Cryptography in a Quantum World

Scientific Introduction to the Winter School

Nir Bitansky
TAU

Zvika Brakerski
Weizmann

Quantum Computing & Computer Science

Quantum Computing: Use physical principles of quantum mechanics to achieve new computational capabilities

Potential Applications: Simulate quantum systems, generate randomness (locally or jointly), improved algorithms (factoring, lattice, ML)

Race towards full-fledged (”fault tolerant”) quantum computer. Current technology noisy with specialized architecture (“NISQ era”)

More philosophically: Computational perspective on a quantum universe

Implications: Refuting (?) the Extended Church-Turing hypothesis, characterization of possible correlations without communication, black-hole information paradox (using crypto!), quantum gravity (using crypto!)

Quantum Computing & Cryptography

If QC is a valid computational model, what are the implications on cryptography?

- **Assumptions** get broken quantumly ("Q cryptanalysis")
- **Adversarial models** still valid?
- **Reductions** still hold?
- Some **techniques** are inapplicable. Is this inherent?

Even for **classical** crypto primitives (w/ Q adversary)

a.k.a "post-quantum" cryptography

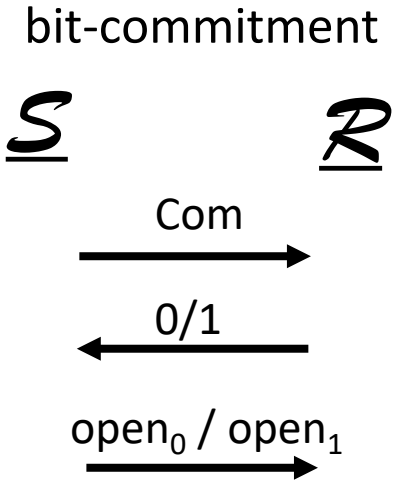
Quantum Computing & Cryptography

If QC is a valid computational model, what are the implications on cryptography?

- **Assumptions** get broken quantumly ("Q cryptanalysis")
- **Adversarial models** still valid?
- **Reductions** still hold?
- Some **techniques** are inapplicable. Is this inherent?

Even for **classical** crypto primitives (w/ Q adversary)

a.k.a "post-quantum" cryptography



Quantum Computing & Cryptography

If QC is a valid computational model, what are the implications on cryptography?

- **Assumptions** get broken quantumly ("Q cryptanalysis")
- **Adversarial models** still valid?
- **Reductions** still hold?
- Some **techniques** are inapplicable. Is this inherent?
- **New cryptographic objects**
  - Enc/Sig/MPC/Obf/… for quantum data
  - C-Q interaction (e.g. delegation)
  - Pseudorandomness for Q objects
- New crypto **capabilities** from Q information (QKD, MPC in QMiniCrypt)
- Q crypto as perspective on physical phenomena

What is the School About?

Focus on foundations: Basic challenges and techniques for Crypto in a Q world

~~**Assumptions** get broken quantumly ("Q cryptanalysis")~~

Will not cover constructing QC or standardization of PQ crypto

- **Adversarial models** still valid?

- **Reductions** still hold?

- Some **techniques** are inapplicable. Is this inherent?

- **New cryptographic objects**
  - Enc/Sig/MPC/Obf/… for quantum data
  - C-Q interaction (e.g. delegation)
  - ~~Pseudorandomness for Q objects~~

- New crypto **capabilities** from Q information (QKD, MPC in QMiniCrypt)

~~Q crypto as perspective on physical phenomena~~

Outline of the School

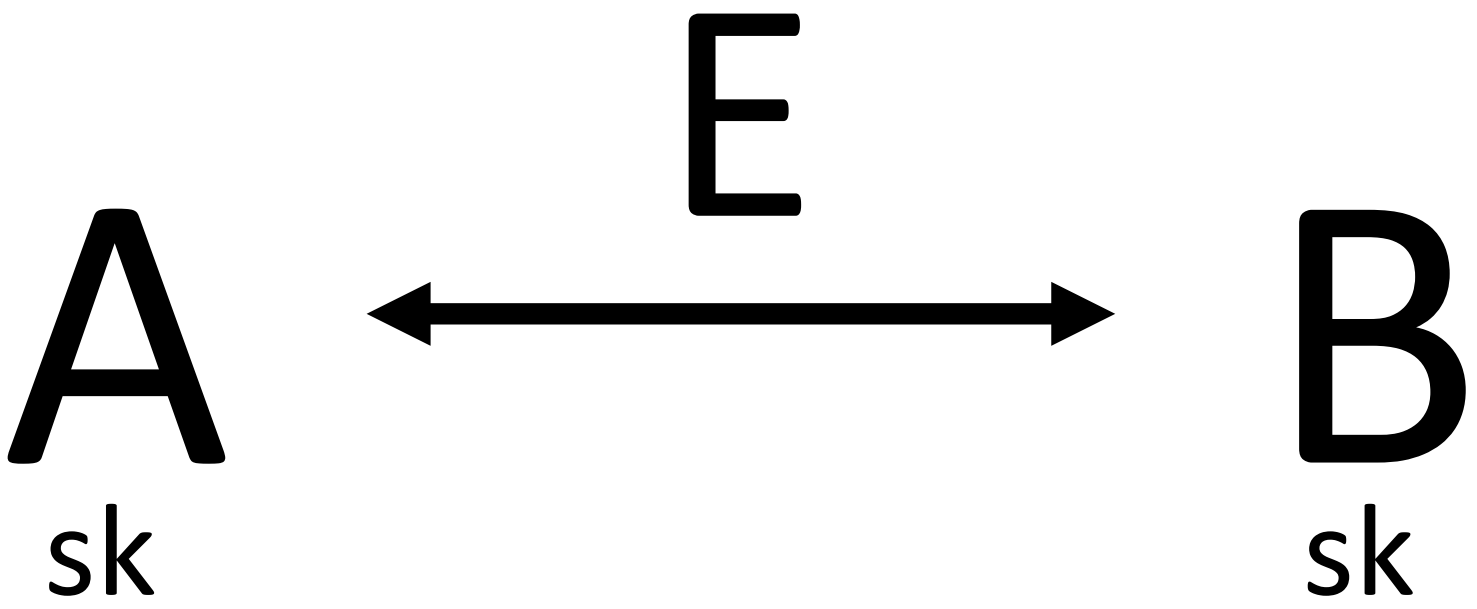
Crash Course in Quantum Computing

by Henry Yuen (Columbia University)

- Basic quantum information
  - What is a qubit?
  - Unitary evolution, measurements.
  - Composite quantum systems
  - No Cloning Theorem
  - Measurement in different bases, partial measurements
- Quantum circuits and quantum computation
  - Quantum circuit model
  - Algorithms: Grover, Quantum Fourier Transform
- Advanced quantum information theory
  - BQP, QMA, Hamiltonians
  - Mixed states
  - Distinguishability of quantum states (trace distance)

Quantum Key-Distribution (QKD)

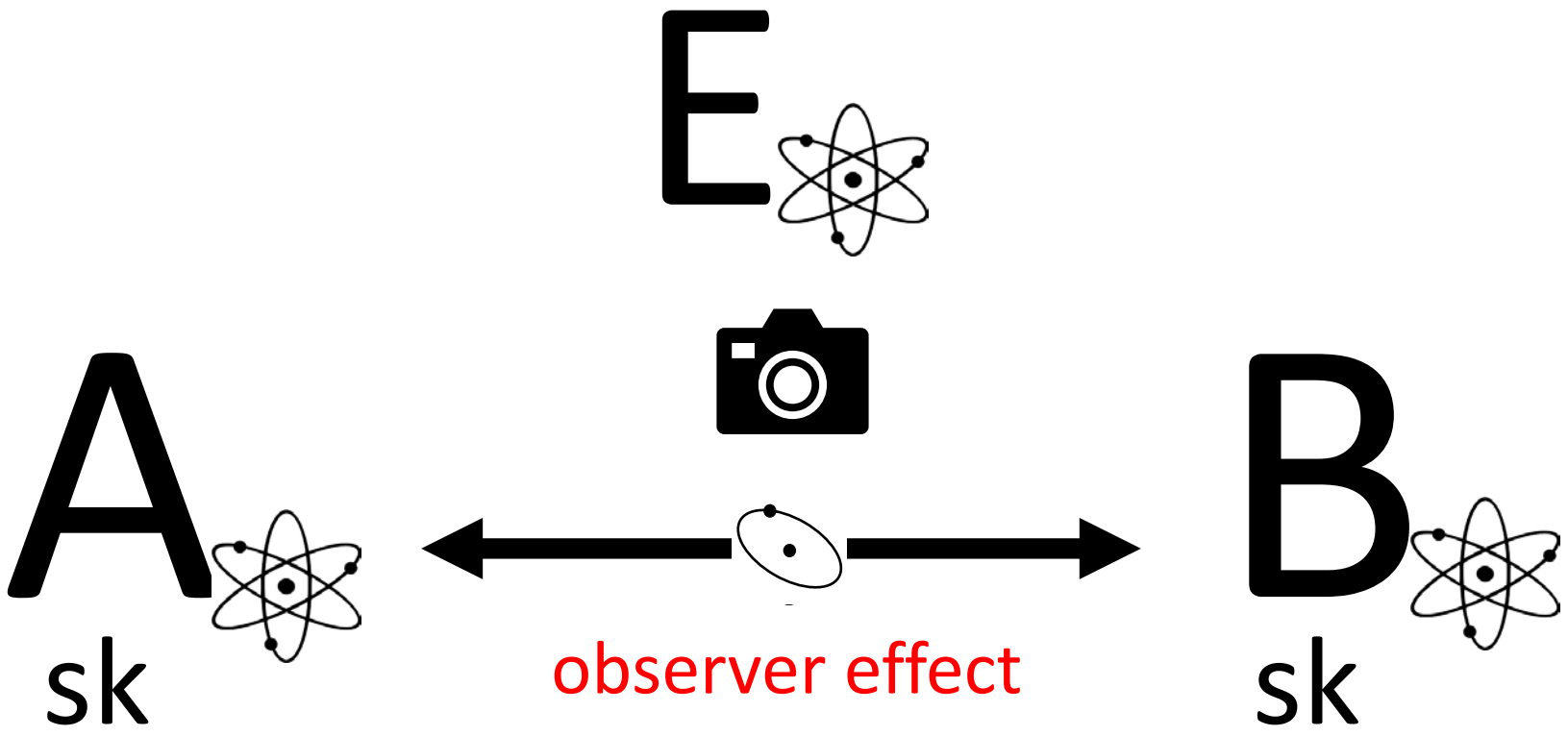
by Rotem Arnon-Friedman (Weizmann Institute of Science)



Classically: requires computational assumptions

at least OWFs, but seemingly much more…

Quantum Key-Distribution (QKD)



Quantumly: no assumptions (but quantum mechanics)

The technology is already out there!

QKD: Topics (Tentative)

by Rotem Arnon-Friedman (Weizmann Institute of Science)

- Defining
- Constructing
- Proving security
  - Quantum uncertainty relations
- Amplifying privacy
  - Quantum-proof randomness extractors
- Device independence (don’t trust that your device is quantum)
  - Non-local games

Post-quantum Security, Beyond Assumptions

by Mark Zhandry (Princeton University and NTT Research)

classical primitives	classical adversary	classical primitives	**quantum adversary**
PRG		Definitions	
PRF			
Signatures		Constructions	
CPA Encryption		Reductions	
CCA			
…		PQ Assumptions	

Post-quantum Security, Beyond Assumptions

Q: how does the quantum adversary interact with the classical system?

Example: is <u>any</u> lattice-based PRF PQ secure?

Not,

if the adversary can query it in **superposition**!

Some constructions (e.g., GGM) are PQ secure

Different security reduction…

PQ Security, Beyond Assumptions: Topics (Tentative)

by Mark Zhandry (Princeton University and NTT Research)

- When does PQ security follow directly?
- When does it break?
- How can we fix it?
- Topics:
  - Superposition queries
  - Quantum random oracle model
  - Rewinding

Zero-Knowledge and MPC in a Quantum World

by Alex Grilo (CNRS / Sorbonne Université)

"G is 3-colorable"

P ⟷ V

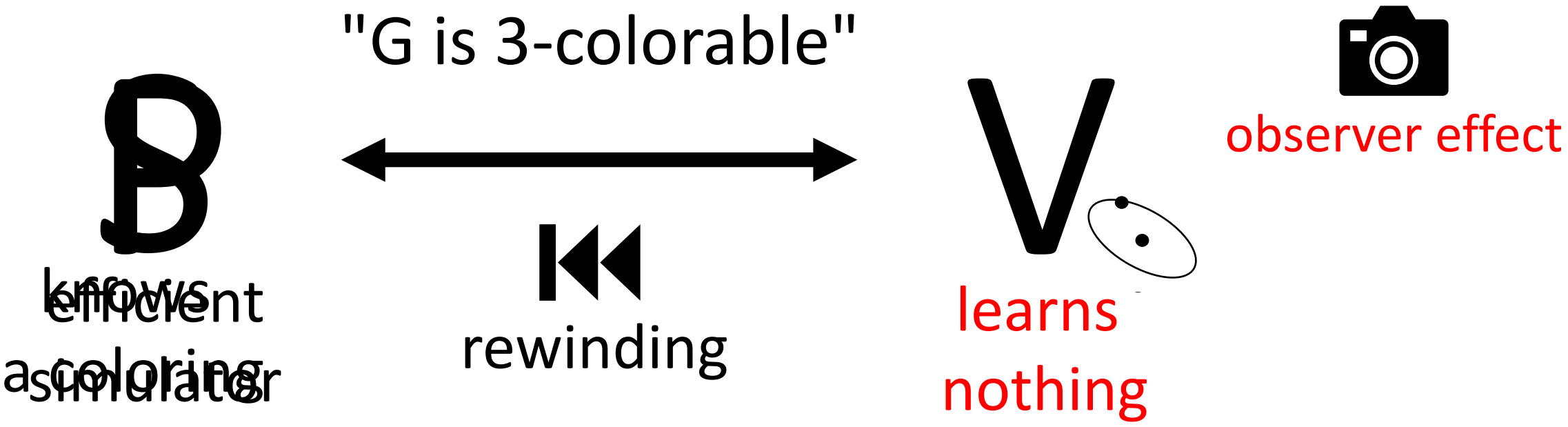
knows a coloring

learns nothing

Classically: doable for all of NP from OWFs.

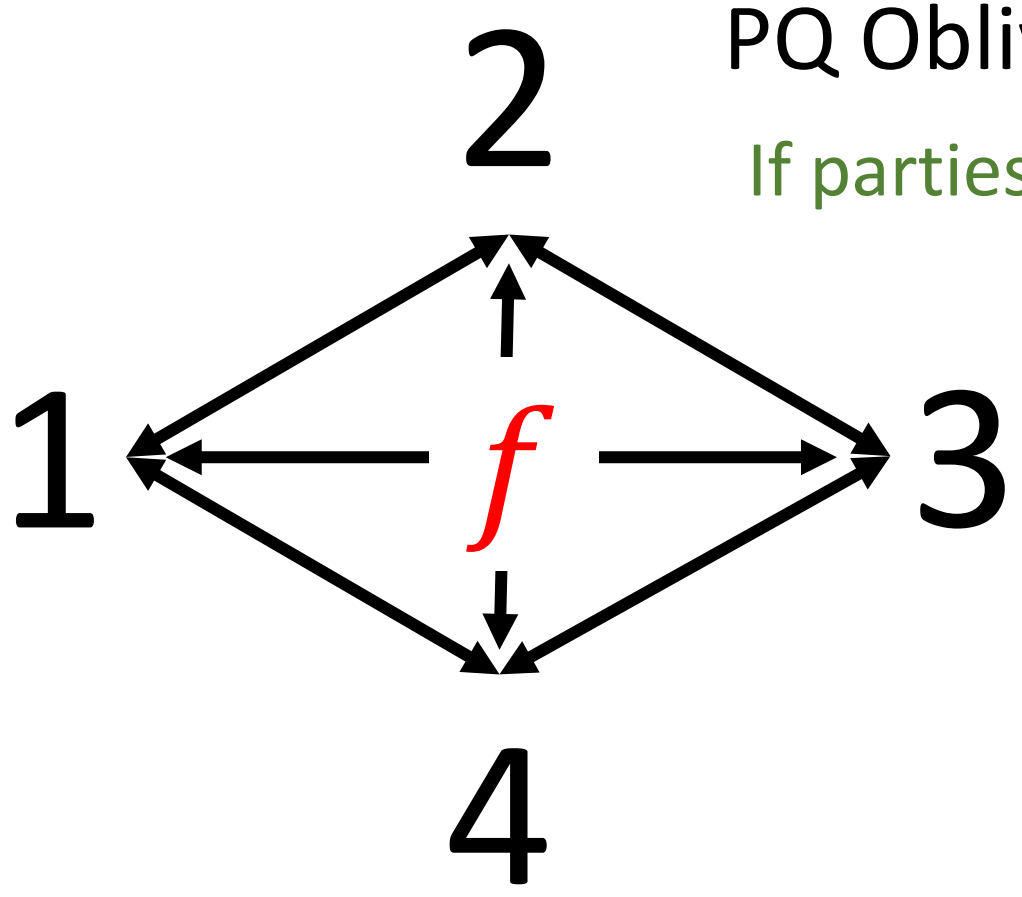
Quantum Verifier (Classical Protocol)

PQ zero knowledge?



Still doable, requires quantum rewinding

Multi-Party Computation: Quantum Adversary



PQ Oblivious Transfer + ZK => PQ MPC

If parties are (mildly) quantum: **OWF suffice!**

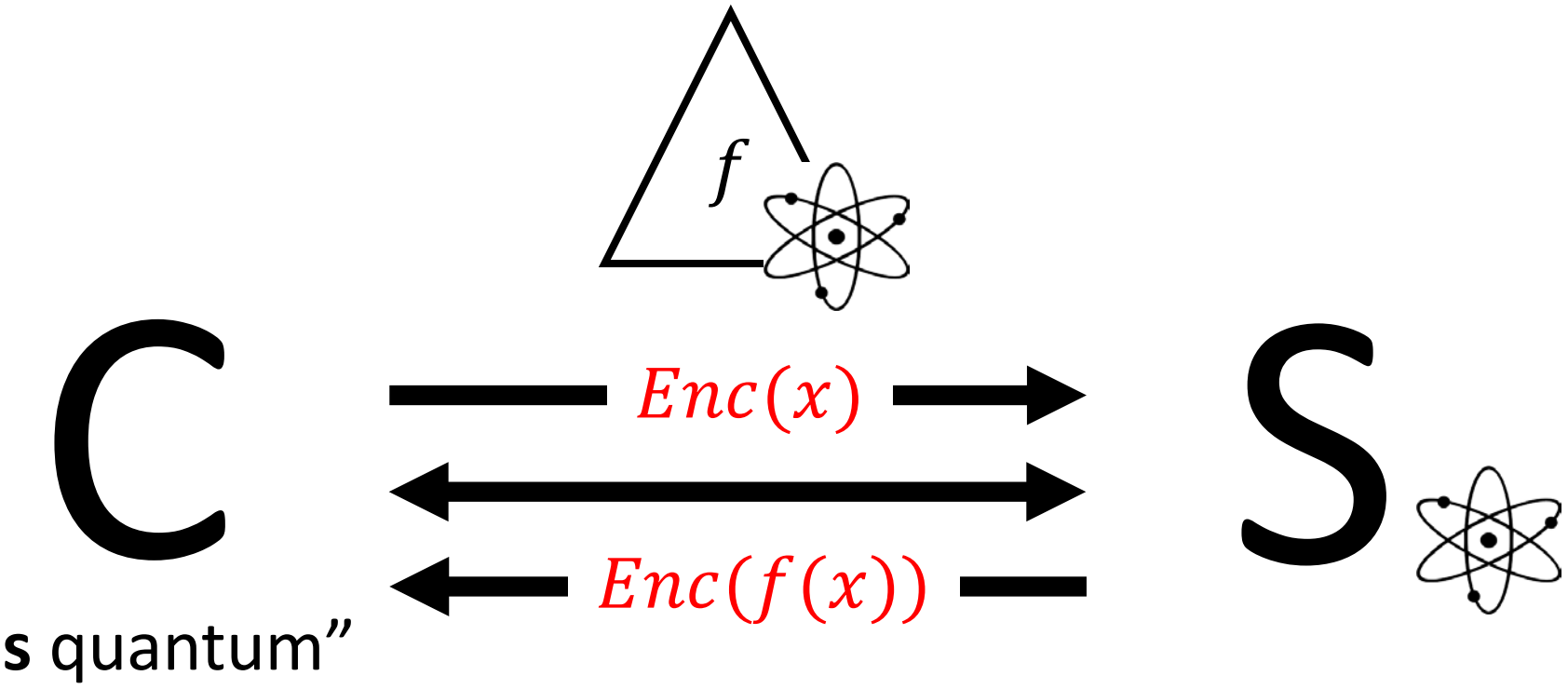
ZK and MPC: Topics (Tentative)

by Alex Grilo (CNRS / Sorbonne Université)

- Classical ZK protocols against quantum verifiers for NP
- Quantum ZK protocols for QMA (quantum analog of NP)
- Quantum MPC protocols from OWF (classical computations).
- Quantum MPQC (quantum computations).

Delegation of Quantum Computation

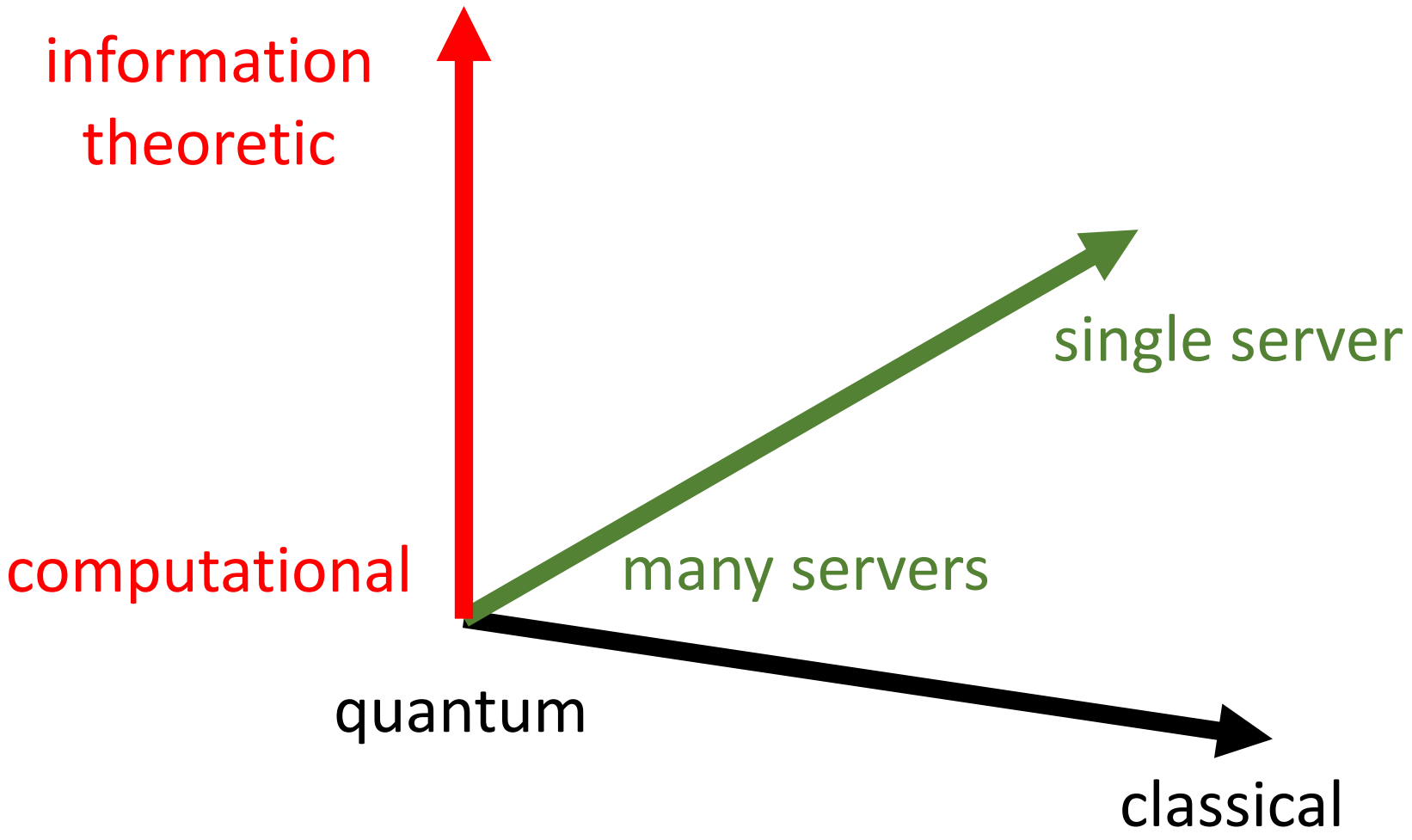
by Thomas Vidick (California Institute of Technology)



Soundness: client should be able to verify correctness

Privacy: client input x remains hidden (aka blindness)

Features



client capabilities

security

servers

Delegation of Q Computation: Topics (Tentative)

by Thomas Vidick (California Institute of Technology)

- Information-theoretic security, quantum client.
- IT security, classical client, two servers.
- Computational security, classical client, single server.
- Tools:
  - Quantum one-time pad
  - Authentication using Clifford gates
  - Quantum homomorphic encryption
  - Self testing
  - ….

Enjoy!