CISSA

CENTRO INTEGRADO DE SEGURANÇA EM SISTEMAS AVANÇADOS

CESAR

EMBRAPII

MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

BRAZILIAN GOVERNMENT

BRASIL

UNITING AND REBUILDING

Dr. Erico Souza Teixeira

Research Leader at CISSA

Principal Research at |QATS>

Head of Quantum Technologies at CESAR

CESAR/CISSA

initiatives in Post-Quantum Cybersecurity

Quantum Computing

Post-Quantum Cryptography

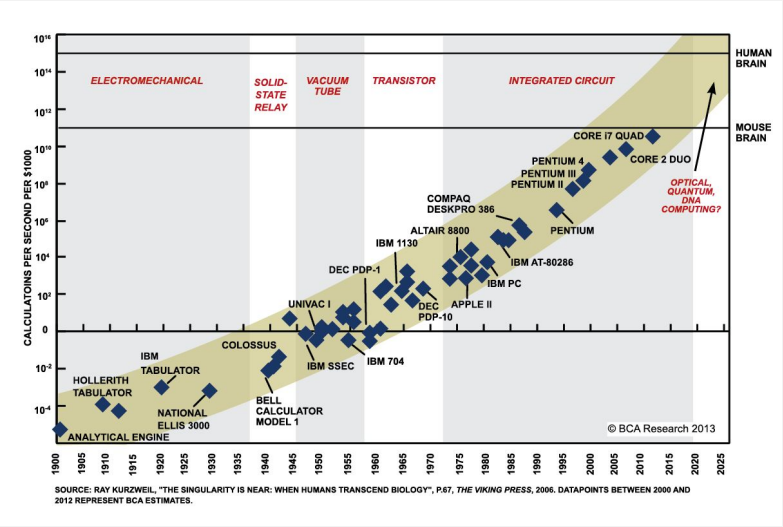
PQC Challenges

CESAR/CISSA PQC

Motivation

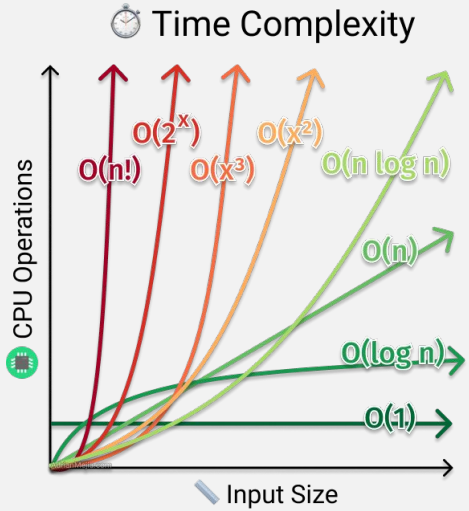
Moore's Law

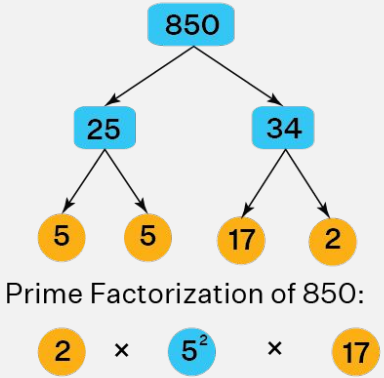
In 1965, Gordon Moore observed that the number of transistors on an integrated circuit would double every 18 months (which he later revised to two years), thus increasing processing power.

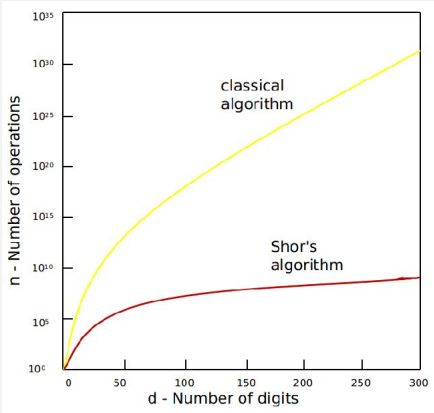


Motivation

Computational Complexity







Motivation

Richard P. Feynman

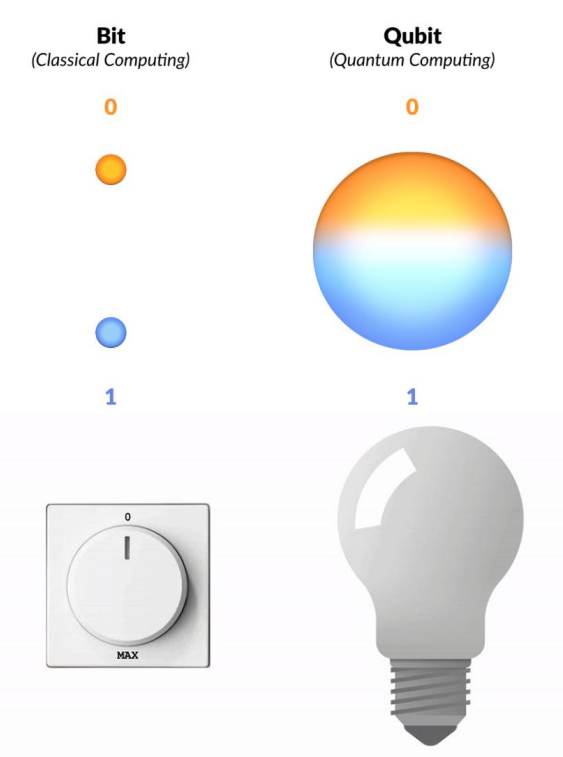
- “... nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.”

- It highlights the limitations of classical simulations and emphasizes the need for new computational approaches when dealing with inherently quantum phenomena.

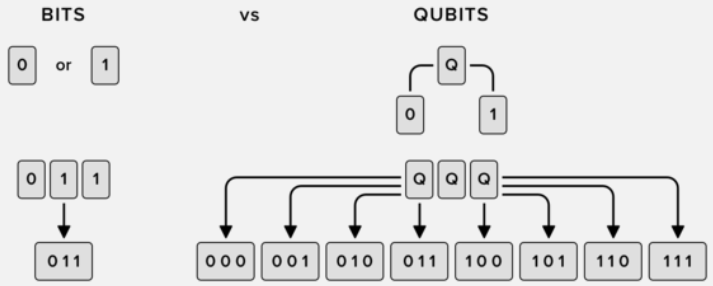
- Feynman's ideas helped spark new research into the development of quantum computers.

Fundamentals Concepts

Bit & Qubit



- Processing Speed.
- Simulation Capacity.
- Large-Scale Data Processing.
- Encryption and Security.



CESAR/CISSA

initiatives in Post-Quantum Cybersecurity

Quantum Computing

Post-Quantum Cryptography

PQC Challenges

CESAR/CISSA PQC

Shor's Algorithm

Quantum Attack

- In 1994, Peter Shor developed an algorithm for quantum computers that could be a breakthrough in factoring large integers.
- Shor's Algorithm was designed to run on a Quantum Computer rather than a classical computer, using the Quantum Fourier Transform.
- Standard cryptographic methods like RSA, ECC, and Diffie-Hellman rely on problems that can be efficiently solved by Shor’s Algorithm on a quantum computer.

Post-Quantum Cryptography

Quantum Attack

- A set of classical cryptographic algorithms that are designed to be secure against attacks carried out by quantum computers.

- The National Institute of Standards and Technology (NIST) has been leading an effort to select new cryptographic standards resilient to quantum attacks:
  - 2016: Call for submissions.
  - 2022: Initial selection of algorithms.

- Finalists and Standards (2024):
  - Public-Key Encryption/KEMs: CRYSTALS-Kyber (ML-KEM)
  - Digital Signatures: CRYSTALS-Dilithium (ML-DSA), SPHINCS+ (SLH-DSA)

Post-Quantum Cryptography

Global Initiatives

- PQCrypto Project (European Union):
  - Focused on developing and analyzing PQC algorithms.
  - Aims to address the security challenges posed by quantum computing.

- UK National Quantum Technologies Programme:
  - Develop quantum technologies, including PQC, to ensure national security and economic competitiveness.

- CISA Post-Quantum Cryptography Initiative (USA):
  - The Cybersecurity and Infrastructure Security Agency (CISA) coordinate efforts across government agencies and critical infrastructure sectors.

Post-Quantum Cryptography

Global Initiatives

- Google, IBM, Microsoft, and Amazon:
  - Investing in PQC research and integrating quantum-safe solutions into their cloud and computing platforms.
  - Developing hybrid cryptographic systems (combining classical and PQC algorithms) for transitional security.

- Open Quantum Safe Project:
  - An open-source initiative led by researchers to develop and test PQC algorithms.
  - Provides a library of PQC implementations for experimentation and deployment.

CESAR/CISSA

initiatives in Post-Quantum Cybersecurity

Quantum Computing | Post-Quantum Cryptography | PQC Challenges | CESAR/CISSA PQC

Key Challenges

PQC Adoption

- Key Size and Performance Trade-offs:
  - Many PQC algorithms require significantly larger key sizes and signature lengths compared to classical algorithms like RSA and ECC.
  - This can impact storage, transmission efficiency, and computational performance.

- Integration with Existing Protocols:
  - Modern security protocols (TLS, VPNs, SSH, etc.) need updates to support PQC.
  - Ensuring compatibility with legacy systems is a major challenge.

Key Challenges

PQC Adoption

- Hybrid Cryptographic Approaches:
  - During the transition period, hybrid models combining classical and PQC methods are needed.
  - Managing hybrid systems adds complexity and requires careful design.

- Security Assumptions:
  - Some PQC schemes rely on mathematical problems that haven't been as extensively studied as factorization and discrete logarithms.
  - Further research is needed to ensure their long-term security.

Key Challenges

PQC Adoption

- Implementation Complexity:
  - Efficient software and hardware implementations are required to minimize performance overhead.
  - Side-channel attacks on implementations must be mitigated.

- Adoption Resistance:
  - Organizations may be slow to migrate due to costs, lack of expertise, or inertia in updating cryptographic infrastructure.
  - Education and awareness are needed to drive adoption.

Key Challenges

PQC Adoption

- Regulatory and Compliance Issues:
  - Regulatory frameworks and compliance standards have not yet fully incorporated PQC requirements.
  - Different countries and industries may adopt PQC at different rates, leading to potential inconsistencies in security practices.

- Cost and Resource Constraints:
  - Transitioning to PQC requires significant investment in research, development, and deployment.
  - Smaller organizations or devices with limited computational resources (e.g., IoT devices) may struggle to adopt PQC due to its higher resource demands.

CESAR/CISSA

initiatives in Post-Quantum Cybersecurity

Quantum Computing

Post-Quantum Cryptography

PQC Challenges

CESAR/CISSA PQC

CISSA PQC Project

Integrated Performance and Robustness Assessment

- Conduct a comprehensive analysis of the **performance and robustness** of PQC algorithms, using parallel and interconnected approaches to optimize the development, evaluation and implementation of secure solutions on critical platforms:
  - Test lab: Creation of an environment for testing PQC solutions containing classical and quantum attacks.
  - Performance comparison: Evaluate PQC algorithms on different hardware platforms.
  - Robustness tests: Develop and reproduce attacks that simulate adverse scenarios, including classical attacks and quantum attacks.

CISSA PQC Project

Integrated Performance and Robustness Assessment

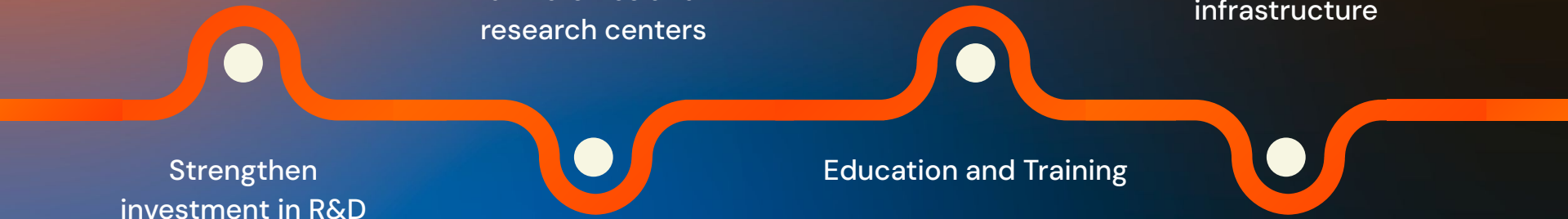
- Collaboration with Nationals Institutes:
  - Federal University of Campina Grande (UFCG).
  - Research and Development Center for Communications Security (CEPESC-Abin).
  - State University of Campinas (Unicamp).
  - Eldorado Institute.

CISSA PQC Project

How to join?

- Technological Association at CISSA:
  - CISSA also aims to develop an ecosystem of associated companies, fostering knowledge exchange and cybersecurity development aligned with current and future market demands.
  - Through financial contributions from members, the ecosystem also enhances the long-term sustainability of its projects.

PQC National Initiative



Thank you!

erico.teixeira@cesar.org.br

CISSA

QATS
Quantum Application in Technology and Software

CESAR

EMBRAPII

MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

BRAZILIAN GOVERNMENT
BRASIL
UNITING AND REBUILDING