Commission’s view on the journey towards quantum-safe cryptography

Fabiana Da Pieve

Program Manager
Directorate General for Communications Networks, Content, and Technology (DG CONNECT)
Unit Emerging and Disruptive Technologies

Cryptography: cornerstone of cybersecurity

Cryptography ensures the confidentiality, integrity, and authenticity of digital assets

It involves implementing cryptographic primitives (algorithms) and protocols which include such primitives for (among others):

- securing key exchange for encryption, and encrypting communication and data at rest
- creating fingerprints of messages and data to preserve the integrity of communication and other digital assets
- creating signatures to ensure proper authentication for entities and individuals, and the proper data/assets origins for messages, devices and software

Cryptography: cornerstone of cybersecurity

Cryptography ensures the confidentiality, integrity, and authenticity of digital assets

It involves implementing cryptographic primitives (algorithms) and protocols which include such primitives for (among others):

- securing key exchange for encryption, and encrypting communication and data at rest
- creating fingerprints of messages and of data to preserve the integrity of communication and other digital assets
- creating signatures to ensure proper authentication for entities and individuals, and the proper data/assets origins for messages, devices and software

Public-key cryptography

- A key pair – one public and one private
- Asymmetric encryption when security is paramount, such as encrypting sensitive data or securing communication within an open system
- Also: non-repudiation

Cryptography: cornerstone of cybersecurity

Cryptography ensures the confidentiality, integrity, and authenticity of digital assets

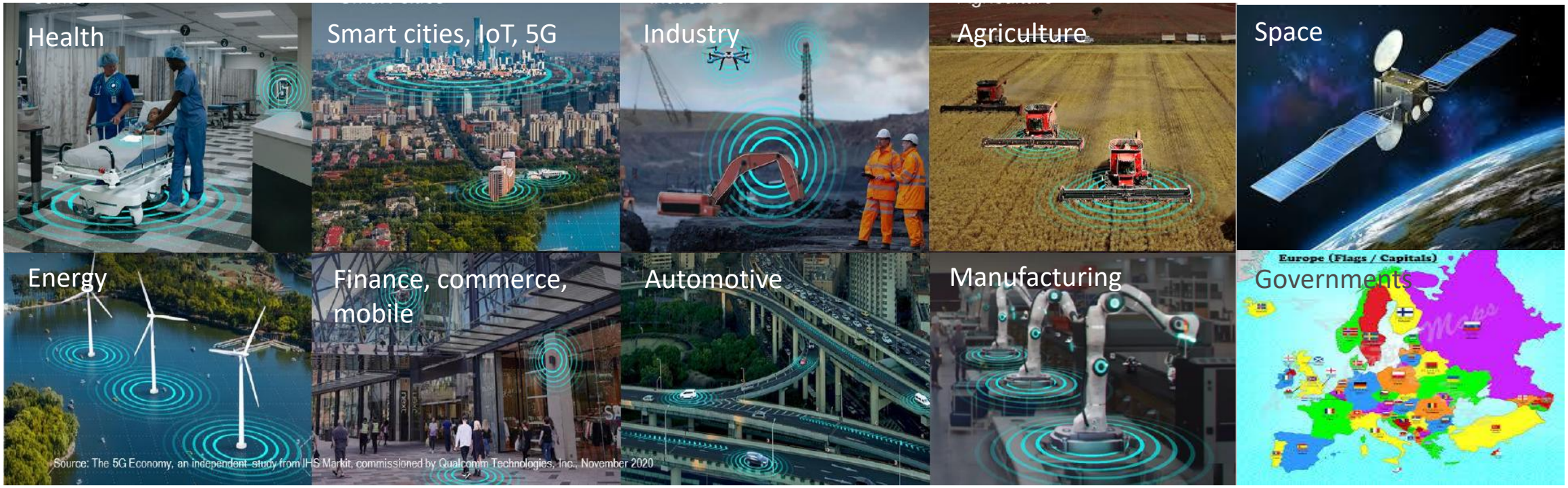
It involves implementing cryptographic primitives (algorithms) and protocols which include such primitives for (among others):

- securing key exchange for encryption, and encrypting communication and data at rest
- creating fingerprints of messages and of data to preserve the integrity of communication and other digital assets
- creating signatures to ensure proper authentication for entities and individuals, and the proper data/assets origins for messages, devices and software

Symmetric Cryptography

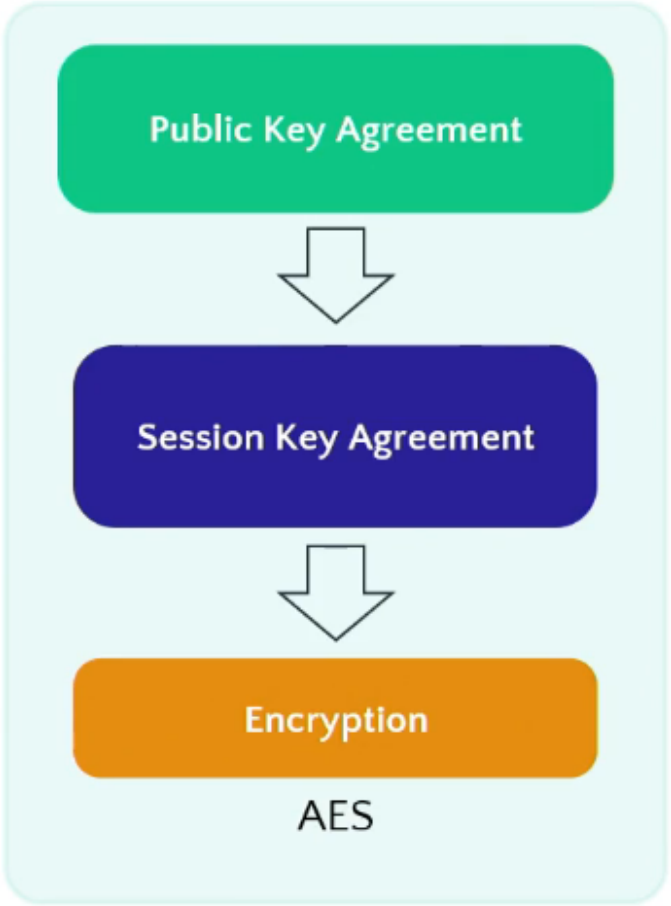
- A single secret key for both encryption and decryption
- Used to secure large amounts of data, and enabling fast and efficient encryption in various applications
- Simple and efficient – chosen when efficiency is critical
- Relies on secure key exchange and meticulous key management

We rely on public-key cryptographic in all areas of our society …



European Commission

Most commonly used applications use a **combination** of public-key and symmetric cryptography to secure communications

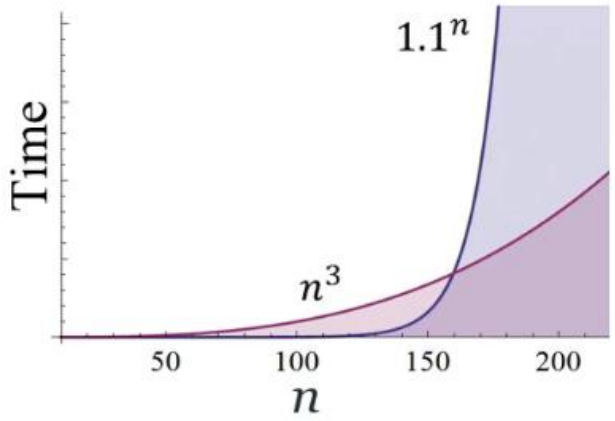


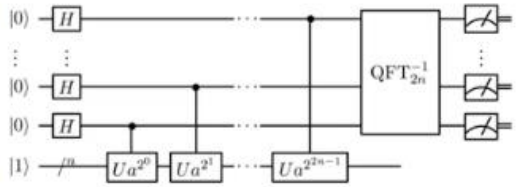
This combination allows us to use symmetric key encryption for the core encryption and then protect the symmetric key with a public key. We can then use our private key to discover the required symmetric key.

Shor's and Grover's algorithms

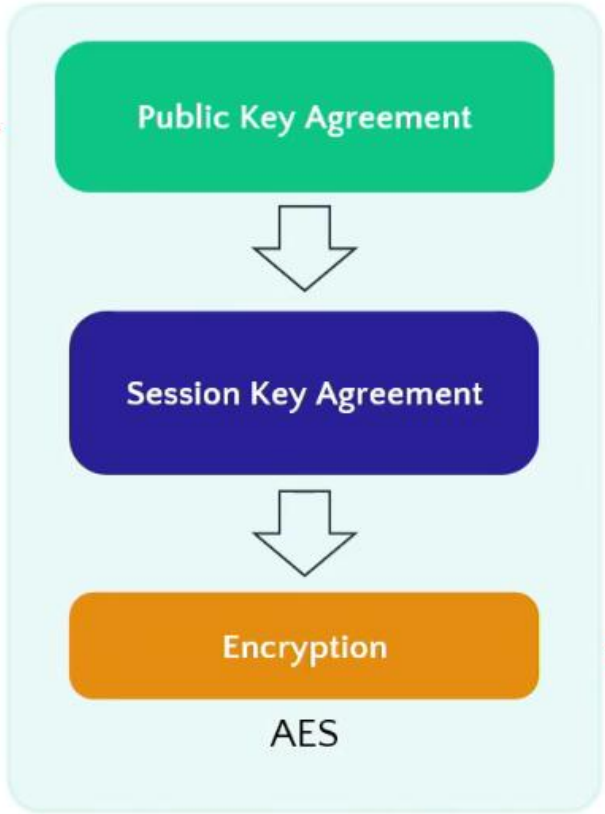
Exponential speed-up in factoring!

breaks



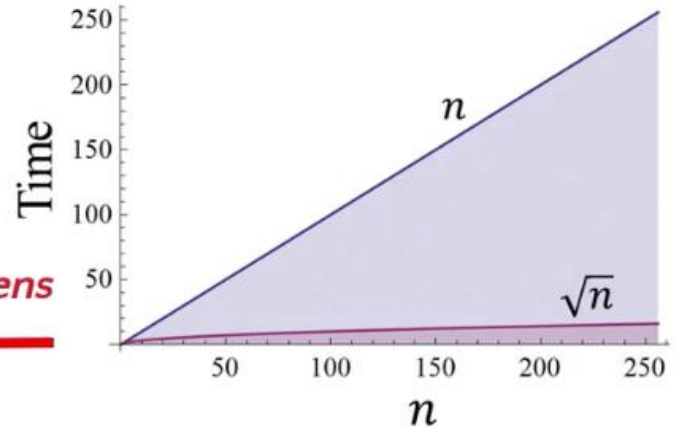


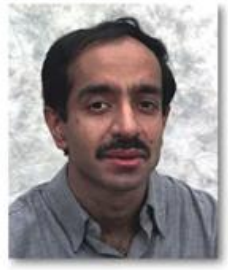
P. W. Shor, **Algorithms for quantum computation: Discrete logarithms and factoring,** *Proc. 35nd Annual Symposium on Foundations of Computer Science* (Shafi Goldwasser, ed.), IEEE Computer Society Press (1994), 124-134.

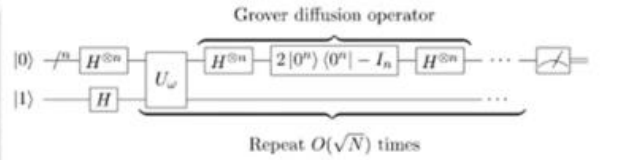


Quadratic speed-up in searching!

weakens







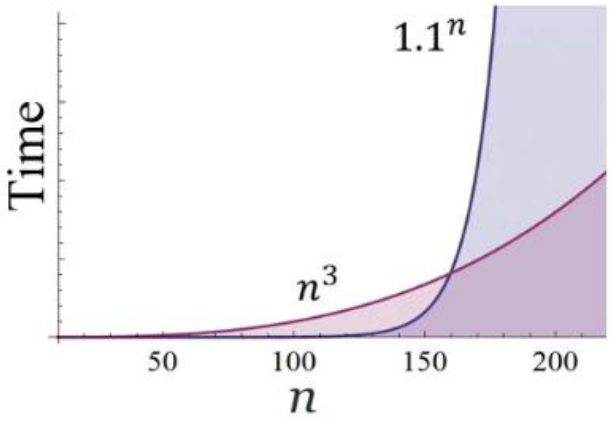
Quantum Mechanics Helps in Searching for a Needle in a Haystack

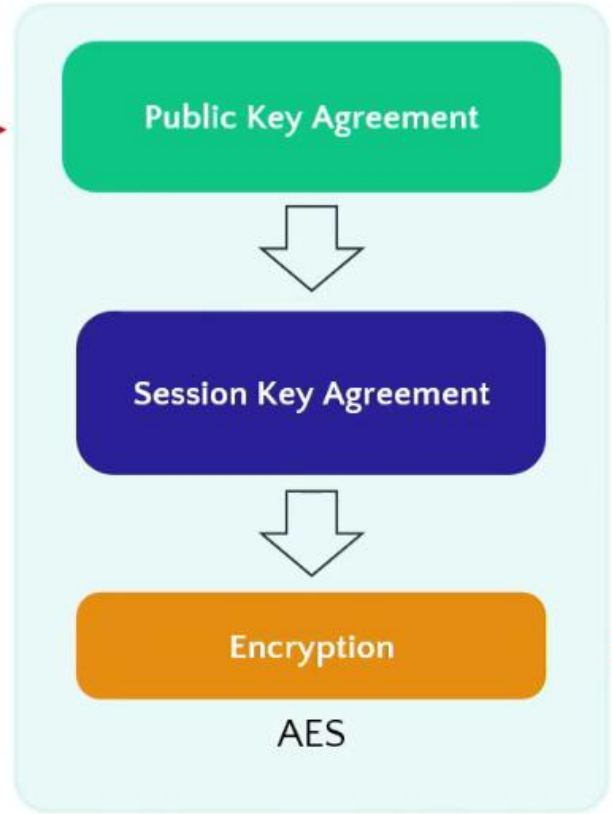
Lov K. Grover
Phys. Rev. Lett. 79, 325 – Published 14 July 1997

Shor's and Grover's algorithms

Exponential speed-up in factoring!

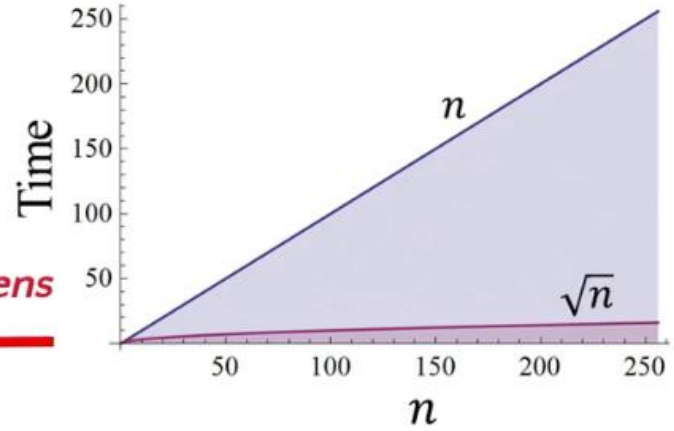
breaks

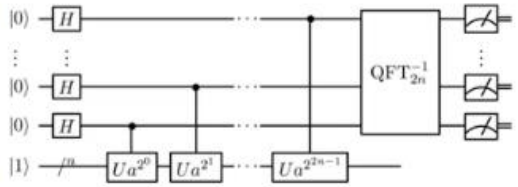




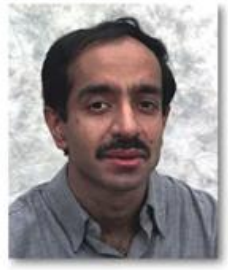
weakens

Quadratic speed-up in searching!



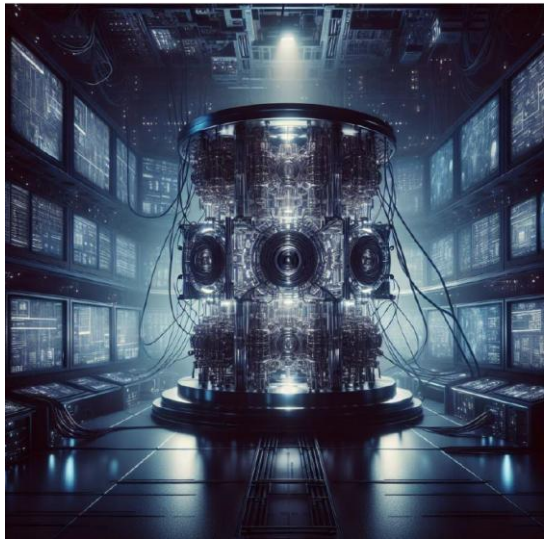


P. W. Shor, **Algorithms for quantum computation: Discrete logarithms and factoring,** *Proc. 35nd Annual Symposium on Foundations of Computer Science* (Shafi Goldwasser, ed.), IEEE Computer Society Press (1994), 124-134.



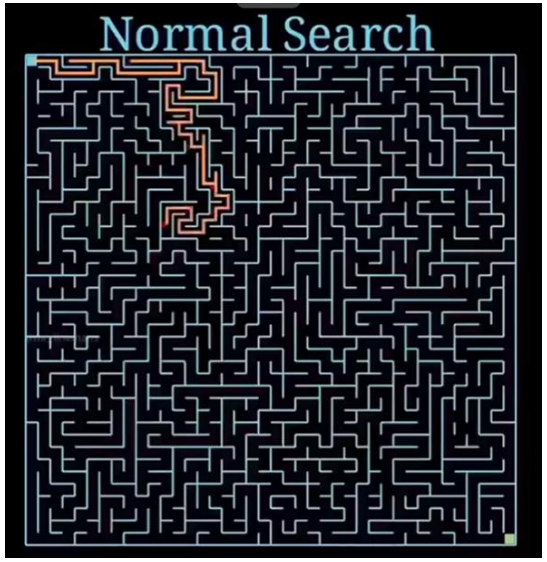
Luckily it parallelizes badly

Quantum Computers

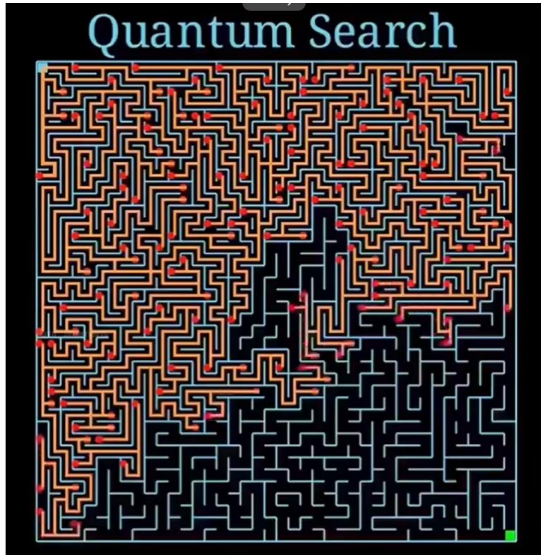


Quantum bits (qubits)
Unlike classical bits (0 or 1), quantum bits can exist in multiple states simultaneously through superposition

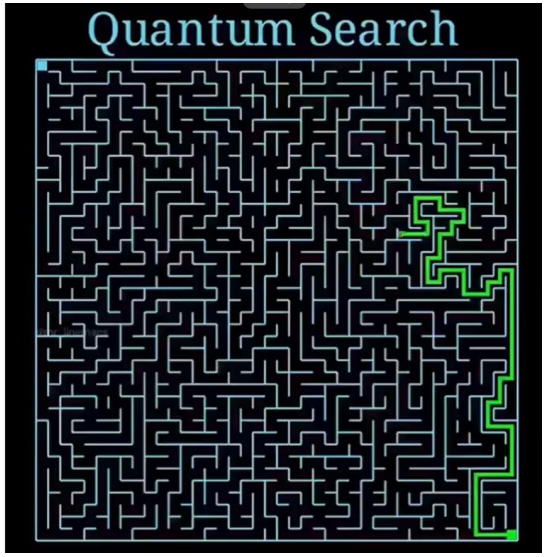
Entanglement
links qubits together, allowing them to share information instantaneously, regardless of distance.



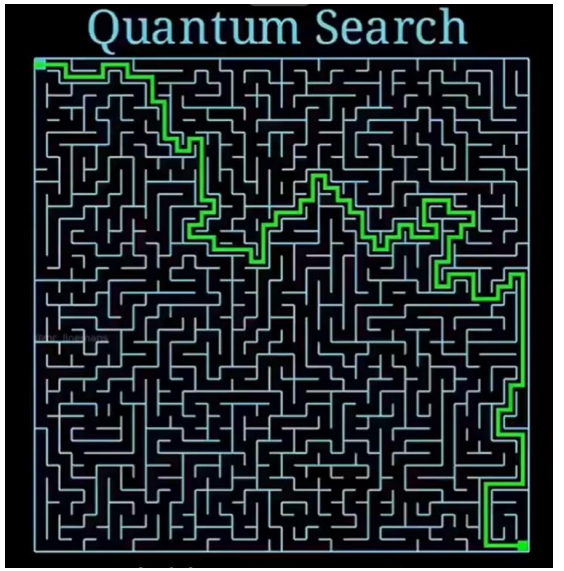
One path at a time



One agent in multiple paths at the same time - quantum superposition

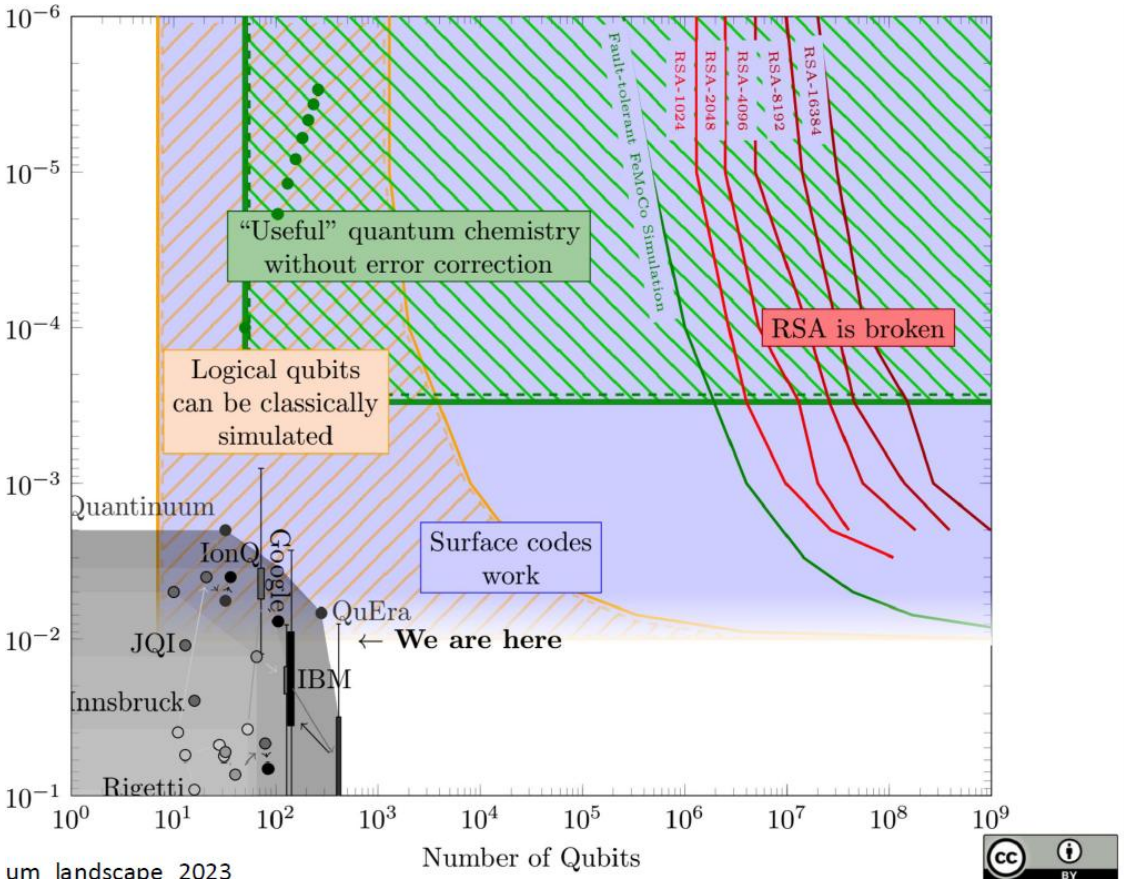


When we find the solution, all the other agents disappear



And the real existence of the agent is at the destination

The quantum threat to cryptography



13 Apr 2021

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

Craig Gidney[1] and Martin Ekerå[2]

[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

We significantly reduce the cost of factoring integers and computing discrete logarithms in finite fields on a quantum computer by combining techniques from Shor 1994, Griffiths-Niu 1996, Zalka 2006, Fowler 2012, Ekerå-Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney-Fowler 2019, Gidney 2019. We estimate the approximate cost of our construction using plausible physical assumptions for large-scale superconducting qubit platforms: a planar grid of qubits with nearest-neighbor connectivity, a characteristic physical gate error rate of 10^{-3}, a surface code cycle time of 1 microsecond, and a reaction time of 10 microseconds. We account for factors that are normally ignored such as noise, the need to make repeated attempts, and the spacetime layout of the

https://sam-jaques.appspot.com/quantum_landscape_2023

European Commission

The quantum threat to cryptography accelerates
hardware progress + quantum algorithms optimization

Google Quantum AI – Dec 2024

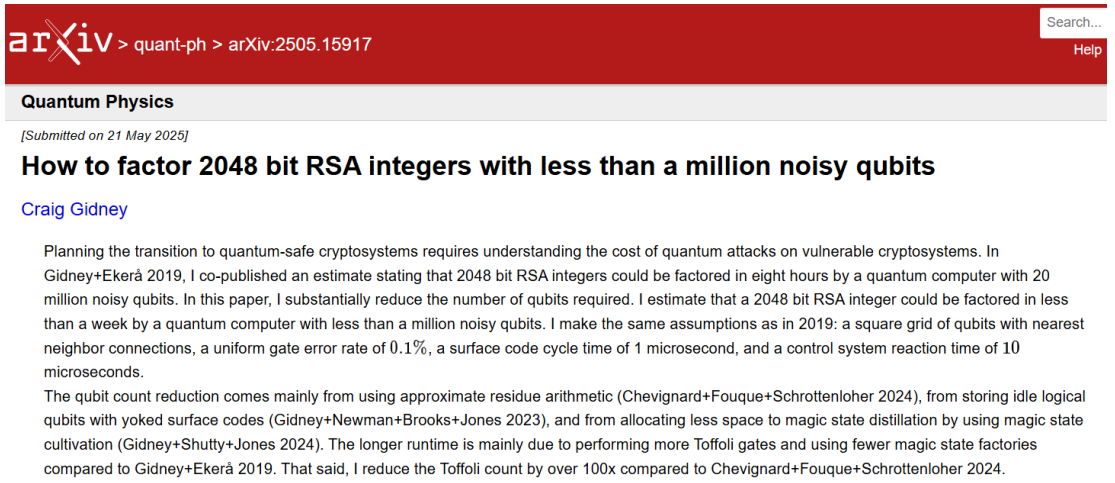
“Willow can reduce errors exponentially as we scale up using more qubits. This cracks a key challenge in quantum error correction that the field has pursued for 30 years.”

currently the only chip which is both:
"break even" = error correction removes errors instead of adding
"below threshold" = adding qubits results in lower error rates

IBM roadmap 2025:

Starling (2029) will be capable of running 100 million-gate quantum circuits on 200 qubits

will be able to run 20,000 times more operations than today’s quantum computers, with memory of more than a quindecillion (10^48) of the world’s most powerful supercomputers of today
https://www.ibm.com/quantum/blog/large-scale-ftqc


arXiv > quant-ph > arXiv:2505.15917

Search... Help

Quantum Physics

[Submitted on 21 May 2025]

How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.
The qubit count reduction comes mainly from using approximate residue arithmetic (Chevignard+Fouque+Schrottenloher 2024), from storing idle logical qubits with yoked surface codes (Gidney+Newman+Brooks+Jones 2023), and from allocating less space to magic state distillation by using magic state cultivation (Gidney+Shutty+Jones 2024). The longer runtime is mainly due to performing more Toffoli gates and using fewer magic state factories compared to Gidney+Ekerå 2019. That said, I reduce the Toffoli count by over 100x compared to Chevignard+Fouque+Schrottenloher 2024.

The quantum threat to cryptography accelerates
hardware progress + quantum algorithms optimization

Google Quantum AI – Dec 2024

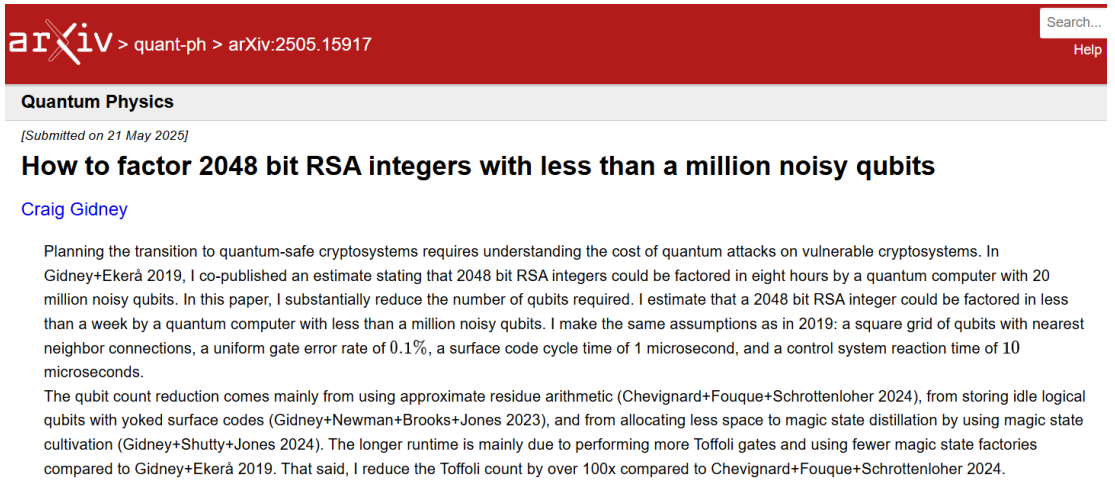
"Willow can reduce errors exponentially as we scale up using more qubits. This cracks a key challenge in quantum error correction that the field has pursued for 30 years."

currently the only chip which is both:
"break even" = error correction removes errors instead of adding
"below threshold" = adding qubits results in lower error rates

IBM roadmap 2025:

Starling (2029) will be capable of running 100 million-gate quantum circuits on 200 qubits

will be able to run 20,000 times more operations than today's quantum computers, with memory of more than a quindecillion (10^48) of the world's most powerful supercomputers of today
https://www.ibm.com/quantum/blog/large-scale-ftqc


arXiv > quant-ph > arXiv:2505.15917

Search... Help

Quantum Physics

[Submitted on 21 May 2025]

How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.
The qubit count reduction comes mainly from using approximate residue arithmetic (Chevignard+Fouque+Schrottenloher 2024), from storing idle logical qubits with yoked surface codes (Gidney+Newman+Brooks+Jones 2023), and from allocating less space to magic state distillation by using magic state cultivation (Gidney+Shutty+Jones 2024). The longer runtime is mainly due to performing more Toffoli gates and using fewer magic state factories compared to Gidney+Ekerå 2019. That said, I reduce the Toffoli count by over 100x compared to Chevignard+Fouque+Schrottenloher 2024.

All modern public-key cryptography has to be replaced [Shor'94]

- RSA
- Diffie-Hellman (including elliptic curves)

Symmetric key sizes: x2 [Grover'96]
Hash function outputs x2 [Grover'96]
But huge factors – impractical [Jacques'24]
https://www.youtube.com/watch?v=eB4po9Br1YY

Post-Quantum Cryptography and Quantum Cryptography

Post-quantum Cryptography (PQC)

relies on computational assumptions; based on mathematical problems difficult to solve even for quantum computers

correspondent of Public Key Cryptography

- Mostly software, but implies a fundamental and challenging shift in algorithms and protocols
- Implementations bring computational overhead and also to the need of new countermeasures to possible attacks
- **Most promising and most urgent technology for our increasingly connected world**

Post-Quantum Cryptography and Quantum Cryptography

Post-quantum Cryptography (PQC)

relies on computational assumptions; based on mathematical problems difficult to solve even for quantum computers

correspondent of Public Key Cryptography

- Mostly software, but implies a fundamental and challenging shift in algorithms and protocols
- Implementations bring computational overhead and also to the need of new countermeasures to possible attacks
- **Most promising and most urgent technology for our increasingly connected world**

Quantum Cryptography

uses new primitives based on unhackable laws of physics - Quantum Key Distribution (QKD) secures agreement of shared key against unbounded adversary – deals with the **establishment of a key for symmetric encryption**

- Requires completely new hardware, based on quantum technologies
- May be often subject to Denial of Service attacks
- Standards and certification: still a long path
- **Limitations on distances, trusted nodes, performance, costs, compelling use cases, but progress is steady**

Can be combined in hybrid scenarios

European Commission

The need for PQC

Implicit in several EU policies
and explicit in the PQC Recommendation
- now also linked to Cyber Resilience Act

Today's encrypted communication likely being stored by attackers and will be decrypted years later with quantum computers

Others may be worried more about other aspects – **trust services and authentication**

NIS 2

L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Economic Security Strategy

EUROPEAN COMMISSION

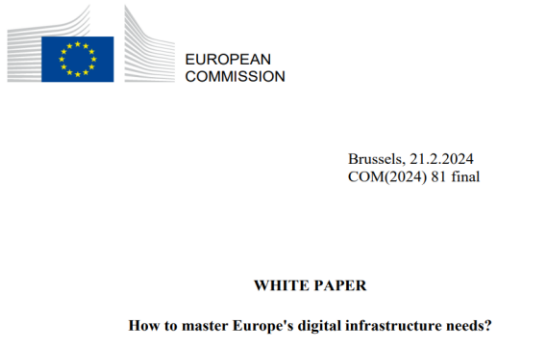
HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Brussels, 20.6.2023
JOIN(2023) 20 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL

ON "EUROPEAN ECONOMIC SECURITY STRATEGY"

DG CNECT White Paper



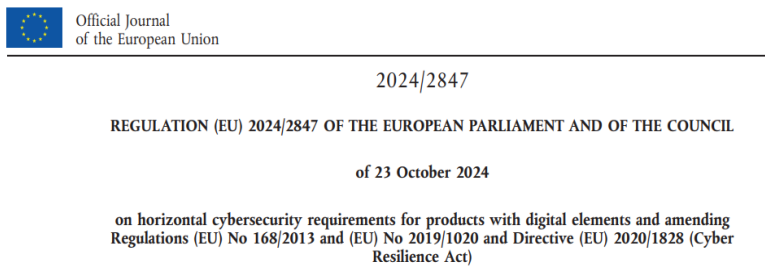
EUROPEAN COMMISSION

Brussels, 21.2.2024
COM(2024) 81 final

WHITE PAPER

How to master Europe's digital infrastructure needs?

Cyber Resilience Act



Official Journal of the European Union

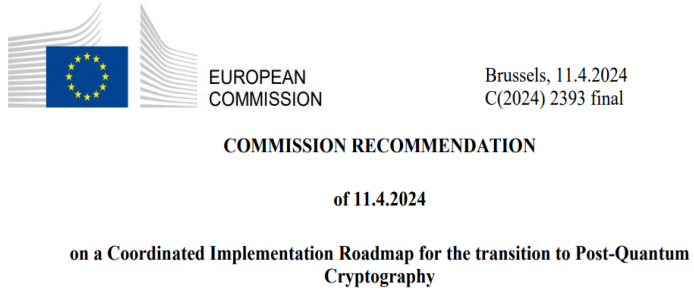
2024/2847

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2024

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

Recommendation on PQC



EUROPEAN COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

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

Funds & Governance - PQC

Ongoing, past, just started EU projects (Horizon Europe, DEP)

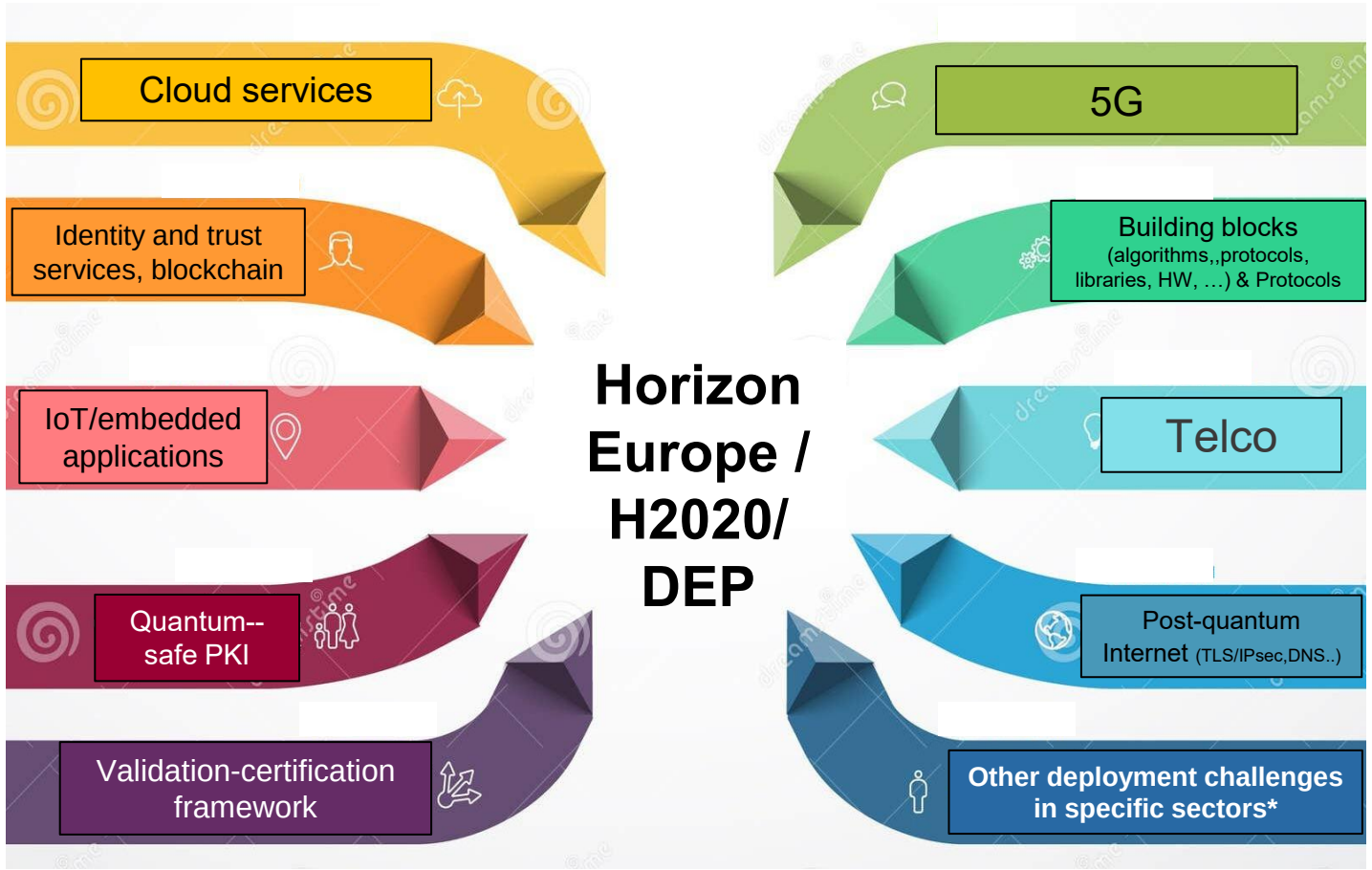
PQCRYPTO

QUBIP, PQC4eMRTD, PQ-REACT, PROMETHEUS, PRIViLEDGE

QUBIP, PQCRYPTO

PQC4eMRTD, PiQASO, HAPKIDO (NL, national)

WORK IN ECCG CHAIRED BY ENISA



Projects for both 6G we have CONFIDENTIAL6G

QUBIP, ERC EPOQUE (integ. in procotols), ERC ARTICULATE (libraries), SAFECrypto, PiQASO (HW), ERC ISOCRYPT (non-lattice based)

QUBIP, PQ-REACT

QUBIP, PQCRYPTO

Automotive (PQCSA)
Financial sector (NGI-TALER, EPOQUE)
Administrations (Q-PREP)
Several sectors (PIQASO)
Work of PQC in space, energy grids …

Current Governance : Commission, ENISA, ECCC
(a bit complex ! Good for certain things, need for more efficiency for others)

European Commission

What are we doing for PQC

Research and Deployment:

- Launch of an EU testing infrastructure
- Initiative to support transition of the Public-Key Infrastructures
- Research priorities (cryptanalysis, countermeasures to implementation attacks, integration into protocols, new signatures, Privacy-Enhancing Technologies…)
- design ad-hoc actions and insert PQC horizontally in Horizon Europe, DEP, IRIS²

EU Roadmap following Commission's Recommendation on PQC:

- Milestones for high-risk/medium-risk use cases
- Starting date is not anymore a moving target !

https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

Image below from PQShield - do NOT re-use

Next steps

More open approaches & feedback loops on several fronts

Invite inputs on drafts
Report on/include comments and publish the final document

Regulatory

Revise the 2019 Cybersecurity Act: mandate of ENISA, the European Cybersecurity Certification Framework, supply chain challenges

Feedback by 20 June: Commission opens consultation on revising EU Cybersecurity Act | Shaping Europe's digital future

Critical Infrastructures & emergency communications

Coordinate the work towards the definition of cross-border tests in the EU and the timeline for such tests

Digital Identities

New digital signatures and advanced cryptographic schemes for enhanced privacy

Authentication schemes meeting real-world requirements for constrained devices (contactless security controllers for ePassports and eIDs)

Standardization

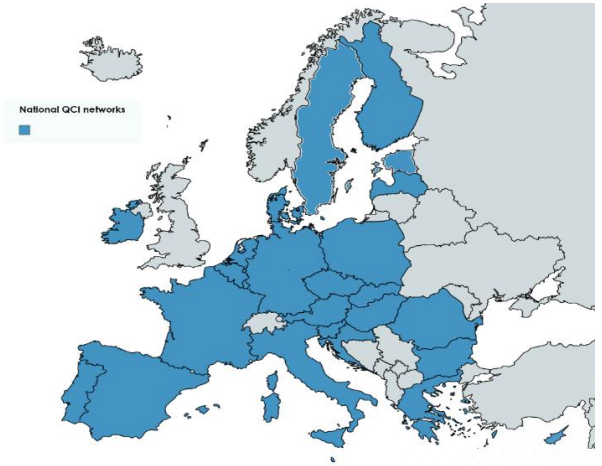
"Standardization provides a powerful platform to consolidate fragmented global research efforts in the development of quantum-safe algorithms and associated business practices that will protect the Internet (and not only) and everyone who relies on it."

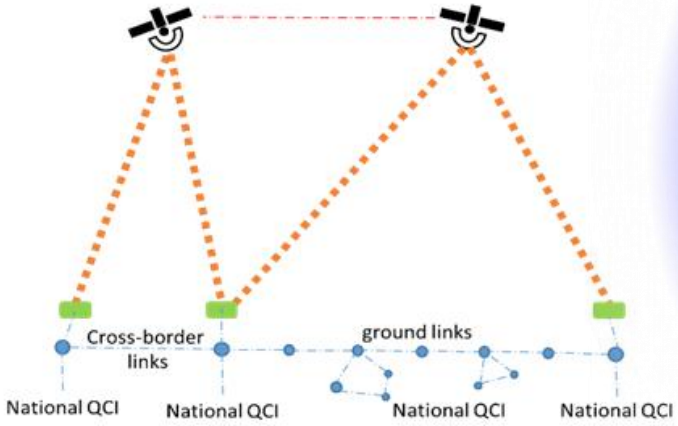
Jan Ellsberger,
ETSI Director General

EuroQCI - Funds & Governance

- 6 Industry projects maturing EU QCI technologies (DEP1, 44M€)
  - QKD systems ready for integration into telecommunication networks
  - QKD modules (QRNGs, optical components), KMS, encryptors, protocols
- 26 MS deploying national QCI networks (DEP2, 108M€)
  - Started January 2023, 30 months, technologies, test architecture, develop use cases, prepare for full deployment
- Coordination and support action (PETRUS) (DEP3, 2M€)
- Testing & evaluation infrastructure (Nostradamus) (DEP4, 16M€)
- Connecting Europe Facility - Terrestrial & Space (CEF, 90M€)
- Other calls will come with IRIS²

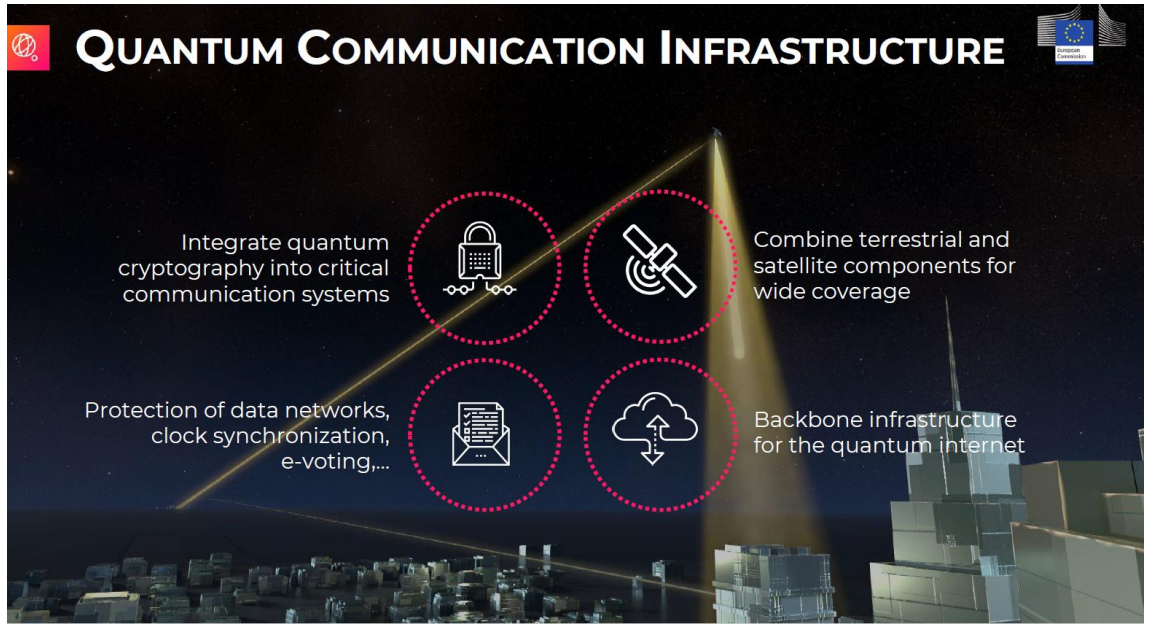
Governance: Commission, ESA





EuroQCI & other activities in the Quantum Flagship

from exchanging keys to “beyond QKD” to the Quantum Internet



Two strategies running simultaneously

Make the first-generation the first-generation quantum networks with the sole QKD functionality applicable

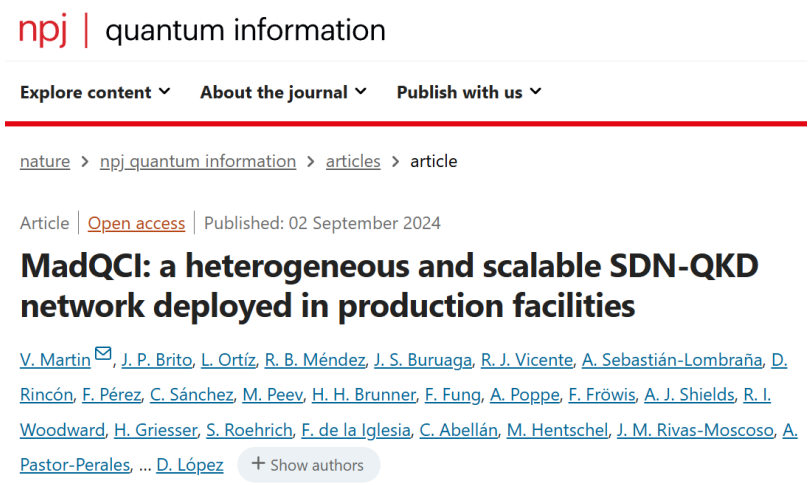
Accelerate the development of next generation(s) Quantum Network Technology

EuroQCI

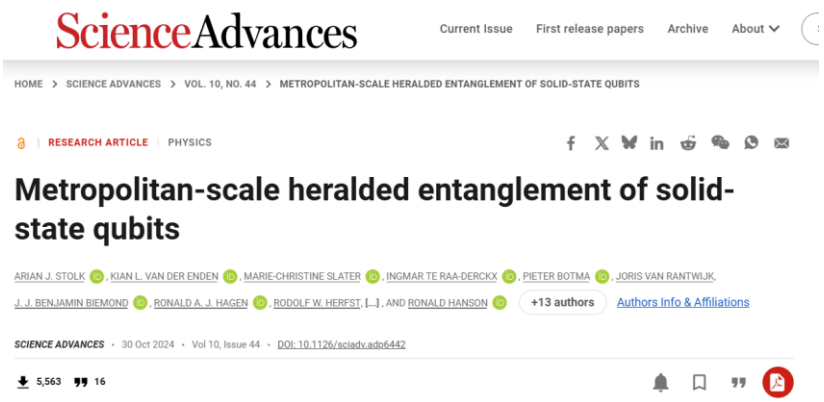
QUANTUM INTERNET ALLIANCE

QSN PARTNERSHIP

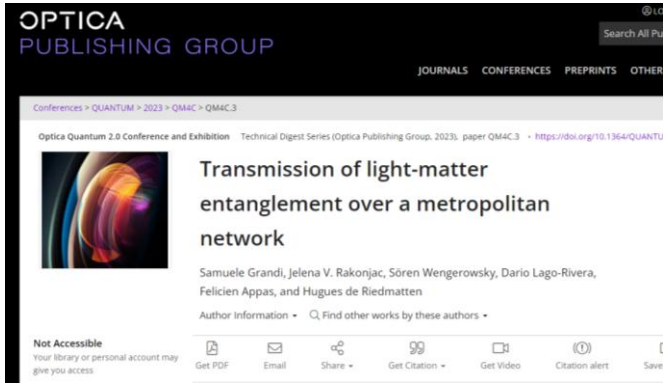
A number of demonstrator cases for QKD & several exciting results



Metropolitan Network nodes

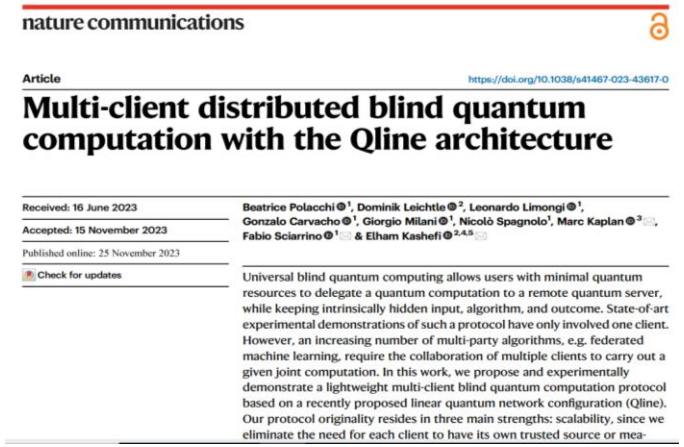


Quantum memories



+ quantum memory from Welinq – product press release March 2025

Demonstrating potential application in different domains



QKD has to evolve from excellence in research to relevance in applications

Limitations:

Distance, no end-to-end security, performance, cost

Current deployments of QKD are mostly a **patchwork of specific link-by-link set up,** trusted nodes, hybrid PQC-QKD schemes

Quantum Key Distribution with Efficient Post-Quantum Cryptography-Secured Trusted Node on a Quantum Network

Yoann Piétri,[1] Pierre-Enguerrand Verdier,[2] Baptiste Lacour,[2] Maxime Gautier,[2] Heming Huang,[3] Thomas Camus,[4] Jean-Sébastien Pegon,[4] Martin Zuber,[5] Jean-Charles Faugère,[5] Matteo Schiavon,[1] Amine Rhouni,[1] Yves Jaouën,[3] Nicolas Fabre,[3] Romain Alléaume,[3] Thomas Rivera,[2] and Eleni Diamanti[1]

[1] *Sorbonne Université, CNRS, LIP6, F-75005 Paris, France*
[2] *Orange Innovation, F-92326 Châtillon, France*
[3] *Telecom Paris, Institut Polytechnique de Paris, F-91120 Palaiseau, France*
[4] *ID Quantique SA, CH-1227 Genève, Switzerland*
[5] *CryptoNext Security, F-75005 Paris, France*
(Dated: April 3, 2025)

A Critical Analysis of Deployed Use Cases for Quantum Key Distribution and Comparison with Post-Quantum Cryptography

Nick Aquina[1,3†], Bruno Cimoli[1,3†], Soumya Das[2,3†], Kathrin Hövelmanns[2,3†], Fiona Johanna Weber[2,3†], Chigo Okonkwo[1,3], Simon Rommel[1,3], Boris Škorić[2,3], Idelfonso Tafur Monroy[1,3], Sebastian Verschoor[4]

arXiv > cs > arXiv:2411.04030

Computer Science > Cryptography and Security

[Submitted on 6 Nov 2024]

Quantum-Safe Hybrid Key Exchanges with KEM-Based Authentication

Christopher Battarbee, Christoph Striecks, Ludovic Perret, Sebastian Ramacher, Kevin Verhaeghe

QKD has to evolve from excellence in research to relevance in applications

Limitations:

Distance, no end-to-end security, performance, cost

Current deployments of QKD are mostly a **patchwork of specific link-by-link set up,** trusted nodes, hybrid PQC-QKD schemes

Progress in R&D efforts is steady: metropolitan QKD networks linking multiple city via trusted nodes, test quantum repeaters

To reach truly global quantum-secure communications, we need:

- Breakthroughs in quantum memories, and much research in novel quantum protocols
- Collaboration between quantum physicists and cryptographers

Quantum Key Distribution with Efficient Post-Quantum Cryptography-Secured Trusted Node on a Quantum Network

Yoann Piétri,[1] Pierre-Enguerrand Verdier,[2] Baptiste Lacour,[2] Maxime Gautier,[2] Heming Huang,[3] Thomas Camus,[4] Jean-Sébastien Pegon,[4] Martin Zuber,[5] Jean-Charles Faugère,[5] Matteo Schiavon,[1] Amine Rhouni,[1] Yves Jaouën,[3] Nicolas Fabre,[3] Romain Alléaume,[3] Thomas Rivera,[2] and Eleni Diamanti[1]

[1] *Sorbonne Université, CNRS, LIP6, F-75005 Paris, France*
[2] *Orange Innovation, F-92326 Châtillon, France*
[3] *Telecom Paris, Institut Polytechnique de Paris, F-91120 Palaiseau, France*
[4] *ID Quantique SA, CH-1227 Genève, Switzerland*
[5] *CryptoNext Security, F-75005 Paris, France*
(Dated: April 3, 2025)

A Critical Analysis of Deployed Use Cases for Quantum Key Distribution and Comparison with Post-Quantum Cryptography

Nick Aquina[1,3†], Bruno Cimoli[1,3†], Soumya Das[2,3†], Kathrin Hövelmanns[2,3†], Fiona Johanna Weber[2,3†], Chigo Okonkwo[1,3], Simon Rommel[1,3], Boris Škorić[2,3], Idelfonso Tafur Monroy[1,3], Sebastian Verschoor[4]

arXiv > cs > arXiv:2411.04030

Computer Science > Cryptography and Security

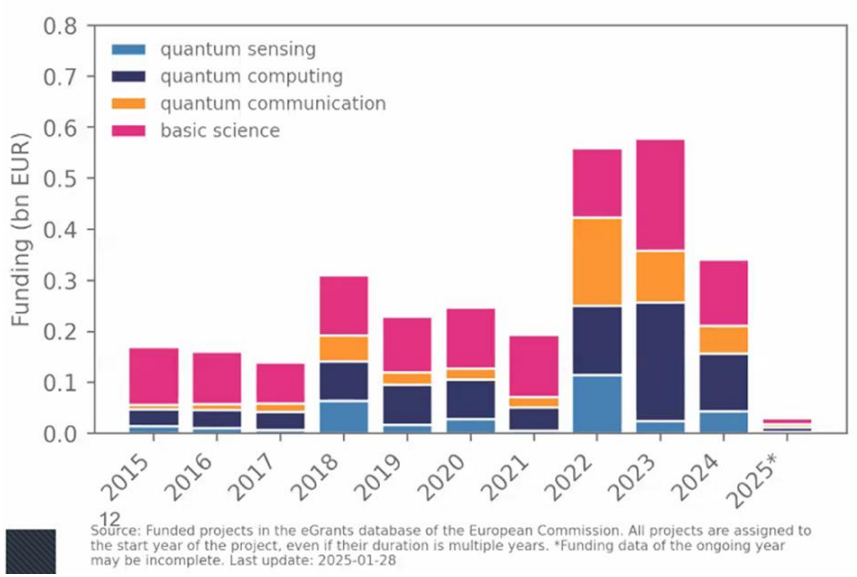
[Submitted on 6 Nov 2024]

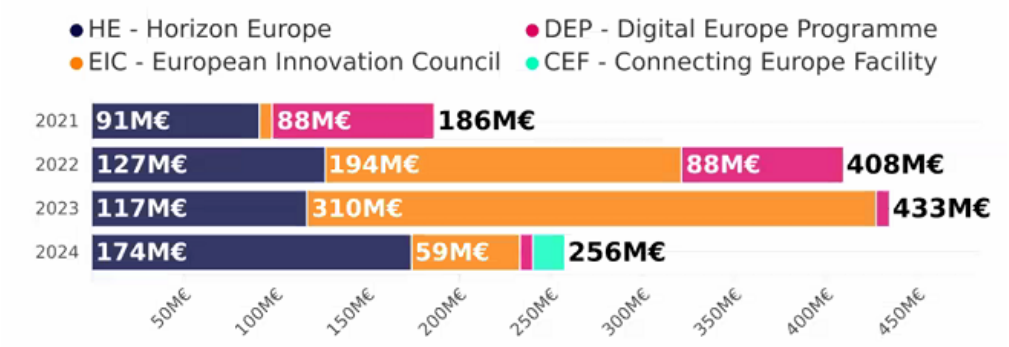
Quantum-Safe Hybrid Key Exchanges with KEM-Based Authentication

Christopher Battarbee, Christoph Striecks, Ludovic Perret, Sebastian Ramacher, Kevin Verhaeghe

EU approach to quantum technologies

EU Quantum Flasghip





EU Quantum Strategy

- **Concrete actions:** align national programs, invest in shared infrastructure, stand up chip pilot lines, and deploy dedicated platforms for quantum computing, communication, and sensing

- **Spans the full spectrum:** sensing platforms, quantum computing, quantum repeaters, MDI-QKD, and the enabling layers like cryogenics, photonics, packaging, and precision timing...

- **Help companies** to grow locally, access infrastructure without relocating, and bring vertical industries in early. Talent development.

- **Scaling science into infrastructure** across all layers of the tech stack. That includes using quantum networking for **far more than secure communication: it becomes a backbone** for distributed computing, remote quantum sensing, shared timing systems - **via real integration with classical infrastructure**

The Quantum Strategy proposes a “Quantum Act” by the end of 2025

The vision for the future

The urgency for deploying PQC gets higher, due to potential acceleration of quantum threats

- Establishing and running the coming EU testing infrastructure
- Continuous support measures for developing new algorithms & implement them securely, in all ICT infrastructures
- Translating EU Cybersecurity Policies into Action (and revise those that need to be revised)

The vision for the future

The urgency for deploying PQC gets higher, due to potential acceleration of quantum threats

- Establishing and running the coming EU testing infrastructure
- Continuous support measures for developing new algorithms & implement them securely, in all ICT infrastructures
- Translating EU Cybersecurity Policies into Action (and revise those that need to be revised)

QKD must progress, from research to compelling use cases where both security and performance are met. Progress will not slow down. But innovation must be built on solid bases.

- The EU is navigating through the new cryptography of the future. Careful design & proactive oversight needed
- Hybrid quantum-classical networks and then future quantum networks
- Need for collaboration between different communities - both progress & real innovation accelerate when silos fall

We need to have in mind **a convergence of technology, policy, and security in the age of quantum computing**, offering valuable perspectives on how European and global entities can navigate the emerging quantum landscape