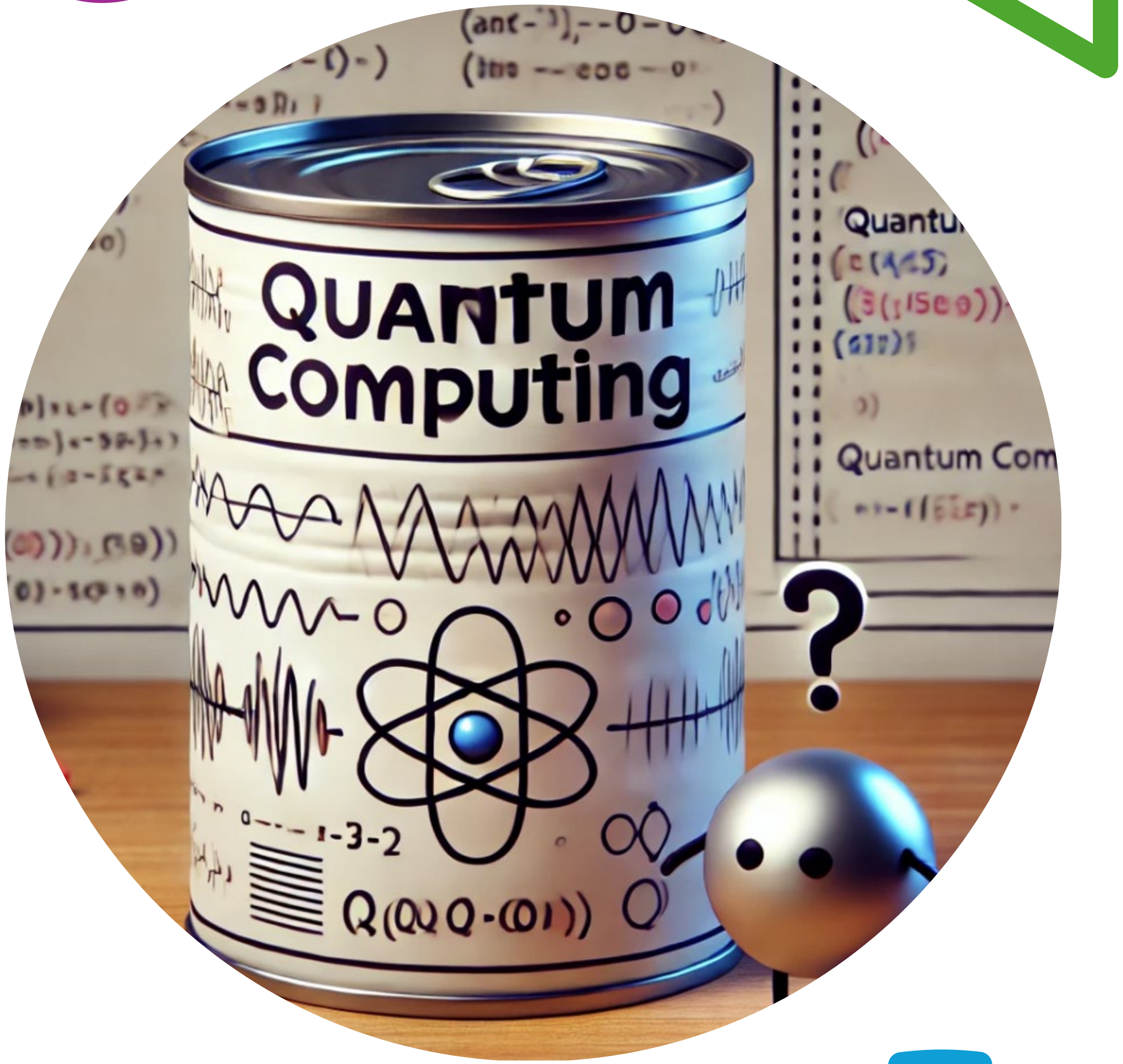


Securing mission-critical systems in a digital and post-quantum world

Quantum Cryptography - Alexandre Baron Tacla - CIMATEC

CESAR/CISSA initiatives in Post-Quantum Cibersecurity - Erico Souza Teixeira – CISSA

Session Chair: Jay Lala

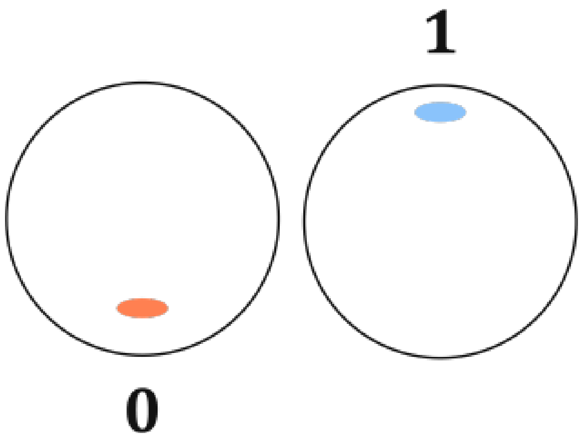
Rapporteur: Andrea Ceccarelli

What is quantum computing

Speakers explained basics of quantum computing

- From bit to Qubit, which are no longer binary values
- If with 2 bits you get 00, 01, 11, 10
  - Many combinations with 2 Qbit, leading to a high number of possible states
  - How many more data can you represent?

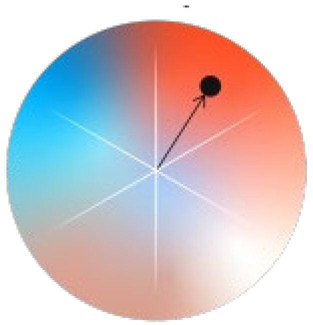
Bit



Speakers agree that the technology to create quantum computers is already available and getting more and more mature!

- Hardware with hundreds of Qbits are a reality! (and some are available as services)
- Many centers all around the word (with China on the forefront)

Qubit



Why quantum computers: a «dream» technology

Speakers share same motivations to build quantum computers: all relate to the exponential speed-up when combining multiple Qbits

- Solve problems with increased computational complexity in many domains (petroleum, chemistry, finance, ...)
- «build a simulation of nature with quantum mechanical laws»

The risks of quantum computing: a «nightmare» technology

- Speakers share also the risks!
  - quantum computing can «break codes»: cost of data breach is high (more or less depending on the country, but anyway high)

- Currently RSA is «overall secure» (3072 bits are considered secure), not sure until when
  - Cyphered data cannot be considered protected for 10-20 years
  - What about all previously-secure stored data with shorter keys?

Specific observations - Alexandre Baron Tacla

- **P**ost-**Q**uantum **C**ryptography: classical algorithms but designed to secure against attacks carrieted out by quantum computers. Can increase computational complexity

- **Q**uantum **C**ryptography **P**rotocols as Quantum Key Distribution for the distribution of keys

How soon do we need to worry?

X years: how long do you need encryption to be secure

Y years: how much time will it take to replace your system with a quantum safe solution?

Z years: how long will it take to break current solutions?

if x + y > z →

Specific observations - Erico Souza Teixeira

Focus on Post-Quantum Cryptography

- NIST selected 3 algorithms in 2024 (ML-KEM, ML-DSA, SHL-DSA)
- Require larger keys and signature methods compared to traditional RSA
- Integration with existing protocols is not granted (has been demonstrated that PQC can save against quantum attack but not traditional attack)
- Also, new quantum algorithm may come (Shor's algorithm is very old) and break new protocols

It is a reality but…

- Which regulations/standards, national and international
- What about smaller companies? Costs are currently very high!