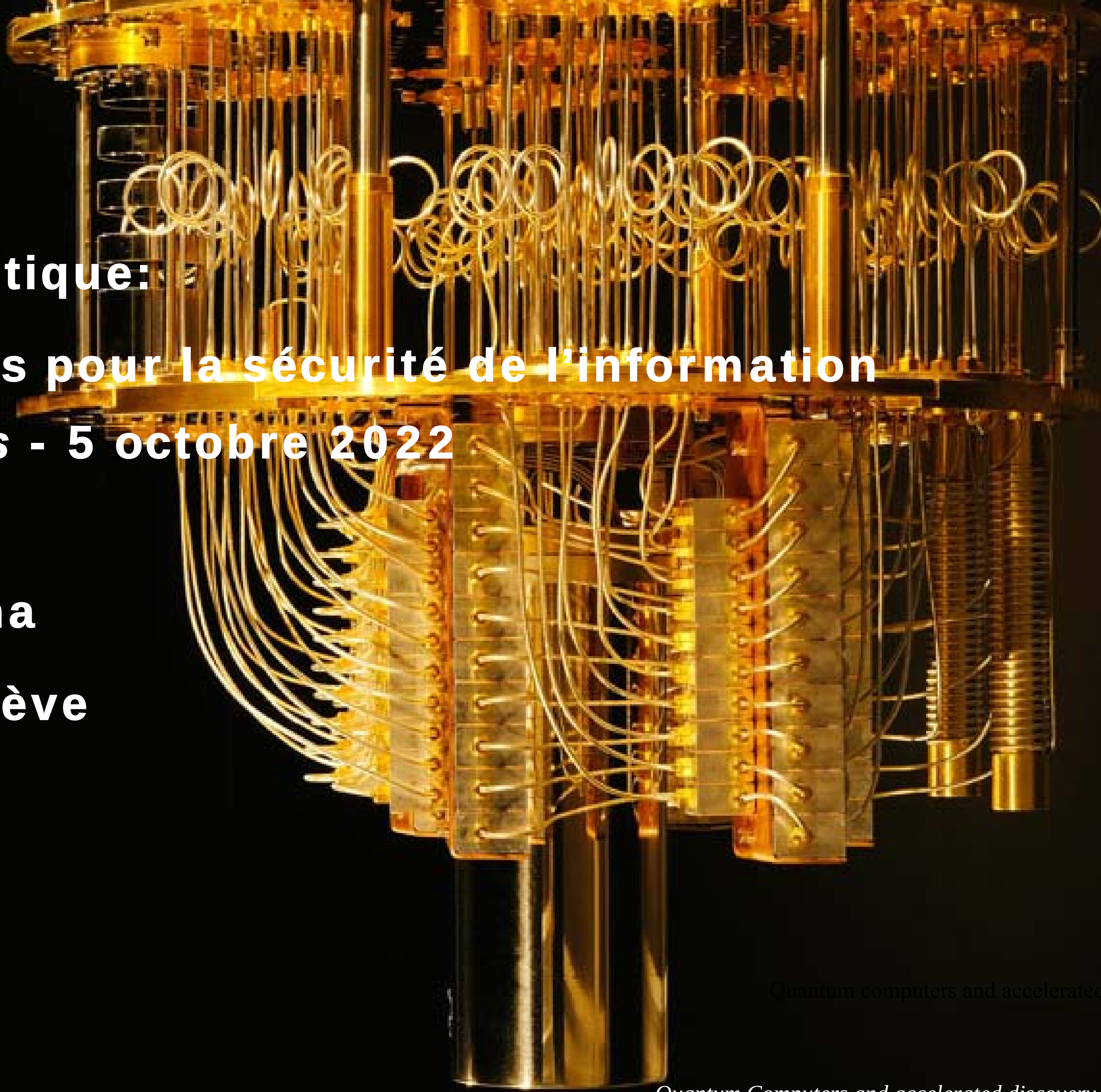
L’ordinateur quantique:

Enjeux et menaces pour la sécurité de l’information

Digital Innovators - 5 octobre 2022

Dr. Eduardo Solana

Université de Genève



Quantum Computers and accelerated discovery
IBM Media Center Gallery

It’s All about *Qubits*...

- ***Quantum bits*** (***qubits***) instead of classical bits that can exist not only in the **0** and **1** state but in both simultaneously (***superposition property***)
- The ***entanglement property*** enables several *qubits* to exist in a quantum state that cannot be described independently of each other. ***True parallel computing power!***

- In 1994 ***Peter Shor*****’s algorithm** introduced a way to **exponentially reduce the complexity of computationally hard problems** using a quantum computer
- These problems (*prime factorization*, *discrete logs over integers mod p*, *discrete logs over elliptic curves*, etc.) constitute the foundations of today’s **asymmetric cryptography (**including **digital signatures)**

- ***Lov Grover*****’s quantum algorithm** (1996) showed **a quadratical improvement in database searches** resulting in a **potential threat to the secrecy of cryptographic keys**
- His results significantly impact the security of today’s **symmetric cryptography and hashing algorithms**

Existing beliefs on tractability and theory of computation dramatically reshaped by a functional, general purpose quantum computer

Impact on Current Cryptography

- **Symmetric Algorithms**: Mandatory increase of key sizes (**256 bits minimum!**) – ***Grover's algorithm***

- **Crypto hashes and MACs**: Mandatory increase of *digests* and *MAC-values* (**512 bits minimum!**) – ***Grover's algorithm***

- **Asymmetric (public-key) Algorithms**: **Totally broken by Shor's algorithm**.
  This includes **most current encryption and signature schemes as well as key establishment protocols protecting the Internet!**

Symmetric algorithm resistance is practically irrelevant since crypto keys are shared through quantum unsafe asymmetric primitives…

Beware of the *store now decrypt later* risk...

Today's Internet cryptography would be totally devastated by the "quantum apocalypse" !

On the Positive Side

***Quantum Random Number Generators* (QRNG)** enable best quality (maximum entropy) cryptographic keys strengthening current and future algorithms

***Quantum Key Distribution* (QKD)** protect secrets from unauthorized disclosure relying quantum physics principles

Post-Quantum Cryptography (**PQC**) algorithms provide protection against a quantum-enabled adversary

Mathematical problems intractable to date will become solvable by a powerful and universal quantum computer: *factoring*, *discrete logarithms*, *finite fields computation*, *optimization problems*, etc.

Generalized ***quantum supremacy*** will expand horizons in **artificial intelligence**, **machine learning**, **molecular modeling**, **weather forecasting**, **logistics, financial modeling**, **particle physics**, **gene study**, etc.

Quantum computing will bring countless benefits to science and society (healthcare, physics, biology, finance, etc.)

From *Moore's Law* to *Neven's Law*

Moore's law describes the evolution of computing capabilities. According to this law, **the computing power doubles every two years** and, as such, **grows exponentially**:

$$2,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ \ldots$$

According to Google's scientist ***Hartmut Neven***[1], quantum computers would benefit from **double exponential growth**:

- The intrinsic exponential advantage of a quantum computer
- The advances in the building process of quantum computers (*error rate reduction*)

As a result, **Neven's Law** states that the growth rate of quantum computer power will follow a **double exponential rate**:

$$2^{2^1},\ 2^{2^2},\ 2^{2^3},\ 2^{2^4},\ 2^{2^5},\ \ldots$$

Neven foresees that <u>10 years from now</u> classical computers will be <u>32 times</u> more powerful whereas quantum computers will improve their capacity <u>more than 4 billion times</u> !

[1] ***A New Law to Describe Quantum Computing's Rise?*** Quanta Magazine. https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618/

Down to Earth

- The race for **quantum supremacy where a quantum computer executes a calculation intractable to a classical computer** has started
- As of today, **quantum supremacy remains limited to very specific computations**
- The execution of the **Shor and Grover algorithms is well beyond current quantum computers' execution capabilities**.
- Quantum ***noise control related to multi-qubits platforms*** and ***extremely cold processing conditions*** (barely above *Kelvin-zero*, *-273.15* ^{o}C) **remain serious challenges**
- ***Prof. M. Mosca***[1] points out the **three variables** that define the quantum transition:

  How long does your encryption needs to be secure (x years)?

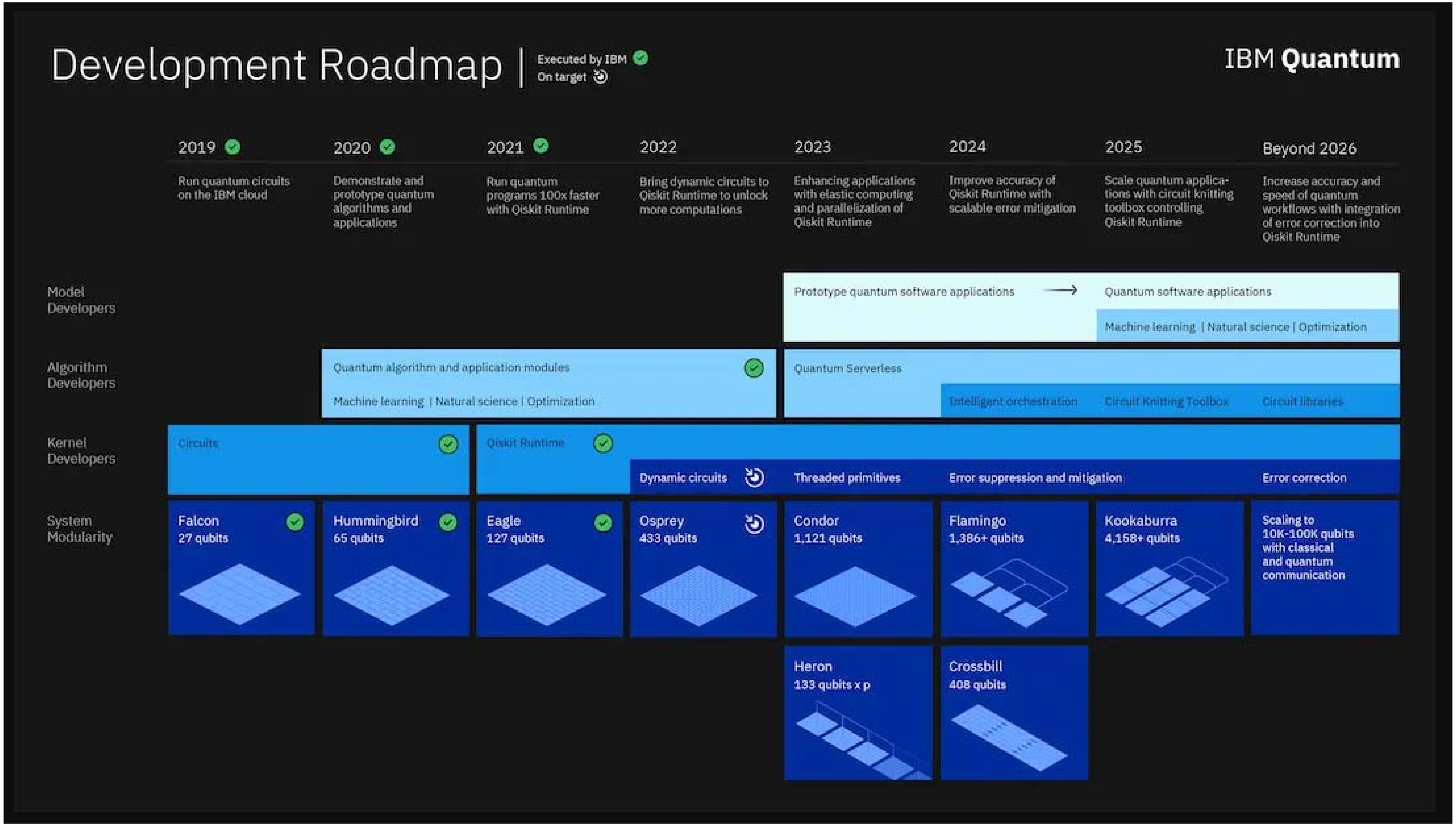
  How long will it take to re-tool your existing infrastructure with a quantum-safe solution (y years)?

  How long will it be until a large-scale, general purpose quantum computer is built (z years)?

If x + y > z then you should start making steps to prepare now

[1] ***Cybersecurity in an era with quantum computers: will we be ready?*** Michele Mosca. https://eprint.iacr.org/2015/1075.pdf

IBM’s Roadmap for Large Scale Quantum Computers

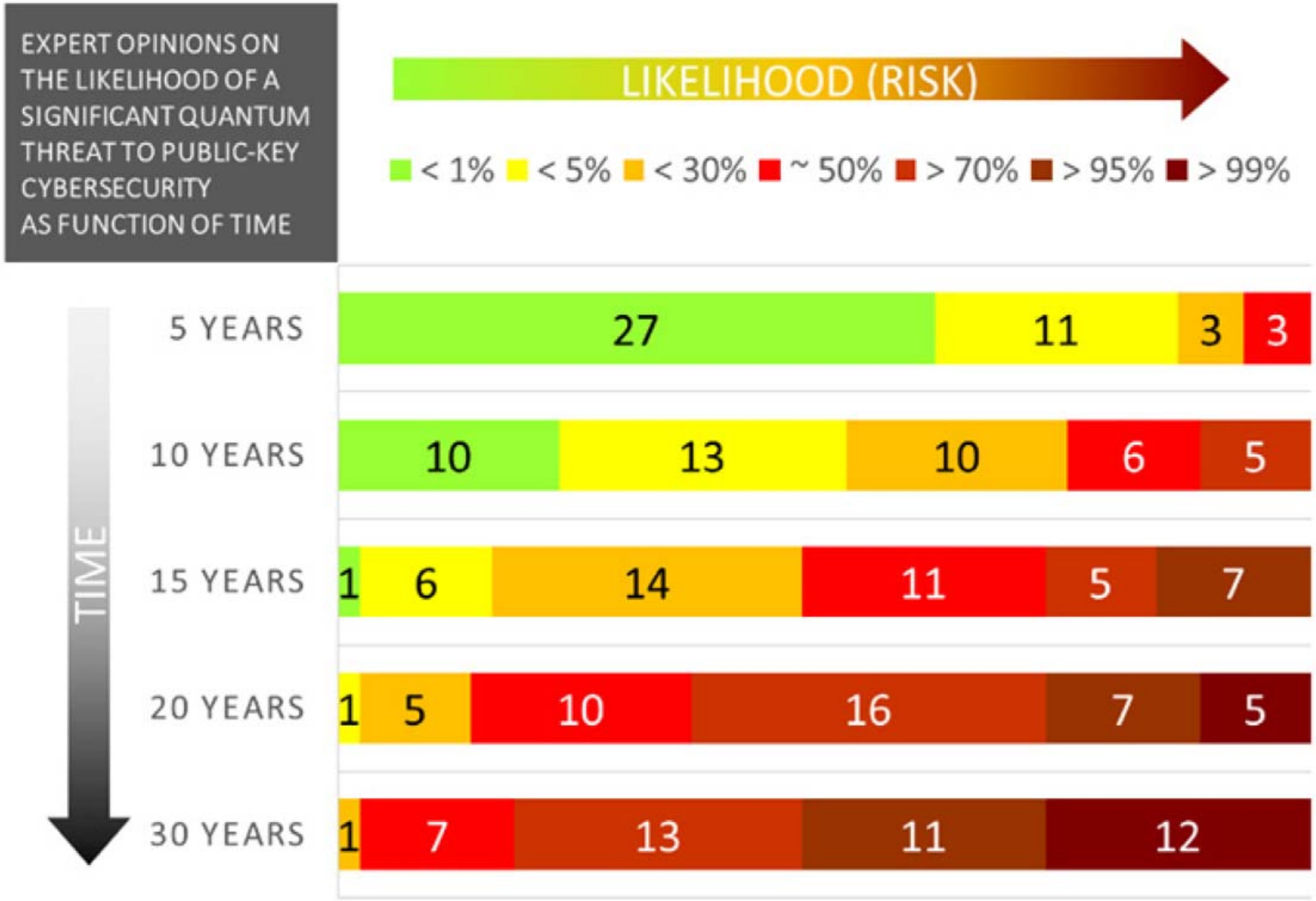


Development Roadmap | Executed by IBM ✓ On target

IBM Quantum

	2019 ✓	2020 ✓	2021 ✓	2022	2023	2024	2025	Beyond 2026
	Run quantum circuits on the IBM cloud	Demonstrate and prototype quantum algorithms and applications	Run quantum programs 100x faster with Qiskit Runtime	Bring dynamic circuits to Qiskit Runtime to unlock more computations	Enhancing applications with elastic computing and parallelization of Qiskit Runtime	Improve accuracy of Qiskit Runtime with scalable error mitigation	Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime	Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime
Model Developers					Prototype quantum software applications →		Quantum software applications Machine learning | Natural science | Optimization	
Algorithm Developers		Quantum algorithm and application modules ✓ Machine learning | Natural science | Optimization			Quantum Serverless	Intelligent orchestration	Circuit Knitting Toolbox	Circuit libraries
Kernel Developers	Circuits ✓		Qiskit Runtime ✓	Dynamic circuits ↻	Threaded primitives	Error suppression and mitigation		Error correction
System Modularity	Falcon ✓ 27 qubits	Hummingbird ✓ 65 qubits	Eagle ✓ 127 qubits	Osprey ↻ 433 qubits	Condor 1,121 qubits	Flamingo 1,386+ qubits	Kookaburra 4,158+ qubits	Scaling to 10K-100K qubits with classical and quantum communication
					Heron 133 qubits x p	Crossbill 408 qubits		

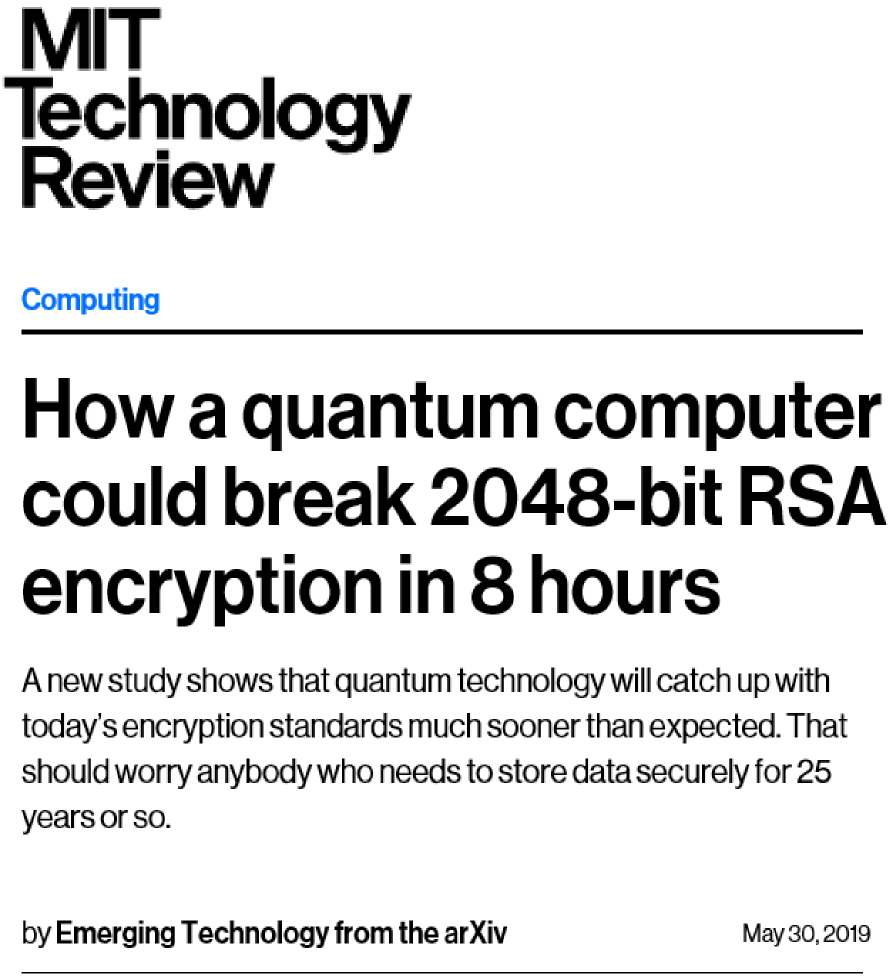
Expert Opinions[1]



Numbers reflect how many experts (out of 44) assigned a certain probability range.

[1] *Quantum Threat Timeline Report 2020*. Dr. Michele Mosca and Dr. Marco Piani, Global Risk Institute.

A First Call...



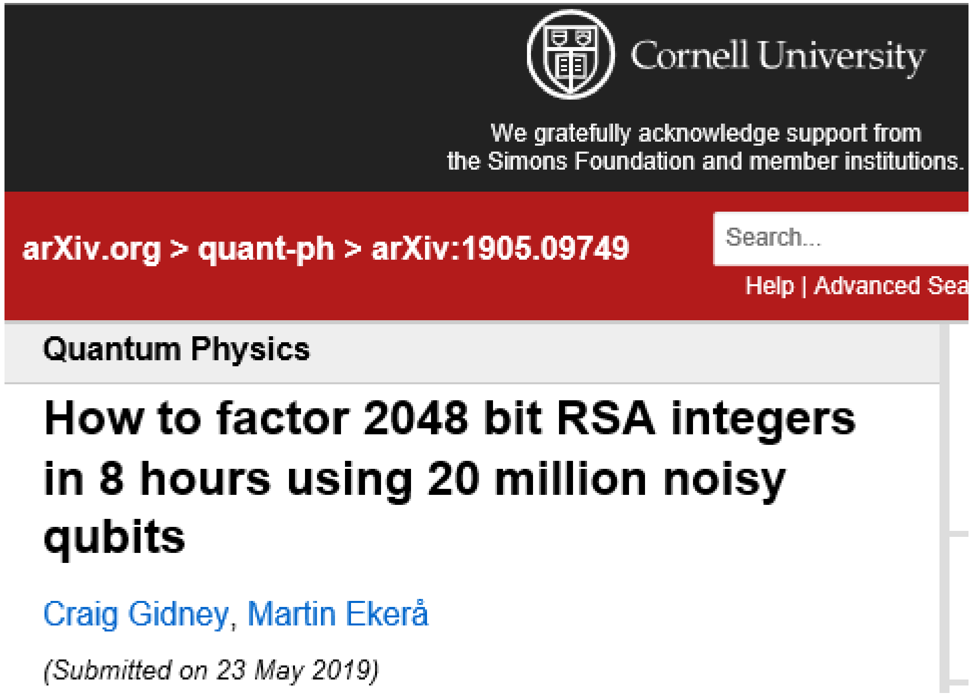
MIT Technology Review

Computing

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

by **Emerging Technology from the arXiv** May 30, 2019



Cornell University

We gratefully acknowledge support from
the Simons Foundation and member institutions.

arXiv.org > quant-ph > arXiv:1905.09749

Quantum Physics

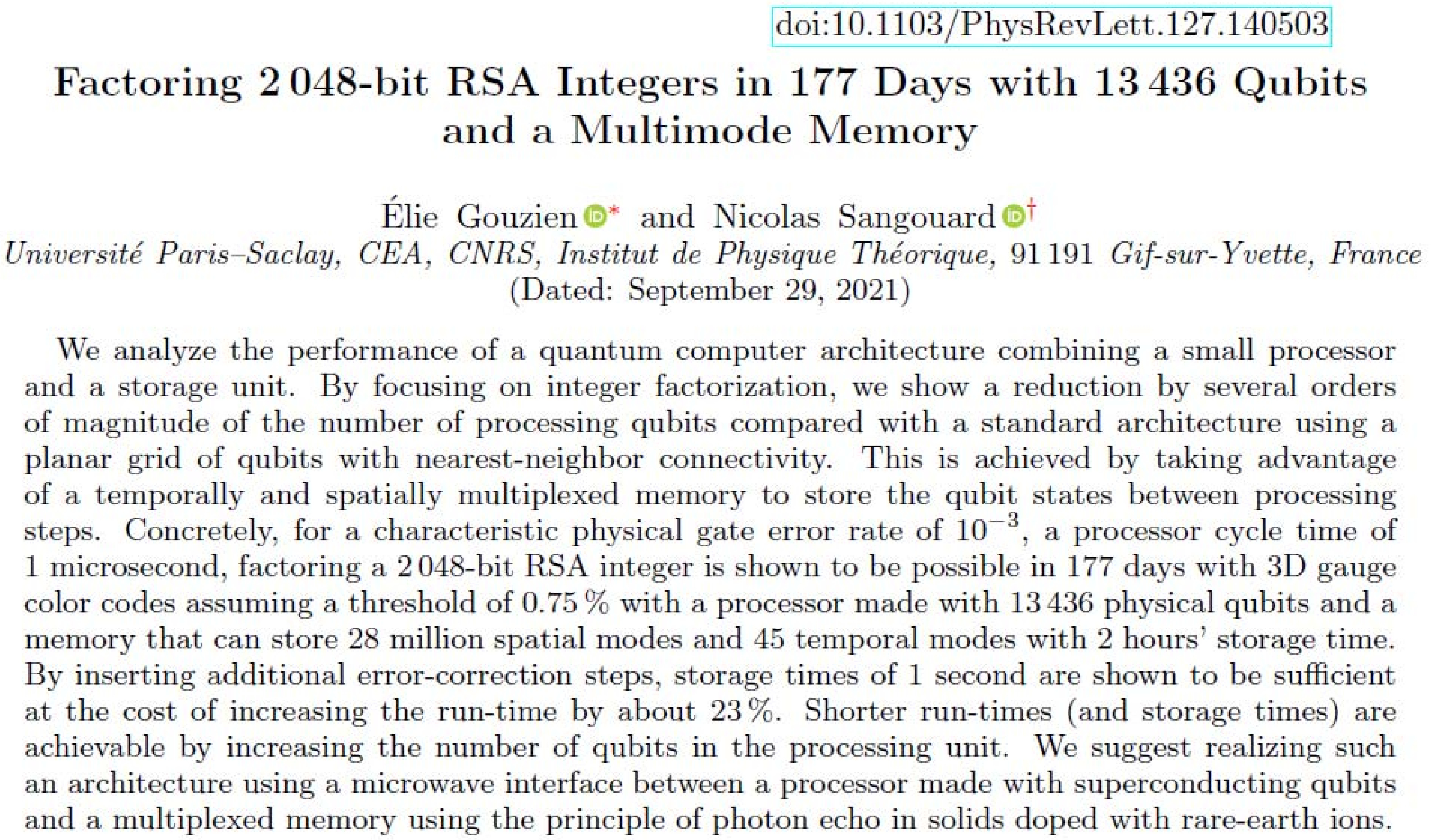
How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney, Martin Ekerå

(Submitted on 23 May 2019)

... and then a Second

arXiv:2103.06159



doi:10.1103/PhysRevLett.127.140503

Factoring 2 048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory

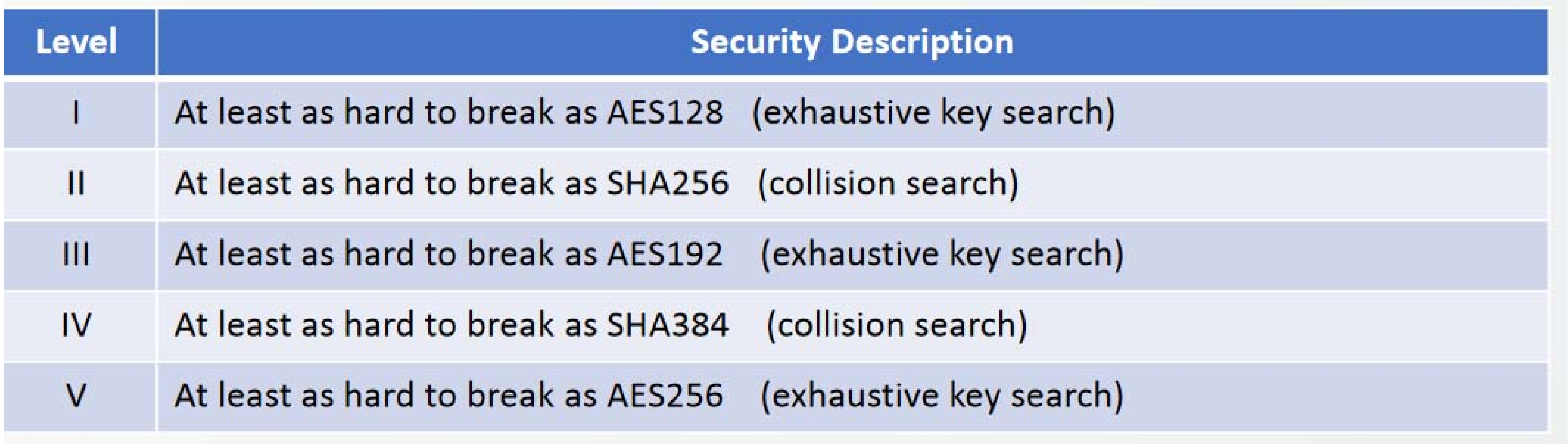
Élie Gouzien[*] and Nicolas Sangouard[†]
Université Paris–Saclay, CEA, CNRS, Institut de Physique Théorique, 91 191 *Gif-sur-Yvette, France*

(Dated: September 29, 2021)

We analyze the performance of a quantum computer architecture combining a small processor and a storage unit. By focusing on integer factorization, we show a reduction by several orders of magnitude of the number of processing qubits compared with a standard architecture using a planar grid of qubits with nearest-neighbor connectivity. This is achieved by taking advantage of a temporally and spatially multiplexed memory to store the qubit states between processing steps. Concretely, for a characteristic physical gate error rate of 10^{-3}, a processor cycle time of 1 microsecond, factoring a 2 048-bit RSA integer is shown to be possible in 177 days with 3D gauge color codes assuming a threshold of 0.75 % with a processor made with 13 436 physical qubits and a memory that can store 28 million spatial modes and 45 temporal modes with 2 hours' storage time. By inserting additional error-correction steps, storage times of 1 second are shown to be sufficient at the cost of increasing the run-time by about 23 %. Shorter run-times (and storage times) are achievable by increasing the number of qubits in the processing unit. We suggest realizing such an architecture using a microwave interface between a processor made with superconducting qubits and a multiplexed memory using the principle of photon echo in solids doped with rare-earth ions.

The NIST PQC Competition[1]

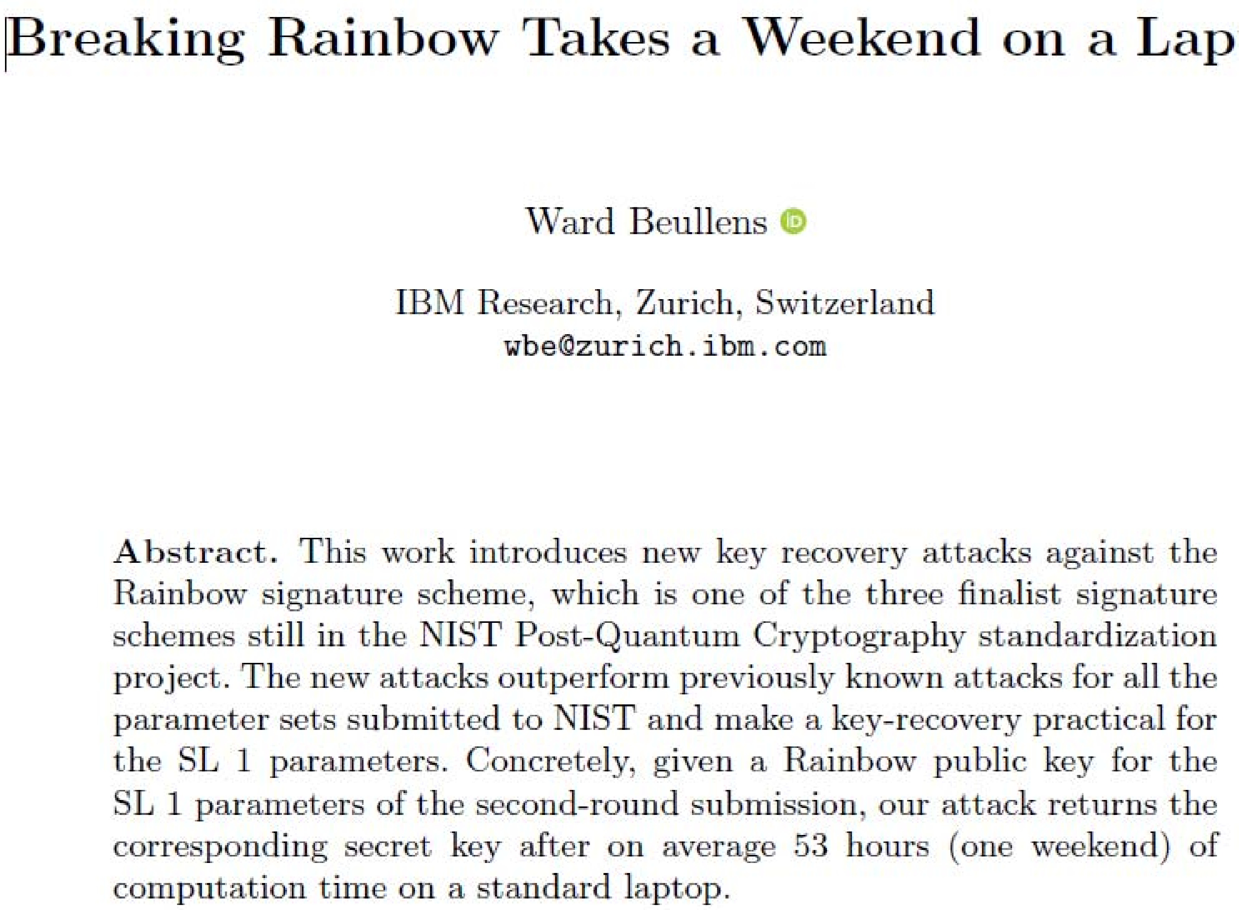
- **In 2016 NIST issued a Call for Proposals for Post Quantum Cryptography (PQC) algorithms**. First round features **82 initial candidate algorithms**.
- A first group of standardization candidates **has been announced (July, 5th, 2022):**
  - **1 encryption/key establishment** (*CRYSTALS-Kyber)*
  - **3 digital signature** (CRYSTALS-*Dilithium, FALCON and SPHINCS+)*
- **4 encryption candidates advance to 4th round (***BIKE*, *Classic McEliece*, *HQC* and *SIKE***)**
- In terms of **computational strength**, five security levels are considered:



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)

[1] Dustin Moody. *Let’s Get Ready to Rumble - The NIST PQC “Competition”. https://csrc.nist.gov/CSRC/media/Presentations/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti/images-media/PQCrypto-April2018_Moody.pdf*

…and here Comes Immaturity (February 2022)



Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

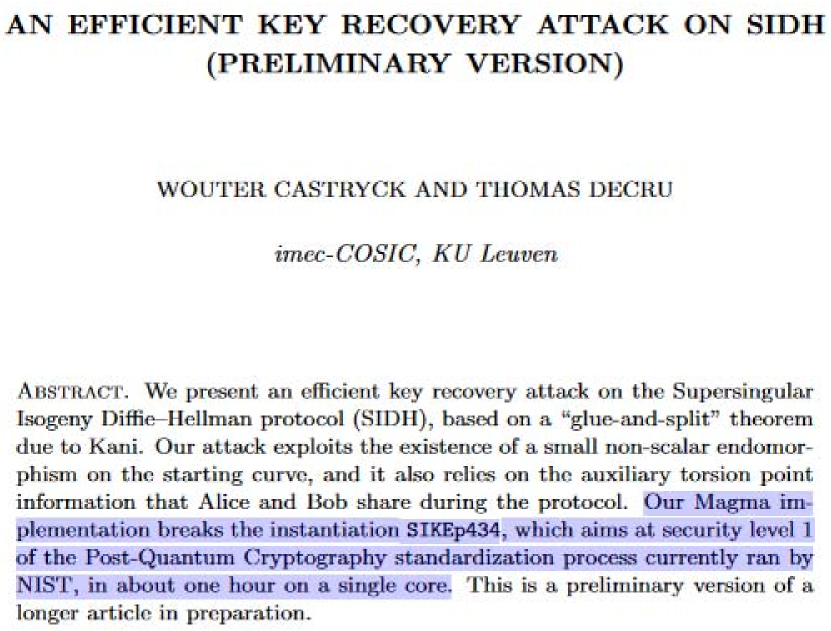
IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

Abstract. This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks outperform previously known attacks for all the parameter sets submitted to NIST and make a key-recovery practical for the SL 1 parameters. Concretely, given a Rainbow public key for the SL 1 parameters of the second-round submission, our attack returns the corresponding secret key after on average 53 hours (one weekend) of computation time on a standard laptop.

"Serves as a reminder to not put candidates into products until the standard is done"

(*The Beginning of the End: The First NIST PQC Standards*. March 2022. Dustin Moody, NIST)

...and here comes Immaturity AGAIN (August 2022)!



AN EFFICIENT KEY RECOVERY ATTACK ON SIDH (PRELIMINARY VERSION)

WOUTER CASTRYCK AND THOMAS DECRU

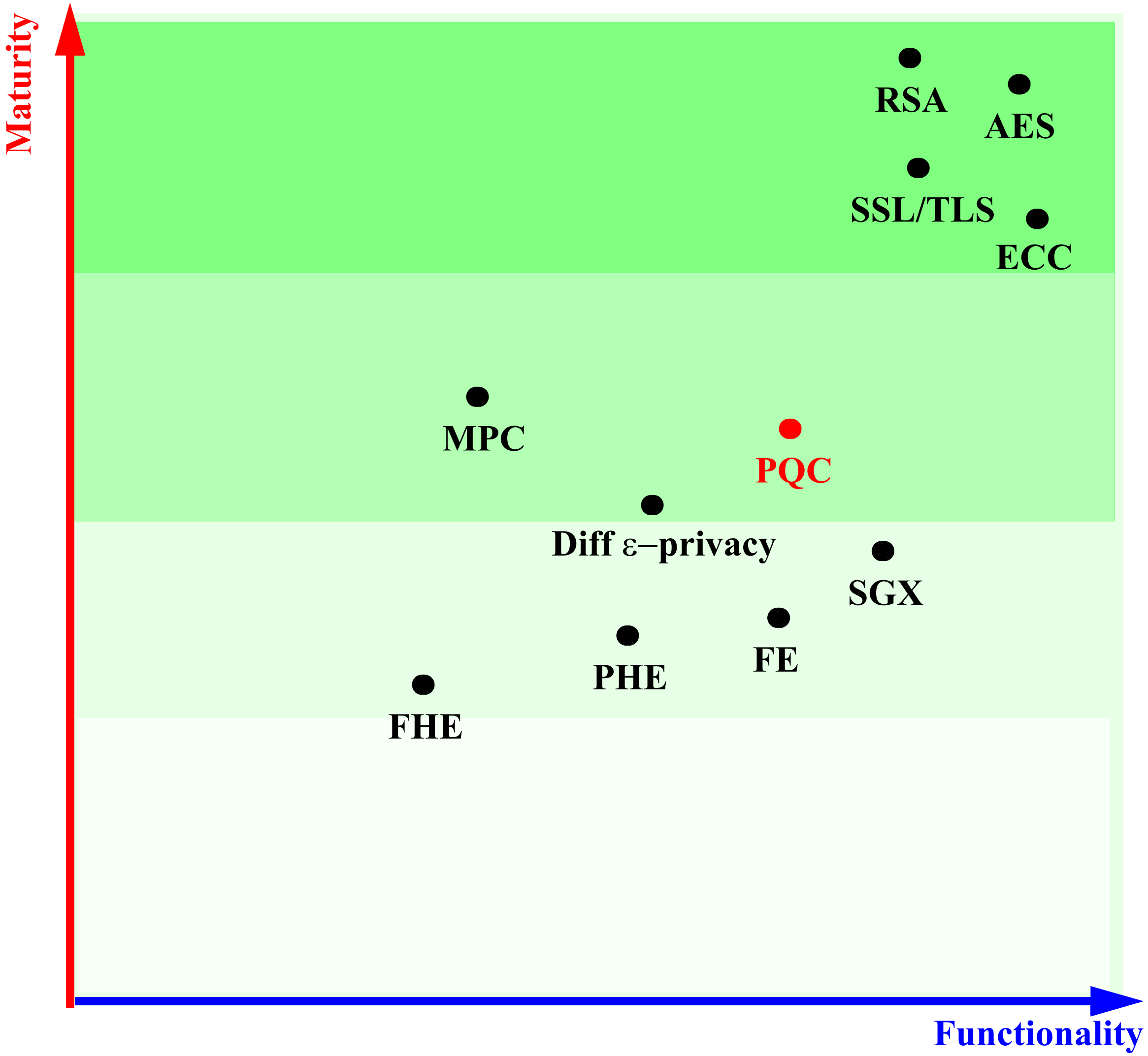
imec-COSIC, KU Leuven

ABSTRACT. We present an efficient key recovery attack on the Supersingular Isogeny Diffie–Hellman protocol (SIDH), based on a "glue-and-split" theorem due to Kani. Our attack exploits the existence of a small non-scalar endomorphism on the starting curve, and it also relies on the auxiliary torsion point information that Alice and Bob share during the protocol. Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core. This is a preliminary version of a longer article in preparation.

David Jao, professor at the University of Waterloo and co-inventor of SIKE:

"In general, there is a lot of deep mathematics which has been published in the mathematical literature but which is not well understood by cryptographers. I lump myself into the category of those many researchers who work in cryptography but do not understand as much mathematics as we really should. So sometimes, all it takes is someone who recognizes the applicability of existing theoretical math to these new cryptosystems. That is what happened here."

Maturity of Post Quantum Encryption (PQC) Algorithms



***Crypto-Agility* transcends immature PQC algorithms**

Takeaways

- Quantum technology has evolved from a promising research direction into a **viable technological solution for real cyber-security problems**
- ***Quantum Random Number*** (**QRNG**) and ***Quantum Key Distribution*** (**QKD**) are implemented and mature technologies available **Today!**
- ***Post-Quantum Cryptography*** (**PQC**) algorithms **still immature** and **not yet standardized**
- **General purpose, full-scale quantum computers are still years away** but:
- **Stakes are so high that unprecedented research efforts and massive investments** are being devoted to the design and implementation of these systems.

The cloud may bring quantum power to our fingertips *but...*

Technology wars between quantum and non-quantum enabled countries/organizations are foreseeable

Quantum may become the nuclear technology of computation