



Advertisements !

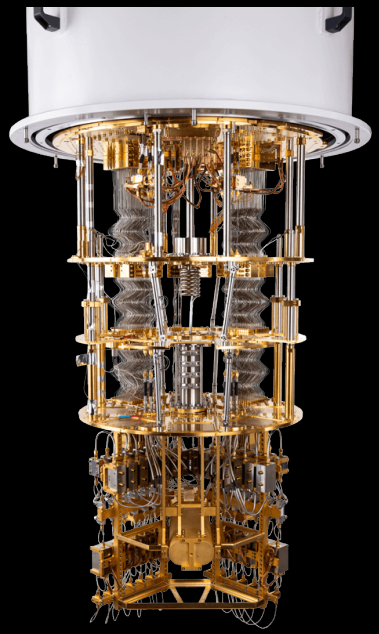


Pascal Lafourcade
Friday November 13th, 2026
Grenoble, France

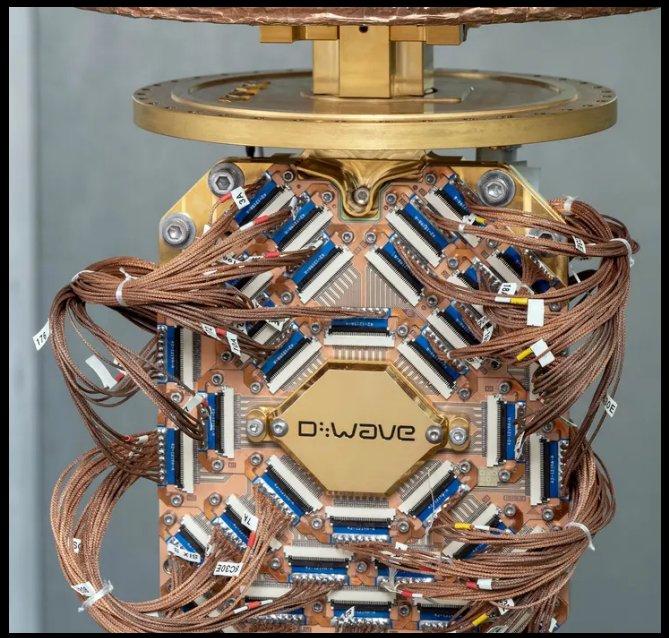
Quantum Computers



IBM



rigetti



D:wave

2017 NIST Competition



- 30 novembre 2017 : 69 sousmissions Round 1
- 30 janvier 2019 : 26 sousmissions choisies pour le Round 2
- 22 juillet 2020 : 7+8 sousmissions choisies pour le Round 3
- 5 juillet, 2022 :



  - KEM : Kyber
  - Signature : Dilithium, Falcon, SPHINCS+
- 13 août 2024, NIST publie les standards :
  - FIPS 203 (Kyber),
  - FIPS 204 (Dilithium)
  - FIPS 205 (SPHINCS+)
  - FIPS 206 (FALCON)
- 10 mars 2025, NIST annonce le vainqueur du Round 4 : KEM HQC

To know



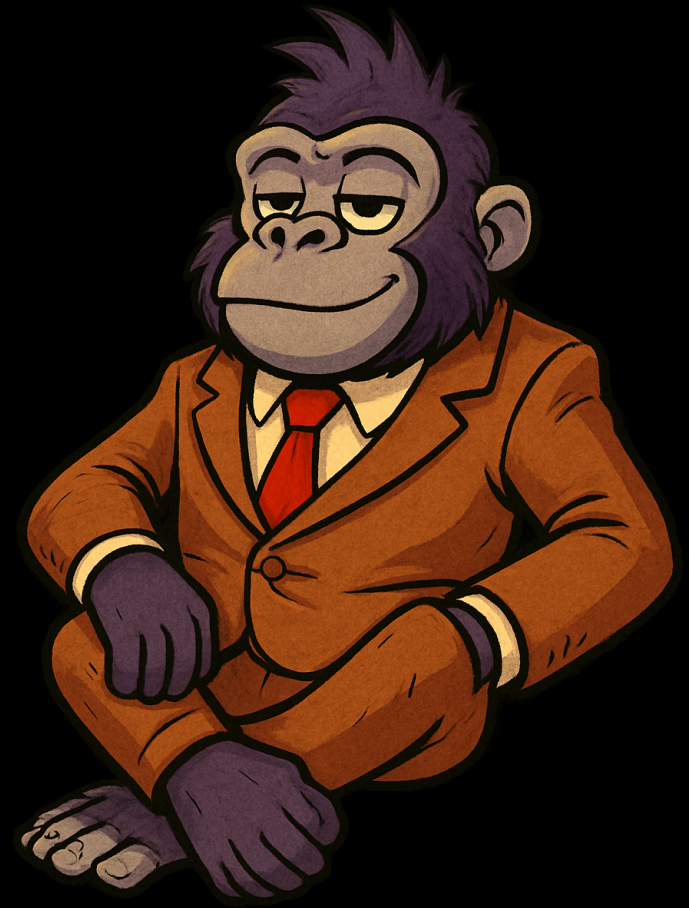
Novembre 2024

Algorithmes	Transition
ECDSA	Deprecated in 2030
	Forbidden in 2035
RSA	Deprecated in 2030
	Forbidden in 2035



Post-Quantum Cryptography





Post-Quantum Cryptography in English soon !





1. Introduction to Post-Quantum Cryptography
2. Fundamental Concepts of Cryptography
3. Quantum algorithms for cryptography
4. Post-Quantum Migration Plan
5. Hash-based Signature Schemes
6. Code-based Cryptography
7. Lattice-based cryptography
8. Further Insights into Lattices
9. Other Approaches to Post-Quantum Signatures
10. Mathematical Background

Solution of the exercises

Preface by



David Pointcheval

Scientific Directr at Cosmian,
Médaille d'argent 2021 CNRS
Prix Lazare Carnot 2025 de l'Académie des Sciences.
2024 IACR Fellow

English Version work in Progress ...

