ILLINOIS
Information Trust Institute

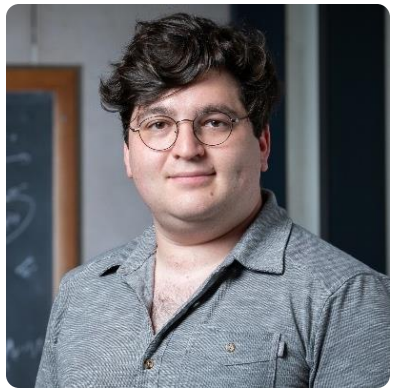
Quantum Cryptography (@ Illinois)

Information theoretic security from quantum resources

Maxwell Gold, Selina Nie

Our group

Maxwell Gold (PHYS)



- mjgold2@illinois.edu
- Provable cryptography
- Quantum resource theories
- Multipartite entanglement
- Certification protocols for quantum resources
- Neutral atom hardware

Selina Nie (CS)

- selina2@illinois.edu
- Near-term cryptography
- Position verification
- Joint measurements
- Nonlocal quantum computations
- Cybersecurity and incident response

Eric Chitambar (ECE)

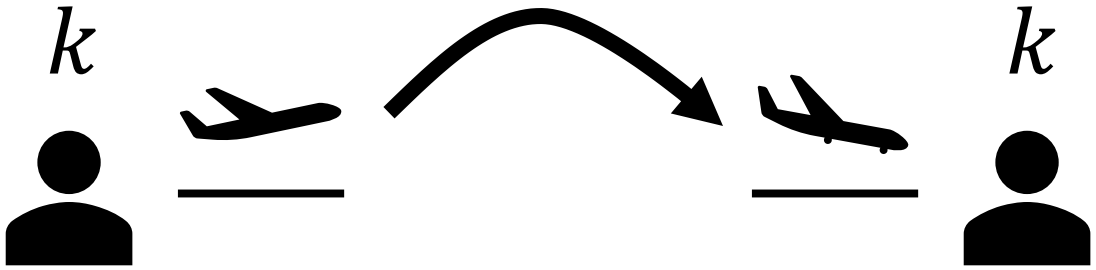
Group website: https://quantum-entangled.ece.illinois.edu/ [pardon our dust!]

- Quantum information theory
- Quantum resource theories
- Quantum computing
- Cryptographic systems and protocols
- Lasers and optical physics

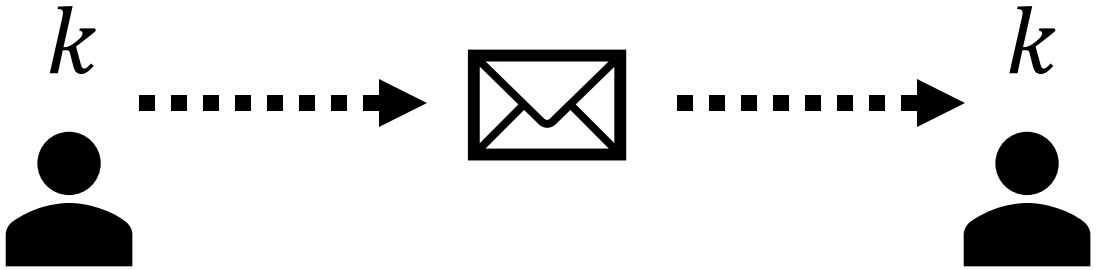
Cryptographic agility and quantum technology

Communication technology for security

- Should secrets ever leave your person?

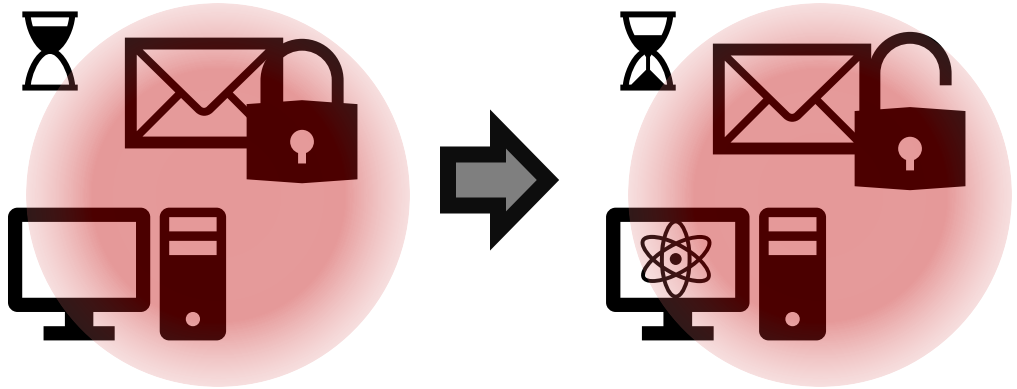


- Cryptography: cost of decryption is greater than the value of the secret.



Future-proof security

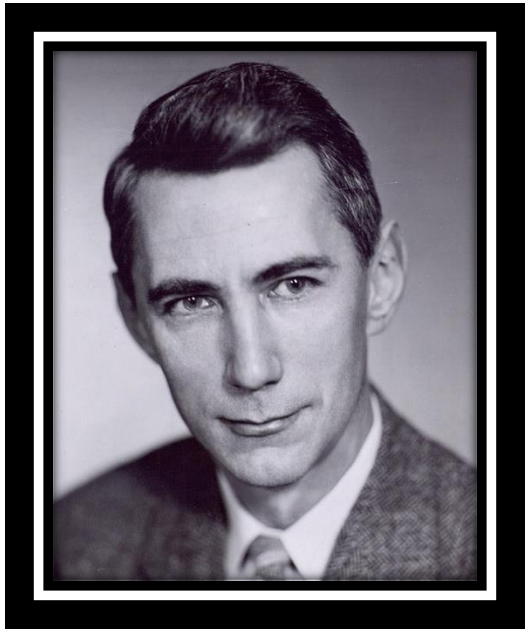
- All classical cryptography has a lifetime.



- Quantum can provide **information theoretic** privacy.
- A unique advantage?

Abstract cryptography w/o computational hardness

- Information theoretic (provable, non-cryptographic) security: privacy with a proof!
- Classical cryptography assumes the existence of **one-way functions** (pseudo-randomness that is hard to invert)
- Quantum cryptography demands **security without such assumptions**:
  - Establish provable security without computational hardness
- What does information theoretic privacy mean? Think a uniformly random **one-time pad**
  - Security formalized by Claude Shannon [Sha89]



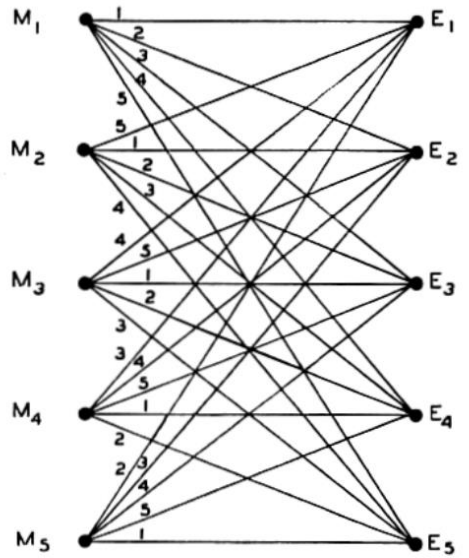
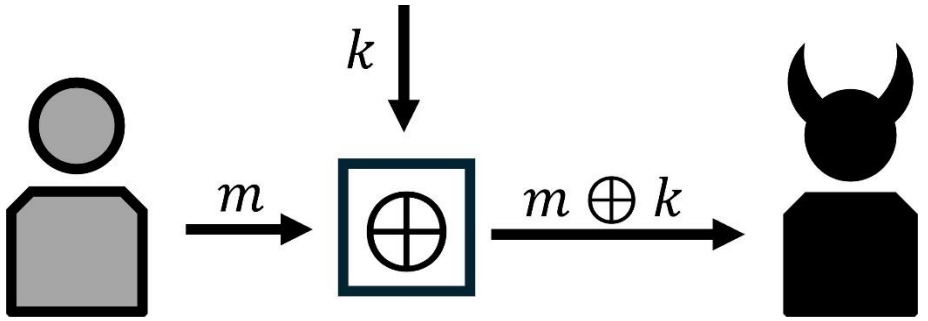


Fig. 5—Perfect system.

Quantum cryptography
- Quantum measurements generate probability distributions
- Quantum systems can't be copied arbitrarily
- Pioneers: Bennet, Brassard, Ekert, Mayers, Yao, Lo, Chau, etc.



Information processing with quantum systems

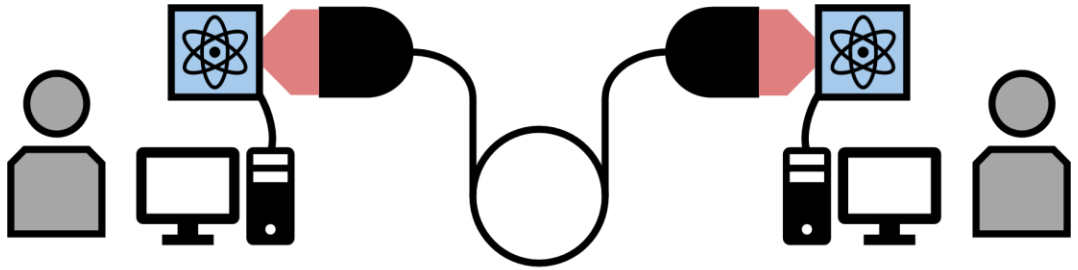
Quantum Computing (QC)

- A general tool for running quantum algorithms (e.g. Shor's factoring algorithm)
- Requires many qubits and gates
- SotA/near-term hardware is noisy

- Cryptanalytically relevant quantum computers (CRQC) — the threat to classical cryptosystems

Quantum Networking (QN)

- A problem specific tool for (multi-party) networking
- Resource efficient
- More hardware mature and near-term

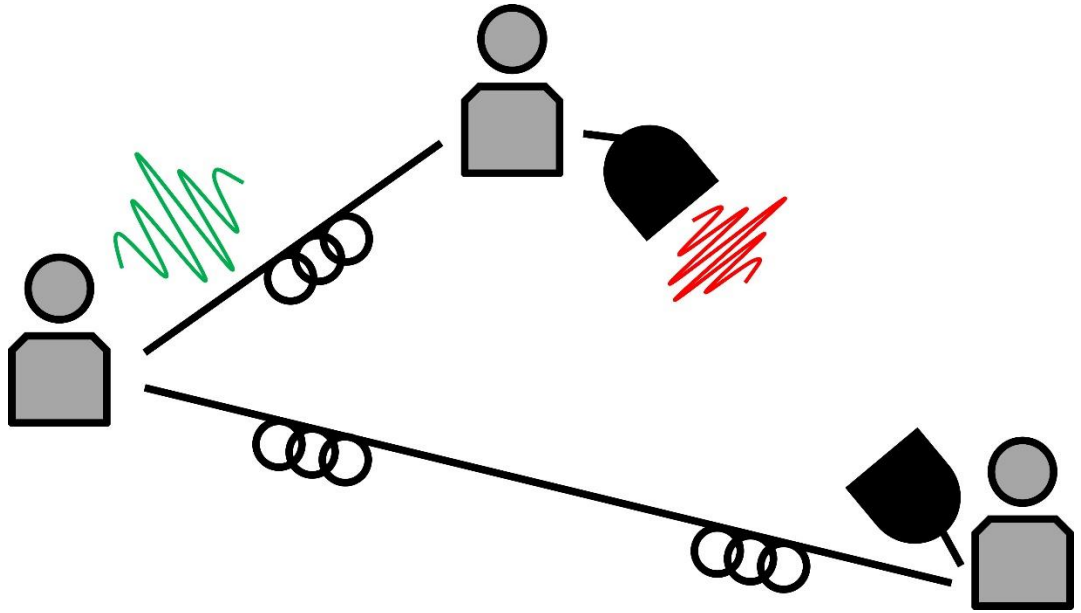


- A quantum network can serve as a communication layer within a cryptosystem

Quantum networking tools in the near-term

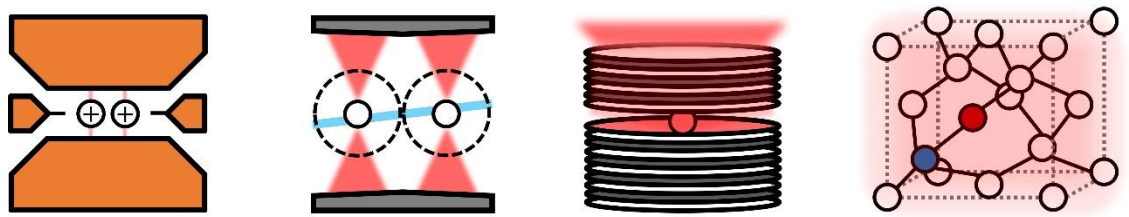
Communication (flying qubits)

- How do we send information? Fiber (free-space) optical networks
- Photons are subject to little noise, but they can be lost
- All optical networks exist for limited tasks (e.g. key distribution)



Memory (matter qubits)

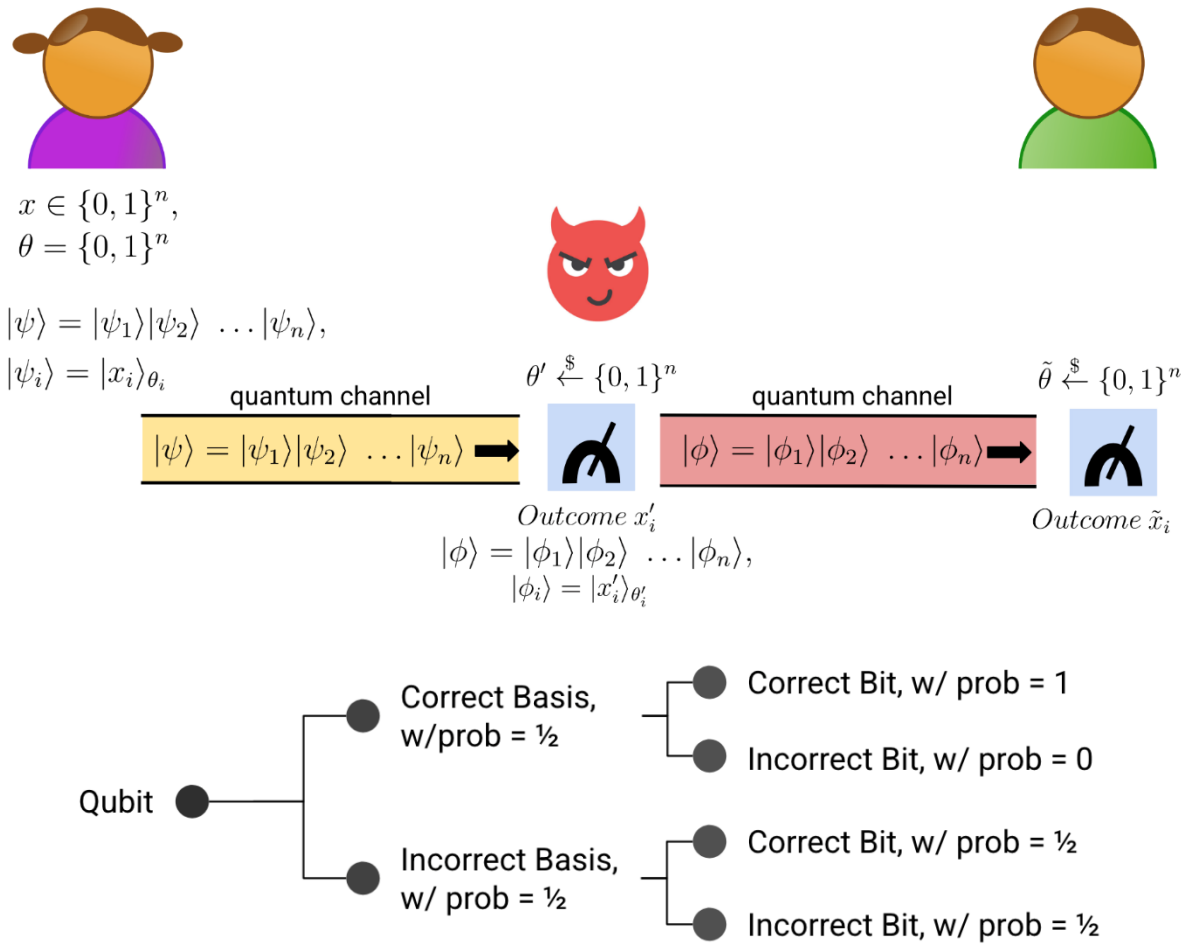
- How do we store information? Network nodes that interact with light
- A multitude of architectures with varying advantages (i.e. coherence, photon collection, etc.)
- Memory nodes allow additional functionality (e.g. two-way communication/computation)



Quantum Key Distribution (QKD)

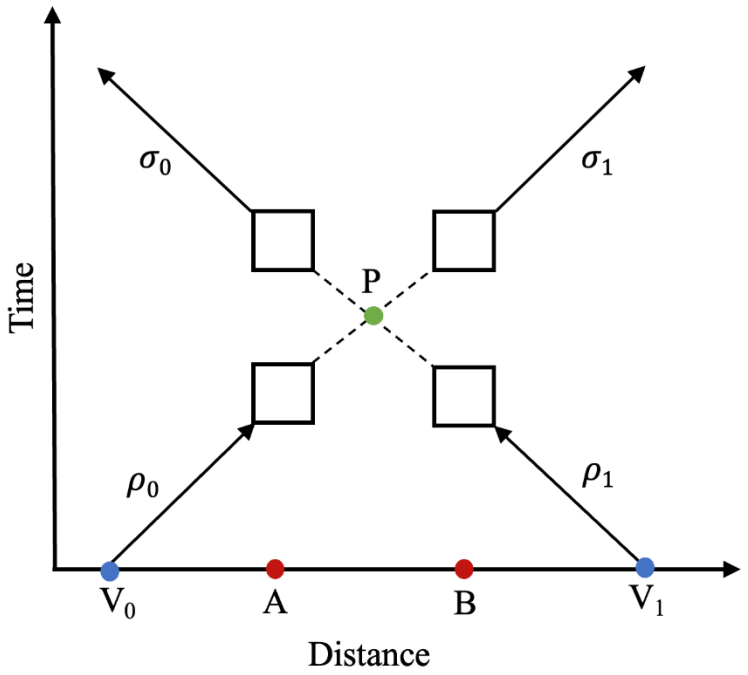
- Protocol for expanding symmetric bipartite secret **key** in the presence of an eavesdropper [BB84, Eke91]
- Requires authenticated public channel (achieved by an initial shared secret) to communicate measurement results and detect the eavesdropper
- Security comes from a physical assumptions: **no-cloning theorem**
  - Eavesdropper cannot clone an arbitrary quantum state
- Various forms of **device-independent** QKD (DIQKD) further removes assumptions on hardware
  - Allow the adversary to prepare the quantum states

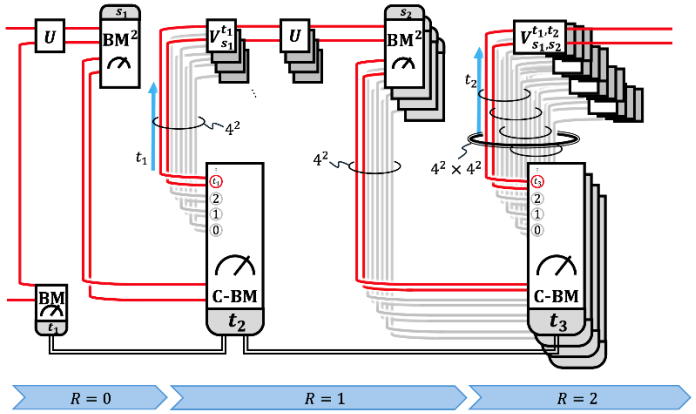
Pros	Cons
Protocol security is well understood	Implementation security requires more research
Hardware gap can shrink	Specialized hardware is required
Future proof, i.e. PQC may break	PQC is sufficient for a CRQC (we think)

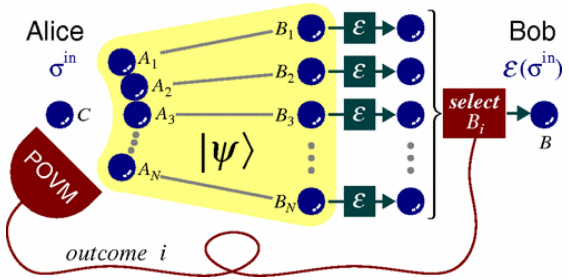


Quantum Pos.-Verification (QPV)

- Utilizing a party's geographic location as their *only* cryptographic credential
- Exploits the **relativistic no-signaling principle**: messages cannot travel faster than the speed of light
  - Based on response time, can guarantee that the prover is within a certain distance of the verifier
- Currently [BCF+14]: Any protocol can be broken if adversaries share an exponential amount of EPR Pairs (quantum resources)
  - Open question: Are there protocols that can be executed efficiently (poly-time/resources) by honest players but require exponential resources for attackers to break it?
- [OUR WORK]: Interpolating between [Vai03] and [BK11]
  - Quantum circuit complexity vs. needed entanglement
- Actions of honest parties are simple enough, can be implemented using current quantum technology
  - Future Applications: Military Communications and Financial Transactions



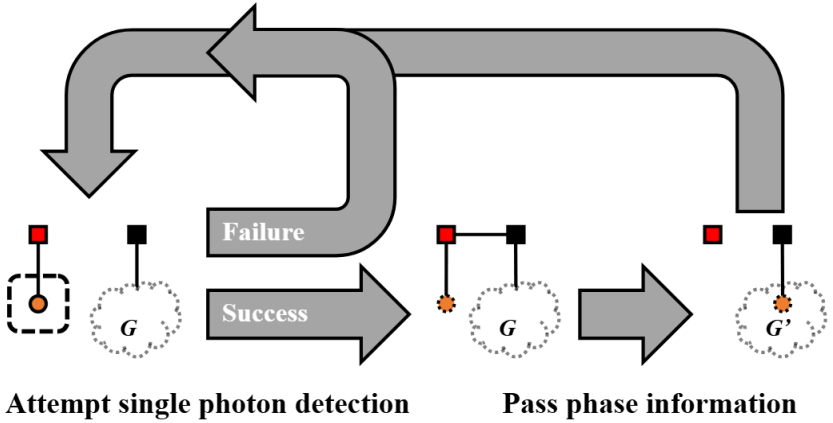


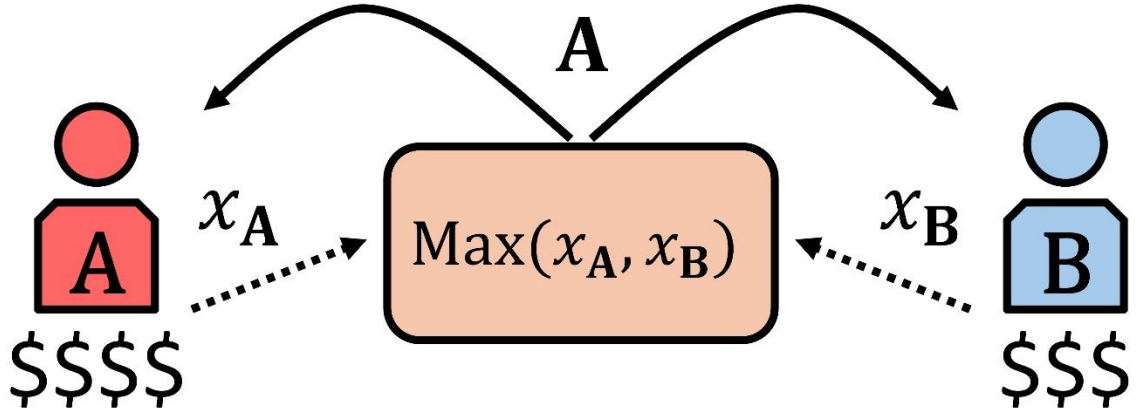


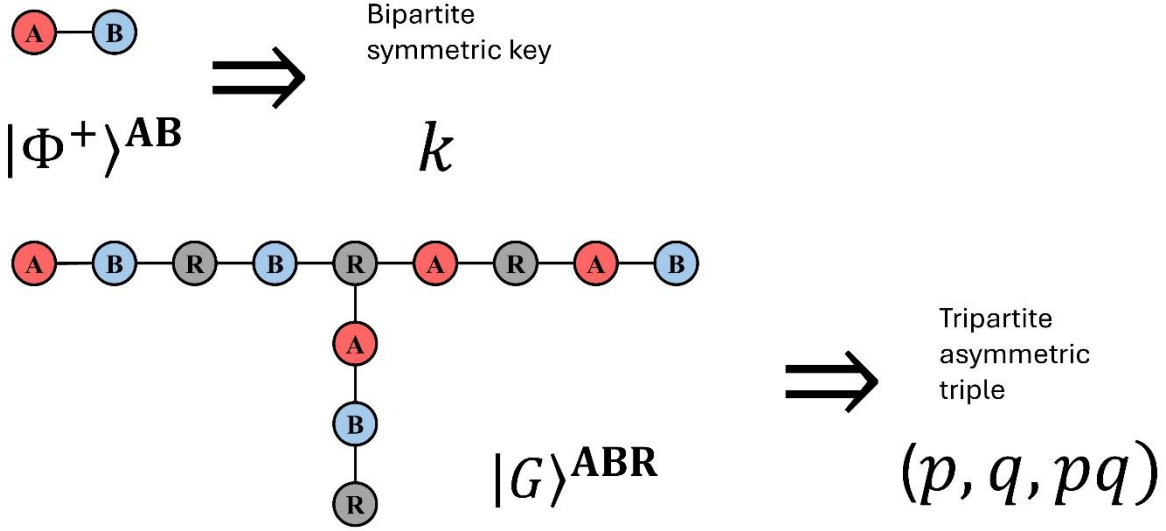
[IH08]

Multi-party computation (MPC)

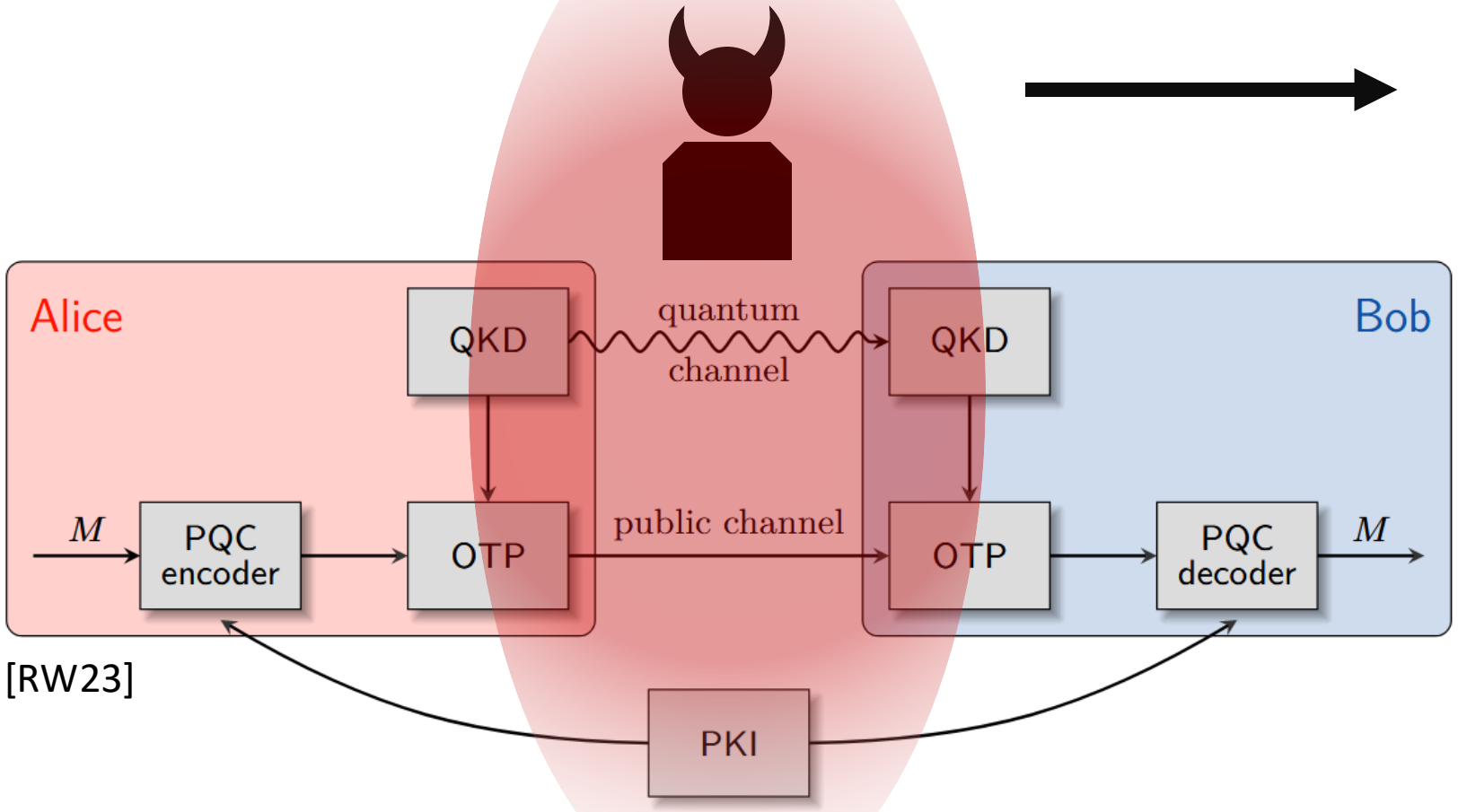
- Symmetric key enables sending private message. What enables private function (circuit) evaluation?
  - **MPC**: Parties want to evaluate some shared function, without revealing anything about their inputs.
  - E.g., Yao's famous millionaire problem.
- Multiplication of party inputs requires interaction! Access to a multiplication (Beaver) **triple** minimizes this interaction [Bea92].
- [OUR WORK] Triples can be obtained directly from entangled states, such as **graph states** [GC25].
  - Can perform efficiently on near-term QN hardware [GLGC25].



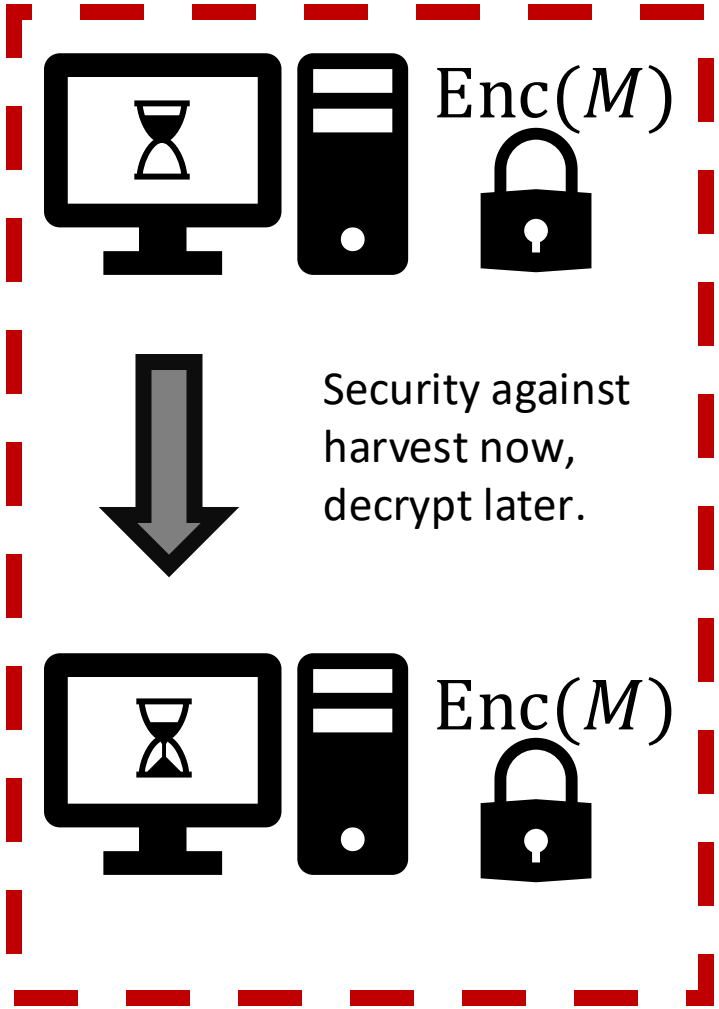




Provable security layers in hybrid cryptosystems

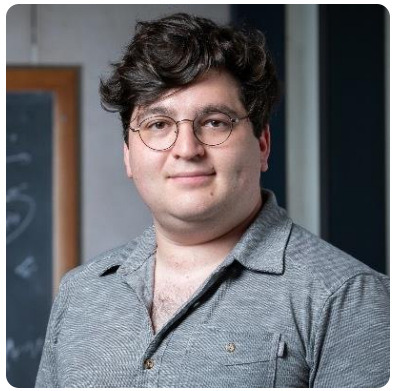


[RW23]



Our group (reach out via email for more!)

Maxwell Gold (PHYS)



- mjgold2@illinois.edu
- Provable cryptography
- Quantum resource theories
- Multipartite entanglement
- Certification protocols for quantum resources
- Neutral atom hardware

Selina Nie (CS)

- selina2@illinois.edu
- Near-term cryptography
- Position verification
- Joint measurements
- Nonlocal quantum computations
- Cybersecurity and incident response

Sources

- Sha89—10.1002/j.1538-7305.1949.tb00928.x
- BB84—10.1016/j.tcs.2014.05.025
- Eke91—10.1103/PhysRevLett.67.661
- BCF+14—10.1137/130913687
- Vai03—10.1103/PhysRevLett.90.010402
- BK11—10.1088/1367-2630/13/9/093036
- IH08—10.1103/PhysRevLett.101.240501
- GC25—arXiv:2505.10385
- GLGC25—arXiv:2405.13263
- RW23—arXiv:2307.15116