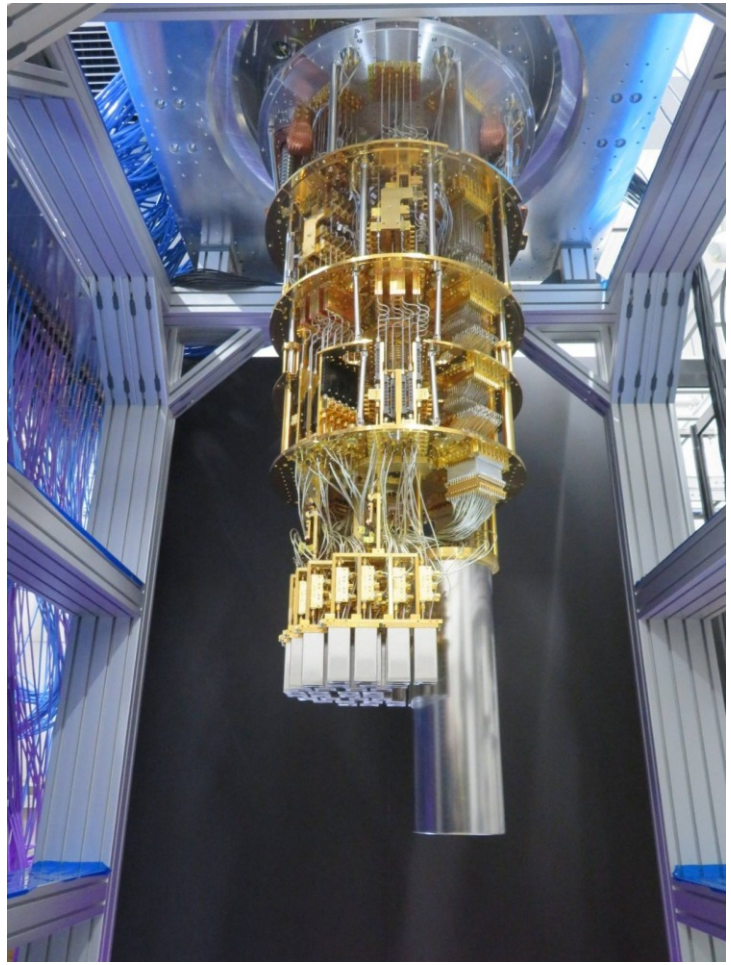
Quantum Computing, AI, and the Canton of Geneva

Rafael Tiedra, October 2026



quantum computer from
Fujitsu and Riken Institute
(April 2025)

Contents

- Introduction
  - Fundamental principles
    - Applications
    - Current limitations and challenges
  - Actions undertaken by Geneva State
- References

Introduction

Quantum computing…

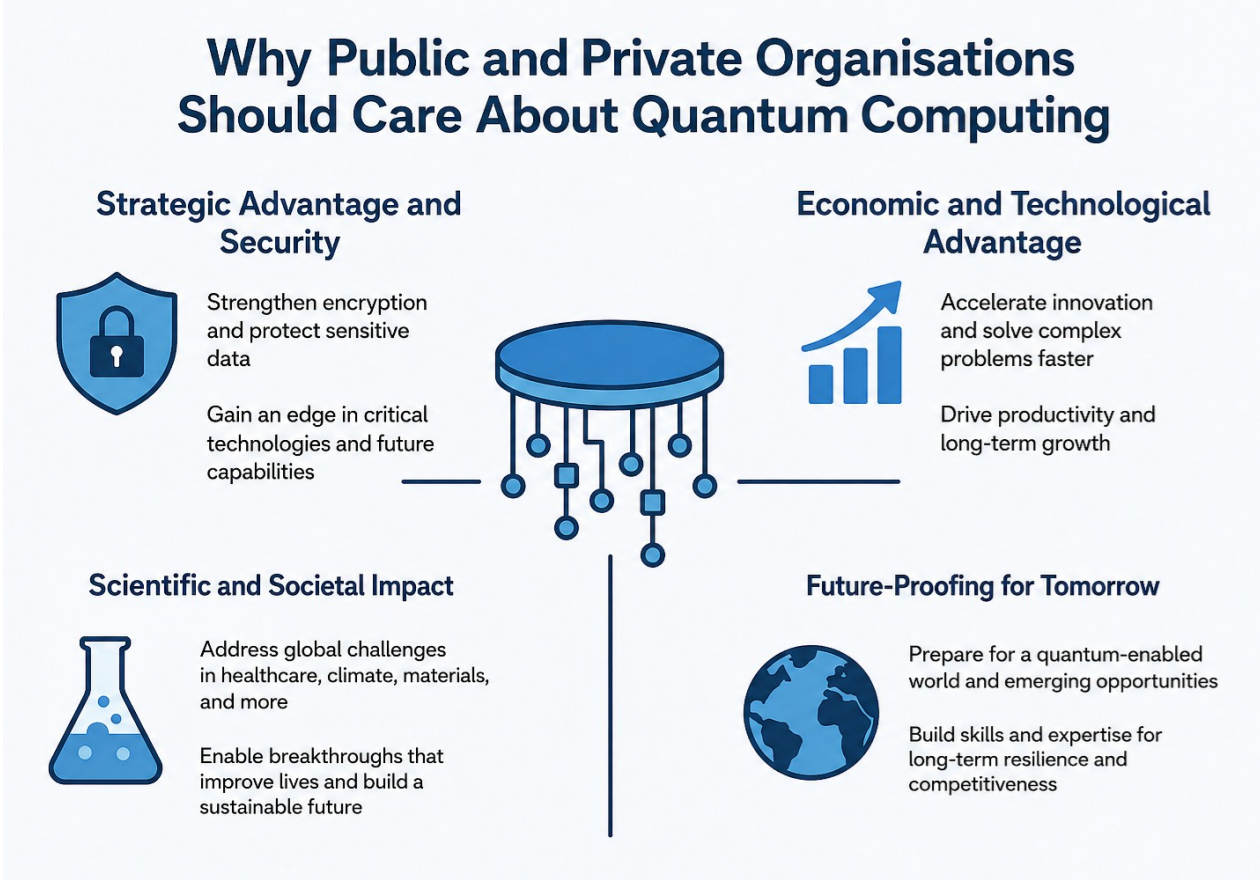
❑ **Why do I care ?**

Quantum computing technology watch at Geneva State – OCSIN, and currently writing a monograph on mathematical methods for quantum mechanics

❑ **Why should organisations care ?**

National security agencies (NCSC in the UK, NIST in the US, ANSSI in France, etc.) estimate that quantum computers might be able of breaking current encryption systems by 2035.

But there is much more :



Introduction

What is quantum computing ?

Quantum computing is a branch of computer science that relies on the principles of quantum mechanics to encode and process information.

Unlike classical computing, which uses bits (0 or 1), it uses qubits governed by the laws of quantum mechanics.

→ Will make possible to solve some problems beyond the capabilities of classical computers.

Fundamental principles

A qubit ("quantum bit") is the unit of information in quantum computing. It can be in the states $|0\rangle$, $|1\rangle$, or in a superposition

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

with α and β complex amplitudes, $|\alpha|^2 + |\beta|^2 = 1$.

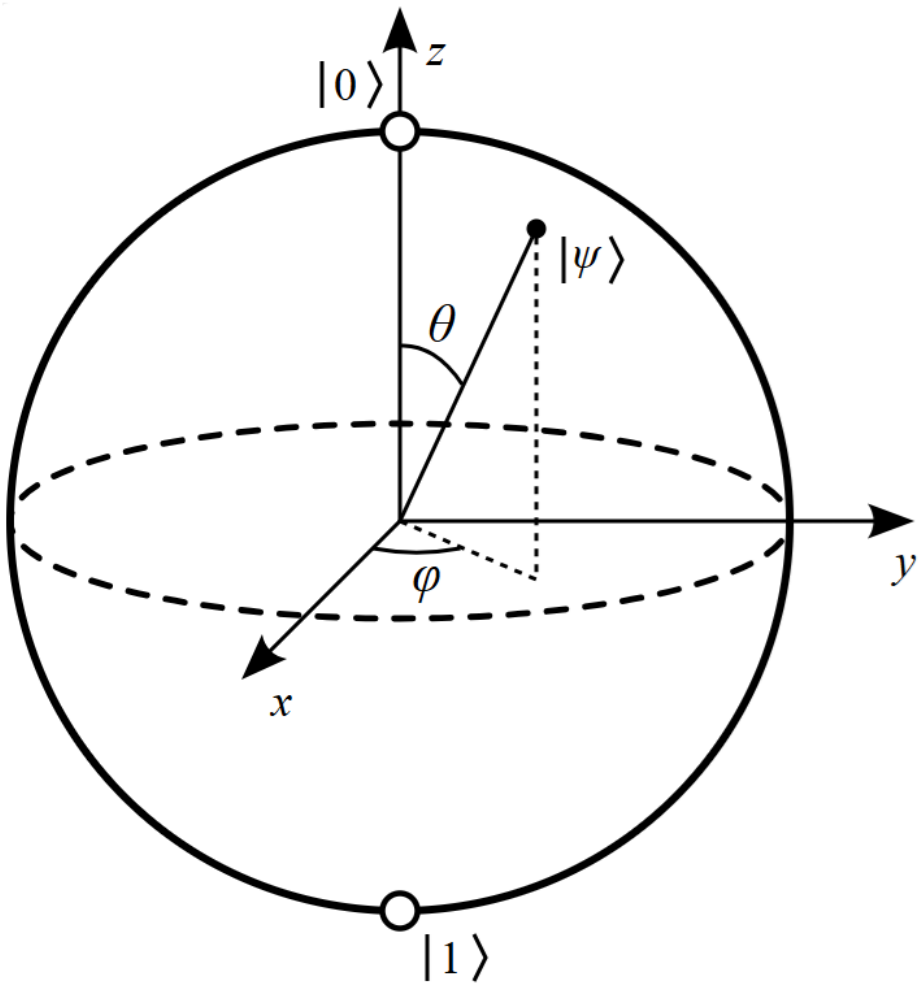
($|\psi\rangle$ can be represented as a point on a sphere of radius 1 called the "Bloch sphere")

Several approaches to manufacturing qubits :

- ❑ Superconducting qubits (Google, IBM, Rigetti, IQM)
- ❑ Trapped ions (IonQ, Quantinuum)
- ❑ Spin qubits (Intel, Silicon Quantum Computing)
- ❑ Photonic qubits (Xanadu)

Not yet clear which technologies will prevail...

Bloch sphere (Wikipedia, September 2025)



Fundamental principles

The principles of quantum mechanics used in quantum computing are (among others) :

❑ Superposition and interference of wave functions
(qubits can be in superposition of several states simultaneously)

For example : $\left(\frac{1}{2}|0\rangle + \frac{1}{4}|1\rangle\right) + \frac{1}{4}|0\rangle = \frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle$

❑ Entanglement of wave functions
(qubits can be correlated "instantly", even at a distance)

For example : $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ (famous example called "Bell state")

❑ Collapse of wave functions when measured

(the classical state of a quantum system is determined when it is measured/observed 🐈)

For example : $\frac{1}{2}|0\rangle + \sqrt{\frac{3}{4}}|1\rangle \longrightarrow$  $\longrightarrow |1\rangle$

Fundamental principles

Quantum logic gates ("quantum gates") are the quantum equivalent of classical logic gates such as AND, OR, NOT, etc., but they operate on qubits rather than bits.

Quantum gates...

- ❑ transform the state of qubits in a quantum circuit
- ❑ perform reversible transformations (unlike classical gates, which can be irreversible)
- ❑ are represented mathematically by unitary matrices (which guarantees reversibility + conservation the total probability of outcomes)

Fundamental principles 😱

Unitary matrices stem from the Schrödinger equation in finite dimension...

$$i\frac{\mathrm{d}}{\mathrm{dt}}|\psi(t)\rangle = H|\psi(t)\rangle \iff |\psi(t)\rangle = \mathrm{e}^{-itH}|\psi(0)\rangle \quad (H = \text{hermitian matrix})$$

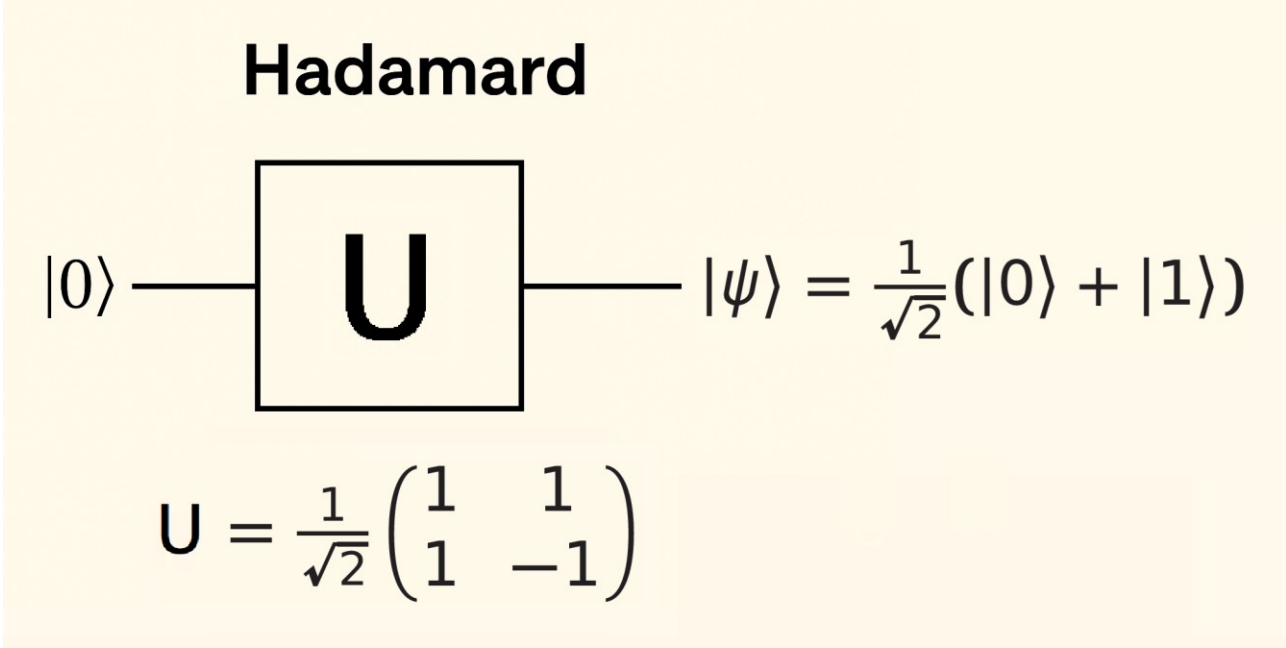
... and in discrete time $t = n$:

$$|\psi(n)\rangle = (\mathrm{e}^{-iH})^n|\psi(0)\rangle \iff |\psi(n)\rangle = U^n|\psi(0)\rangle \quad (U = \text{unitary matrix})$$

(more details: https://www.linkedin.com/short-tour-quantum-computing, October 2026)

Fundamental principles

Example of quantum gate :

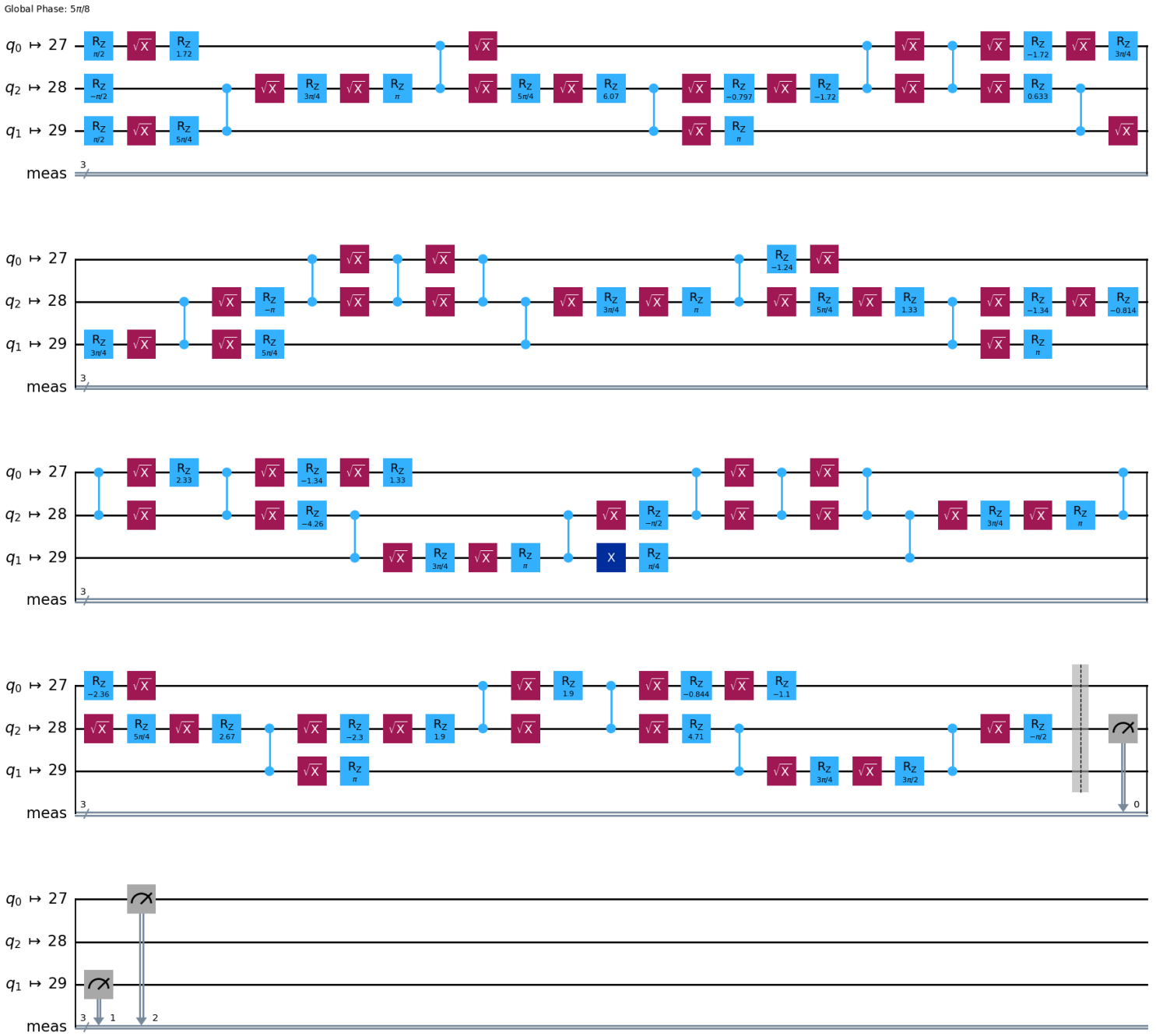


Fundamental principles

Example of a 3-qubit circuit executed on the "ibm_sherbrooke" quantum computer on May 7, 2025.

Programming and diagram created using the open-source Python library Qiskit, introduced by IBM Research in 2017.

(diagram to be read like a musical score...)



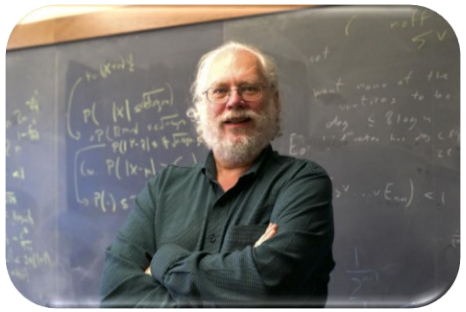
Applications

Two iconic algorithms illustrate the risks and opportunities brought by quantum computing.

❑ **Shor's algorithm ("risk") :**
Makes possible (with a fully functional quantum computer) the factorisation of large numbers in exponentially less time than with classical computers.

→ Will make possible breaking various public key encryption protocols such as RSA, Diffie-Hellman, elliptic curves, etc.

CERN (March 2021)



❑ **Grover's algorithm ("opportunity") :**
Makes possible (with a fully functional quantum computer) the search for an element in an unordered list in quadratically less time than with classical computers.

→ Will improve the speed of multiple industrial applications based on searching for an optimal element/configuration in a large set.

dotquantum.io (unknown date)



(the previous circuit implements Grover's algorithm for a list of $2^3 = 8$ éléments 😀)

Applications

There are numerous areas of application for quantum computing, at various stages of development (academic research, proof of concept, or already deployed) :

- ❑ Cryptography and cybersecurity
- ❑ Optimisation and operational research
- ❑ Simulation of physical and chemical systems
- ❑ AI and Machine Learning
- ❑ Data science and information retrieval
- ❑ Quantum communication
- ❑ Quantum metrology and sensors
- ❑ Finance and economics

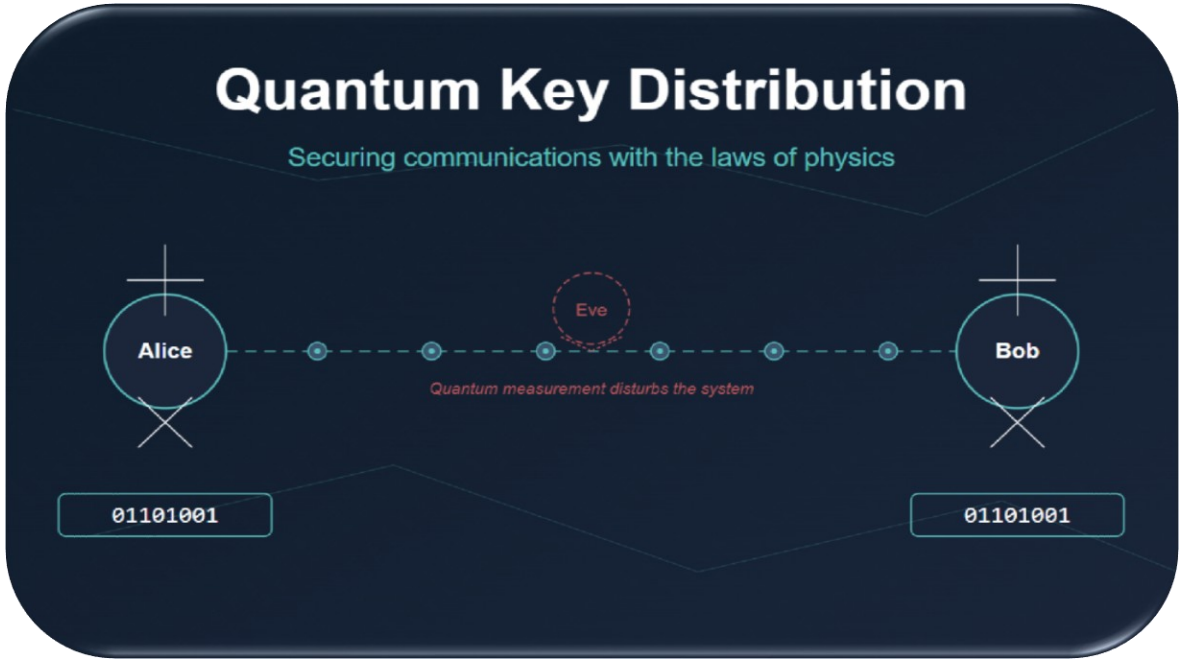


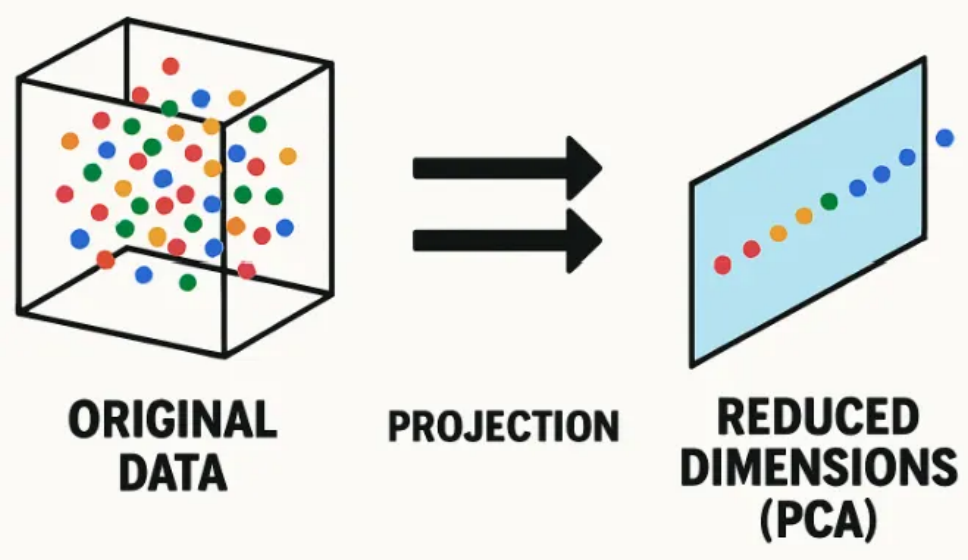
illustration Pranav Sanghadia (April 2025)

(tested by Geneva State for electronic vote between 2007 and 2014, and for encrypted communication in 2026)

Application in AI & ML: qPCA

Classical principal component analysis (PCA) finds the directions of maximum variance in a dataset with N input features :

1) Compute the $N \times N$ covariance matrix A of the dataset
2) Compute its eigendecomposition $A = \Sigma_{k=1}^{N} \lambda_k u_k u_k^T$
3) Eigenvectors u_k = principal components (new axes); eigenvalues λ_k = variance each axis explains
4) Keep only the top-t components ($t \ll N$) to compress the data



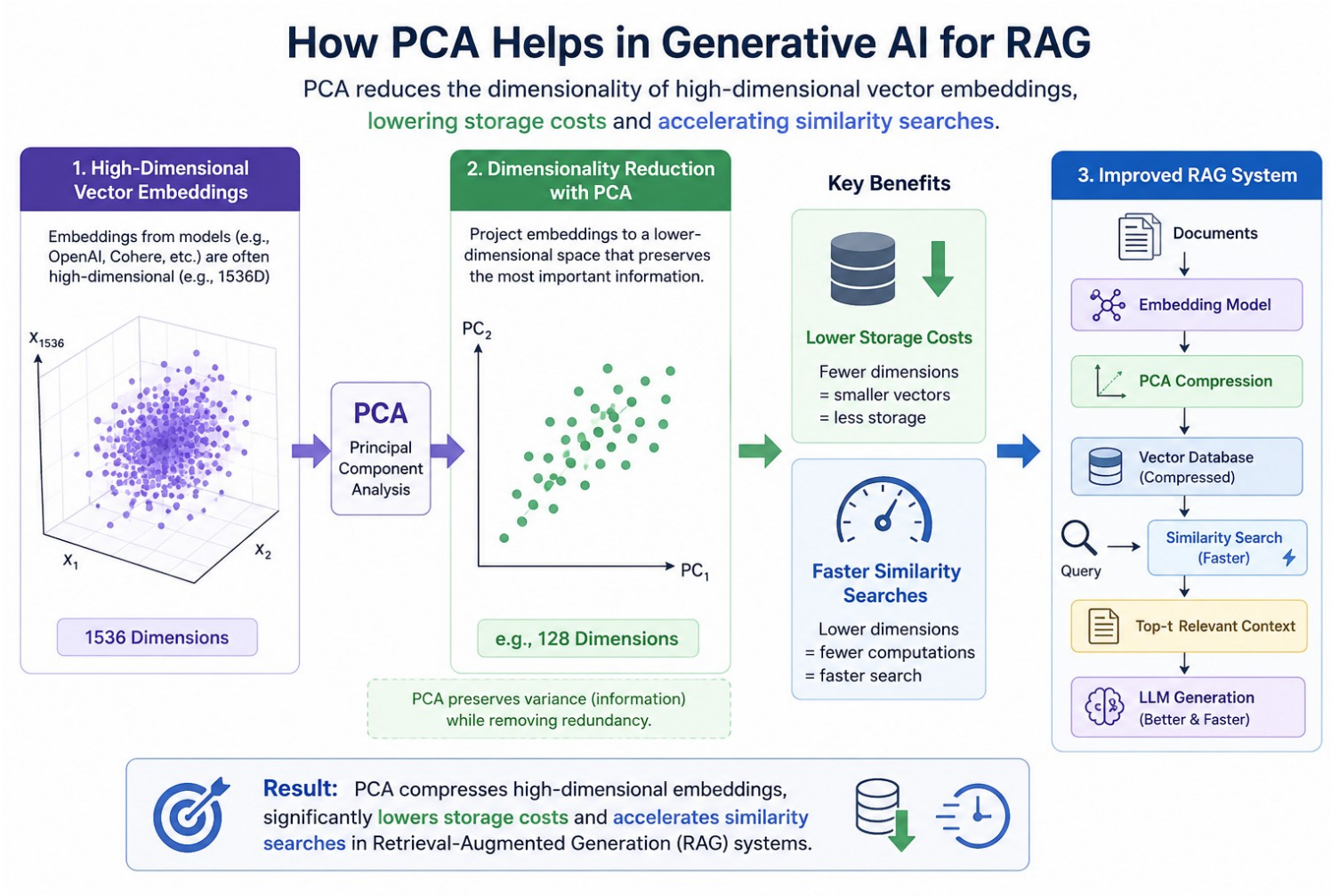
(medium.com, October 2025)

Application in AI & ML: qPCA

For example :

- For asset allocation, PCA can reduce the dimensionality of correlated asset returns by keeping the top principal components that explain most of the variance, which can then be used to build a more diversified portfolio.

- In generative AI, PCA can be used for dimensionality reduction to compress high-dimensional vector embeddings, and thus lower storage costs and accelerates similarity searches in Retrieval-Augmented Generation (RAG) systems.



Application in AI & ML: qPCA

PCA does not scale well since diagonalising $N \times N$ covariance matrices has a computational cost $O(N^3)$, and N grows fast in practice :

Images, genomics, sensor arrays, and financial covariance matrices can have thousands to millions of features.

Number of features : N	Computational cost of PCA : $O(N^3)$
10	1000
100	1000000
1000	1000000000
10000	1000000000000
100000	1000000000000000

Application in AI & ML: qPCA 😱

Quantum PCA (qPCA) extracts the same top eigenvalues/eigenvectors of the covariance matrix, but by encoding the matrix in a quantum state and reading out its spectrum with phase estimation, instead of classically diagonalising it.

1) **Encode :** Load the matrix as a quantum state $|\psi\rangle$ via amplitude encoding

2) **Estimate :** Quantum phase estimation writes eigenvalues λ_k into a register

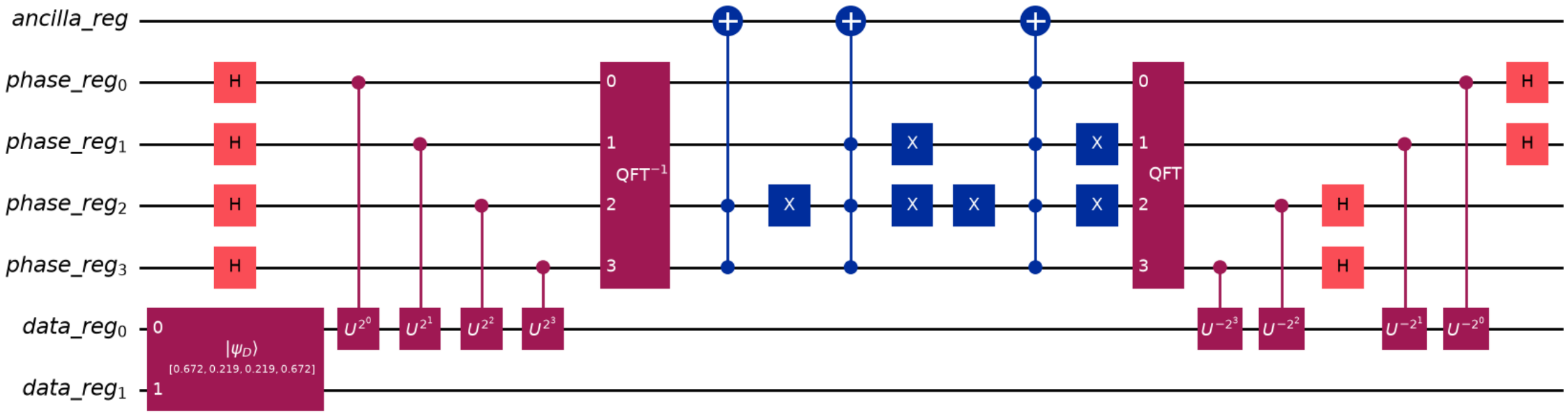
3) **Threshold :** Keep only components above a cutoff value $\tau > 0$ (the top-t principal components)

4) **Measure :** Read out the surviving state to recover components u_k

5) **Output :** $|\psi'\rangle \approx \Sigma_{k=1}^{t} \sqrt{p_k}\, |\lambda_k\rangle |u_k\rangle$, the same top-$t$ principal components classical PCA would find

Application in AI & ML: qPCA

Example of (simplified) qPCA circuit for the matrix $A = \begin{pmatrix} 0.6507 & 0.2122 \\ 0.2122 & 0.6507 \end{pmatrix}$:



(https://github.com/rtiedra, October 2026)

Application in AI & ML: qPCA

Why quantum PCA is worth it :

	Classical PCA	Quantum PCA
Computational cost	$O(N^3)$	$O(t \cdot \mathrm{poly}(\log N))$

- **Exponential speed-up :** Time complexity drops from $O(N^3)$ to $O(t \cdot \mathrm{poly}(\log N))$
- **Exponential memory drop :** $O(\log(N\kappa))$ qubits are needed for qPCA (with κ the condition number of the covariance matrix) in comparison with the $O(N^2)$ memory needed to store the matrix classically
- **Still maturing :** Practical use needs efficient state preparation, tomography for read-out, and noise-resilient hardware

For instance, if $N = 1'000'000$, $t = 100'000$ and $\mathrm{poly} = (\cdot)^3$, then $O\left(t \cdot \mathrm{poly}(\log N)\right)$ is 4 billion times smaller than $O\left(N^3\right)$.

Current limitations and challenges

Quantum computing is still in its NISQ (Noisy Intermediate-Scale Quantum) phase. The main challenges are :

- ❑ Improved stability (coherence time), reliability, and number of qubits
- ❑ More affordable error correction methods (cost and infrastructure)
- ❑ Discovery of more useful quantum algorithms [1]

Progress is rapid, but it will take years to develop fault-tolerant quantum computers capable of solving problems beyond the reach of classical computers.

[1] LLMs can be used to improve or discover quantum algorithms. See for instance :
Discovering state-of-the-art quantum circuits with large language models

Actions undertaken by Geneva State

Actions undertaken :

- ❑ First tests on quantum computers of IBM
- ❑ Participation of OCSIN to the Geneva Quantum Network
- ❑ Creation of a group of stakeholders at Geneva State dedicated to quantum initiatives

Actions in progress :

- ❑ Securing long-term access to quantum computers
- ❑ Defining suitable use-cases for Geneva State

Discussions with various institutions :

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

CERN

UNIVERSITÉ DE GENÈVE

IONQ

IBM Quantum

Hes·so

UNICC

EPFL

HUG Hôpitaux Universitaires Genève

gesda

ETH zürich

IQM

D:Wave The Quantum Computing Company™

Thank you !

References

Quantum Computing :

https://quantum.cloud.ibm.com/learning/en/courses/basics-of-quantum-information

https://quantum.cloud.ibm.com/learning/en/courses/fundamentals-of-quantum-algorithms

https://quantum.cloud.ibm.com/learning/en/courses/quantum-machine-learning/introduction

A Low-Complexity Quantum Principal Component Analysis Algorithm

Towards An End-To-End Approach For Quantum Principal Component Analysis

Discovering state-of-the-art quantum circuits with large language models

https://www.linkedin.com/pulse/short-tour-quantum-computing

https://github.com/rtiedra/quantum-computing/blob/main/low-complexity-qpca.ipynb

Post-Quantum Cryptography :

https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

https://cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique

https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b

https://quantum.cloud.ibm.com/learning/en/courses/quantum-safe-cryptography

https://www.coursera.org/learn/advanced-data-structures-rsa-and-quantum-algorithms

Python Libraries :

https://pennylane.ai/

https://en.wikipedia.org/wiki/Qiskit