Quantum Computing & Cryptography

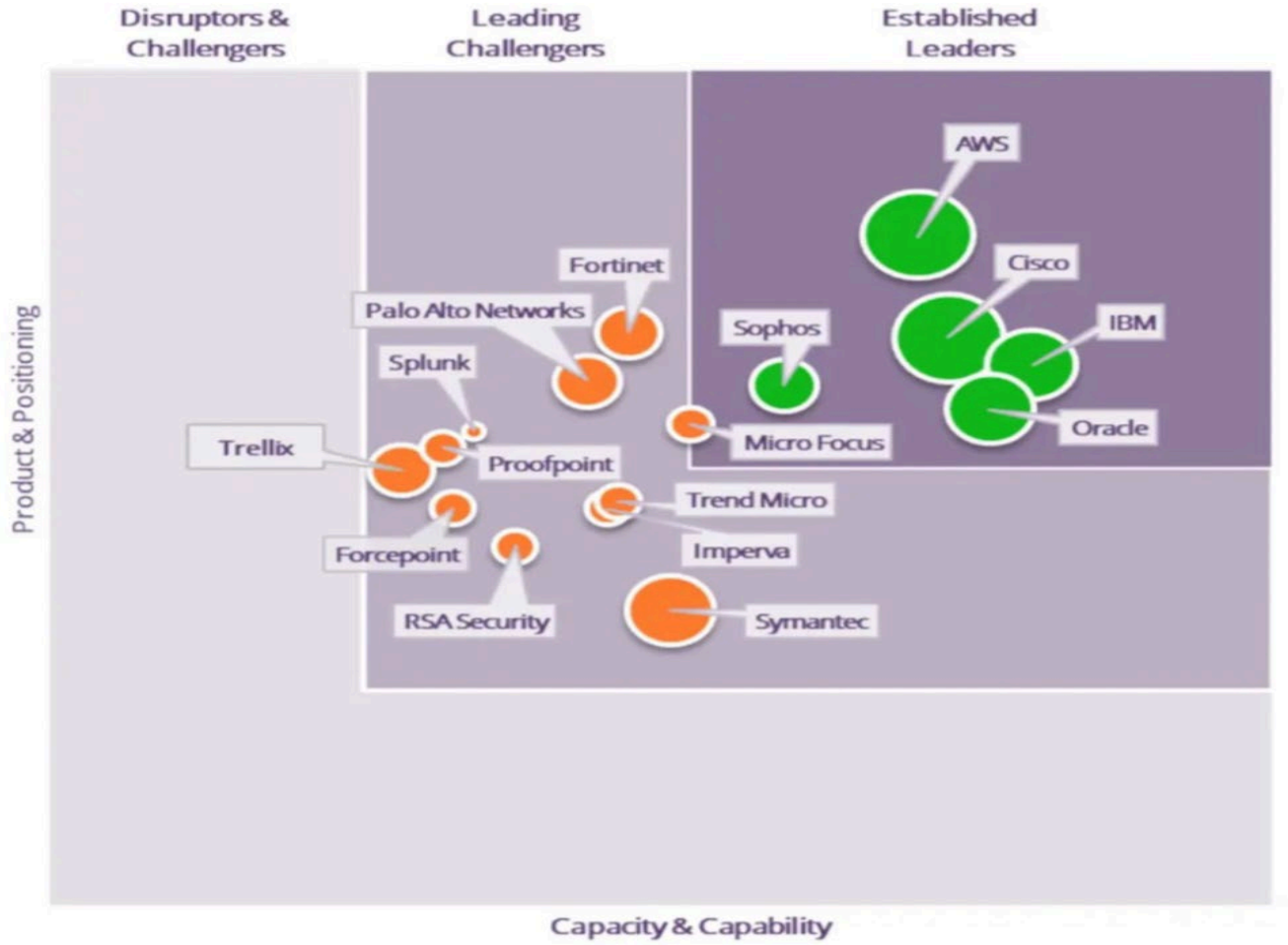
Maurizio Dècina

Emeritus Professor, Politecnico di Milano

ASTRID Cybersecurity Seminar

Rome, October 19th, 2022

Cybersecurity Vendors & 2021 World Market



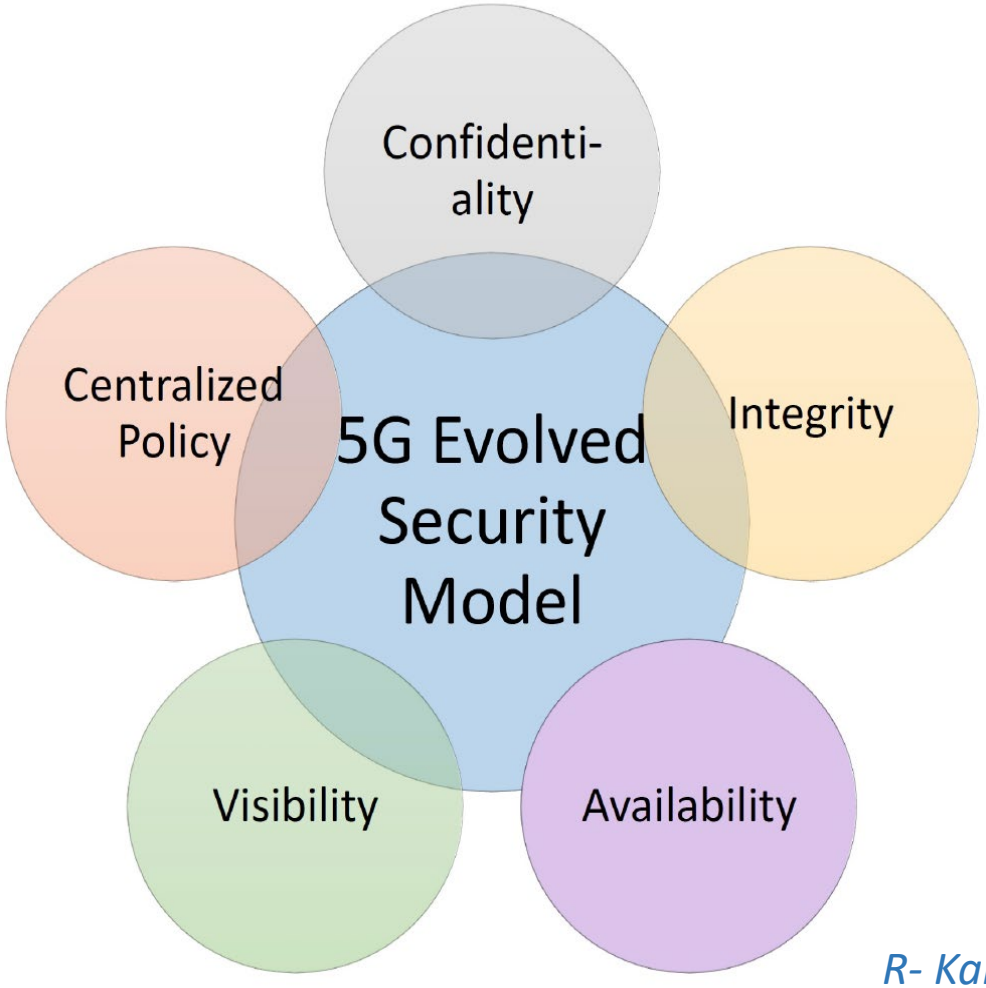
Source: Juniper Research, 2022

USD 197.42 billion in 2021

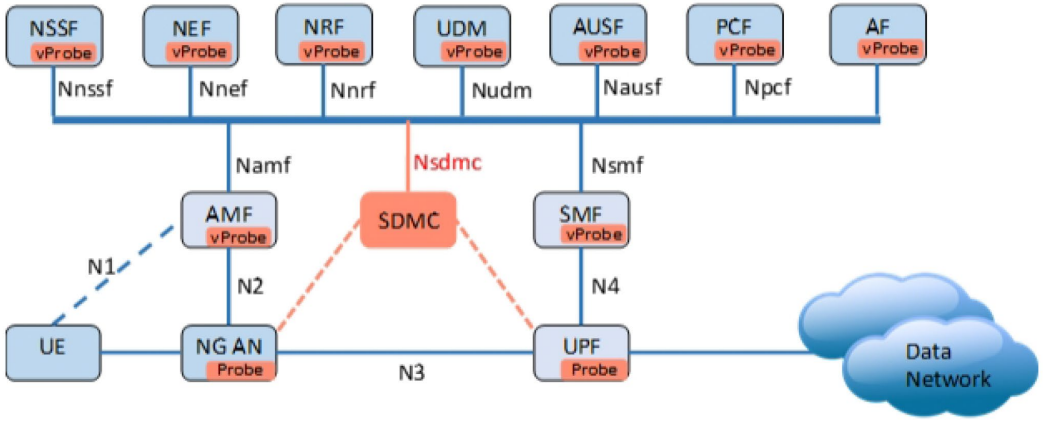
The global cyber security market size was valued at USD 197.42 billion in 2021. **It is projected to reach USD 450.49 billion by 2030, growing at a CAGR of 9.60% during the forecast period (2022–2030)**. Cybersecurity is the defense against cyber threats to systems connected to the internet, including their hardware, software, and data.

Source: Straits Research, 2022

5G Evolved Security Model



Visibility



Software Defined (Security) Monitoring, **SDM**

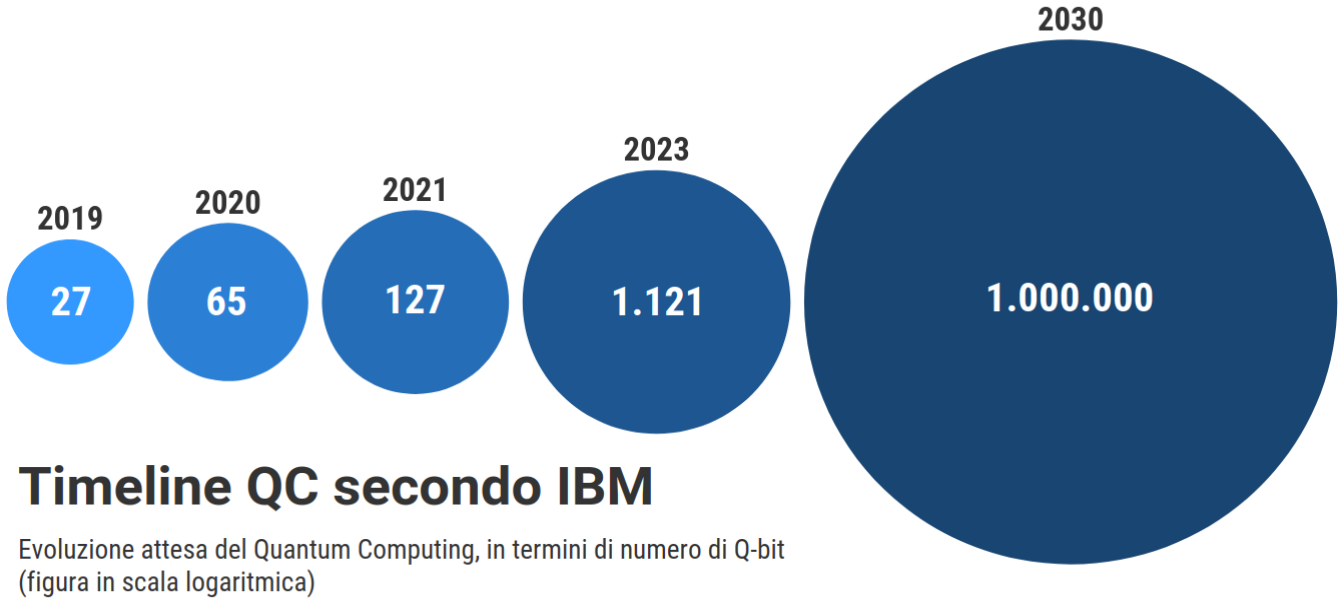
Centralized Security Policy =
Security as a Service

R- Kahn et alii, IEEE Communications Surveys and Tutorials, 2019

Quantum Computing

When a quantum computer becomes available, many of the actual encryption technologies (like DH & RSA protocols for digital certificates, digital signatures, etc.) can be broken.

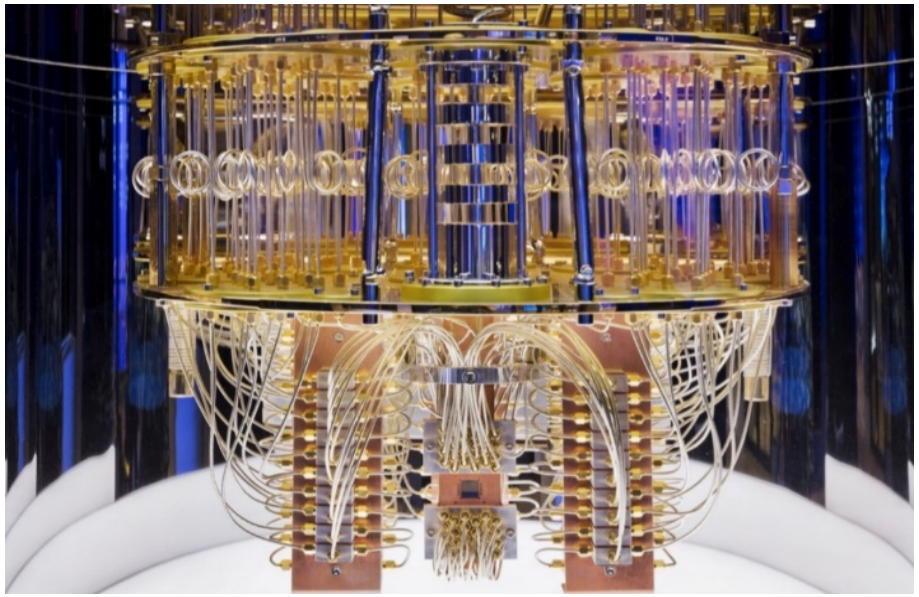
Public (NIST) and private (IBM) organizations are studying post-quantum encryption algorithms



Timeline QC secondo IBM

Evoluzione attesa del Quantum Computing, in termini di numero di Q-bit (figura in scala logaritmica)

Courtesy by G. Pelosi, (2021)



IBM 127 Qubit Eagle Computer, 2021

IBM 127 Qubit Eagle Computer, 2021

NIST Post Quantum Cryptography

PQC Standard Candidates

2 Lattice-based Cryptography

A lattice is a set generated by integer linear combinations of the columns of a matrix. Thus, lattice-based cryptosystems and hard problems typically involve matrices. Lattice-based cryptography is rather recent (1996) compared to the other subfields, but it has seen a steady growth since its inception.

With a few exceptions, lattice-based cryptography started with very theoretical constructions targeting provable security. As it stands, several schemes are proven secure under the hardness of various lattice problems. However, not all proofs are equal, in the sense that some proofs have a limited practical relevance [CKMS16].

Today, there exist several cryptographic constructions based on lattices. Beyond encryption and signatures, more advanced constructions have been proposed, such as homomorphic encryption, identity-based encryption, etc.

The efficiency of cryptographic schemes based on generic lattices is moderate. Many schemes rely on more structured lattices, and achieve high efficiency in the process. In the initial set of standards by NIST [NIS22], three out of the four selected schemes are based on structured lattices: Kyber [SAB+20], Dilithium [LDK+20] and Falcon [PFH+20].

2.1 Hard problems

There is a myriad of conjectured hard problems in lattice-based cryptography. The most common are SIS and LWE. Both work with matrices having their entries in a finite ring $\mathcal{R}$

LWE - learning with errors

Let $\mathbf{A} \in \mathcal{R}^{n \times m}$ be a uniformly random and $\mathbf{b} = \mathbf{A}^t\mathbf{s} + \mathbf{e}$, where $\mathbf{s} \in \mathcal{R}^n$ and $\mathbf{e} \in \mathcal{R}^m$ are vectors sampled from the *'secret' distribution* and *'error' distribu-*

3 Code-based Cryptography

Error-correcting codes usually serve to guarantee the integrity and reliability of communication over unreliable channels, by detecting and removing errors. Code-based cryptography uses them in a completely different way, by deliberately adding errors to the point that removing them is hard, except for someone who knows a secret description of the code. Since it mostly entails simple algebraic operations (Gaussian elimination, multiplication, sometimes inversion) on finite field elements, code-based cryptography is often amenable to fast hardware implementations.

Code-based cryptography was first introduced by McEliece [McE78] in his eponymous encryption scheme. His original scheme remains fundamentally secure, is reasonably fast and has short ciphertexts, but a very large public key. Many attempts have been made at making it more efficient, but doing so in a secure manner has proven to be delicate.

Achieving secure code-based signatures has been an even more difficult task. Novel proposals in this direction are being made, but only the test of time will determine if these efforts are successful. Code-based schemes BIKE [ABB+20], HQC [AAB+20] and Classic McEliece [ABC+20] have been selected as Round 4 candidates and are still being considered for standardization by NIST [NIS22].

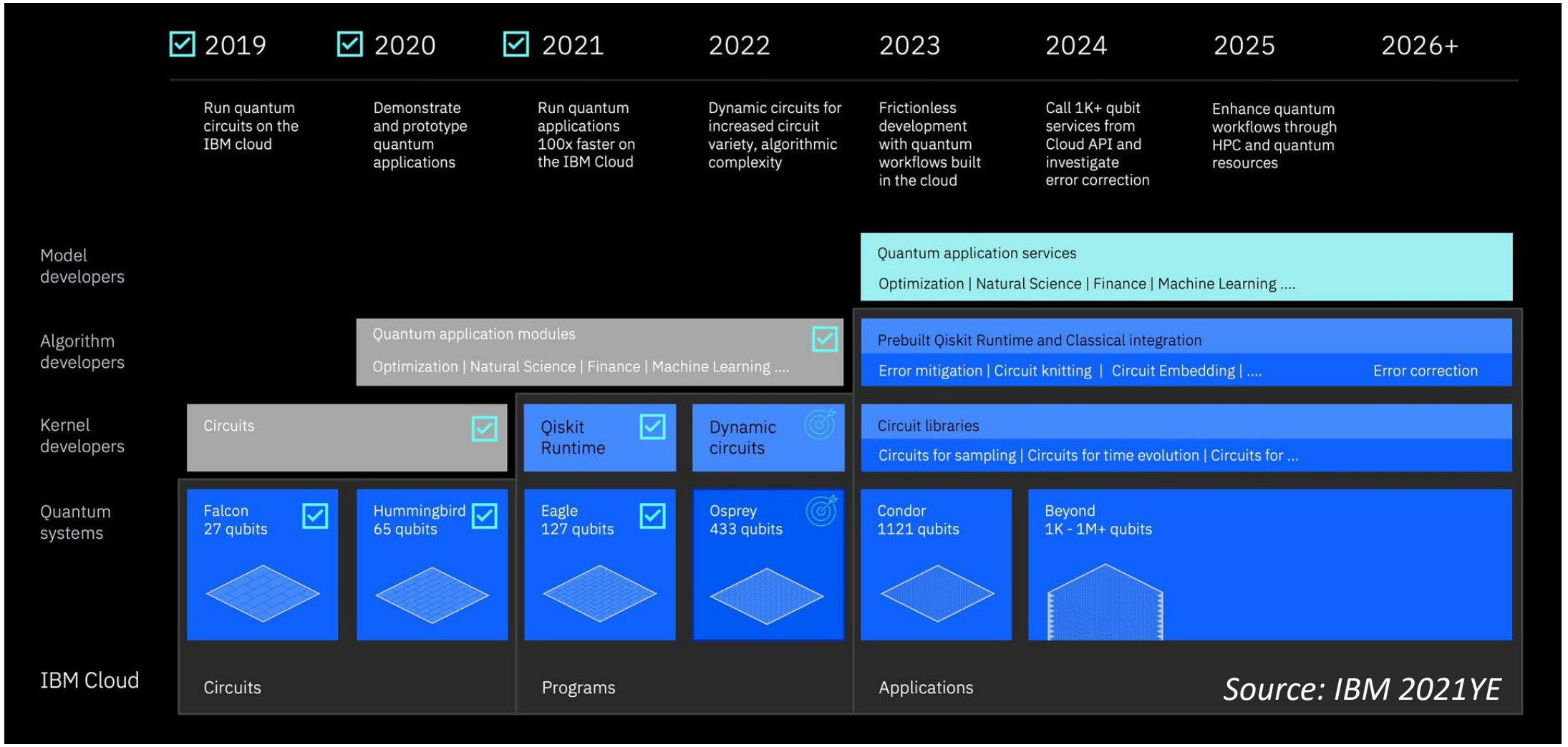
3.1 Problems

Code-based cryptography relies on linear error-correcting codes (or codes for short). These are generated by matrices over finite

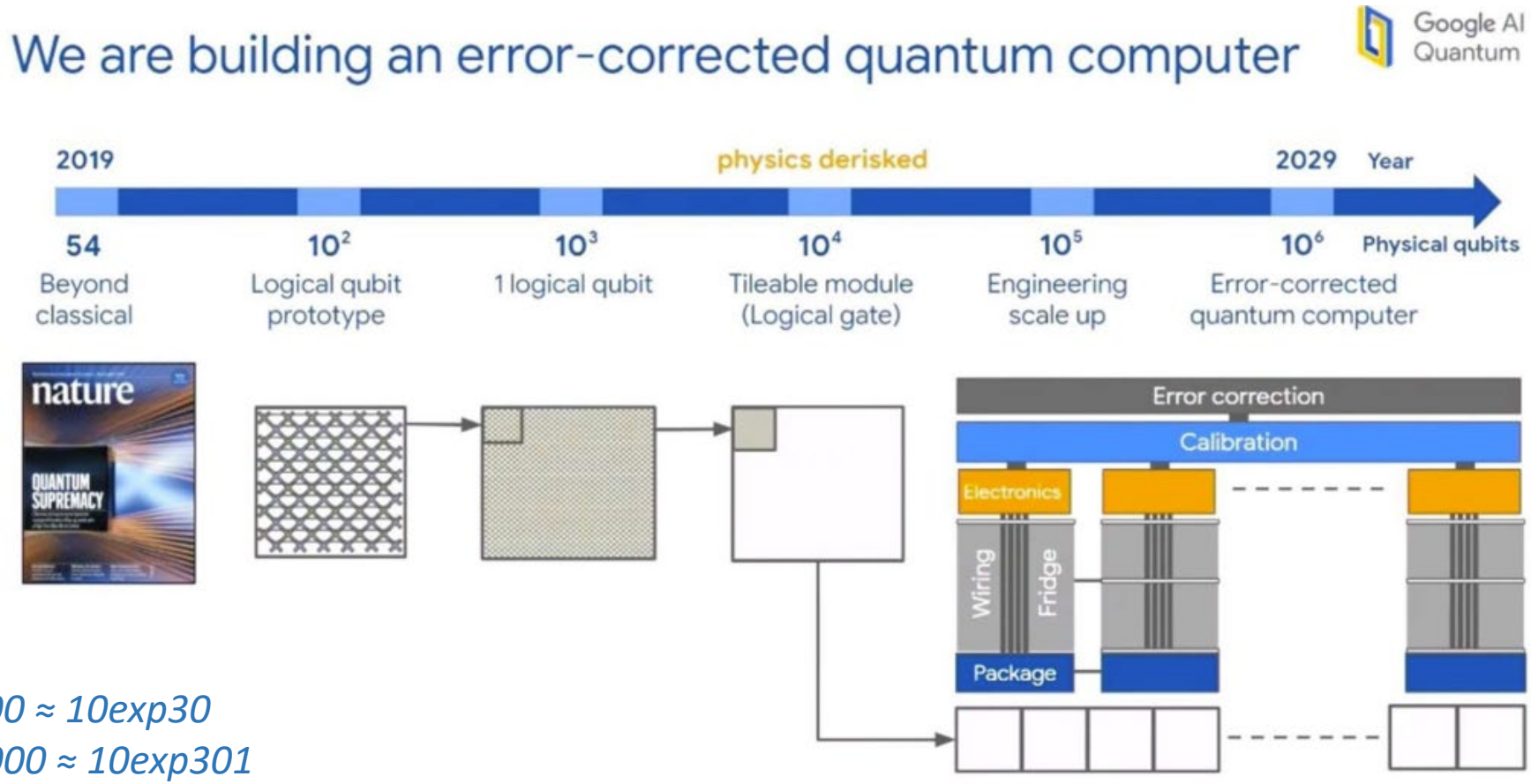
tion 2.1: the matrix $\mathbf{A} \in \mathcal{R}^{n \times m}$ is replaced by $\mathbf{H} \in \mathbb{F}_2^{k \times n}$, and the constraint on the norm of the solution is replaced by a constraint on its Hamming weight. In a certain parameter regime (not used in cryptography), syndrome

Source: PQ Schield, 2022

IBM Quantum Development Roadmap



Google Quantum Technology

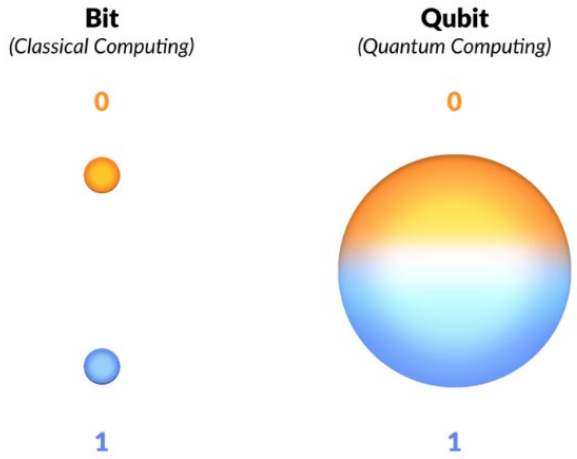


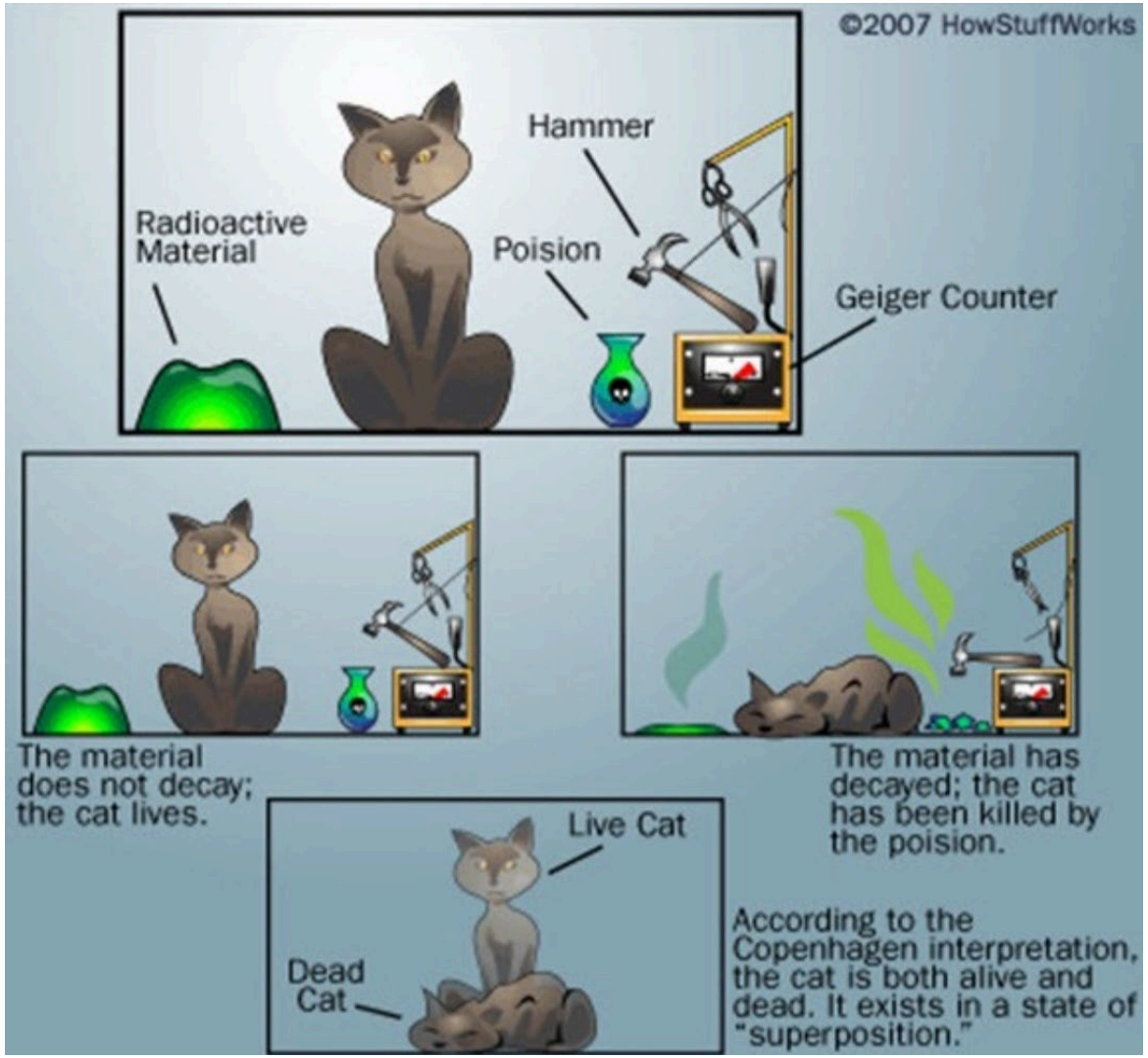
2exp100 ≈ 10exp30
2exp1000 ≈ 10exp301
Pre Webb Universe Atoms ≈ 10exp80

Image credits: H. Neven Google Quantum Summer Symposium 2020

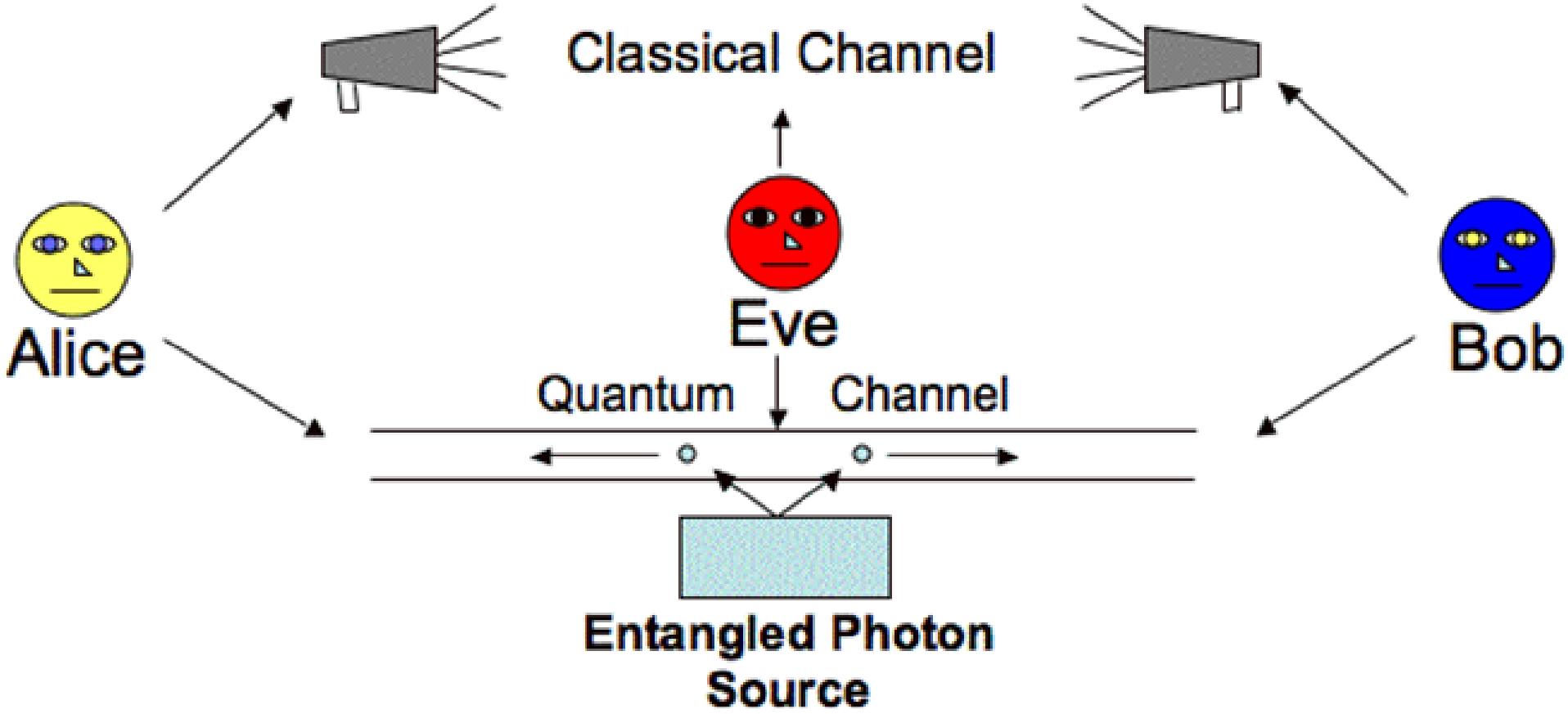
Quantum Superposition: Schrödinger Cat

Bits and Qubits



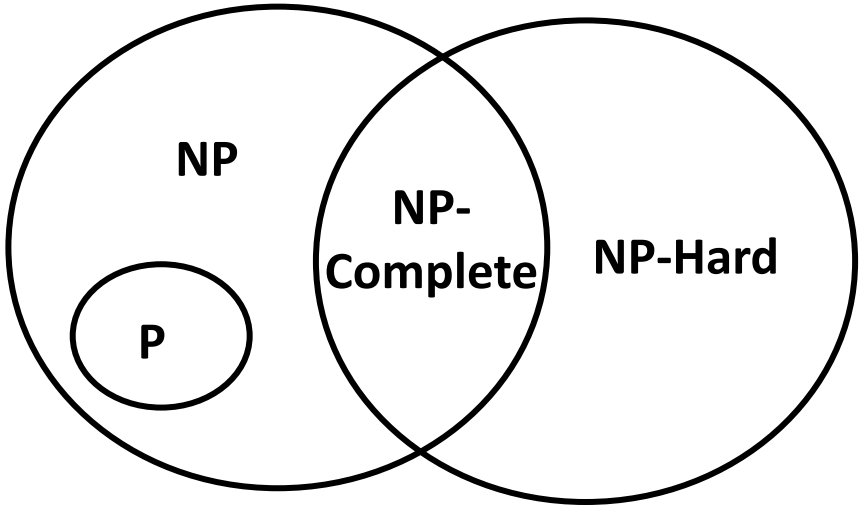


Quantum Key Distribution by Entaglement



Quantum Entanglement

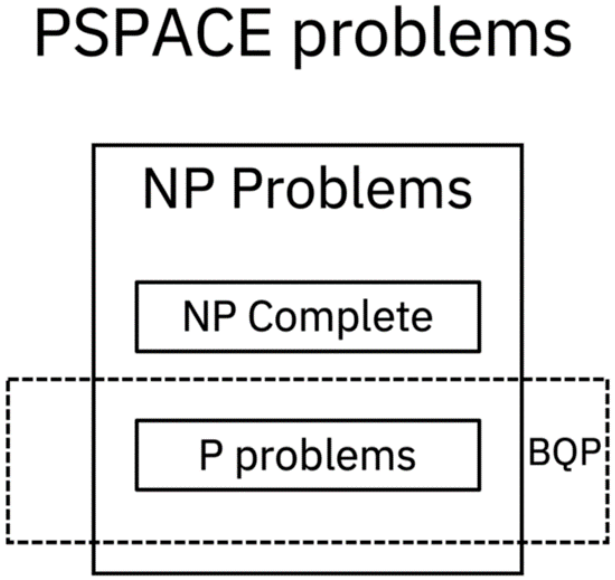
Computational Complexity Theory



P = Polynomial time Problems

NP: Non-deterministic Polynomial time Problems

Polynomial time			Exponential Time		
n	-	Linear Search	2^n	-	0/1 knapsack
logn	-	Binary Search	2^n	-	Travelling SP
n*n	-	Insertion Sort	2^n	-	Sum of Subsets
n*logn	-	Merge Sort	2^n	-	Graph Coloring
n*n*n	-	Matrix Multiplication	2^n	-	Hamilton Cycle



Where BQP lives in the world of complexity classes (*Image credit: Bob Sutor*)

Bounded-error Quantum Polynomial time (BQP)

P, NP, NP-Hard and NP-Complete

- **P (Polynomial) problems**

P problems refer to problems where an algorithm would take a polynomial amount of time to solve, or where Big-O is a polynomial (i.e. O(1), O(n), O(n^2), etc). These are problems that would be considered 'easy' to solve

- **NP (Non-deterministic Polynomial) Problems**

In terms of solving a NP problem, the run-time would not be polynomial. It would be something like O(n!) or something much larger. However, checking the solution would have a polynomial run-time. NP class problems don't have a polynomial run-time to *solve*, but have a polynomial run-time to *verify* solutions

- **Reduction**

We have two problems, A and B, and we know problem B is a P class problem. If problem A can be reduced, or converted to problem B, and this reduction takes a polynomial amount of time, then we can say that A is also a P class problem (A is reducible to B)

- **NP-Hard Problems**

A problem is classified as NP-Hard when an algorithm for solving it can be translated to solve *any* NP problem. Then we can say, this problem is *at least* as hard as any NP problem, but it could be much harder or more complex

- **NP-Complete Problems**

NP-Complete problems are problems that live in both the NP and NP-Hard classes. This means that NP-Complete problems can be verified in polynomial time and that any NP problem can be reduced in polynomial time

Some Quantum Computing Applications

- **Pharmaceuticals**

In the biopharmaceuticals industry, quantum computing will revolutionize molecular research and development. Speed up development of Drugs and Vaccines. New drugs. Precision Medicine. Replacement of Labs & Research by Simulations.

- **Chemicals**

Quantum computing could benefit Chemical companies in production, R&D, and supply chain operations, for example, by improving the design of catalysts

- **Finance**

Quantum computers are opening new possibilities in finance — from deeper analytics to faster trading. Institutions use quantum computing to improve trade, transactions, and data speed

- **Business Benefits**

Quantum computing can help companies to innovate and create new products. In addition, companies can improve their supply chains and develop better customer service. More Revenues, less Costs.

- **Spending Less on Infrastructures**

E.g. in transportation, quantum computers can analyze historical data to help plan your route for best results by adding more routes or creating more deliveries at certain times of the day

IBM Quantum Business Take Off