantum Experience	Falcon Benchmarking 27 qubits	QASM3 ©	Dynamic circuits Eagle Benchmarking 127 qubits	Execution Modes	Heron (5K) Error Mitigation 5k gates 133 qubits Classical modular Up to 133x3 = 399 qubits	Flamingo (5K) Error Mitigation 5k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Flamingo (7.5K) Error Mitigation 7.5k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Flamingo (10K) Error Mitigation 10k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Flamingo (15K) Error Mitigation 15k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Starling (100M) Error correction 100M gates 200 qubits Error corrected modularity	Bluejay (1B) Error correction 1B gates 2000 qubits Error corrected modularity

Quantum Safe Algorithms

Standardization for cryptographic algorithms are usually driven by the US National Institute for Standards and Technology (NIST).

After three rounds of evaluation of Quantum Safe algorithms, NIST identified seven finalists. In July 2022 NIST selected a small number of new quantum-safe algorithms for standardization by 2024.



Algorithms selected for standardization after round 3:

Digital Signatures (document signatures & network certificates)

- 1. ML-DSA k CRYSTALS-Dilithium^{*} (lattices)
- 2. FALCON^{*} (lattices)
- 3. SLH-DSA k Sphincs+ (hash-based)

Key Encapsulation mechanisms (session key establishment)

1. ML-KEM k CRYSTALS-Kyber* (lattices)

A 4th round for non-lattice based KEM submissions is going on, and an evaluation process for non-lattice-_ * / I * ž fl %-) + ,\$)' /z * Ž ‡ y* @ % + *) + /

ML-KEM, ML-DSA and SLH-DSA standards have been issued in August 2024 as FIPS-203/4/5

* CRYSTALS-Dilithium, CRYSTALS-Kyber and Falcon developed by IBM Research team, in collaboration with industry and academic partners.

IBM Quantum

Globally, several recommendations for Post Quantum Cryptography are emerging



National Security Agency (NSA): Commercial National Security Algorithm Suite (CNSA) 2.0)¹⁾

i The CNSA provides the cryptographic base to protect US National Security
ž % fi &) \$ * + ž & % ; ' + & + Ž /
i A timeline has been set for mandatory replacement of algorithms by 2025 and later.



Public-key CRYSTALS-Dilithium CRYSTALS-Kyber

Symmetric-key Advanced Encryption Standard (AES) Secure Hash Algorithm (SHA)

Software and Firmware Updates Xtended Merkle Signature Scheme (XMSS) Leighton-Micali Signature (LMS)



Relevant European Recommendations

European Commission

- i Member states to define -Quantum Cryptography Coordinated
- i Available two years following the publication of Recommendation
- i Roadmap with list of actions, including timeline for different phases and milestones

ndation on a Coordinated Implementation Roadmap for the

ANSSI (France)

- i Hybridization to be used whenever mitigation is needed in the short and medium term
- i Encourages all industries to define progressive transition strategy towards quantumsafe for relevant cryptographic products

ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)

December 21, 2023

BSI (Germany)

- i BSI has published a report in 2021, with a more detailed discussion about quantumsafe algorithms.
- i Recommends the usage of hybrid modes with quantum-safe algorithms.
- i BSI acts on the hypothesis that cryptographically relevant quantum computers will be available in the early 2030s.



NCSC, AIVD (Netherlands)

- i Published a PQC Migration Handbook that defines which organizations need to take action now with mitigation measures.
- i The NCSC recommends organizations to draft a plan of action.



transition to Post-Quantum Cryptography

European Commission

IBM Quantum



Notices and disclaimers

© 2024 International Business Machines Corporation

IBM and the IBM logo are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

E 9: D 5 @ 4 F > 6 ? E : D 5: D E C: 3 F E 6 5 y 2 D : D z H: E 9 @ F E 2 ? J H: E 9 @ F

Client examples are presented as illustrations of how those clients have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

Not all offerings are available in every country in which IBM operates.

2 % 0 * + * + / \$ / % + * *) / fl *) I ž % fl * : 3 > x * * fi , + ,) / * + ž & % r * ž % + / % + * &) * *) & + subject to change or withdrawal without notice.



#