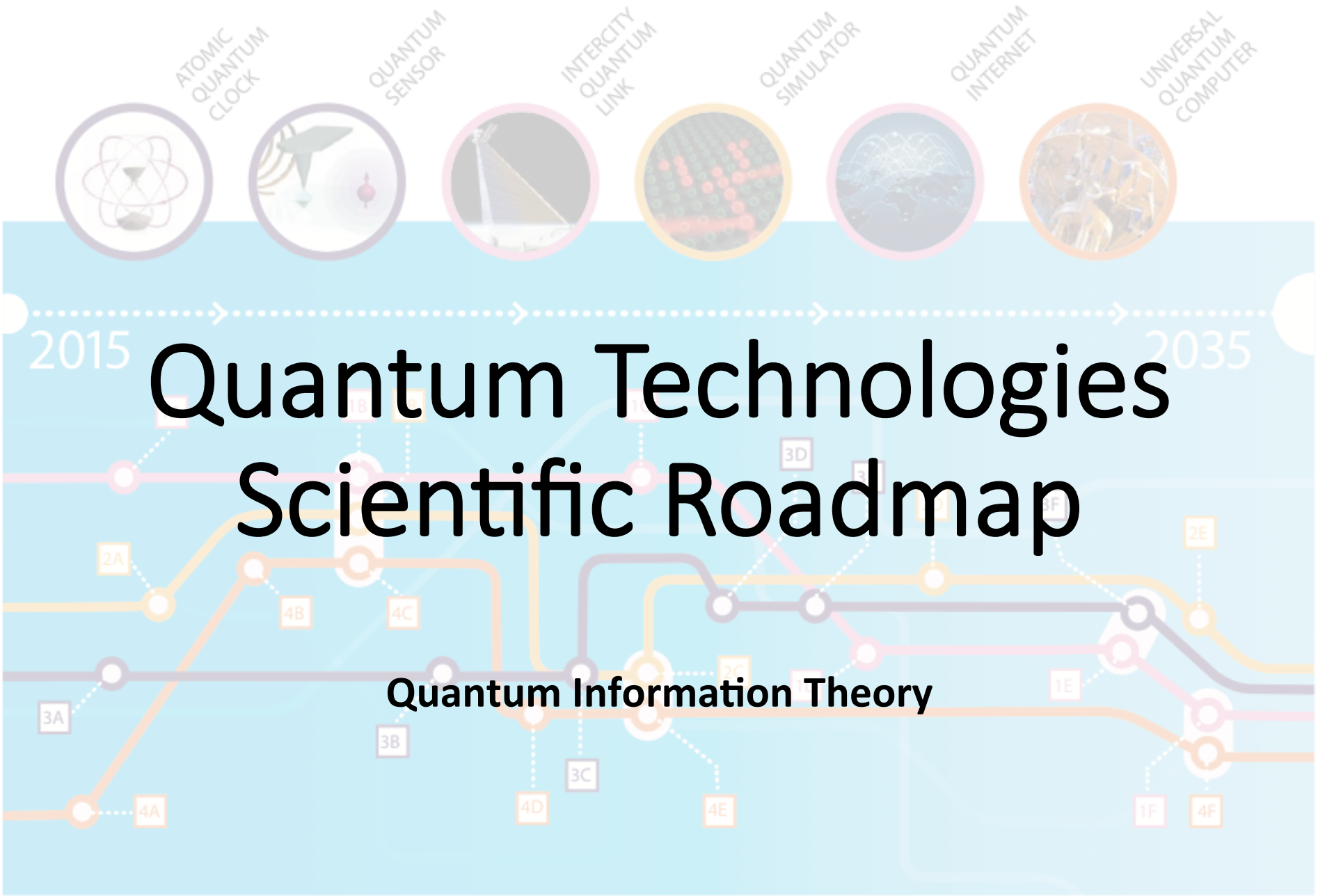

Quantum Technologies Scientific Roadmap

Quantum Information Theory

How can we fully exploit all these nice quantum technologies?

How can we fully exploit all these nice quantum technologies?

Despite impressive progress in the last decades, our understanding of this fundamental question is still limited.

Software for quantum computing devices

Novel algorithms to:

- Solve computationally relevant problems
- Simulate physically relevant systems (material science, quantum chemistry, high-energy physics)
- Extend machine learning and artificial intelligence applications to the quantum realm

Software for quantum computing devices

Novel algorithms to:

- Solve computationally relevant problems
- Simulate physically relevant systems (material science, quantum chemistry, high-energy physics)
- Extend machine learning and artificial intelligence applications to the quantum realm

Novel architectures for quantum computation

Software for quantum computing devices

Novel algorithms to:

- Solve computationally relevant problems
- Simulate physically relevant systems (material science, quantum chemistry, high-energy physics)
- Extend machine learning and artificial intelligence applications to the quantum realm

Novel architectures for quantum computation

Novel methods for **quantum error correction, topological and fault-tolerant** quantum computation

Software for quantum networks

Novel algorithms for **distributed quantum computing**: minimize the amount of communication needed to solve a problem

Software for quantum networks

Novel algorithms for distributed quantum computing: minimize the amount of communication needed to solve a problem

Quantum cryptographic protocols

- Physical security:
    1. Security under weaker assumptions or for realistic implementations, device-independent protocols
    2. Quantum cryptography beyond quantum key distribution: blind quantum computation, position-based cryptography, quantum money
- Computational security: post-quantum cryptography

Software for quantum networks

Novel algorithms for distributed quantum computing: minimize the amount of communication needed to solve a problem

Quantum cryptographic protocols

- Physical security:
    1. Security under weaker assumptions or for realistic implementations, device-independent protocols
    2. Quantum cryptography beyond quantum key distribution: blind quantum computation, position-based cryptography, quantum money
- Computational security: post-quantum cryptography

Quantum Shannon theory: communication capacities in networks

Quantum certification

How can we certify that a given device:

- is a quantum computer?
- is random?
- is secure?
- correctly simulates a physical system

Certification of complex quantum systems (network)

Quantum certification

How can we certify that a given device:

- is a quantum computer?
- is random?
- is secure?
- correctly simulates a physical system

Certification of complex quantum systems (network)

- Proofs of quantum supremacy
- Device-independent protocols (security, randomness, entanglement)
- Errors in quantum simulators
- Classical simulation of quantum systems (tensor-networks states, no-go theorems for quantum computation)

Quantum theory

Quantum information theory: identify the limits for quantum information processing.

- Entanglement theory
- Channel capacities
- Quantum estimation

Quantum theory

Quantum information theory: identify the limits for quantum information processing.

- Entanglement theory
- Channel capacities
- Quantum estimation

Quantum information meets other disciplines

- Condensed matter: new materials, high-T superconductivity
- Quantum biology: quantum effects in biological systems
- Quantum thermodynamics: work, heat, thermodynamic processes at the quantum scale
- High-energy physics: quantum gravity, theories beyond quantum physics, lattice gauge theories, holography
- Classical information theory: quantum-inspired proofs

A twofold approach

Current and near-future limits: what can be done with the existing or near-future quantum technologies?

Ultimate limits: what is possible for information processing using quantum technologies?

Community feedback

- **missing topics/systems/ideas:**
  - Electron quantum optics
  - Computing by observables

- **corrections to:**
  - Quantum thermodynamics: not only theory, more focus on non-equilibrium quantum processes or quantum heat engines

- **misc:**
  - Separation between theory and experiments?