



Industrial Strategy for Post-Quantum Cryptography

Ludovic Perret, ludovic.perret@epita.fr
EPITA/LRE

DGA Post-Quantum Cryptography Days, Rennes, ECW'24



1/ Context of the work



*“The Institute for Higher National Defence Studies (IHEDN) is a public institution with an interministerial dimension, placed under the supervision of the Prime Minister. Its mission is to promote a **defence culture**, help strengthen **national cohesion** and contribute to the development of **strategic thinking** on defence and security issues”.*



Jean Peeters

Professeur des universités
Titulaire

jean.peeters@fdd-ihedn.fr



Vincent Giraud

Docteur en informatique
Chercheur

vincent.giraud@fdd-ihedn.fr

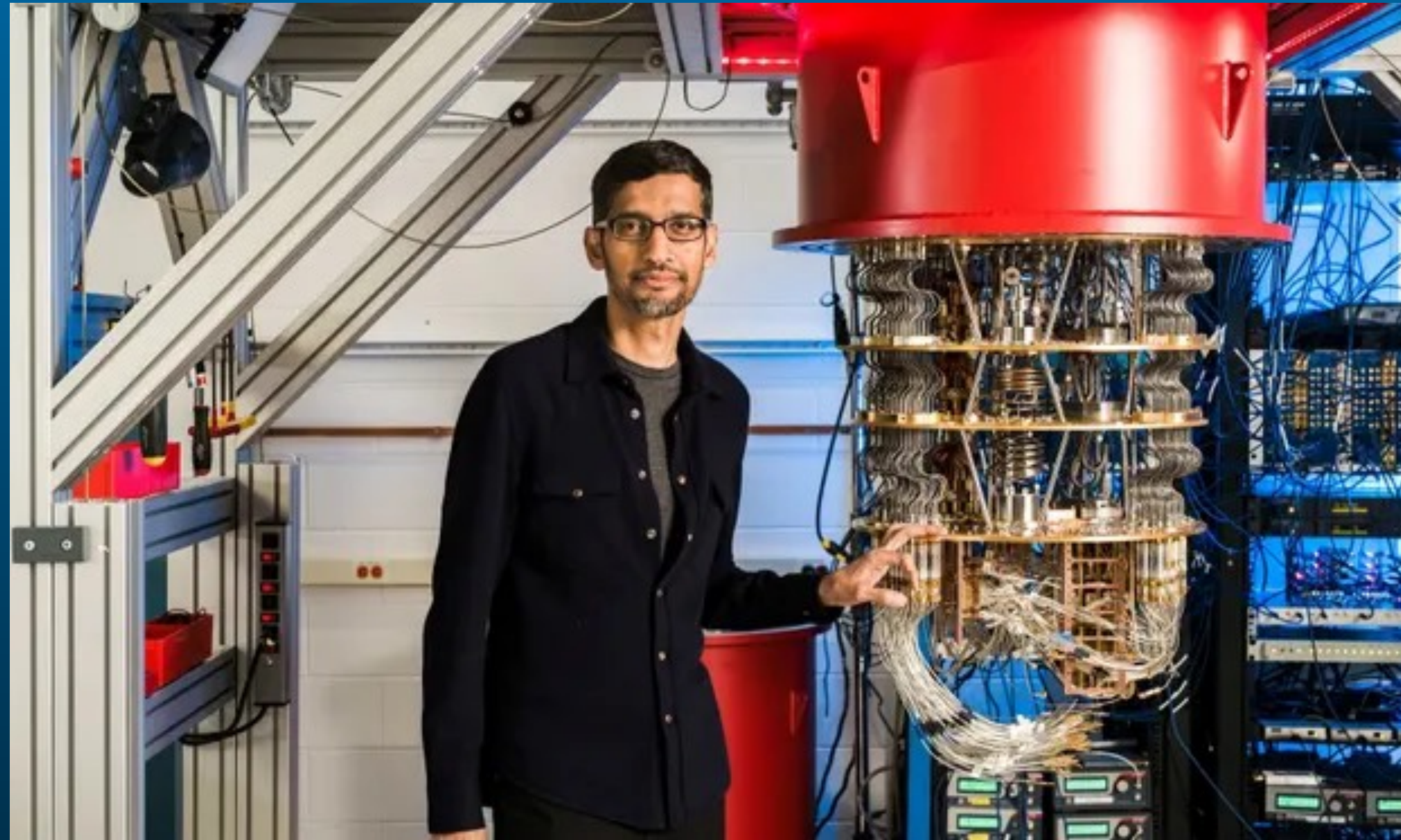
2/ Impact of quantum on cybersecurity

Working group

- Virginia D'Auria, Professor, Quantum communication, Côte d'Azur University
- Maria Christofi, senior cryptographer
- Fabienne Ealet, Ministry of Defense
- Jean-François Funke, Lawyer, Paris Bar
- Gérald Kénanian, Innovation mission director, MEDEF
- **Pierre Loidreau, DGA MI**
- Emmanuel Laurent, ACOSS, Director
- Olivier Senot, Docaposte
- Samih Souissi, ANSSI
- Marina Teller, Professor of Law, Côte d'Azur University
- Simone Vannuccini, Junior Professor of Economy, Côte d'Azur University
- Arthur Villard, senior cryptographer, EDF (R&D)



3/ Quantum threat



[Sundar Pichai](#) (PDG Google)
Sycamore (53 qubits)

Factoring problem

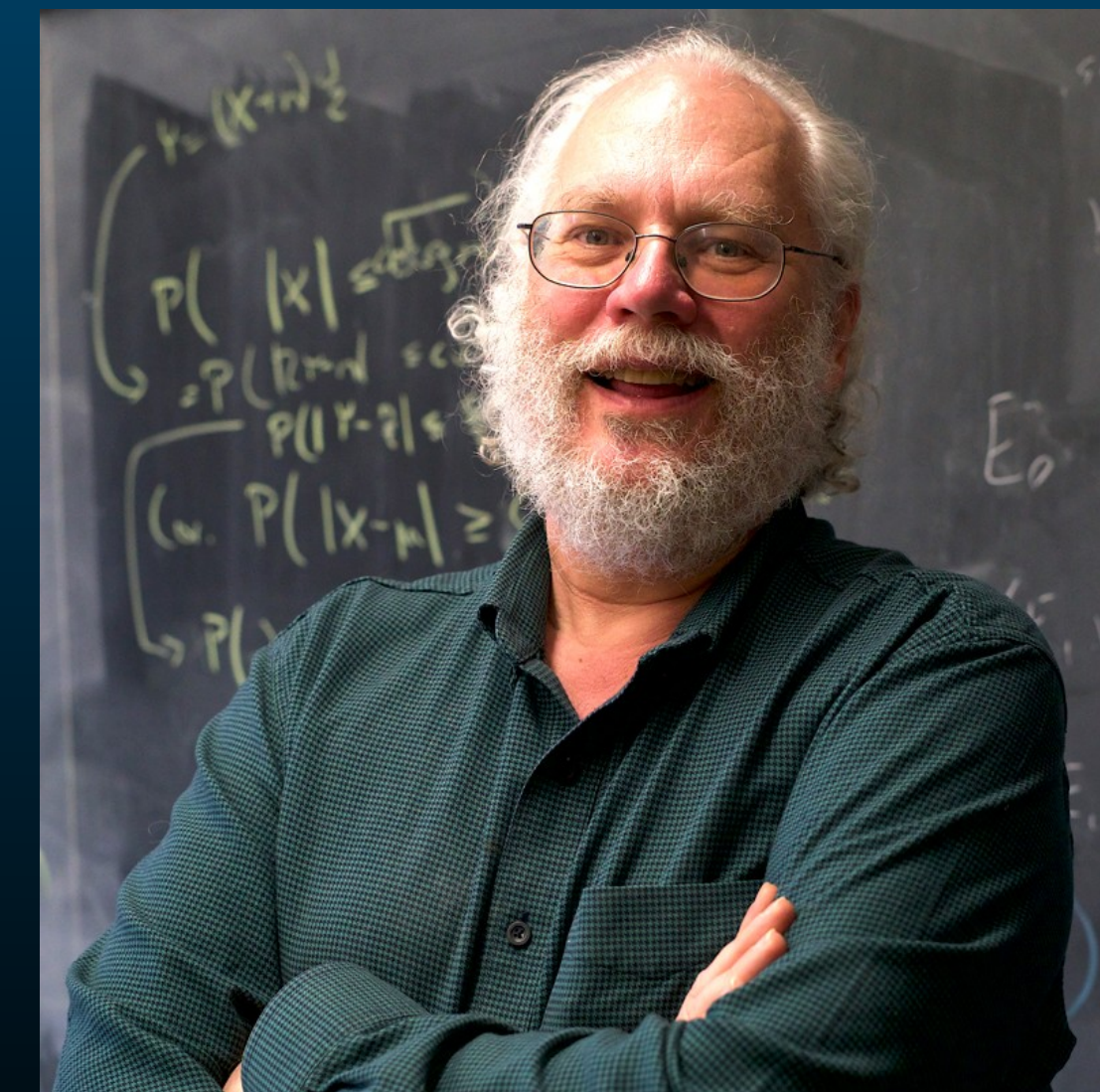
Hard to recover p and q from $N = p \times q$

Poly-time algorithm for factoring (1997)

▸ RSA1048

➔ Classical \approx 400 years

➔ Quantum \approx hours



Peter Shor (MIT)

PASQAL

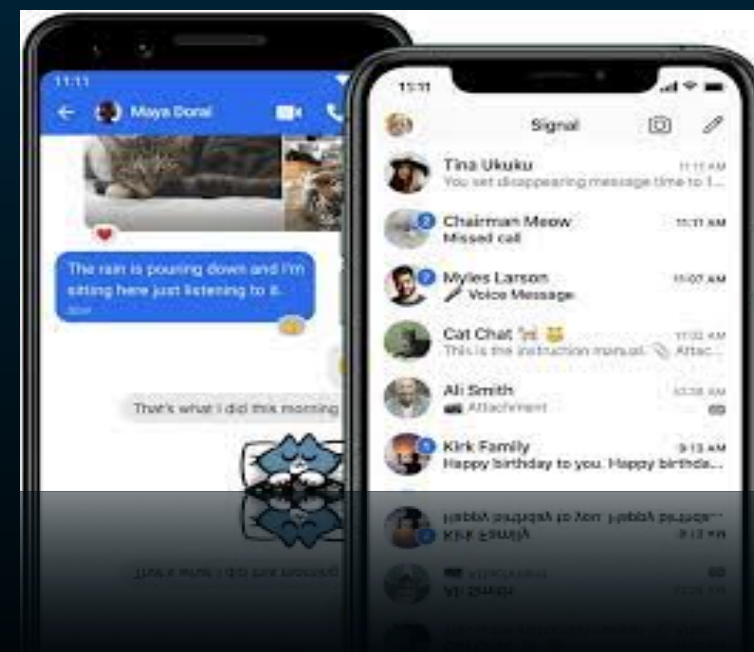
ALICE & BOB

Generation 1	Generation 2
Currently in production	Currently in research & development.
100 QUBITS Today	1,000 QUBITS
200 QUBITS Coming Soon	

4/ Cryptography market



Cyber
market
>150Bn\$



5/ A systemic risk

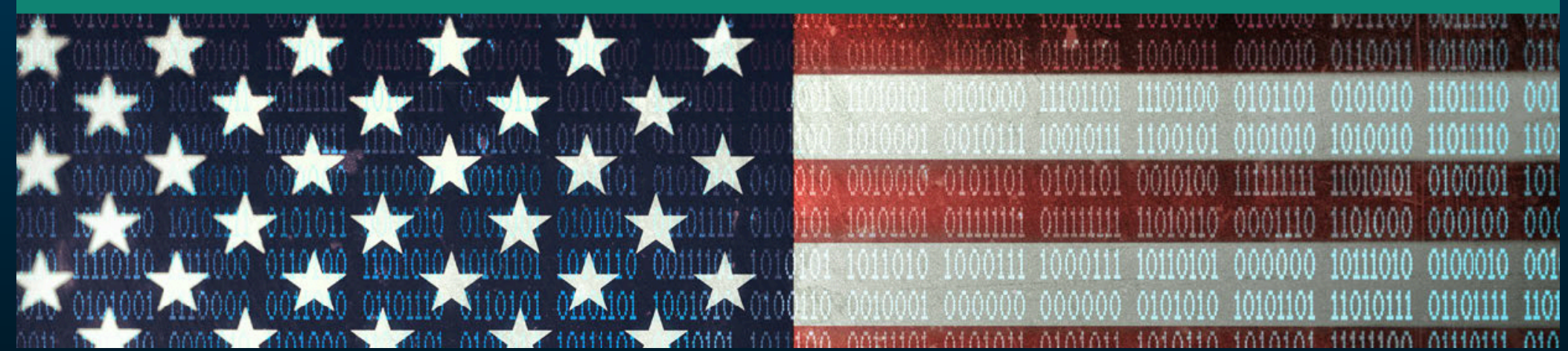
Hudson Institute

APRIL 2023

Prosperity at Risk: The Quantum Computer Threat to the US Financial System

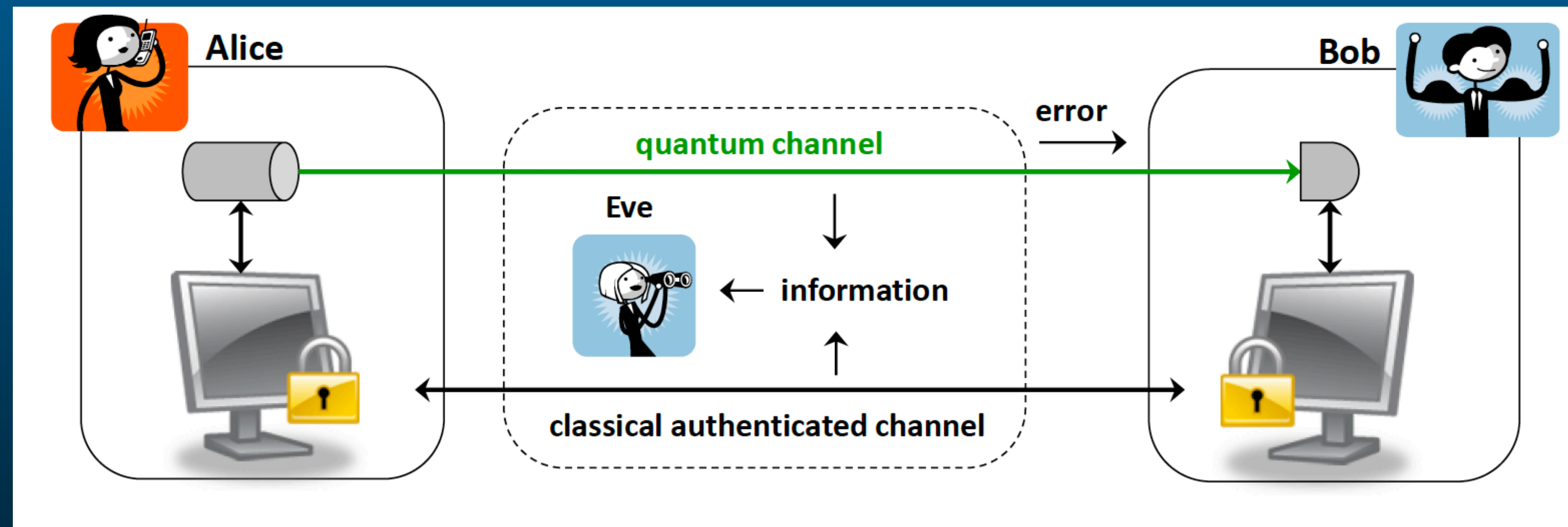
BY ALEXANDER W. BUTLER AND ARTHUR HERMAN
QUANTUM ALLIANCE INITIATIVE

*“Utilizing original econometric models in addition to the Oxford Economics Global Economic Model (GEM), we found that a quantum computer attack on FedWire and against US banks would have drastic consequences for the financial sector itself, and **reverberate throughout the entire US macroeconomy**. On summary, a single-day quantum computer attack on a top-five bank would cost the US economy between **\$2 and \$3.3 trillion** in indirect impacts alone.”*



6/ Quantum-Key Distribution (QKD)

Quantum cryptography : Information-Theoretic Security



- Highest level of security
- Strong practical constraints
 - Limited distance for QKD, expensive (require specific communication channels)

7/ Quantum diplomacy

The man turning China into a quantum superpower

Jian-Wei Pan, China's "father of quantum", is masterminding its drive for global leadership in technologies that could change entire industries.

By Martin Giles

December 19, 2018

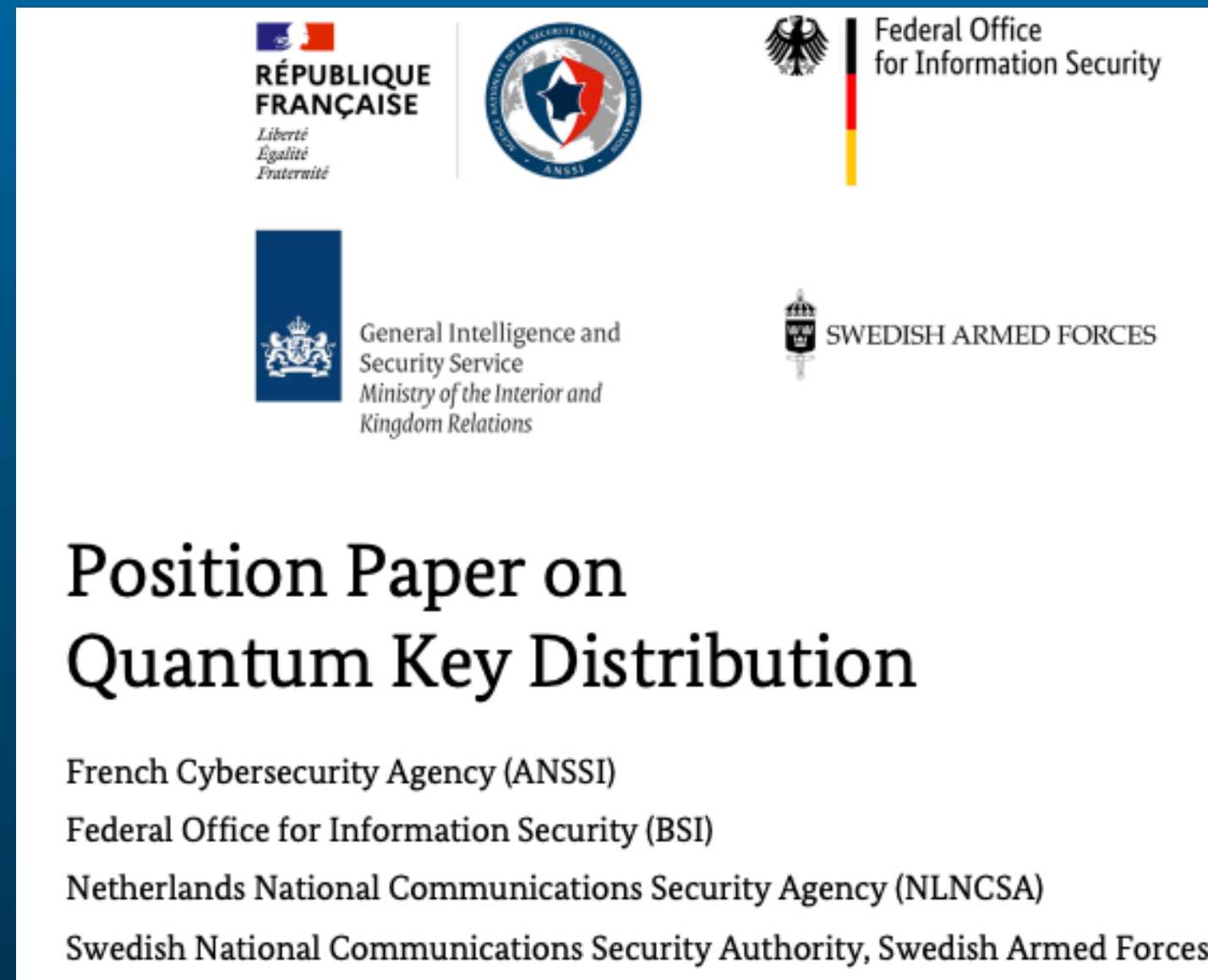


Russia, China Test 'Un-Hackable' Quantum Communications 4,000 KM Away, Ask India To Join Project

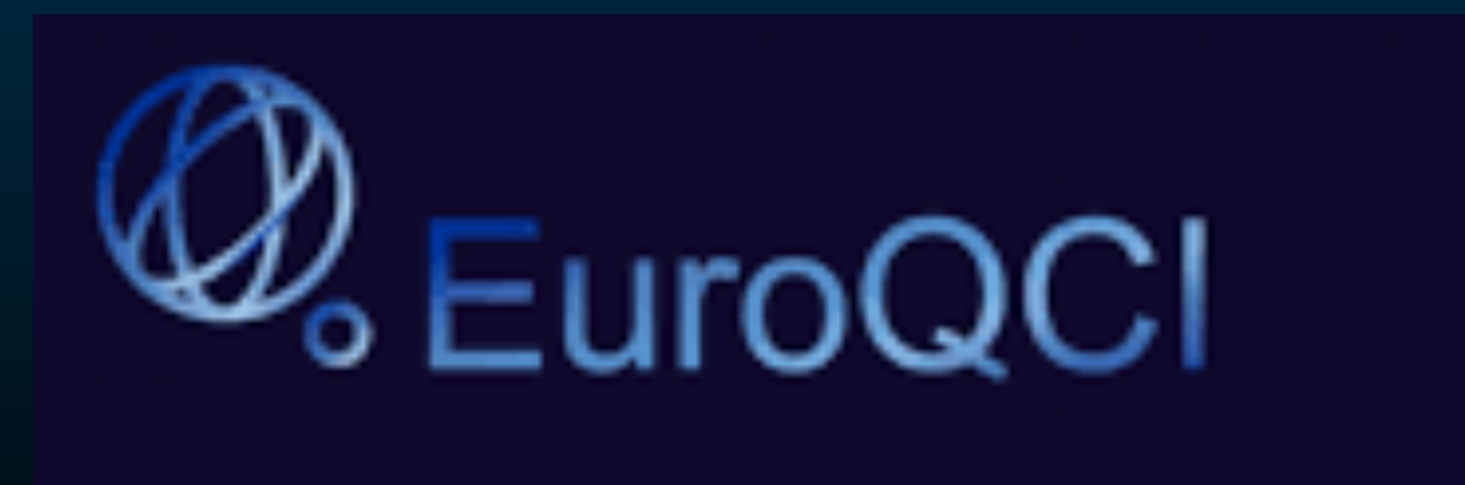
By Parth Satam - January 12, 2024



8/ QKD in the west

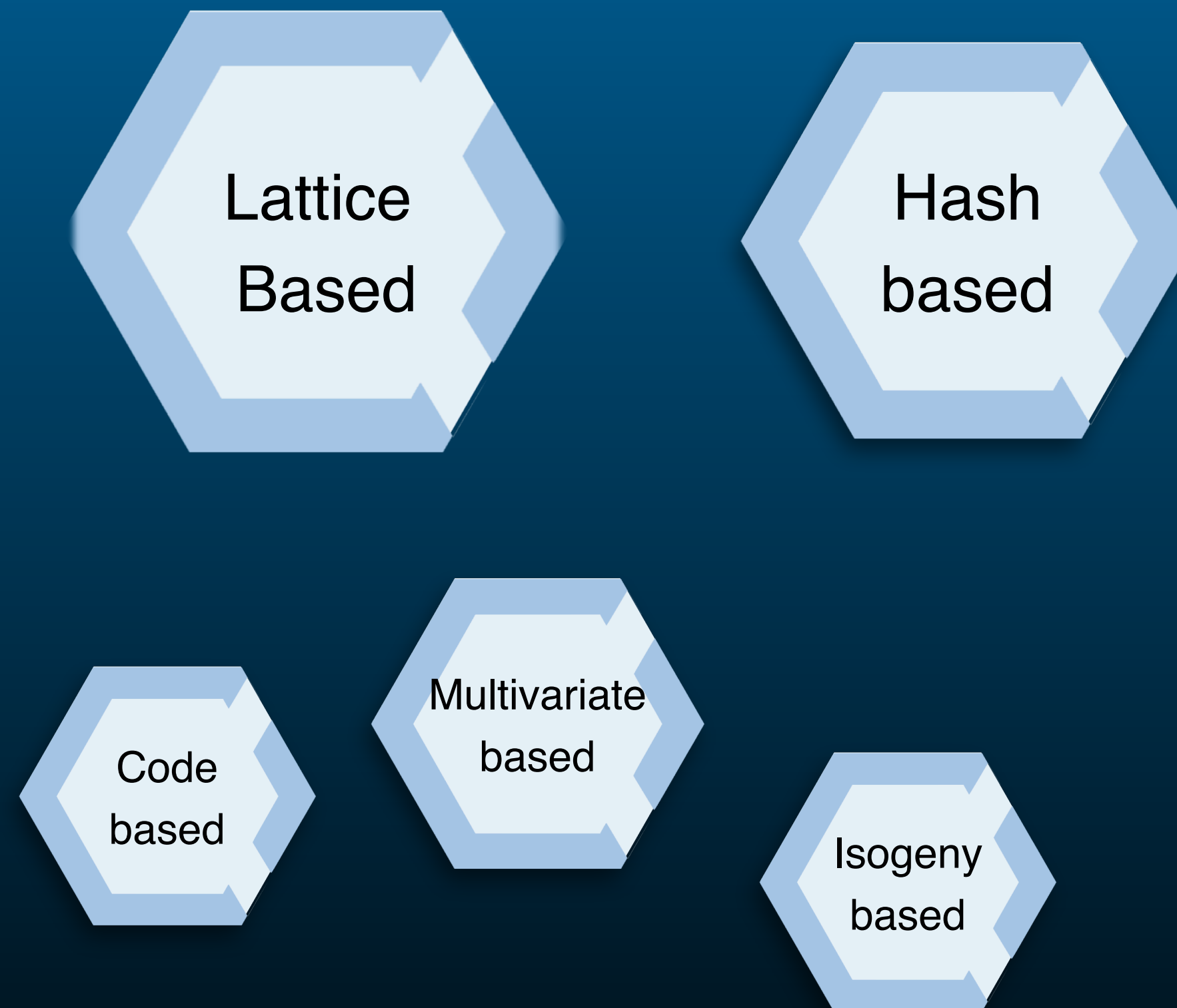


“QKD is an interesting technology and research on this topic should be continued Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. [...] The clear priorities should therefore be the migration to post-quantum cryptography and/or the adoption of symmetric keying”.



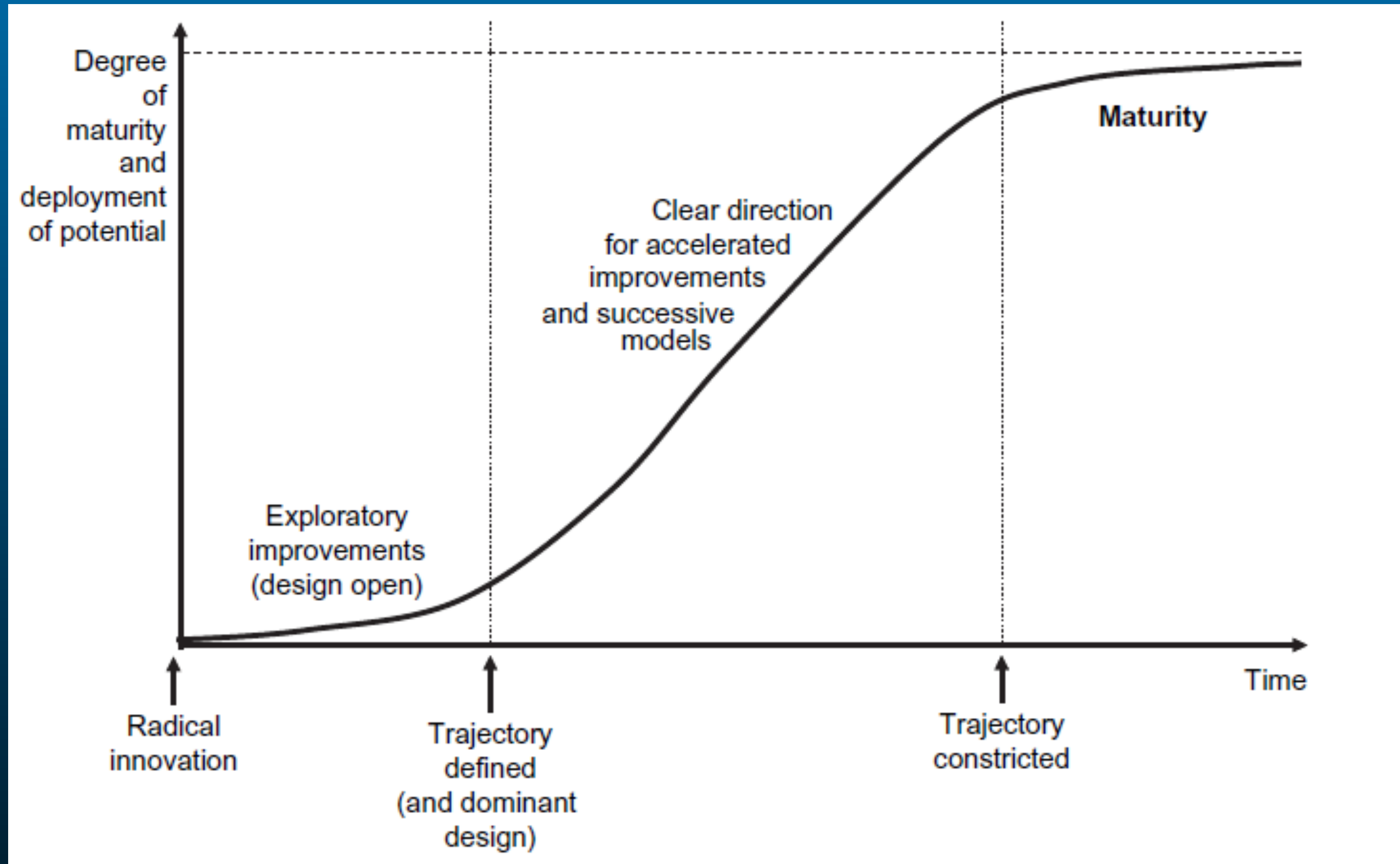
9/ Post-quantum cryptography

New computational problems assumed resistant to quantum



Reco 0. Prioritize PQC/Intensify research on QKD

10/ Technological trajectories



Innovation in cybersecurity

Major role by

- Technical standards
- National Security Organisation (NSO)

- Perez, C. (2010). Technological revolutions and techno-economic paradigms. *Cambridge journal of economics*, 34(1), 185-202.
- Knell, M., & Vannuccini, S. (2022). Tools and Concepts for Understanding Disruptive Technological Change after Schumpeter. In *The Routledge Handbook of Smart Technologies* (pp. 77-101). Routledge.

11/ Post-quantum standardization



“Quantum risk is now simply too high and can no longer be ignored”, US NIST, 2016.

FIRST POST-QUANTUM STANDARDS (ML-KEM , ML-DSA)

2016 — 2018 NIST ROUND 1

2019 — 2020 NIST ROUND 2

2020 — 2022 NIST ROUND 3

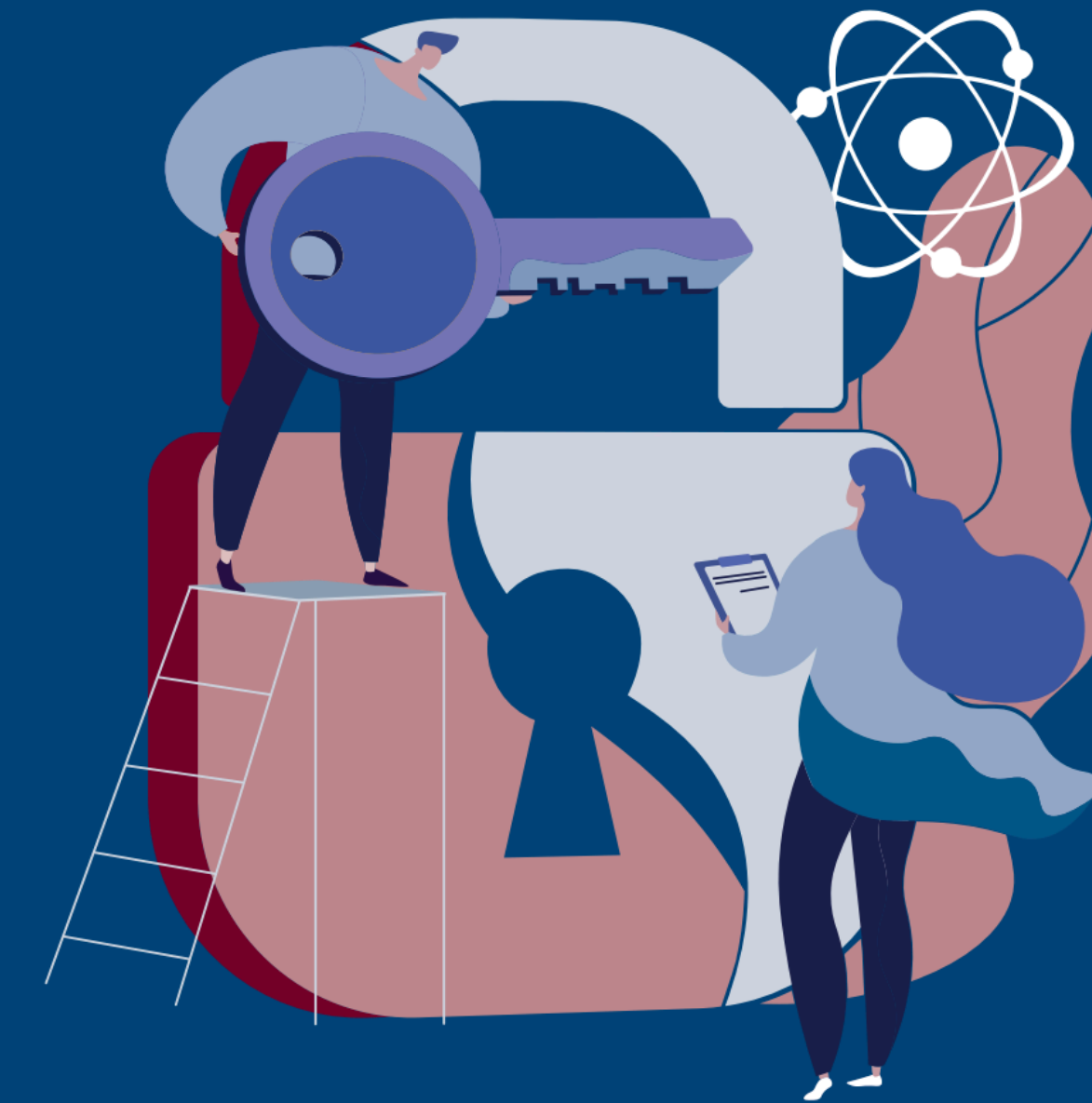
AUGUST 2024 FIRST SET OF OFFICIAL STANDARDS

ANSSI encourages
towards quantum-

ANSSI encourages

ANSSI recommends
soon as possible for
information (after 2

Federal Office
for Information Security



Quantum-safe cryptography –
fundamentals, current developments and
recommendations

on strategy



ptography as
ction of

12/ Few days without PQC

Quantum Algorithms for Lattice Problems

Yilei Chen*

April 18, 2024


Abstract

We show a polynomial time quantum algorithm for solving the learning with errors problem (LWE) with certain polynomial modulus-noise ratios. Combining with the reductions from lattice problems to LWE shown by Regev [J.ACM 2009], we obtain polynomial time quantum algorithms for solving the decisional shortest vector problem (GapSVP) and the shortest independent vector problem (SIVP) for all n -dimensional lattices within approximation factors of $\tilde{\Omega}(n^{4.5})$. Previously, no polynomial or even subexponential time quantum algorithms were known for solving GapSVP or SIVP for all lattices within any polynomial approximation factors.

Update on April 18: Step 9 of the algorithm contains a bug, which I don't know how to fix. See Section 3.5.9 (Page 37) for details. I sincerely thank Hongxun Wu and (independently) Thomas Vidick for finding the bug today.

Now the claim of showing a polynomial time quantum algorithm for solving LWE with polynomial modulus-noise ratios does not hold. I leave the rest of the paper as it is (added a clarification of an operation in Step 8) as a hope that ideas like Complex Gaussian and windowed QFT may find other applications in quantum computation, or tackle LWE in other ways.

13/ Toward large-scale transition to PQC



EUROPEAN COMMISSION

For the Commission
Thierry BRETON
Member of the Commission

Brussels, 11.4.2024
C(2024) 2393 final

CERTIFIED COPY
For the Secretary-General

Martine DEPREZ
Director
Decision-making & Collegiality
EUROPEAN COMMISSION

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

- (6) This Commission Recommendation encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, to ensure a coordinated and synchronized transition among the different Member States and their public sectors. The strategy should define clear goals, milestones, and timelines resulting in the definition of a joint Post-Quantum Cryptography Implementation Roadmap. This should lead to the deployment across the Union of Post-Quantum Cryptography technologies into existing public administration systems and critical infrastructures via hybrid schemes that may combine Post-Quantum Cryptography with existing cryptographic approaches or with Quantum Key Distribution.

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035
RSA [FIPS186]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035

(1) Cryptography is essential for the national security of the United States and the functioning of the economy of the United States.

(2) The most widespread encryption protocols today rely on computational limits of classical computers to provide cybersecurity.

(3) Quantum factorization

(4) The wait until st

SECTION This A SEC. 2. FI (a) Fir

To encour Be it e

Sec. 3. Mitigating the Risks to Encryption. (a) Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a CRQC. To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by **2035**. Currently, the Director of the National Institute of Standards and Technology (NIST) and the Director of the National Security Agency (NSA), in their capacity as the National Manager for National Security Systems (National Manager), are each developing technical standards for quantum-resistant cryptography for their respective jurisdictions. The first sets of these standards are expected to be released publicly by 2024.

14/ A market under structuration

THALES

EVIDEN
Press Release
The first 'post-quantum ready' solutions for Digital Identity

DOCAPOSTE



Public/
private
investments



SANDBOXAQ

ISARA

CRYPTONEXT SECURITY

PQ SHIELD

Post-Quantum

Historical
crypto
providers

Early
adopters

Pure players

15/ Methodology

- **Analysis**

- Define the goals

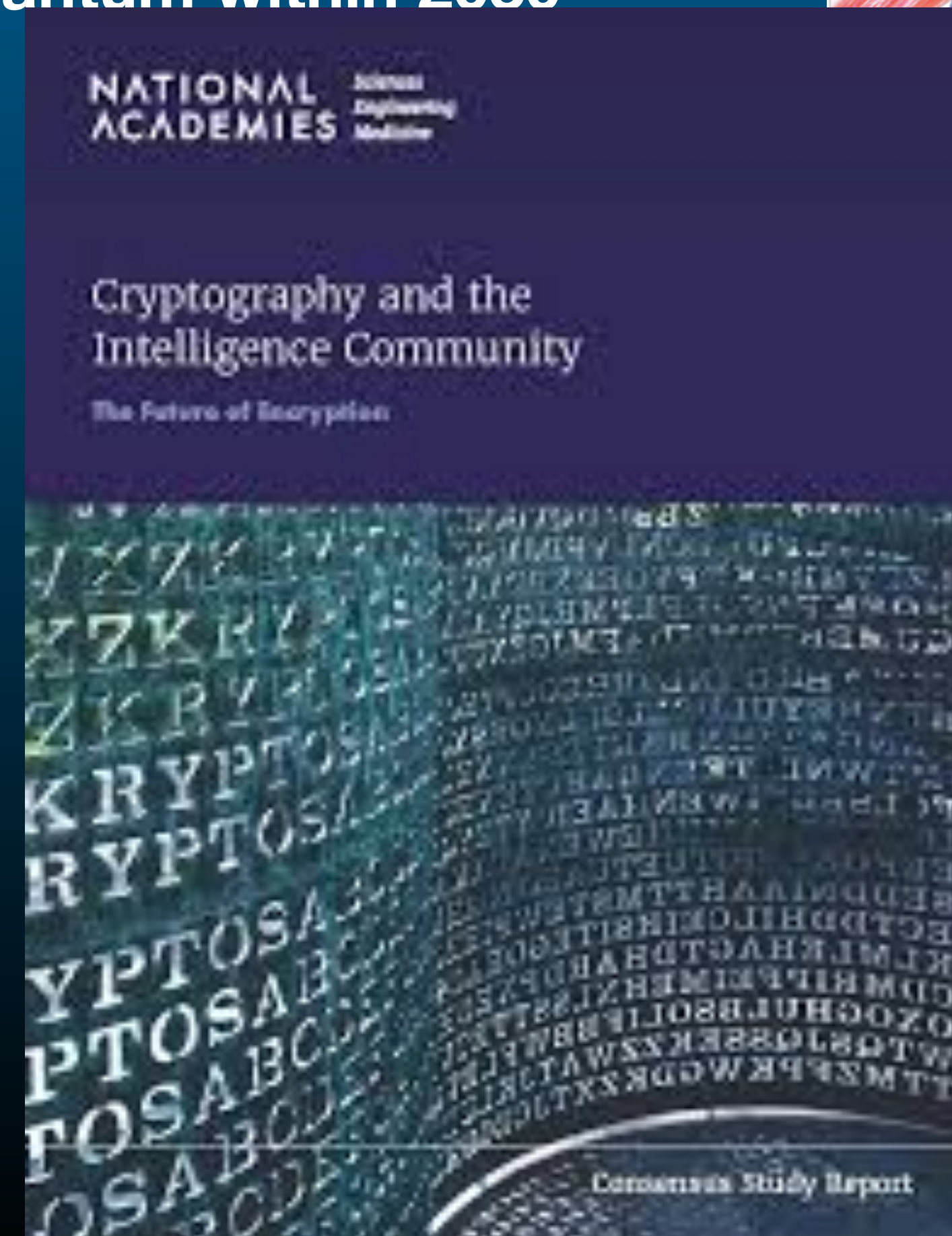
- Political : Industrial strategy for post-quantum cryptography
 - Strategical : **Critical infra. Immune against quantum within 2030**
 - State of the art

- **Prospective analysis**

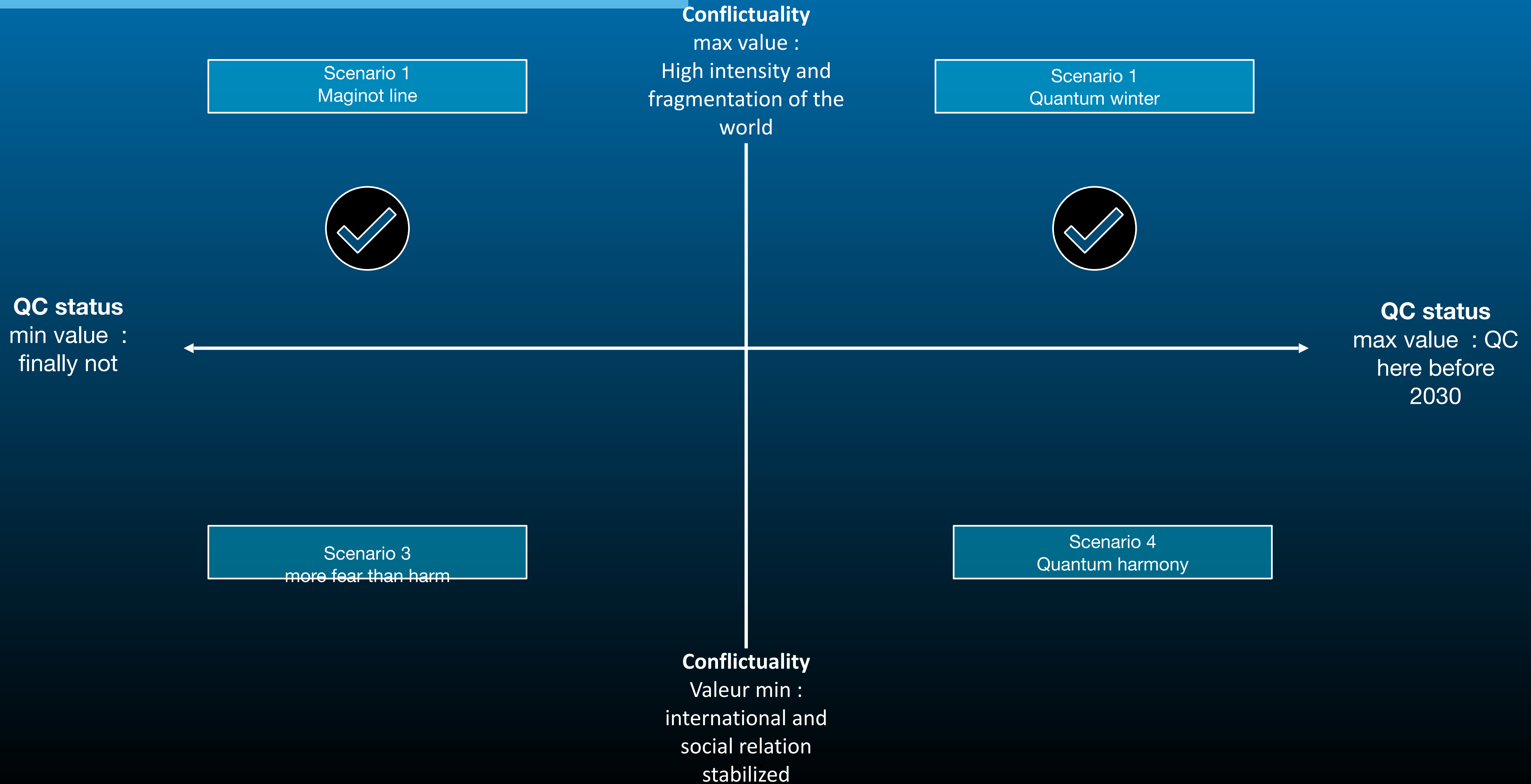
- Main trends in the next 5/7 years
 - Define key variables (2) and define scenarios (4)
 - Consider the most dangerous scenario

- **Define the strategy**

- Interviews
 - Recommendations



16/ Scenarios



17/ Overview of proposals — Sovereign component

Strategic autonomy

Reco 1. Develop training offers in post-quantum

Reco 2. Technical state trades for pq experts

Reco 3. Sovereign capacities

18/ Overview of proposals — Industrial component

Accelerate transition

Reco 4. Prioritize the targets

Reco 5. National plan for post-quantum transition

Reco 6. Public-private partnership for PQC

19/ Overview of proposals — Legal component

Prepare legals

Reco 7. Secure contracts

Reco 8. Impact studies for legal departments

Reco 9. Specific legal monitoring

20/ Overview of proposals — Economic component

Stimulate

Reco 10. pq clause in public procurement

Reco 11. Support for the adoption of pq solutions

Reco 12. Forbid non-pq solutions by 2030

21/ Conclusion

ANSSI post-quantum lead

Clear path to transition

Develop an ecosystem (not a single actor)

Regulation fatigue



<https://nuage.lip6.fr/apps/polls/s/G1KyxYKb>