CLASSICAL CRYPTOGRAPHIC PROTOCOLS IN A $|$QUANTUM$\rangle$ WORLD

Fang Song

Joint work with Sean Hallgren and Adam Smith

Computer Science and Engineering
Penn State University

Quantum Computing Makes Classical Crypto Harder

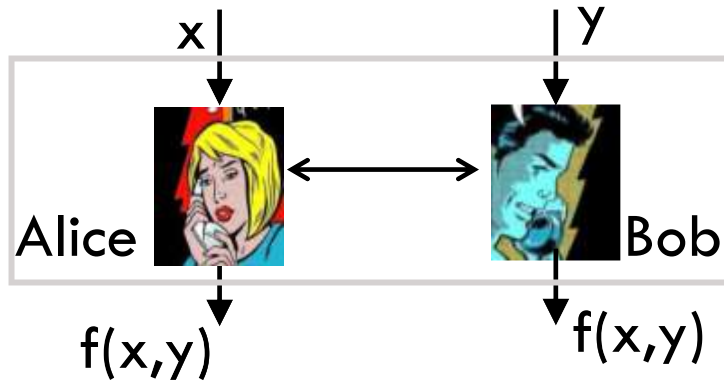
- Efficient quantum algorithms for certain computational problems, e.g.
  - Factoring and discrete log [Shor'94]
  - Principal ideal problem [Hallgren'02]
- Entanglement breaks some classical proofs of security
  - "Information-theoretically" secure scheme broken [CSST'06]
  - Attack does not need large-scale quantum computer

Unclear which existing protocols are secure

- This Talk: **Classical** two-party secure function evaluation (SFE) against **quantum** attacks

Secure Function Evaluation (SFE)

- Secret inputs
  - Alice: x
  - Bob: y



- Informal security goals:
  - Correctness: Jointly evaluate f(x,y) correctly
  - Privacy: Bob does not learn anything about x beyond f(x,y); same for Alice
- Example:
  - Auctions: 2 bidders with bids x, y
    - f outputs the identity of the winning bidder
    - E.g., x = \$3, y = \$2, f(x,y) = “Alice”

SFE: Feasibility Results

- Classically: [Yao'86, Goldreich,Micali,Wigderson'87]

  Any poly-time computable function f can be securely evaluated assuming existence of trapdoor permutations.
- Question: do similar feasibility results exist if adversaries are **quantum**?
- Non-trivial to answer
  - Some classical protocols are provably insecure [CSST'06]
  - Basic proof techniques may fail

    Rewinding: a crucial technique in GMW
    - Tricky for quantum adversaries
    - Possible in special cases: [Watrous'09, Damgard,Lunemann'09]
    - Unclear how to do it in general

Previous Work

- Secure protocols for a few specific tasks
  - Zero-knowledge (ZK) proofs for NP against quantum verifiers [W'09]
  - Quantum secure coin-flipping [DL'09]
- "Limited" security models for SFE
  - Special context [Wolf,Wulschleger'08, Fehr,Schaffner'09]
    - Not general enough to capture [W'09, DL'09]
  - General model for "universal composability" (UC) [Canetti'01, Ben-Or,Mayers'04, Unruh'04 '10]
    - Captures **network** setting; contrast with **stand-alone** setting
    - Very strong: 2-party SFE unrealizable without extra setup
    - Not satisfied by [W'09, DL'09]

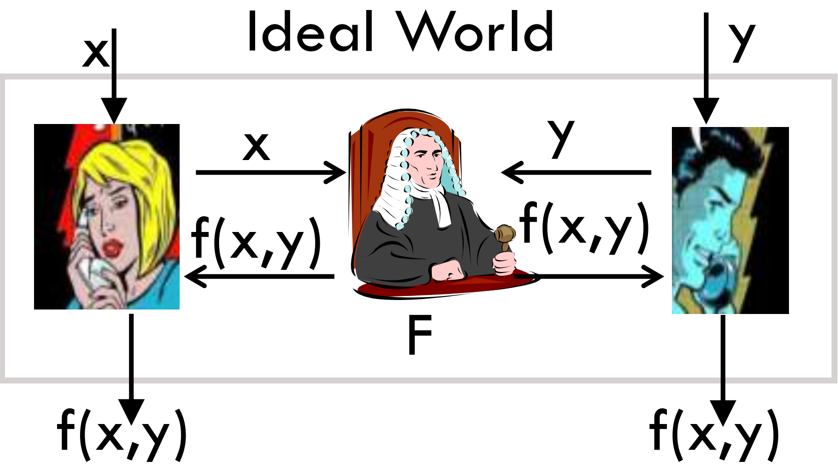
This Work

Classical SFE protocols
secure against **quantum** attacks.

1. Model for stand-alone protocols in quantum setting
   - Captures [W'09, DL'09], in particular
2. Classical proof techniques that work with quantum
   - "Simple hybrid arguments"
3. Protocols for 2-party SFE
   - UC security assuming a "common random string" (CRS)
   - Stand-alone security with no set-up

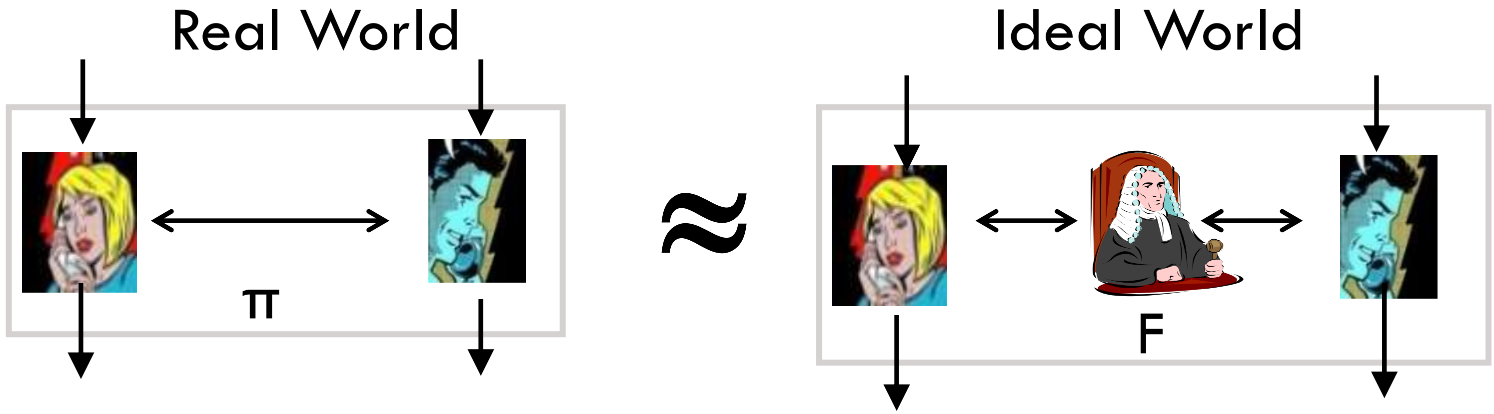
Modeling Security

Ideal World Protocol



- Consider an ideal world,
  - There is a trusted party F:
    - Gets x, y
    - Returns f(x,y)

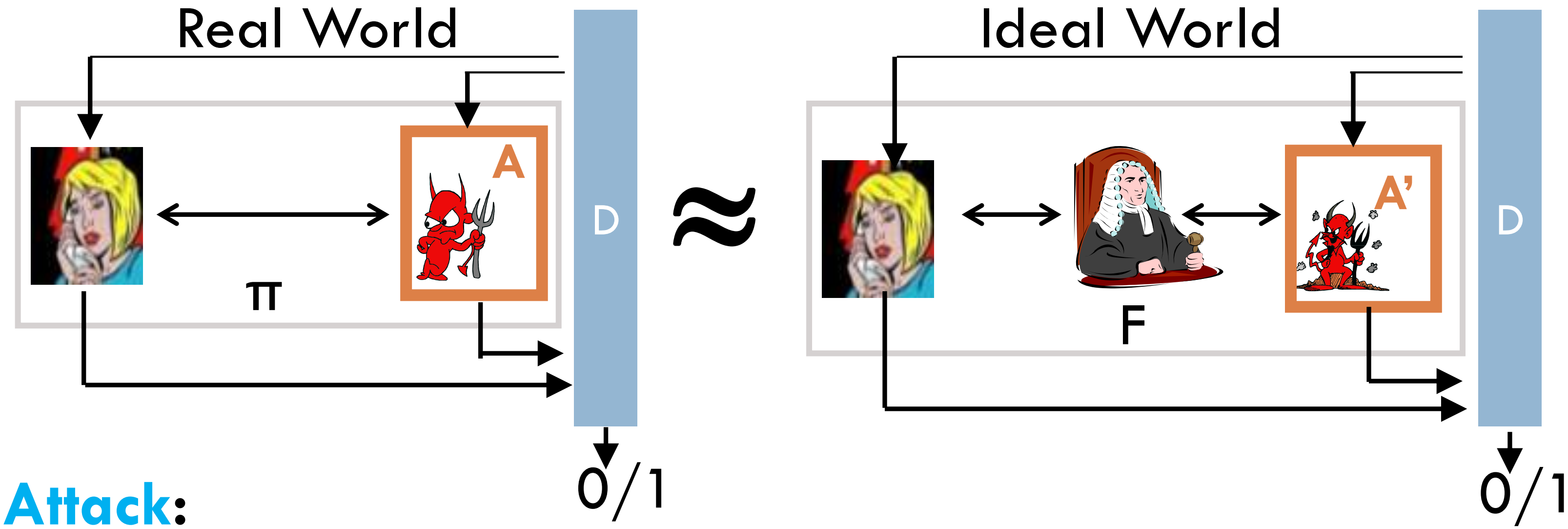
Intuitive Definition of Security



- A protocol π in real world should "emulate" F
- "Emulate" means:
  - if there is an **attack** in real world

    then there is an **equivalent** attack in the ideal world

Formal Definition of Security [Canetti'00]



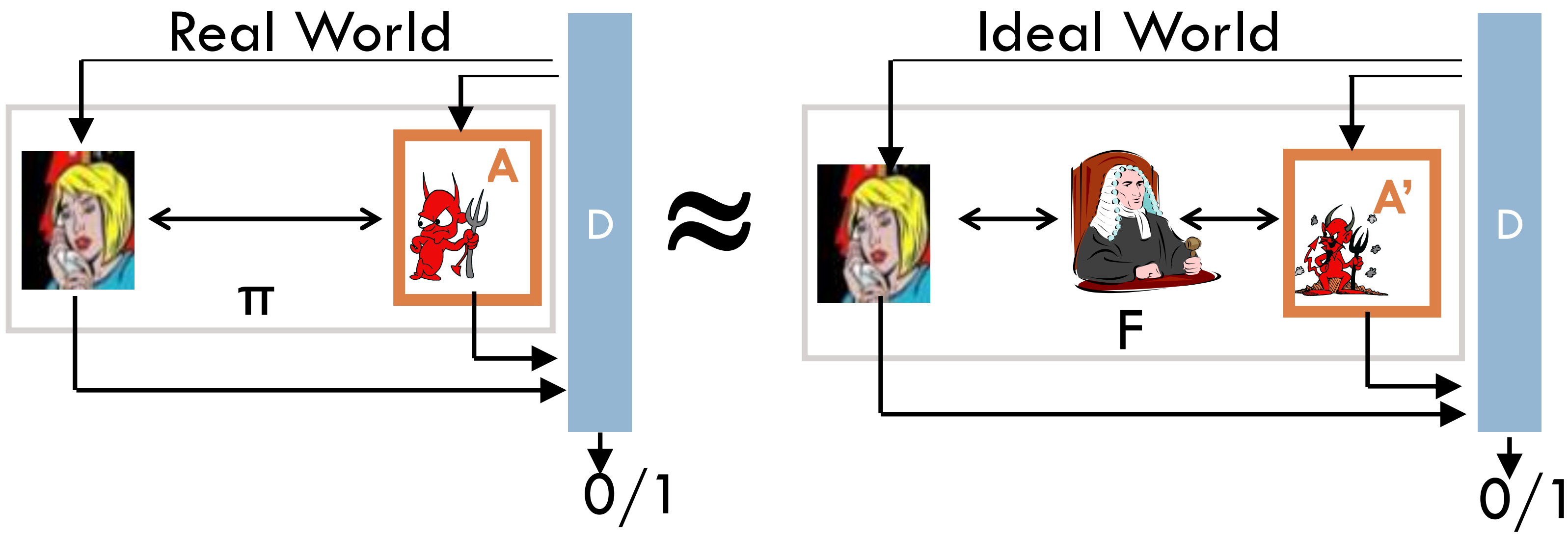
- **Attack**:
  - An adversary described by a circuit/machine
  -
  - A': corrupts Bob in ideal world;

∀distinguisher **D**, ∀ real world **A**, ∃ ideal world **A'**, such that

$$|\Pr[D(\text{Real}) = 1] - \Pr[D(\text{Ideal}) = 1]| < \varepsilon$$

- **Equivalent**: attacks A and A' are equivalent if
  - no distinguishers D can tell apart real/ideal protocols
    - By preparing inputs and observing outputs of real/ideal protocols

Modeling Security with Quantum Adversaries



- Tak
  - A ... ntum n

  ∀ quantum **D**, ∀ quantum **A**, ∃ **A’**, such that

  $$|\Pr[D(\text{Real}) = 1] - \Pr[D(\text{Ideal}) = 1]| < \varepsilon$$

  - Semantics otherwise unchanged
- [W’09, DL’10] fit our model
- A special case quantum UC model [Unruh’10]

Modular Composition in Our Model

- Consider a high level protocol that can be split in to small sub-tasks
- **If** it is secure
  - when sub-tasks are realized by trusted parties

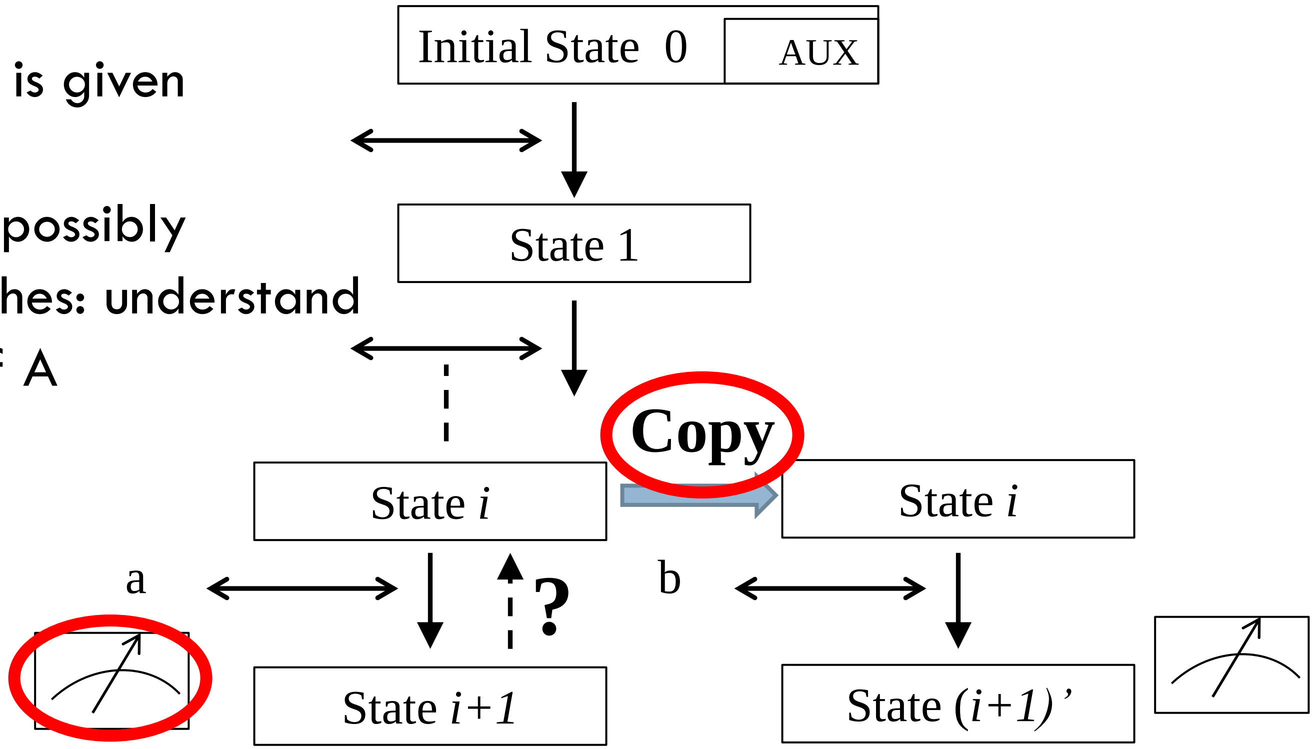
Then it remains secure

  - when sub-tasks are implemented by real world protocols

Proving Security

Why is Quantum Rewinding Difficult?

- Rewinding
  - Adversary A is given as a machine
  - Run A along possibly different branches: understand the behavior of A



- Quantum no-cloning theorem
- Measurement collapses quantum state

Proving security without rewinding?

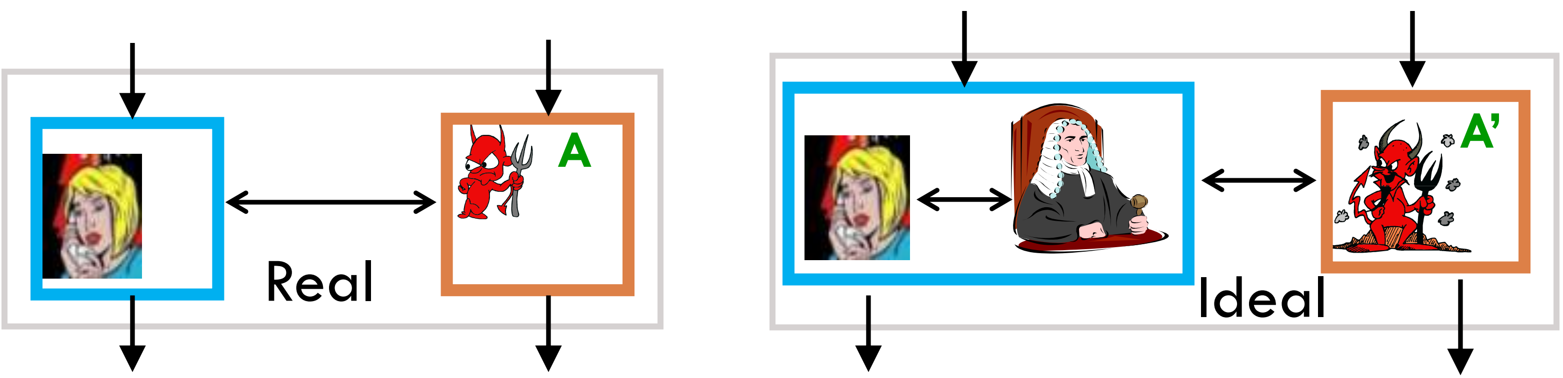
- Canetti et al. [Canetti,Lindell,Ostrovsky,Sahai'02]
  - Classical universal composable SFE protocols
  - Extra set-up: a common random string
  - Proof of security: "hybrid argument"

Real ≈ Real' ≈ Real'' - - · - - · - - ≈ Ideal

  - Defining "imaginary" intermediate protocols that bridge real and ideal protocols
  - Each one obtained by little change from its predecessor, e.g., changing the plaintext of an encryption
  - No rewinding
- Our proposed abstraction: **simple hybrid argument**

Structures of Real/Ideal Executions

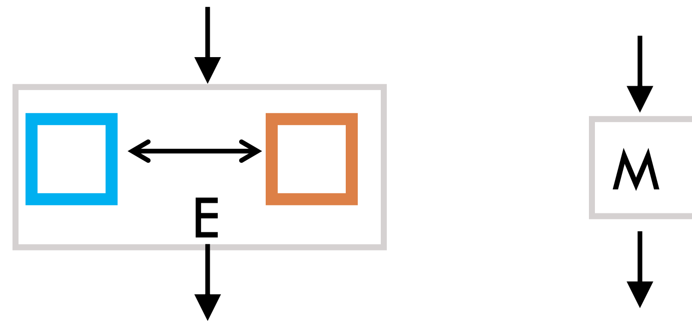
- Call an execution of protocol with an adversary an **experiment**
- Observe: Experiments in real/ideal worlds have similar structures



Describing Experiments by Machines

Denote:

- dishonest player
- world: real/ideal

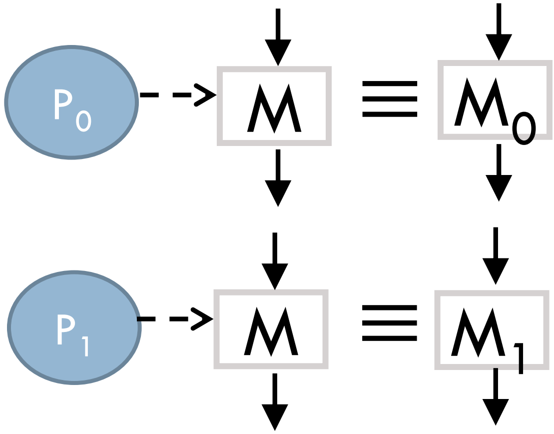


Observation:

- An experiment E is just a (randomized) process that maps input (distribution) to an output (distribution)
- Thus can describe an experiment by a machine M
  - call M the corresponding machine of E
  - will identify an experiment and its corresponding machine, use E/M interchangeably

Simply Related Experiments

- Consider two experiments E_0 and E_1
  - corresponding machines M_0 and M_1
- And consider two indistinguishable probability distributions P_0 & P_1

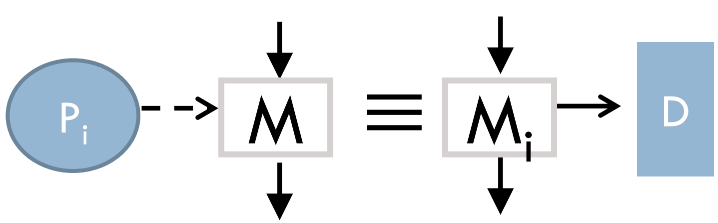


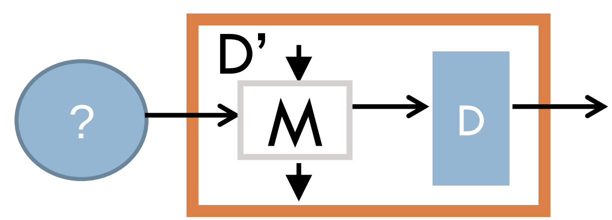
Definition:

- E_0 and E_1 are simply related
  - if there is a machine M
    - taking a sample from either P_0 or P_1 as auxiliary input
    - $M_0 \equiv M(P_0)$, $M_1 \equiv M(P_1)$
    - "$\equiv$" means two machines are the same.

Simply Related Experiments: Property

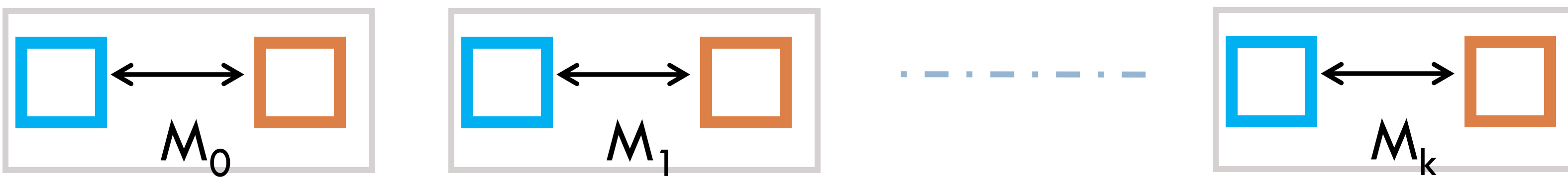
- Suppose M_0 and M_1 simply related
- Consider distinguisher D trying to tell apart M_0 and M_1
  - feed same inputs to M_0 and M_1
  - process the outputs from M_0 and M_1
- Claim: D cannot distinguish M_0 and M_1:
  - $|\Pr[D(M_0) = 1] - \Pr[D(M_1) = 1]| \leq \varepsilon$
- Proof.
  - Because, otherwise, can construct D’ from D that distinguishes P_0 and P_1
  - But P_0, P_1 are indistinguishable by assumption. **Contradiction**!





Simple Hybrid Arguments

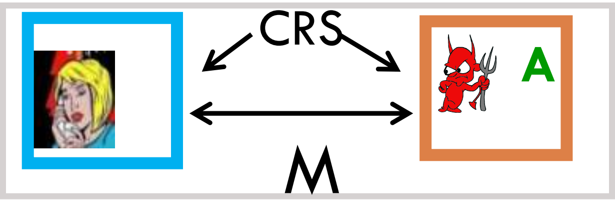
- Two experiments E_0, E_k are related by a simple hybrid argument of length k
- if exist $E_1, \ldots, E_{k-1}$
  - each E_i, E_{i+1} are simply related

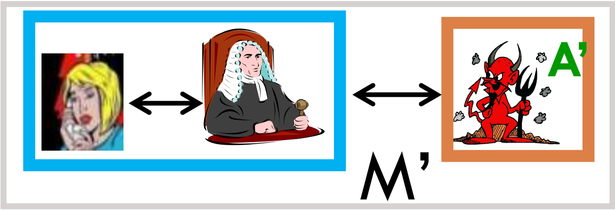


- Claim: ∀ quantum poly-time distinguisher D,
  - $|\Pr[D(M_0) = 1] - \Pr[D(M_k) = 1]| \leq k \cdot \varepsilon$
- **Proof.** By contradiction.
  - otherwise some adjacent machines are distinguishable

Application to [CLOS'02]

∃ UC secure (classical) protocols for any poly-time function f assuming a CRS is available to two parties





Obs.: M, M' are related by a simple hybrid argument

- where each two adjacent experiments are related by
  - switching a public key for a uniformly random string
  - changing the plaintext of an encryption
  - changing the message in the commit phase of a commitment scheme

Application to [CLOS'02] Cont'd

- Three pairs of distributions
  - valid pubic key vs. uniform string ✓
  - encryptions of two messages ✓
  - commitments to two messages ✓
- **Theorem:** ∃ classical SFE protocols for any f that are quantum UC secure given CRS, assuming
  - dense encryption (valid key indist. from uniform string)
  - chosen-plain-text attack (CPA) secure against quantum attackers
  - quantum computationally hiding commitment

Instantiation available based on lattice problems

Putting All Together

- ∃ classical SFE protocols for any f that are quantum UC secure given CRS
  - implies quantum stand-alone secure
- [DL'09]: classical coin-flipping protocol that is quantum stand-alone secure
- Modular composition theorem in our quantum stand-alone model
- Corollary: ∃ classical SFE protocols for any f that are quantum stand-alone secure
  - Generating CRS using [DL'09]

A Few Comments

- One place does not fit simple hybrid argument
  - a witness-indistinguishable proof:
    - Need to show WI proof does not need rewinding to be proven secure;
    - We analyze directly by carefully inspecting existing proofs
    - Similar ideas appeared in concurrent zero knowledge. [Dwork,Naor,Sahai'04]
- [CLOS'02] includes protocols with other properties:
  - More than two parties
  - Adaptive corruptions

We have not verified if these other proofs also fit our abstraction

Conclusion

- Recap:
  - Quantum stand-alone security model
    - Model allows for modular composition
  - Simple hybrid arguments
    - SFE against quantum attacks in CRS model
  - Classical SFE protocols against quantum attacks
    - without set-up assumptions
- Open Questions:
  - Applying simple hybrid framework to other settings
  - Constant round ZK against quantum verifiers
  - Adapting other rewinding techniques to quantum setting

Thank you!

Reference

- [BB’84] C.H. Bennett, G. Brassard "Quantum cryptography: Public-key distribution and coin tossing". Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 1984.
- [BM'05] Michael Ben-Or, Dominic Mayers. “General Security Definition and Composability for Quantum & Classical Protocols”. quant-ph/0409062.
- [C’00] Ran Canetti. “Security and Composition of Multiparty Cryptographic Protocols”. J. Cryptology. 2000.
- [CF’01] Ran Canetti, Marc Fischlin. “Universally Composable Commitments”. Crypto 2001.
- [CLOS’02] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai, “Universally composable two-party and multi-party secure computation”. STOC 2002, pp. 494–503.
- [CSST'05] C. Crepeau, Louis Salvail J.-R. Simard, A. Tapp. “Classical and quantum strategies for two-prover bit commitments”. Manuscript 2005.
- [DL’09] Ivan Damgård, Carolin Lunemann. “Quantum-Secure Coin-Flipping and Applications”. ASIACRYPT 2009.
- [FS’09] Serge Fehr, Christian Schaffner. “Composing Quantum Protocols in a Classical Environment”. TCC 2009.

Reference

- [LC’98] H.-K. Lo, H. F. Chau. “Why Quantum Bit Commitment And Ideal Quantum Coin Tossing Are Impossible”. Physica D120 (1998) 177-187. quant-ph/9711065.
- [LC99] Hoi-Kwong Lo, H. F. Chau. “Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances”. Science 26 March 1999: Vol. 283. no. 5410, pp. 2050 - 2056
- [M’97] D. Mayers. “Unconditonally secure quantum bit commitment is impossible”. Phys. Rev. Lett. 78, (1997) 3414-3417.
- [S'94] Peter W. Shor. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring” FOCS 1994: 124-134.
- [W'09] J. Watrous. “Zero-knowledge against quantum attacks”. J. on Computing, 2009.
- [U’10a] Dominique Unruh. “Universally composable quantum multi-party computation”. EUROCRYPT 2010
- [U’10b] Dominique Unruh. “Quantum proofs of knowledge” April 2010, Preprint on IACR ePrint 2010/212.