Unconditionally secure quantum commitments with preprocessing

Luowen Qian
Boston University

arXiv:2311.18171

Why unconditional security?
(according to cryptographers @ MIT)

“Cryptographers seldom sleep well.” –Silvio Micali

“Their careers are frequently based on very precise complexity-theoretic assumptions, which could be shattered the next morning.” –Joe Kilian (1988)

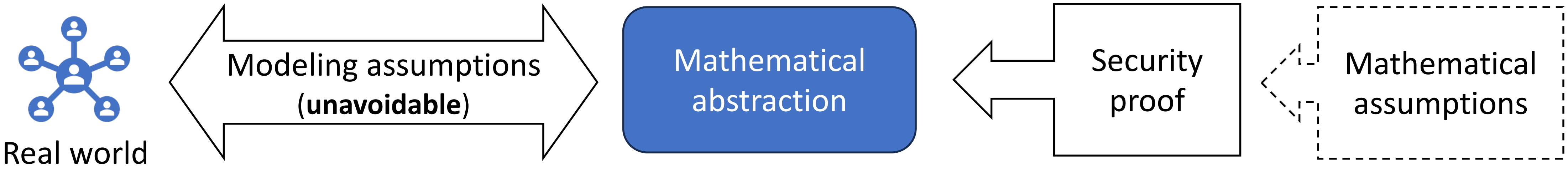
Unconditional security is cryptographers’ ultimate dream!

What is unconditional security?

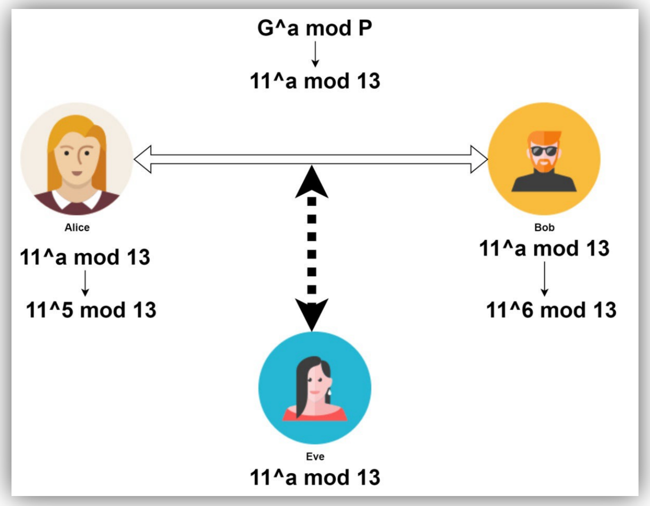
- Conditional security: depends on <u>mathematical assumptions</u>
- Unconditional security: proof without mathematical assumptions

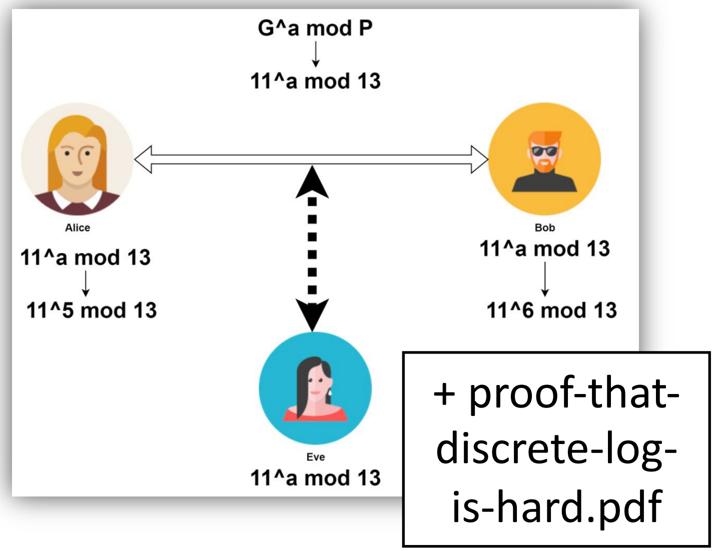
Related concepts concerning <u>modeling attackers</u>:

- Information-theoretic (statistical) security: 💪 against attackers that can perform arbitrary computations (can even solve halting)
- Computational security (standard): 👑 against attackers with a polynomial amount of computational resources



Examples





One-time pad
is an unconditional statistically secure encryption scheme

Diffie-Hellman (as-is)
is a conditional computationally secure key-exchange scheme

Diffie-Hellman with a hypothetical proof
would be an unconditional computationally secure key-exchange scheme

Image: Crypto Museum and InfoWorld

Classical cryptography feasibility matrix

Too strong!

Avoid!

Security proof	Statistically possible 🦄	Only computationally possible 👑
Unconditional	✓	🚧 "P $\stackrel{?}{=}$ NP" 🚧
Conditional	(unnecessary)	✓

*Because of this diagonal matrix, for all practical purposes unconditional security ≈ statistical security (*classically*)

Quantum cryptography feasibility matrix

Still too strong!

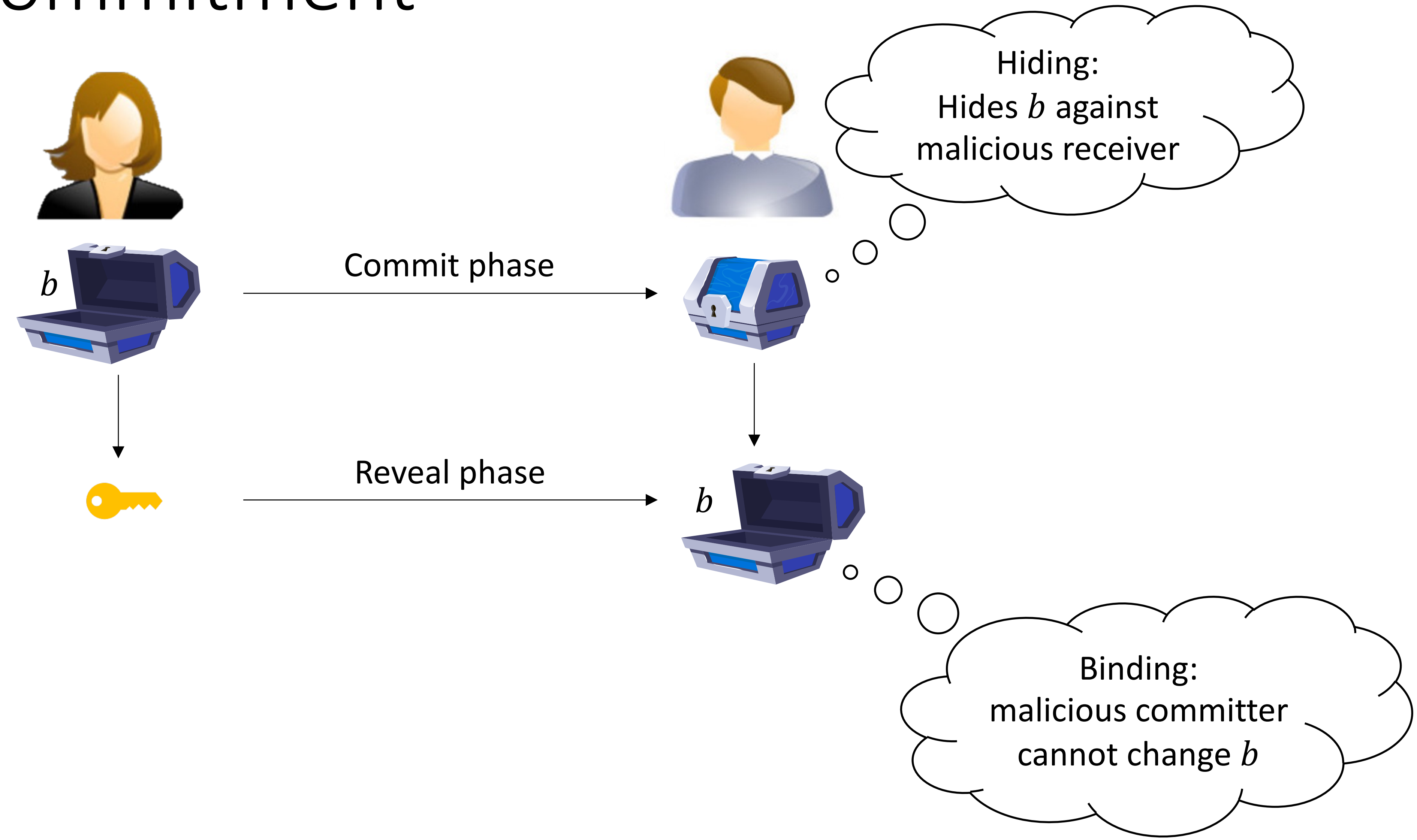
Cryptographic task / Security proof	Statistically possible 🦄	Only computationally possible 👑
Unconditional	✓	???
Conditional	(unnecessary)	✓

Avoid!

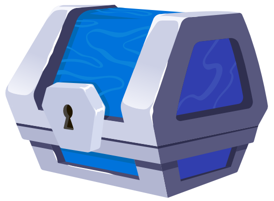
Can we get unconditional computationally secure quantum cryptography?

spoilers: yes*

Bit commitment



Why (quantum) commitments?

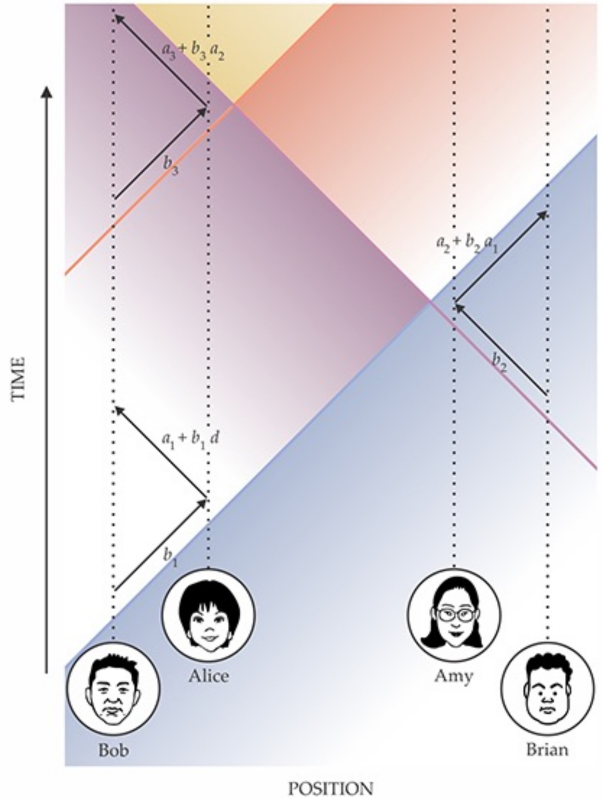


1. **Central**: existential equivalence to many other tasks
   - <u>Other quantum cryptography</u>: oblivious transfer (OT), secure multiparty computation (MPC), zero knowledge (ZK)…
     [Bartusek-Coladangelo-Khurana-Ma'21, Ananth-Q-Yuen'22, Brakerski-Canetti-Q'23]
   - <u>Hardness of quantum information tasks</u>: compression, channel decoding, entanglement distillation, black hole radiation decoding…
     [Brakerski'23, Bostanci-Efron-Metger-Poremba-Q-Yuen'24]
2. "**Easiest**": constructible from almost any computational cryptography
   - Post-quantum one-way functions
   - Quantum pseudorandomness, quantum encryptions, quantum money…
     [AQY'22, Morimae-Yamakawa'22, BCQ'23, Khurana-Tomer'24, Ma-Q-Raizes-Zhandry]

Pursuit of unconditional commitments

- Conceptualized circa ’81, formalized in Brassard-Chaum-Crepeau’88
- Classical commitments require OWFs, thus $\mathrm{P} \neq \mathrm{NP}$ [Impagliazzo-Luby’89]
- Statistical quantum commitment *proposals and attacks* [Brassard-Crépeau’90, Brassard-Crépeau-Jozsa-Langlois’93, Mayers’95, …]
  - Statistical quantum commitment impossibility [Mayers’97, Lo-Chau’97]
- Statistical relativistic commitments [Kent’99, …]
  - Statistical quantum relativistic OT/MPC still impossible [Rudolph’02; Colbeck’06]

Image: Quantum Technologies



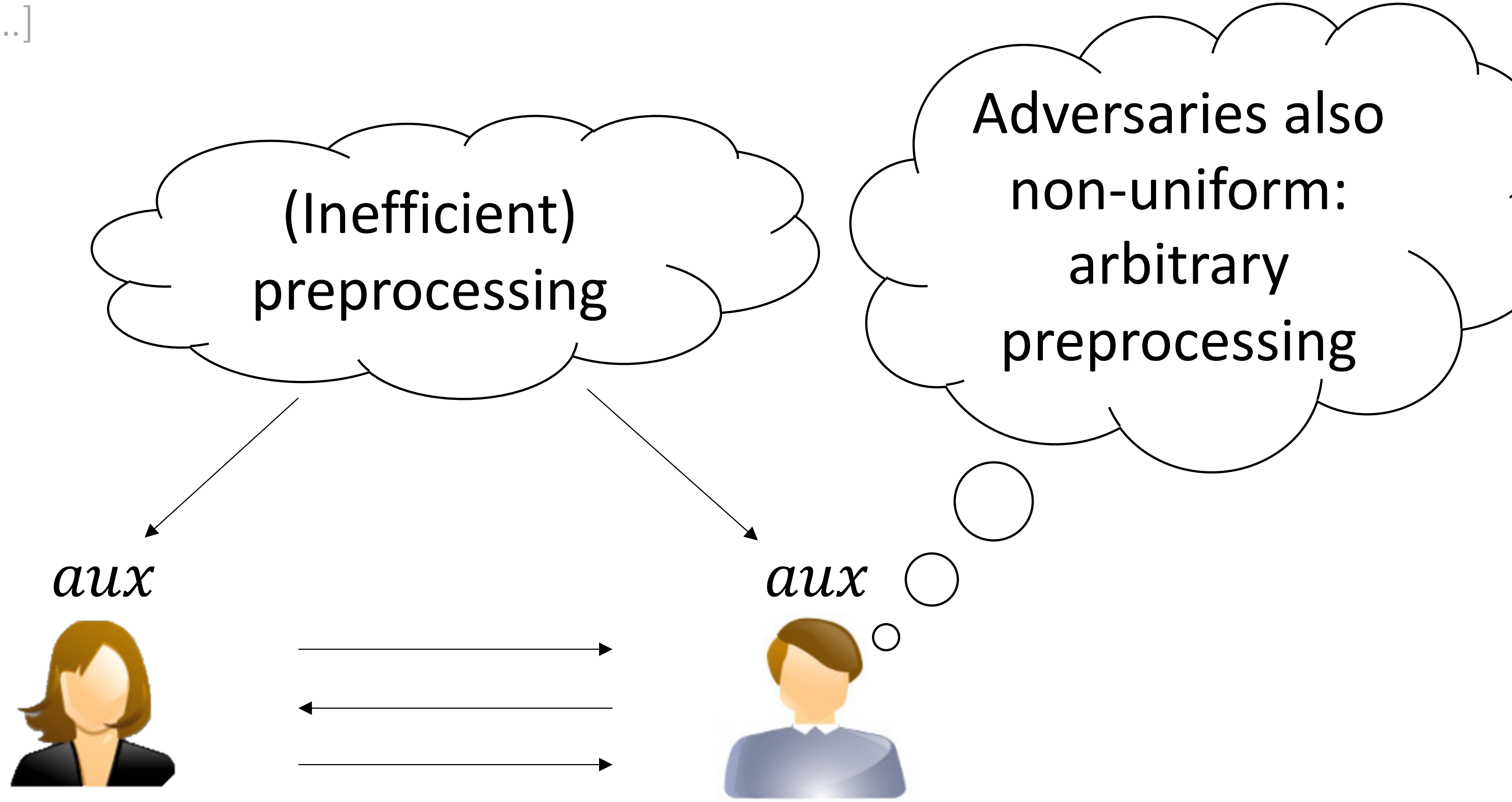
Quantum computational commitments

- Quantum commitments from new quantum assumptions [Chailloux-Kerenidis-Rosgen'11, Kawachi-Koshiba-Nishimura-Yamakami'12]
  - ❖Unclear how these compare to OWFs
- Separation of quantum commitments from $\mathrm{P} \neq \mathrm{NP}$ and more [Kretschmer'21, Ananth-Q-Yuen'22, Morimae-Yamakawa'22, Kretschmer-Q-Sinha-Tal'23, Lombardi-Ma-Wright'24]
  - ❖Underlying assumptions are either "contrived" or not concrete

Computationally secure quantum commitment could still be unconditional?

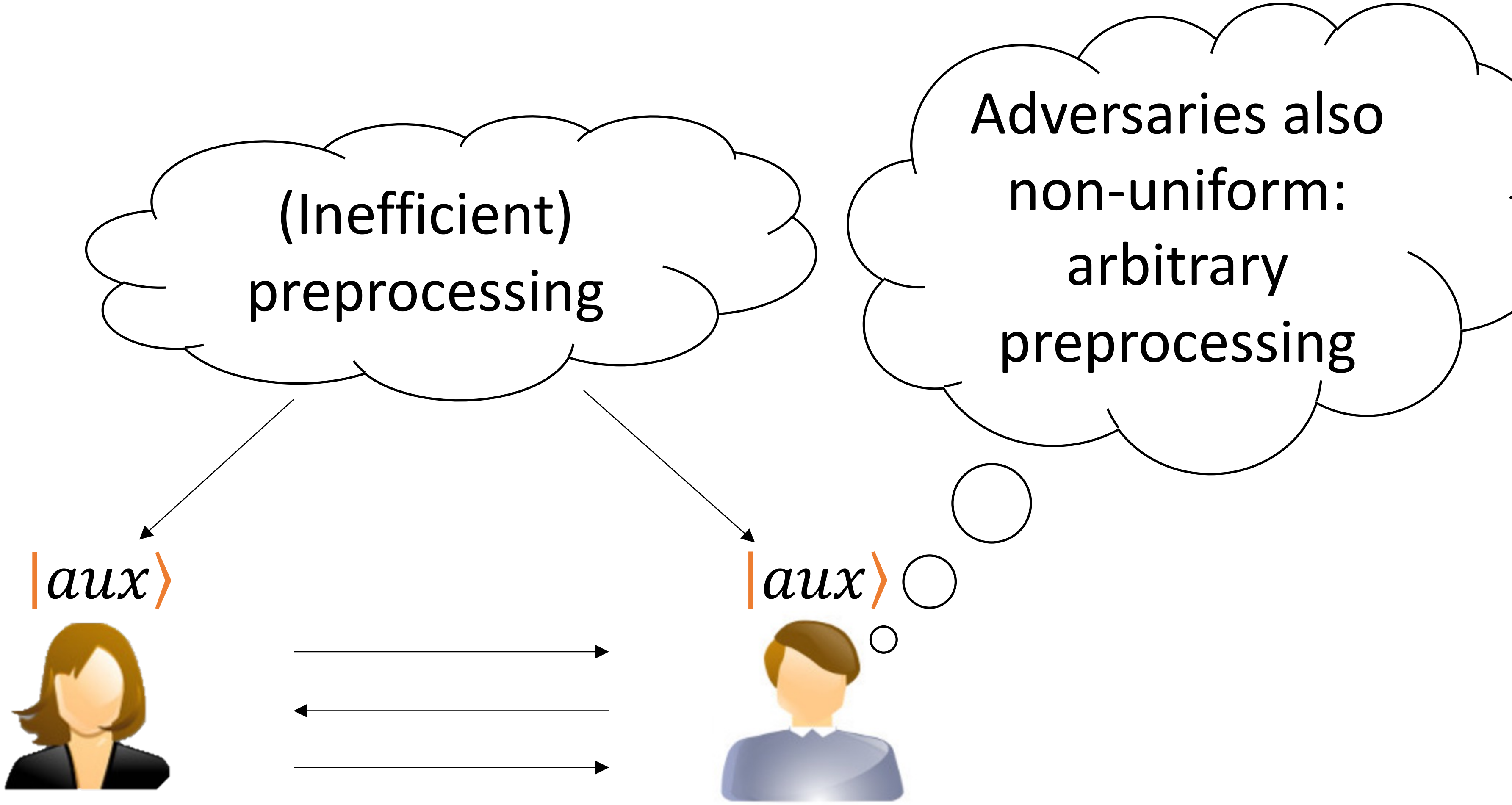
Auxiliary-input (non-uniform) cryptography

[Ostrovsky-Widgerson'93, …]



("P $\stackrel{?}{=}$ NP" barrier still applies)

Quantum auxiliary-input cryptography



Main theorem

Unconditionally, there exists a quantum auxiliary-input commitment scheme with inverse exponential security error that is:

- Statistically binding against (unbounded) committer
- Computationally hiding against exponential-size receiver

❖ Non-interactive
(one-message commit phase + one-message reveal phase)

❖ Preparing $|aux\rangle$ takes at most uniform doubly-exponential time

(can be further applied for MPC: secure multiparty computations)

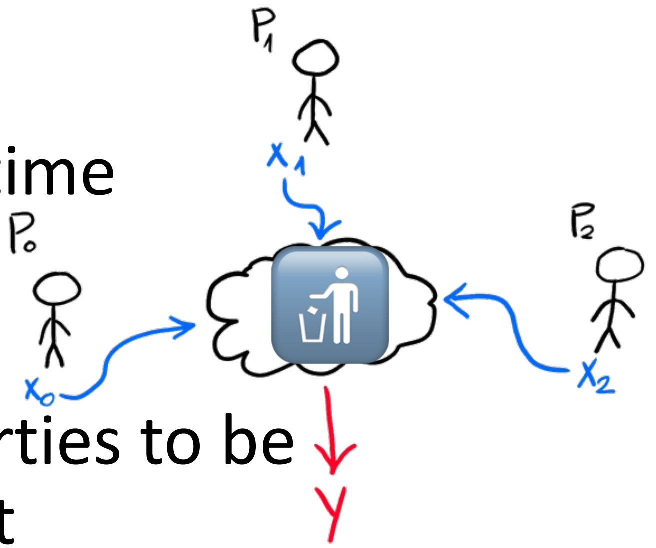
*concurrent with Morimae-Nehoran-Yamakawa

Exponential-time preprocessing means it is practically irrelevant, right?

Well, you could pick a smaller security parameter... (48? so that preprocessing time is at most 2 years)

Image: [Cronokirby]

Application: high-stakes MPC



- **Preprocessing phase**: All parties run in exponential time (independent of their inputs)
  - Adversaries are unbounded
- **Online phase**: (after obtaining inputs) enforce all parties to be polynomial time by enforcing a reasonable time limit
  - Adversaries also must be efficient

❖After protocol concludes, one party may be able to recover others' private inputs if they spend exponential time (inherent limit of computational security)

➢Use a commitment combiner with another post-quantum scheme with a larger security parameter (say 512 bits instead of 48)

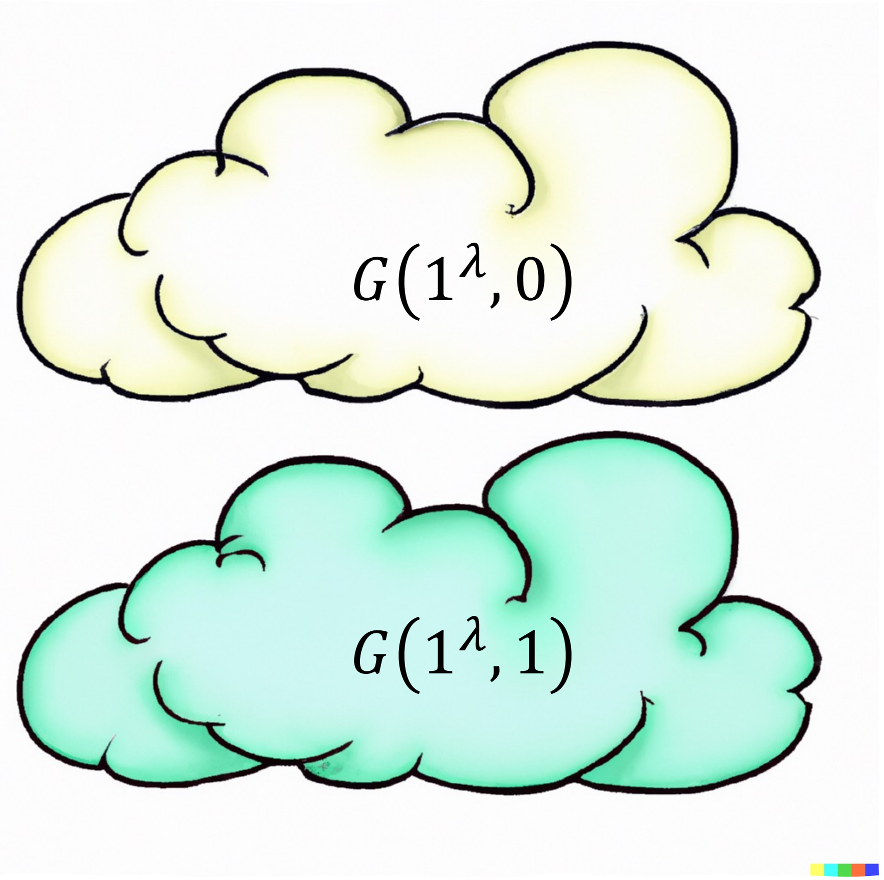
➢"Certified everlasting transfer" secrets to a trusted referee [Bartusek-Khurana'23]

Roadmap

✓ Main theorem
- Construction with trusted $|aux\rangle$
- Variation 1: prepare $|aux\rangle$ with efficient (stateful) trusted setup
- Variation 2: prepare $|aux\rangle$ with exponential communication
- Improved classical impossibility
- Future directions & conclusions

EFI pairs (of quantum states)

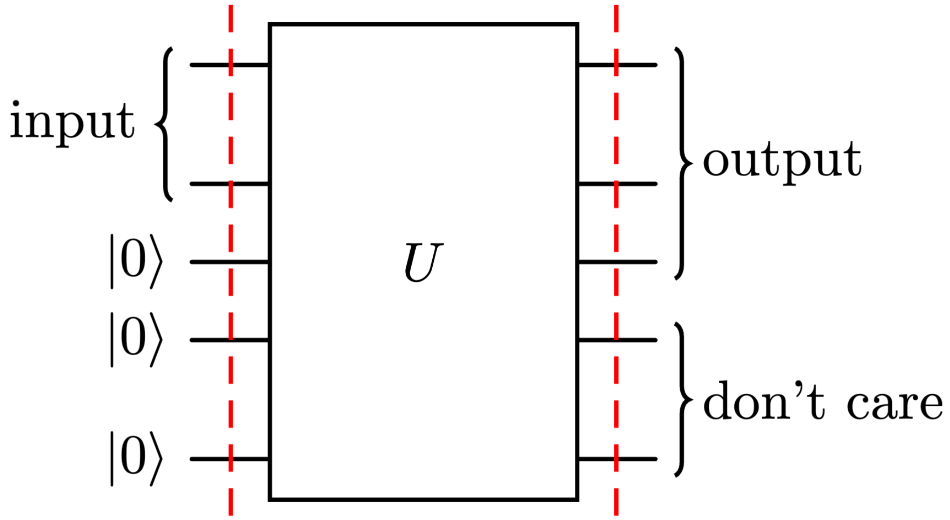
[Brakerski-Canetti-Q'23]



- **E**fficient generation: $G(1^\lambda, b)$ is an efficient quantum algorithm sampling an arbitrary mixed state (distribution over pure states)
- Statistical **F**arness: $G(1^\lambda, 0)$ vs $G(1^\lambda, 1)$ are inefficiently distinguishable
- Computational **I**ndistinguishability: $G(1^\lambda, 0) \approx_c G(1^\lambda, 1)$ are indistinguishable against any quantum polynomial-time algorithms

Stinespring's dilation theorem (1955)

- Every classical deterministic computation can be written in a "reversible form":
  add auxiliary wires, apply reversible gates, remove auxiliary wires
- Every quantum computation can be written in a "unitary form":
  add auxiliary registers, apply unitary gates, remove auxiliary registers

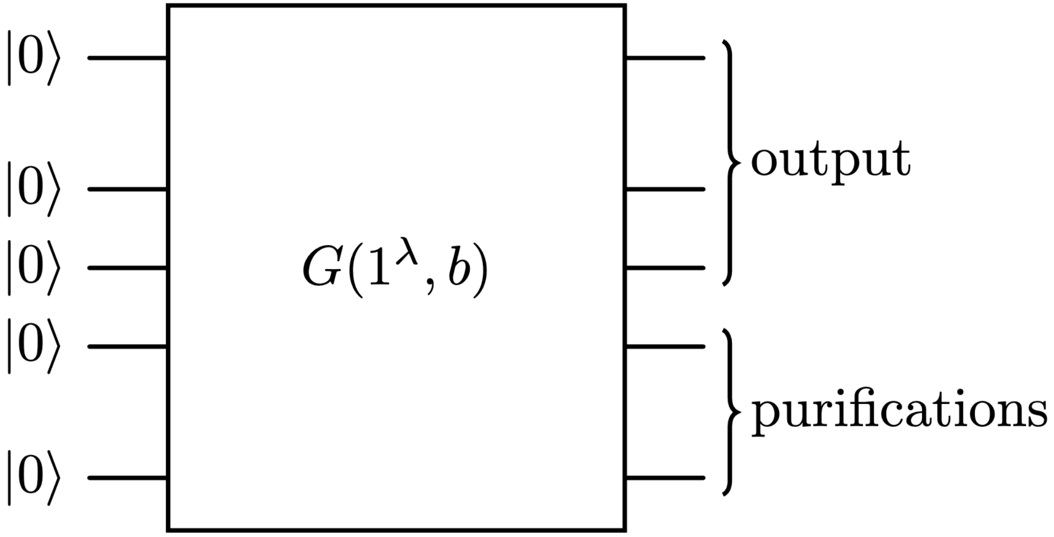


EFI circuit in unitary form

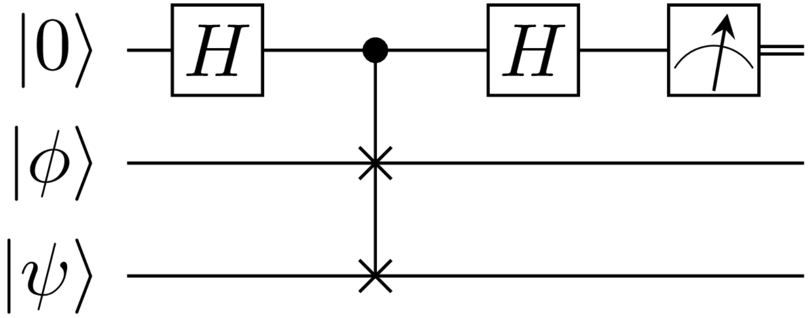
How does a quantum unitary circuit generate randomness?

Randomness is caused by ignorance to purifications

- With access to purifications, the overall state is pure (deterministic)



Fact: "SWAP test" algorithm* can efficiently test equality of two *unknown* <u>pure</u> states



*Barenco-Berthiaum-Deutsch-Ekert-Jozsa-Macchiavello'97

Quantum commitments from EFI pairs

Canonical form commitment [Chailloux-Kerenidis-Rosgen'11, Yan-Weng-Lin-Quan'15, Yan'22]

$b \in \{0,1\}$

$|\psi^{(b)}\rangle_{\mathrm{OP}} \xrightarrow{\text{Commit}} \psi_O^{(b)} = G(1^\lambda, b)$

$\psi_P^{(b)} \xrightarrow{\text{Reveal}} |\psi^{(b)}\rangle_{\mathrm{OP}}$

SWAP test with $|\psi^{(b)}\rangle$

- Computational hiding = computational indistinguishability
- Statistical binding: statistical farness $\Rightarrow$ b is statistically determined

$|aux\rangle$ commitment from ~~E~~FI pairs

[Chailloux-Kerenidis-Rosgen'11]

$b \in \{0,1\}$

$|\psi^{(b)}\rangle_{\mathrm{OP}} \xrightarrow{\text{Commit}} \psi_O^{(b)} = G(1^\lambda, b)$

$\downarrow \qquad\qquad \downarrow$

$\psi_P^{(b)} \xrightarrow{\text{Reveal}} |\psi^{(b)}\rangle_{\mathrm{OP}}$

SWAP test with $|\psi^{(b)}\rangle$

➢ *Only* preparing $|\psi^{(b)}\rangle$ is inefficient

$$|aux\rangle = |\psi^{(0)}\rangle \otimes |\psi^{(1)}\rangle$$

Where do we find ~~E~~FI pairs?

- CKR11: from $\mathrm{QMA} \not\subseteq \mathrm{QIP}$
- This work: *unconditional*

Unconditional ~~E~~FI pairs?

Q: Unconditional ~~E~~FI pairs of classical Distributions?

A: An expanding random function $H: [N] \to [N^3]$ is an inefficient classical pseudorandom generator [Goldreich-Krawczyk'92]

- Fix a distinguisher circuit
- Exponential concentration $\exp(-N)$ via Chernoff's bound
- Apply union bound over all $\exp(N)$ exponential-size circuits

⇒ A random function is pseudorandom with high probability

Generalizes to quantum circuits without quantum advice

Non-uniform quantum adversaries can run multiple circuits in superposition

Post-quantum sparse pseudorandomness

$H: [N] \to [N^3]$ is an inefficient pseudorandom generator against quantum non-uniform circuits (with quantum advice)?

1. Invoke non-uniform QROM security [Chung-Guo-Liu-Q'20, Liu'23]
   - Random functions are pseudorandom against quantum advice even if they could query the random function oracle during execution phase
   - Underlying proof is general and more algorithmic: multi-instance interactive game, compressed oracle, quantum rewinding
2. A more GK-style algebraic proof [Ma (private communication)]
   - Same idea as GK but use a matrix Chernoff's bound for spectral norm
   - Less general but slightly tighter security: $\sqrt{S/N}$ instead of $\sqrt[3]{S/N}$ (matches GK classical bound: sqrt loss from Hoeffding's bound)

Putting pieces together

Takes doubly-exponential time, or exponential time if $\mathrm{P} = \mathrm{PSPACE}$

Fix a good function H (lexicographically smallest):

$$\left|\psi^{(0)}\right\rangle \propto \sum_{x\in\{0,1\}^\lambda} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}} \qquad (4\lambda \text{ qubits in total})$$

$$\left|\psi^{(1)}\right\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}} \qquad (\text{efficient})$$

$b \in \{0, 1\}$

$$\left|\psi^{(b)}\right\rangle_{\mathrm{OP}} \xrightarrow{\text{Commit}} \psi_O^{(b)} = G(1^\lambda, b)$$

$$\psi_P^{(b)} \xrightarrow{\text{Reveal}} \left|\psi^{(b)}\right\rangle_{\mathrm{OP}}$$

SWAP test with $\left|\psi^{(b)}\right\rangle$

Instantiating quantum auxiliary input

- Variation 1: prepare $|aux\rangle$ with efficient (stateful) trusted setup
  - Need to prepare: $\left|\psi^{(0)}\right\rangle \propto \sum_{x\in\{0,1\}^\lambda}|H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ for a random function H
  - If H is a random oracle, this can be prepared efficiently with 1 quantum query
  - ➢ Use Zhandry's compressed oracle to statefully simulate a random function
  - ➢ Statistically hiding if # of copies prepared is polynomial
- Variation 2: prepare $|aux\rangle$ with exponential communication
  - ➢ Naïve approach: ask one party to prepare copies of $\left|\psi^{(0)}\right\rangle$ for both

    Efficiently broken! (using compressed oracles again)
  - ➢ A step back: jointly pick a random function H and prepare $\left|\psi^{(0)}\right\rangle$ separately

Image by DALL·E

Jointly picking H

Issue: How do parties agree on the random function H without trusting each other?

Solution: ask the committer to pick H

- Computational hiding against receiver if committer is honest
- Statistical binding against committer if H is expanding

Reflection

- Classical cryptography stops at inefficient pseudorandomness (not cryptographically useful)
- Quantum cryptography can further achieve commitments with preprocessing through purification and SWAP tests

Paradoxically, quantum auxiliary input (or advice) helps cryptographers more than adversaries

Can randomized advice be useful?

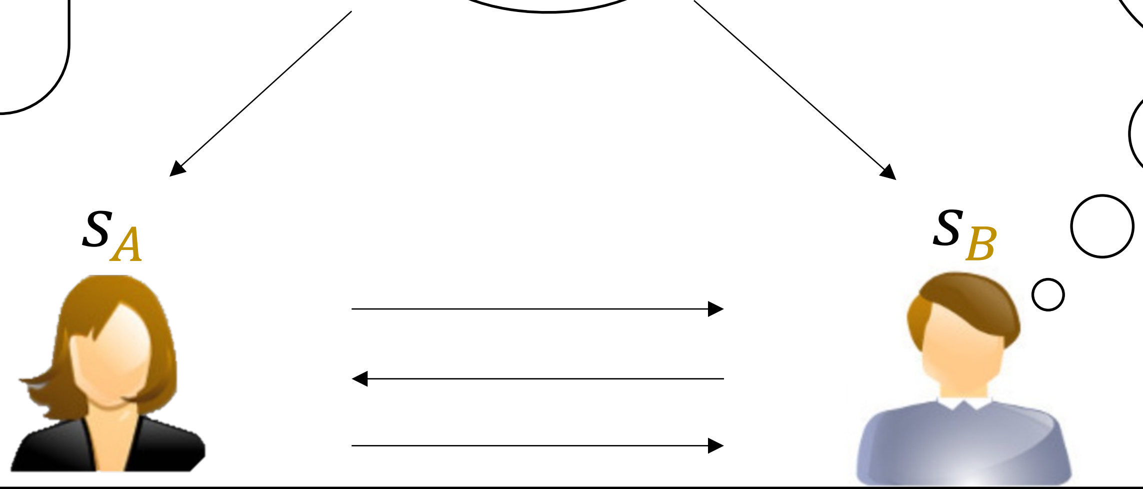
(Raz'05: $\mathrm{QIP}/\mathrm{qpoly} = \mathrm{IP}/\mathrm{rpoly} = \mathrm{ALL}$)

Randomized auxiliary-input cryptography

Public randomized advice can be derandomized through averaging argument

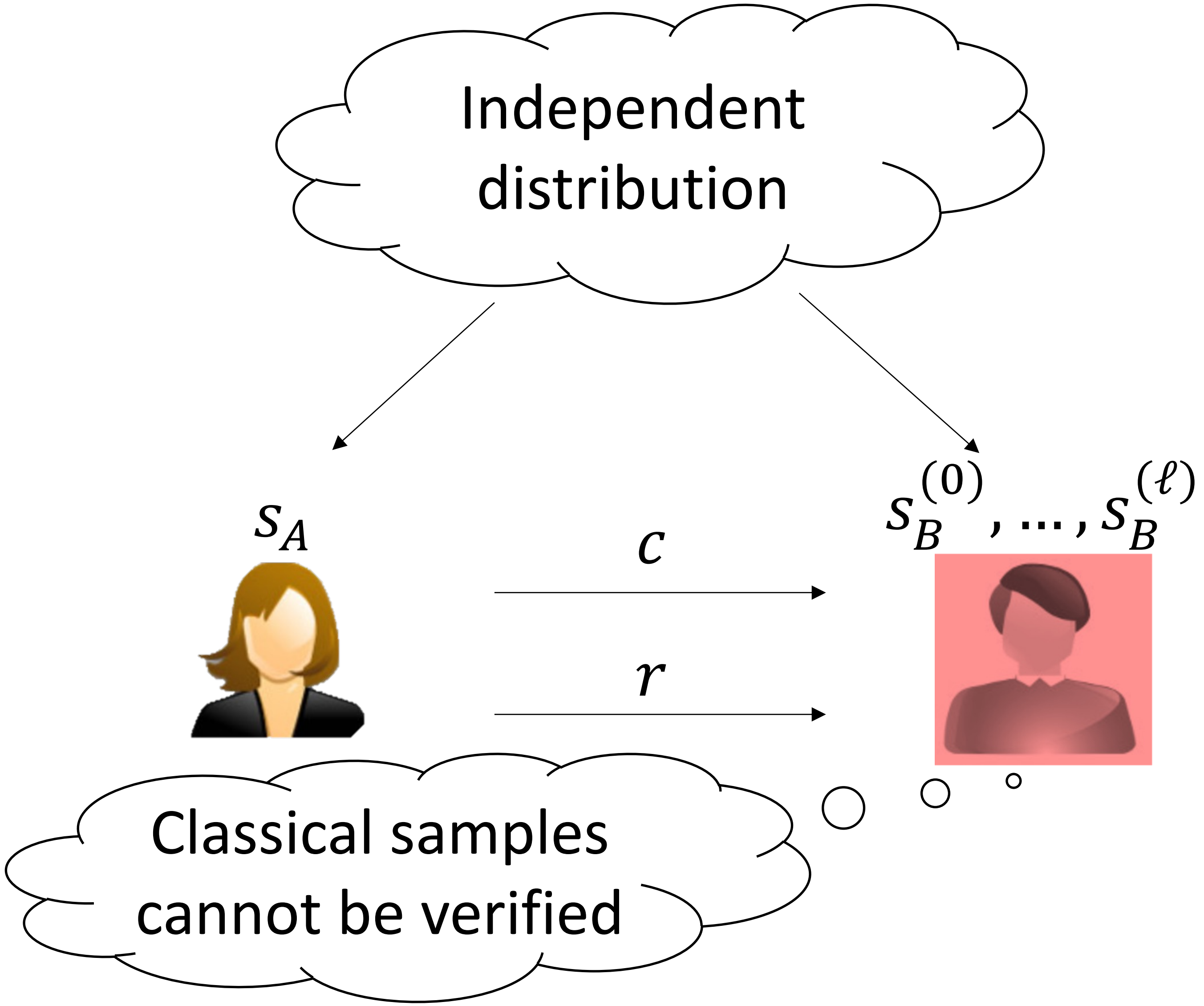
Independent distribution

Adversaries also non-uniform: arbitrary preprocessing



Example (Naor non-interactive commitment):
$s_A = s_B =$ a good receiver's "first message"

Impossibility of randomized commitments



With high probability,

- If 0 was committed, by completeness:
  $\exists r \colon \mathrm{Accept}\left(c, r, s_B^{(i)}, 0\right)$
- If 1 was committed, by statistical binding:
  $\forall r \colon \neg\mathrm{Accept}\left(c, r, s_B^{(i)}, 0\right)$

Therefore, an NP algorithm can efficiently break hiding with just a few samples

Conclusions

- Quantum computational advantage through cryptography if $\mathrm{P} = \mathrm{NP}$
- First demonstration of useful cryptography with unconditional inherently-computational security
- Reassess the necessity of computational assumptions and the existence of barriers for quantum cryptography

Thank you! Questions?

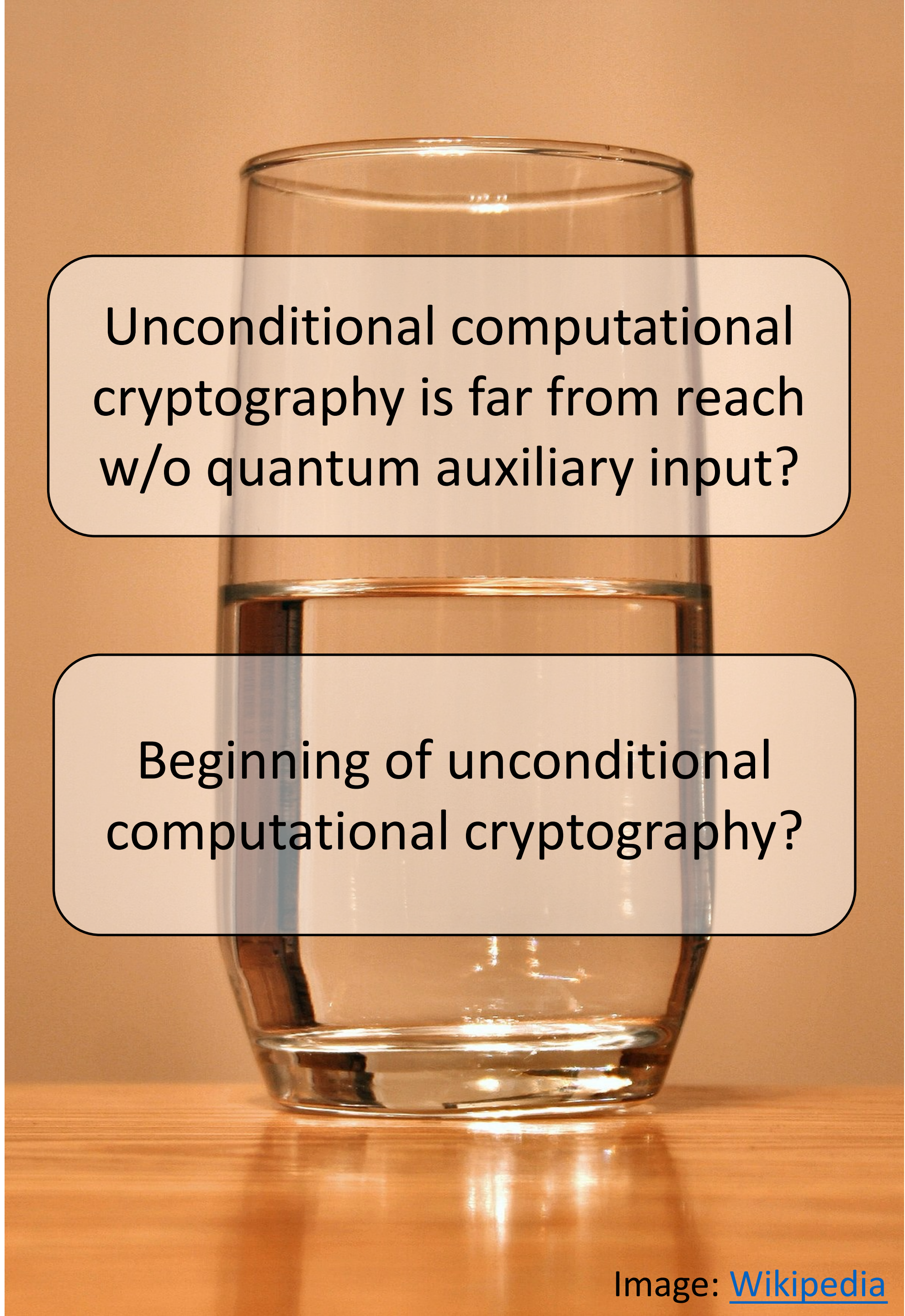


Image: [Wikipedia]