

# Classical Cryptographic Protocols in a Quantum World

Fang Song

Joint work with Sean Hallgren and Adam Smith

Computer Science and Engineering  
Penn State University

Are classical cryptographic protocols  
secure against  
quantum attackers?

# Are classical cryptographic protocols secure against quantum attackers?

- Some protocols: no longer secure
  - Computational assumptions broken by efficient quantum alg's
    - Factoring and Discrete Logarithm [Shor'94]
    - Principal ideal problem [Hallgren'02]
  - Information-theoretical classically secure protocol also broken
    - A two prover commitment scheme becomes non-binding [Crepeau, Salvail, Simard, Tapp'06]
    - Attackers only need storing entanglement
- Many protocols: unknown how to prove security
  - Classical proof techniques may no longer apply: e.g. **rewinding**
  - General question: how to reason about quantum adversaries?

# Classical Protocols Secure against Quantum Attacks

---

- Some tasks are achievable
  - Zero-Knowledge (ZK) for NP [Watrous'09]
    - Quantum rewinding in a special case
  - ZK for a larger class of languages [Hallgren,Kolla,Sen,Zhang'08]
  - Coin-flipping [Damgaard,Lunemann'09]
  - Proofs of knowledge (PoK) [Unruh'10]

**Question:** using classical protocols, is every task achievable against classical attackers also achievable against quantum attackers?

- a. proving security of existing protocols
- b. designing new protocols

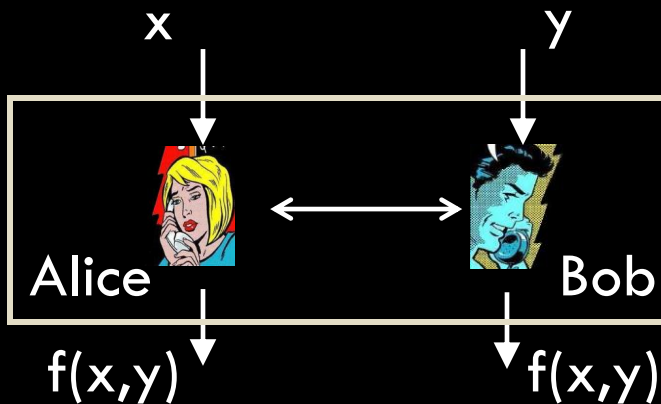
# Our Contribution

---

## Main Result:

$\exists$  classical *secure function evaluation* protocols  
against **quantum** attacks

Parallels classical feasibility results: [Yao'86; Goldreich, Micali, Wigderson'87]



## Secure Function Evaluation (SFE)

- **Correctness:** Jointly evaluate  $f(x, y)$  correctly
- **Privacy:** Bob does not learn anything about  $x$  beyond  $f(x, y)$ ; same for Alice

# Our Contribution

---

## Main Result:

$\exists$  **classical** *secure function evaluation* protocols  
against **quantum** attacks

Parallels classical feasibility results: [Yao'86; Goldreich, Micali, Wigderson'87]

**a.** Prove a family of classical arguments goes through against quantum adversaries

- **Corollary:** *fully simulatable ZKPoK*  $\Rightarrow$  **quantum-secure SFE**

**b.** Construct a fully simulatable **ZKPoK** against quantum adv's

- Get around difficulty of quantum rewinding
- Revisit quantum stand-alone security models (see paper)

# Building SFE from ZKPoK

---

- Identify a family of *hybrid arguments* that goes through against quantum adv's



- Adjacent pairs only differs by “simple” changes:
  - E.g., changing the plaintext of an encryption
- Formalize a **Simple Hybrid Argument** framework
  - Resembles code-based games [Bellare,Rogaway'06]
- A classical construction [Canetti,Lindell,Ostrovsky,Sahai'02] fits SHA framework
  - [CLOS'02]: fully simulatable ZKPoK  $\Rightarrow$  classically secure SFE
- **Corollary:** fully simulatable ZKPoK  $\Rightarrow$  quantum-secure SFE, assuming
  - Quantum-secure dense encryption & pseudorandom generators
  - Implied by, e.g, Learning-with-errors (LWE) assumption

# Our Contribution

---

## Main Result:

$\exists$  classical *secure function evaluation* protocols  
against **quantum** attacks

Parallels classical feasibility results: [Yao'86; Goldreich, Micali, Wigderson'87]

a. Prove a family of classical arguments goes through against quantum adversaries

- **Corollary:** Fully simulatable **ZKPoK**  $\Leftrightarrow$  quantum secure SFE

b. Construct a fully simulatable **ZKPoK** against quantum adv's

- Get around difficulty of quantum rewinding

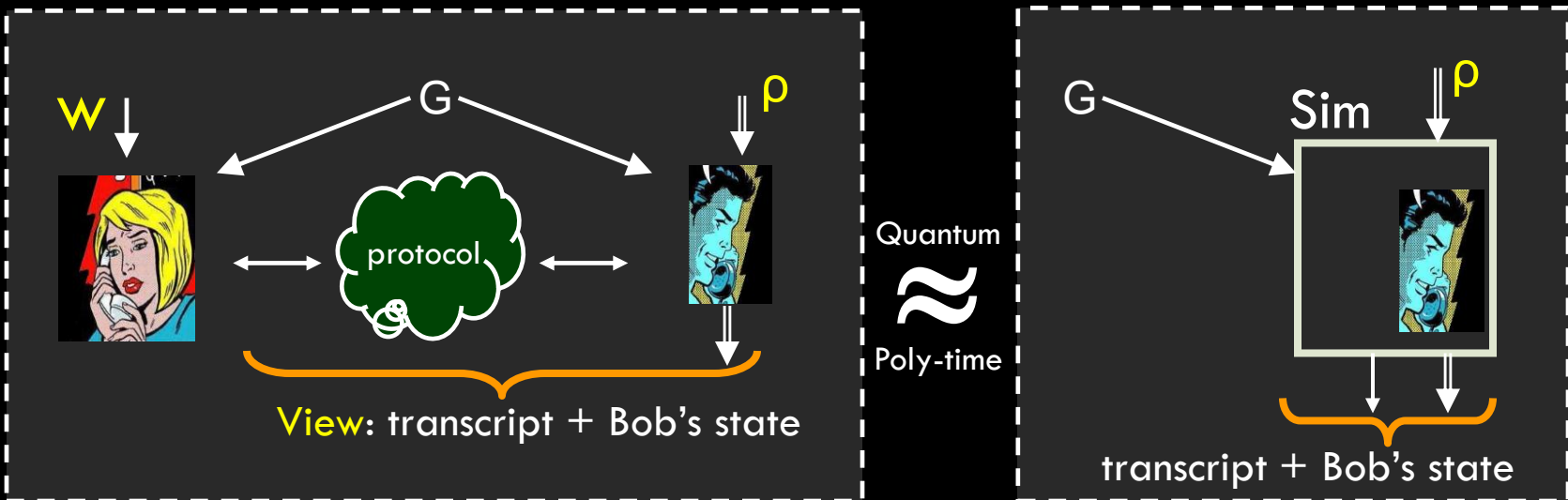
- Revisit quantum stand-alone security models (see paper)



# Formalizing Zero-Knowledge

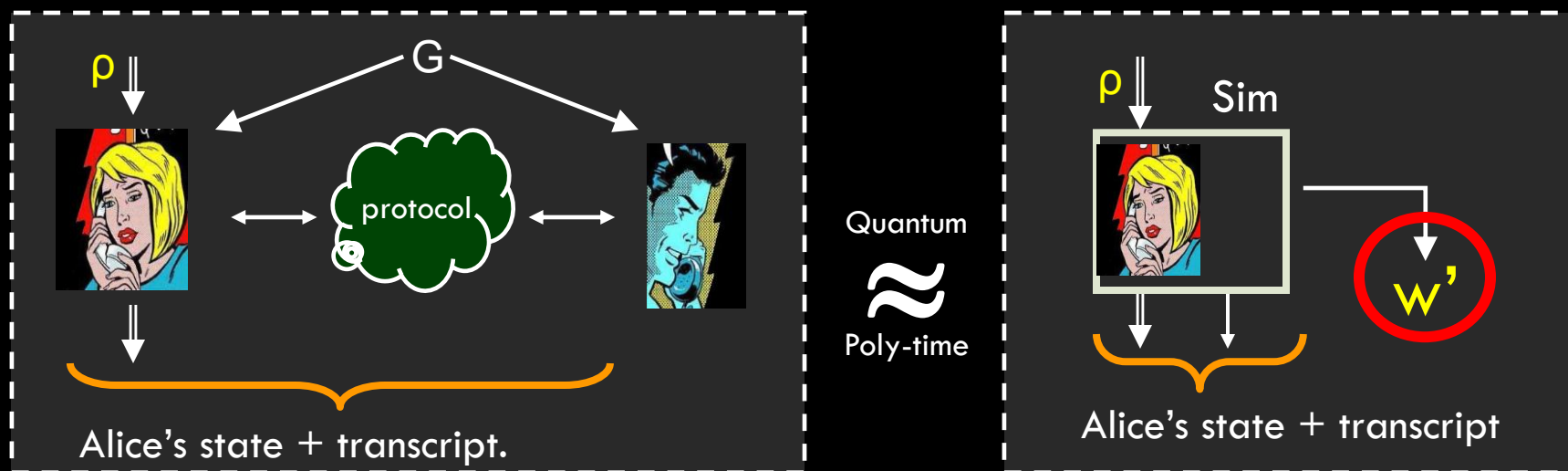
Alice wants to convince Bob graph  $G$  is 3-colorable

- **Zero knowledge:** Bob does NOT learn the coloring  $w$
- $\forall$  Bob,  $\exists$  **Simulator** such that  $\forall$  quantum state  $\rho$ :



# Formalizing Proofs of Knowledge

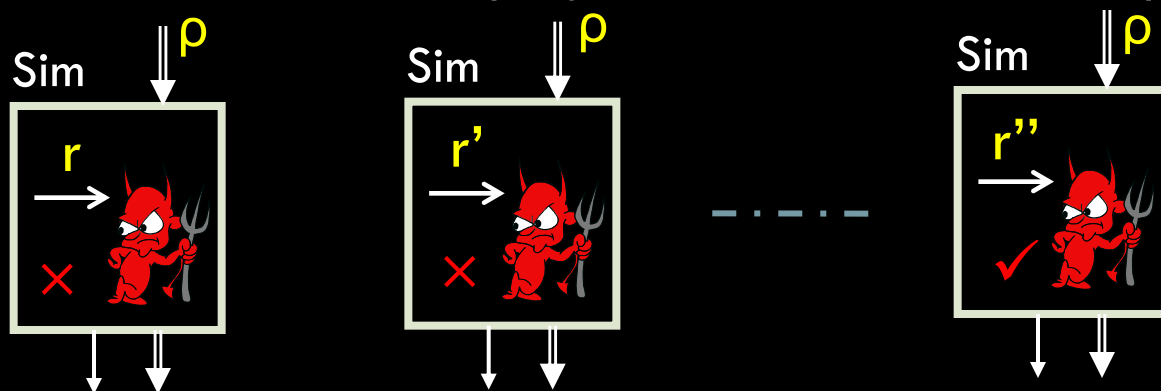
- PoK: Bob wants to be sure that Alice has some real  $w$  in mind
- $\forall$  Alice,  $\exists$  Simulator such that  $\forall$  quantum  $\rho$



- Extra condition on simulator: if simulated transcript accepts, then **extracting** a 3-coloring  $w'$  of  $G$ .
  - "Witness-extended simulator"
- **Fully simulatable:** Simulation + Extraction

# Difficulty of Quantum Rewinding

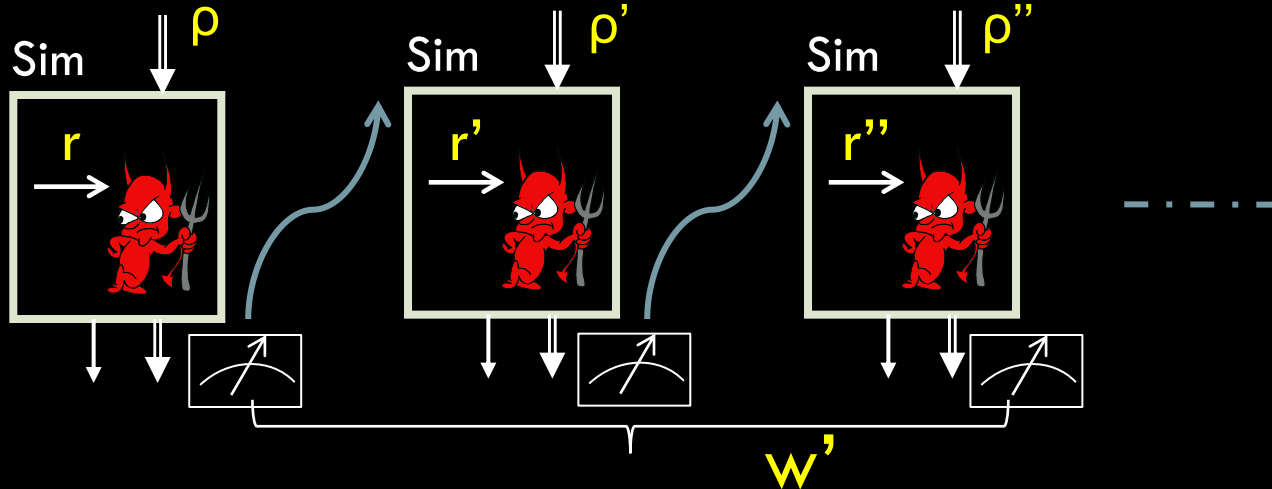
- Classical technique to construct a simulator: **Rewinding**
  - In every real interaction, prover answers questions from verifier
  - Without a witness, simulator may not be able to answer all questions
  - Pick a random branch from all interactions, check if could proceed
  - If NOT, “rewind” and try again from the **same** auxiliary input  $\rho$



- Naïve rewinding requires taking a snapshot of the adversary's state and later returning to it
  - **Quantum no-cloning!**
  - Even just checking success/failure may destroy  $\rho$

# Watrous's Rewinding Technique & Limit

- **Theorem** [Watrous'09]:  $\exists$ ZK proof for **NP** against quantum verifiers.
- “Oblivious” quantum rewinding
  - If: probability of succ/failure independent of  $\rho$
  - Then: safe to go back; but cannot remember anything

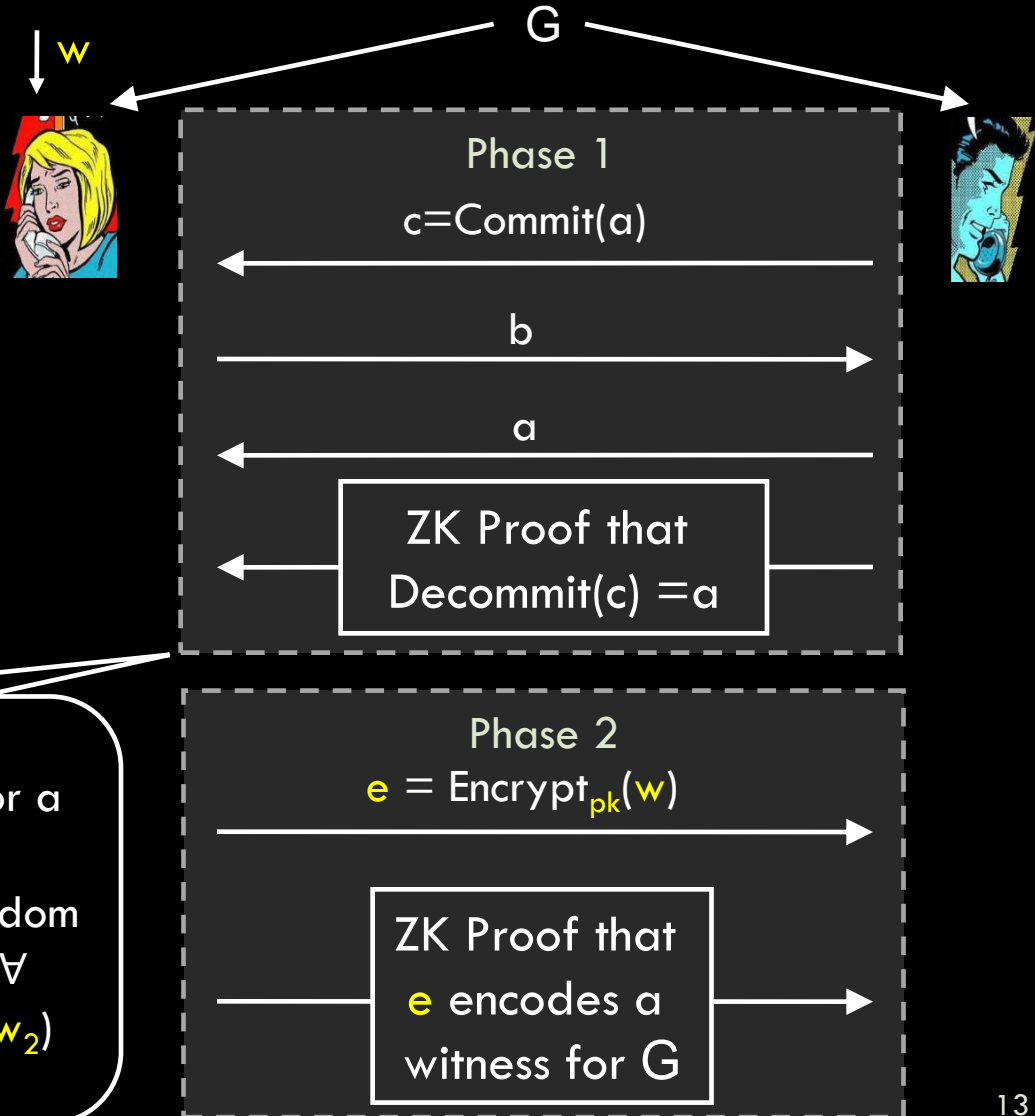


- **However, NOT** enough for **PoK**: Simulation + **Extraction**
  - Collecting answers from multiple branches
  - Mere extraction is possible [Unruh'10]
  - Unclear how to do **both** simultaneously

# Fully Simulatable ZKPoK: Our Construction

Idea (inherited from Non-interactive ZK):

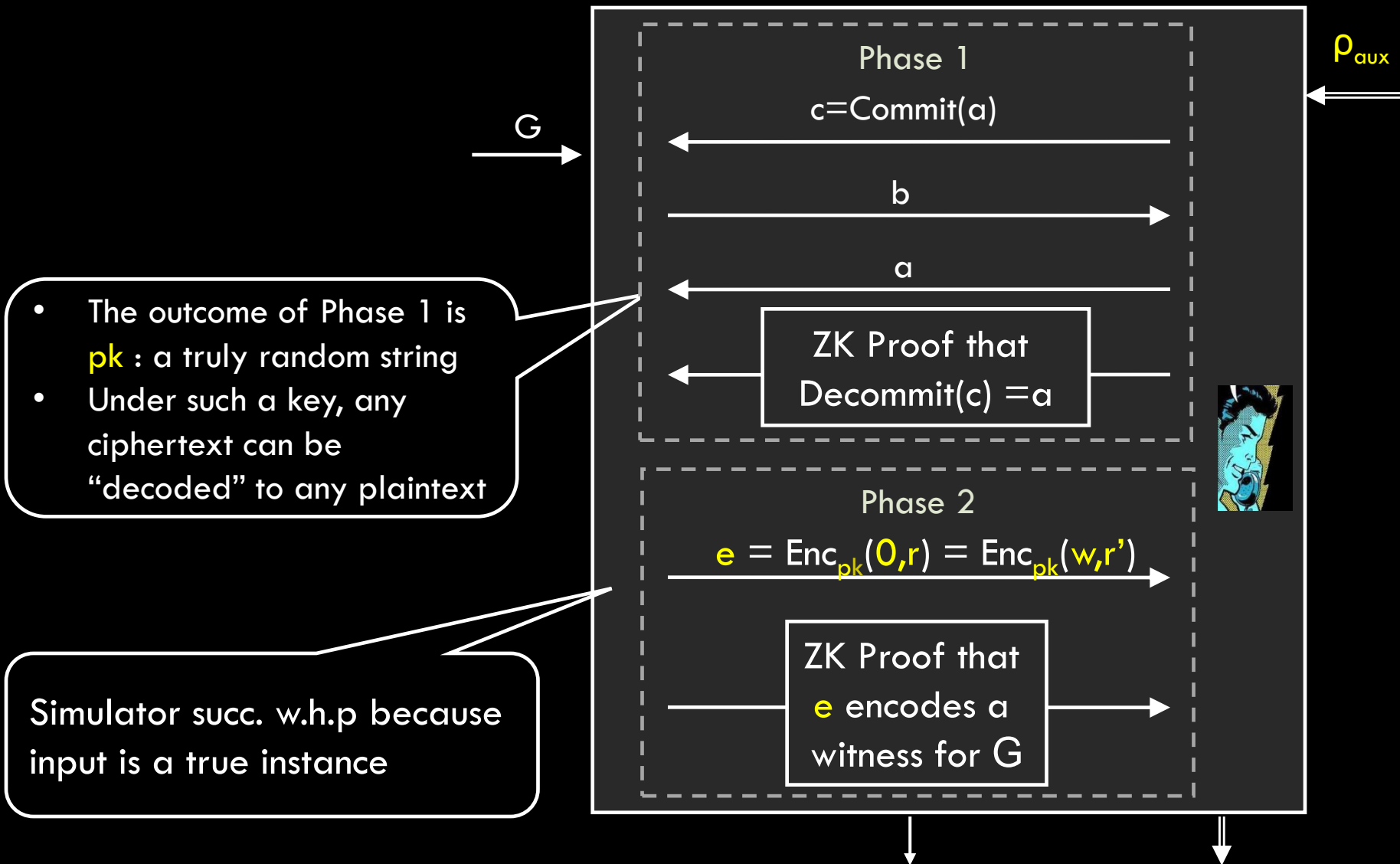
- Start with a “coin-flipping” preamble
  - Honest prover can make sure the outcome is **uniformly random**
  - A PoK simulator (playing the verifier) can **control** the outcome



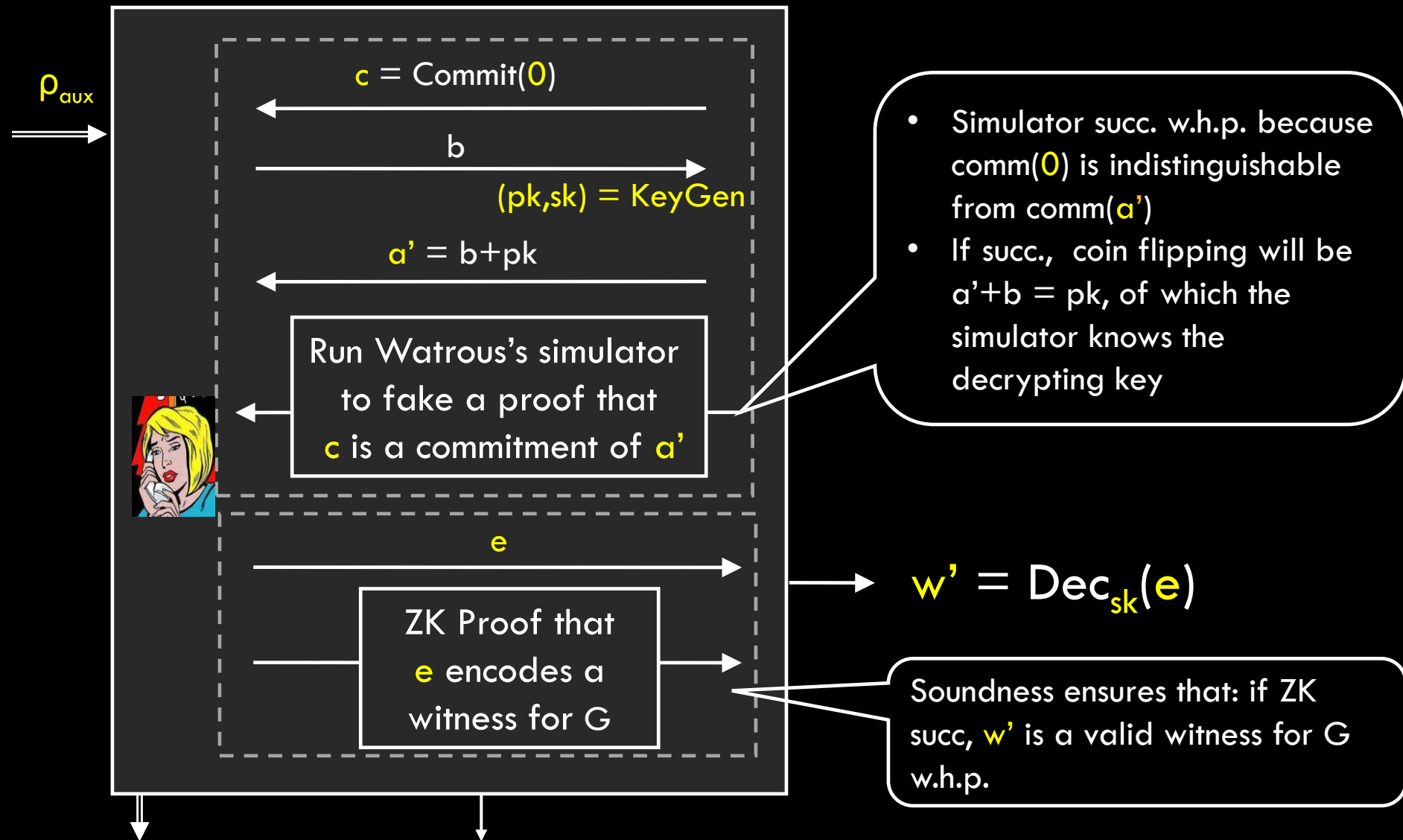
$pk = a+b$ : interpret as public key for a special encryption scheme

- **Dense**: valid public key looks random
- **Lossy**: if  $pk$  is truly random, then  $\forall w_1, w_2 \text{ Encrypt}_{pk}(w_1) \equiv \text{Encrypt}_{pk}(w_2)$

# ZK: simulating dishonest verifiers



# PoK: simulating dishonest provers



# Putting It All Together

- Recap:
  - Fully simulatable ZKPoK  $\Leftrightarrow$  quantum-secure SFE
  - $\exists$  Fully simulatable ZKPoK Protocol
- **Corollary 1**: Modular composition  $\Leftrightarrow$  Quantum-secure SFE in plain model (i.e., no trusted set-up) assuming quantum-secure
  - dense & lossy encryption
  - pseudorandom generator
- **Corollary 2**: An interesting equivalence: CF = ZKPoK
  - Round-complexity preserving reductions
- Independent Work [Lunemann, Nielsen'11]
  - Fully simulatable quantum-secure coin-flipping
  - Plug into [GMW'87] and obtain similar feasibility results as ours
- What I didn't talk about our work: Models, UC-security etc. (see paper)



# Conclusion

- Some key pieces of classical crypto unchanged in presence of quantum attackers
- A lot more remains unclear...
- Open Questions:
  - Can we extend to other settings: e.g., multi-party and concurrent security?
  - Round complexity:  $\exists$  quantum-secure constant round ZK/CF?
  - Is there any natural two-party classical protocol that is broken by quantum adv's **NOT** because of computational assumptions?

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.
- [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. "Unconditionally 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. "Quantum proofs of knowledge" April 2010, Preprint on IACR ePrint 2010/212.
- [U'10b] Dominique Unruh. "Universally composable quantum multi-party computation". EUROCRYPT 2010