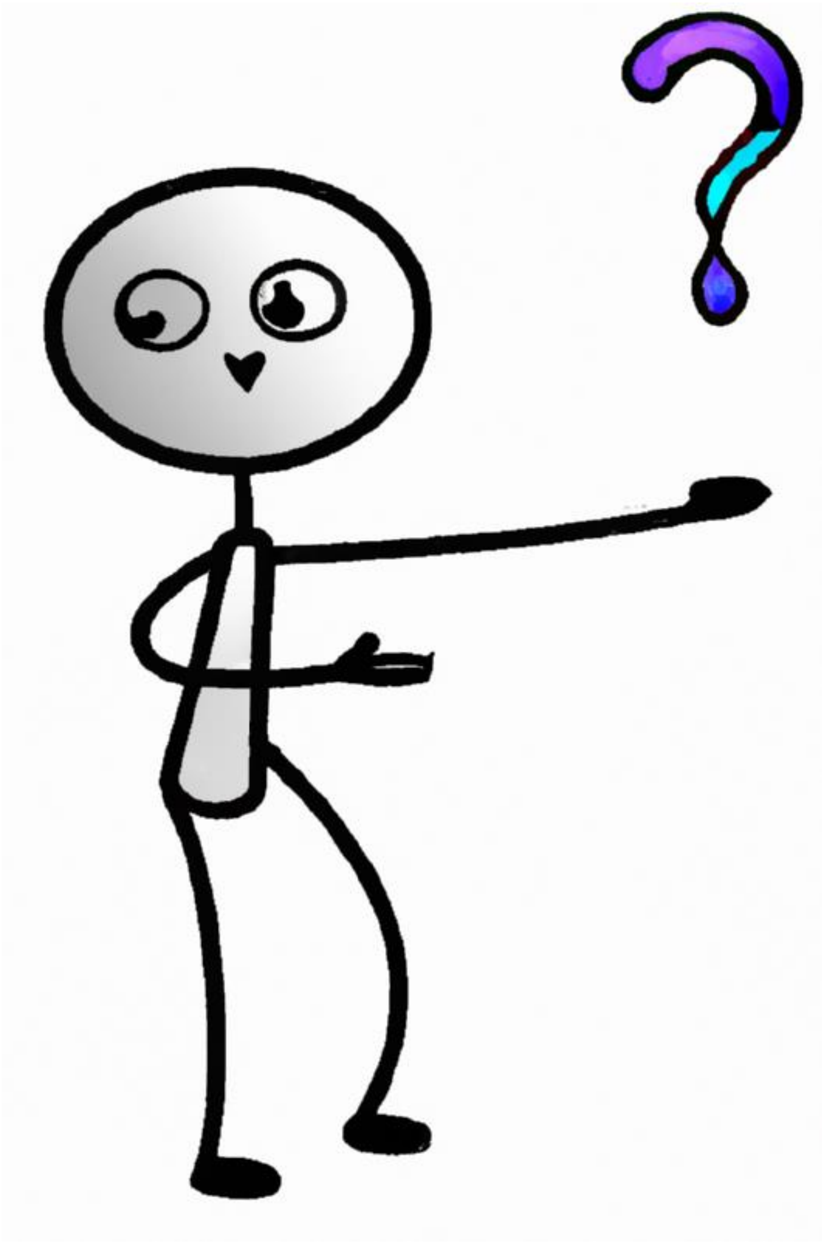


On computational hardness needed for quantum cryptography

Zvika Brakerski
Weizmann Institute of Science

Ran Canetti
Boston University

Luowen Qian
Boston University

Root of classical crypto: one-way functions

- OWFs: functions that are easy to compute but hard to invert
- Sufficient for: a lot of cryptography (secret-key encryption, signature, commitment, ZK, (weak) coin flipping, pseudorandomness…)
- Necessary for: almost all cryptography that is information-theoretically impossible! (encryption, signature, commitment, *key exchange*, *MPC*, pseudorandomness…)
- Holy grail for theory of crypto: minimize assumptions

Landscape of classical cryptography

In terms of Impagliazzo’s five worlds (1995)…

OWFs seem insufficient

Not “Algorithmica”
$P \neq NP$

$\Leftarrow$

“Minicrypt”
One-way functions
PRG, PRF,
secret-key encryption,
identification, commitment,
zero knowledge, coin flipping…

$\Leftarrow$

“Cryptomania”
public-key encryption,
key exchange, multiparty
secure computation…

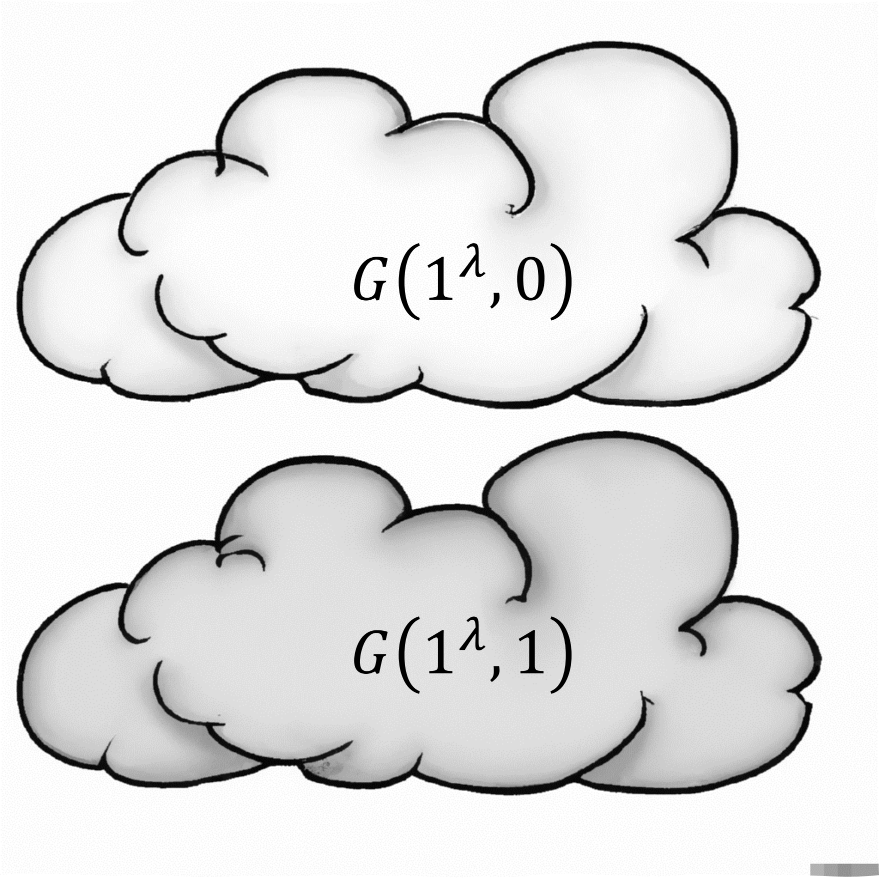
Quantum changes landscape dramatically

- Information theoretically secure key exchange [Bennett, Brassard'84]
- MPC from OWFs
  [Crépeau, Kilian'88; …; Bartusek, Coladangelo, Khurana, Ma'21; Grilo, Lin, Song, Vaikuntanathan'21]
- MPC without OWFs [Kretschmer'21; Ananth, Q, Yuen'22; Morimae, Yamakawa'22]
  - "Quantum pseudorandomness" (PRS) suffices for MPC, signature…
  - It does not appear to imply OWFs (more on this later)

Is there still a minimal assumption for (computational) quantum cryptography?

[Goldreich'90]

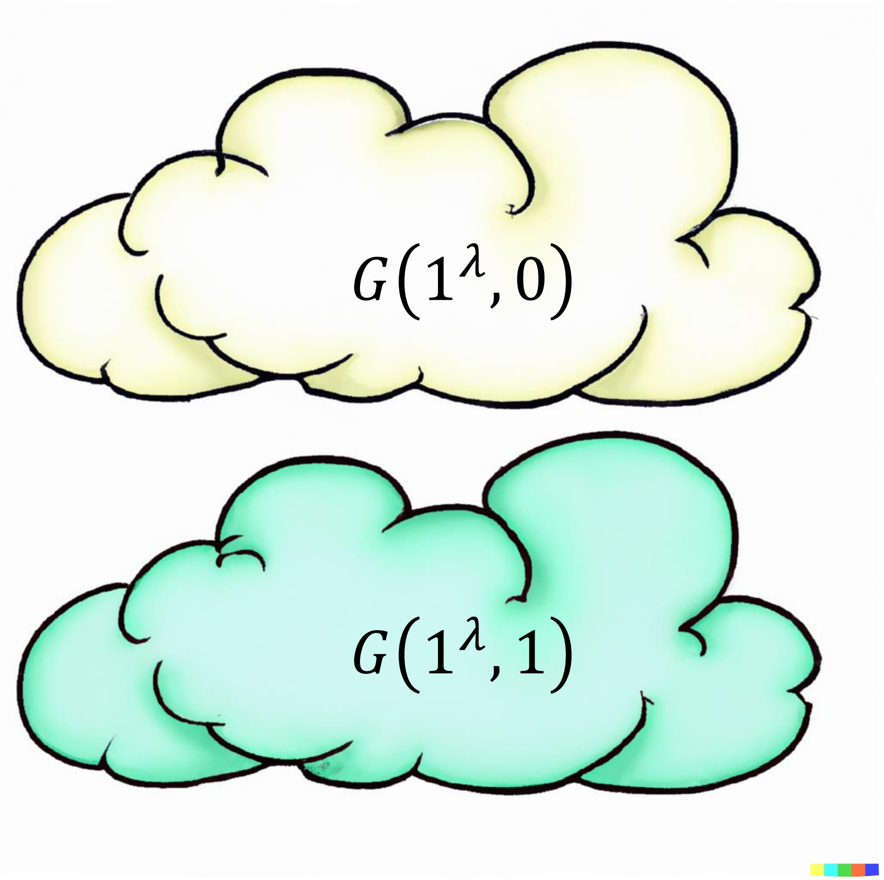
EFID pairs: non-trivial computational indistinguishability



- **E**fficient generation: $G(1^\lambda, b)$ is an efficient randomized algorithm sampling from certain **D**istributions over bit strings
- Statistical **F**arness: $G(1^\lambda, 0)$ vs $G(1^\lambda, 1)$ are statistically far (in total variation distance)
- Computational **I**ndistinguishability: $G(1^\lambda, 0) \approx_c G(1^\lambda, 1)$

EFID pairs $\Leftrightarrow$ OWFs [Goldreich'90]

EFI pairs (of quantum states)



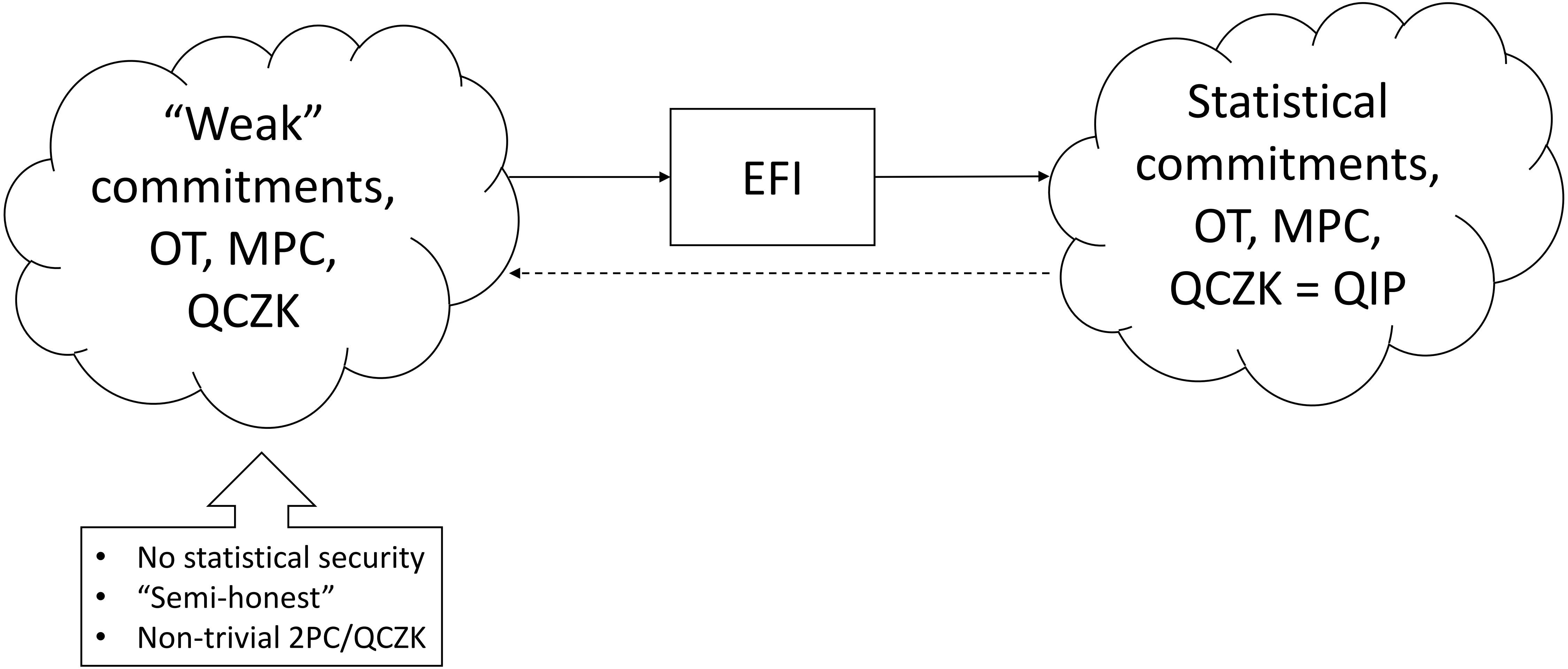
- **E**fficient generation: $G(1^\lambda, b)$ is an efficient quantum algorithm outputting an arbitrary mixed state (distribution over pure states)
- Statistical **F**arness: $G(1^\lambda, 0)$ vs $G(1^\lambda, 1)$ are statistically far (in trace distance)
- Computational **I**ndistinguishability: $G(1^\lambda, 0) \approx_c G(1^\lambda, 1)$

[Yan'22] also informally considered EFI in context of commitments

What is so different about EFI vs EFID?

- EFID $\Leftrightarrow$ OWFs, but EFI pairs do not imply OWFs as PRS $\Rightarrow$ EFI (many classical equivalences crucially go through OWFs)
- Randomized algorithms take random coins as input, but quantum algorithms generate randomness from entanglement
- Many classical techniques do not carry over:
  - Cannot assume deterministic
  - Cannot program randomness
- *Quantum* techniques needed for approaching EFI

Minimality of EFI in a quantum world



*These implications are a combination of results in multiple works including ours. Details to come.

Additional significances of EFI pairs

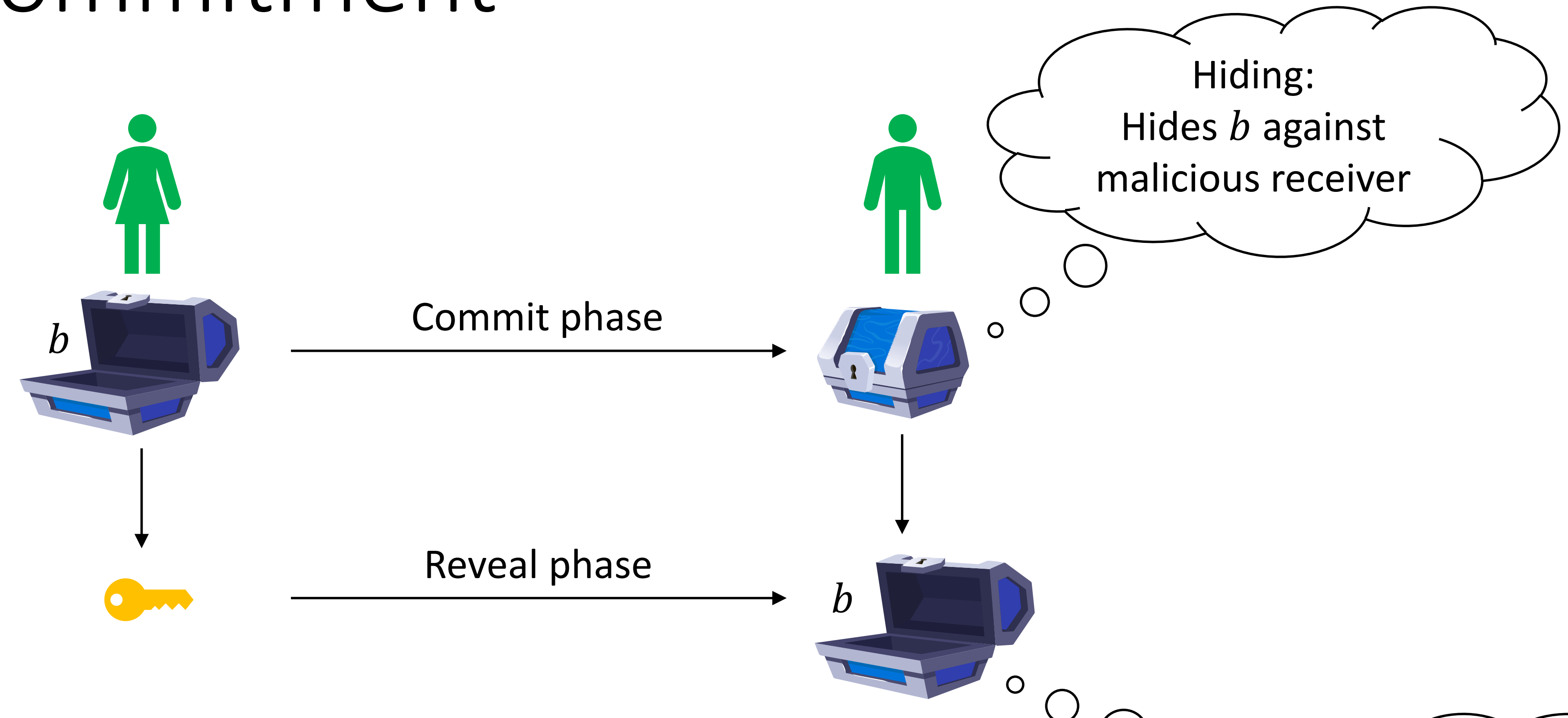
Like OWFs, EFI pairs are:

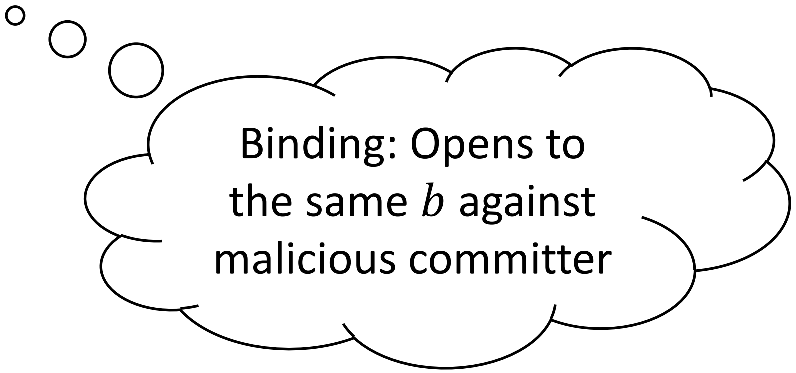
- Simple
- Natural
- Immediately implied by various cryptography like encryptions and PRS
- Serve as a linchpin for demonstrating equivalence

Why should we care?

- Equivalences are great (mathematically)…
  - *Quantum* equivalences more so: they reveal fundamental properties of quantum information & quantum computation!
- But what does it mean to cryptographers if quantum-secure one-way functions exist after all?
  - (As we all believe, hopefully? Are these just abstract nonsense?)
  - What are the *concrete* candidate hardness assumptions that imply EFI pairs, and hold even if one-way functions do not exist?
  - Answer is complicated, stay tuned until the end of the talk!

Bit commitment





Semi-honest security: [Yan22]
commit phase is honest up to purifications
(not measuring and not forgetting)

Weak to strong commitment via EFI

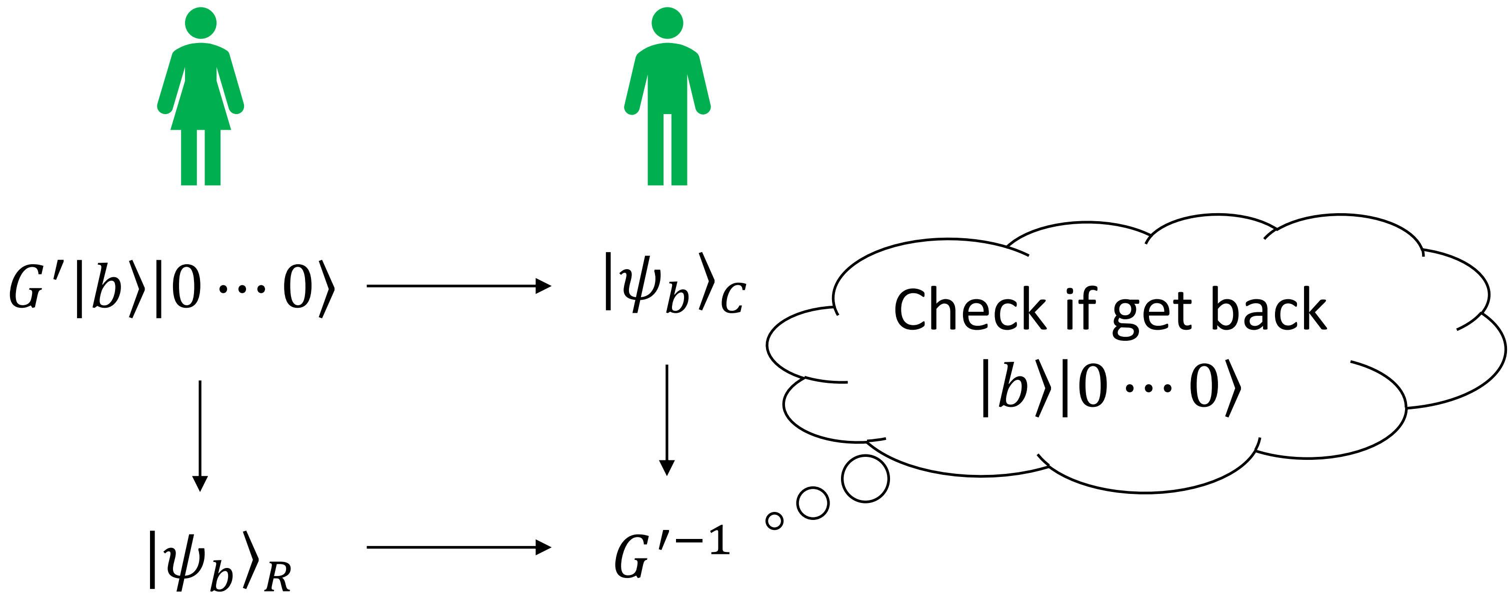
Roadmap:

- Semi-honest computational commitments ⇒ EFI pairs
- EFI pairs ⇒ statistically binding commitments
- From there, can get:
  - Statistically hiding commitments [Yan22]
  - Simulatable (equivocal and/or extractable) commitments [BCKM21, AQY22]

Commitment from EFI via purification

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

- Run purified generation $G'|b\rangle|000\cdots0\rangle \to |\psi_b\rangle_{CR}$ (C is output register, R is its purification)
- Prove correct generation via uncomputing G'

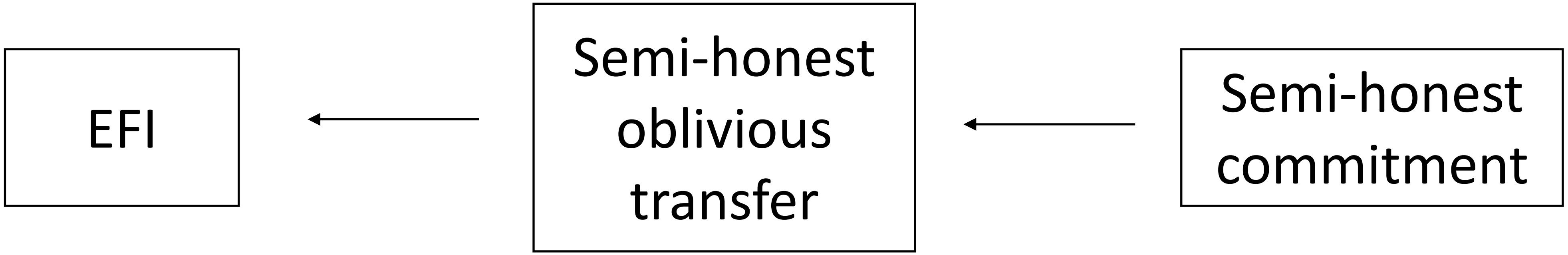


- Computational hiding $\Leftarrow$ computational indistinguishability
- Statistical binding: statistical farness + Uhlmann's theorem

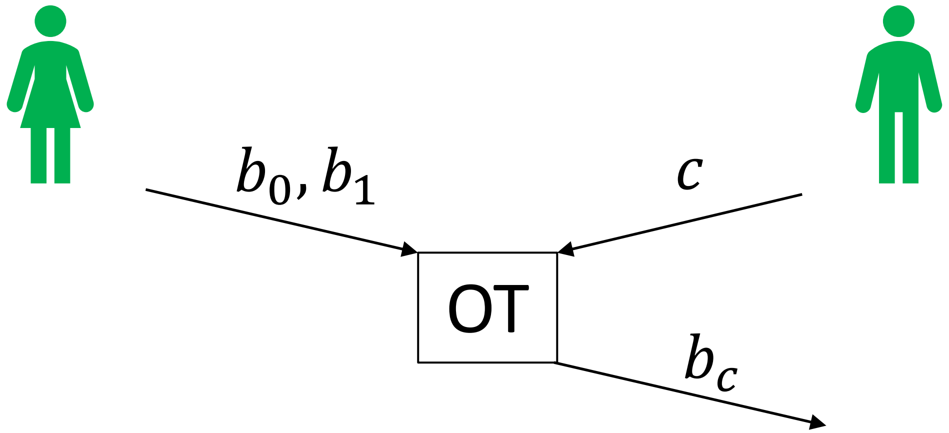
EFI from weak commitment: high level idea

- EFI pair is a **statistical-computational gap** in a distinguishing task
  - Exhibit two efficient distributions
  - Assert computational indistinguishability
  - Break statistical indistinguishability via an attack
- A commitment scheme also inherently has such a gap as information theoretical commitments are impossible by Mayers–Lo–Chau (1997)
  - A gap in breaking hiding $\Leftrightarrow$ a gap in distinguishing
  - A gap in breaking binding is less clear
- More convenient to consider (equivalently) oblivious transfer, where security for both sides are distinguishing tasks

EFI from weak commitment: roadmap



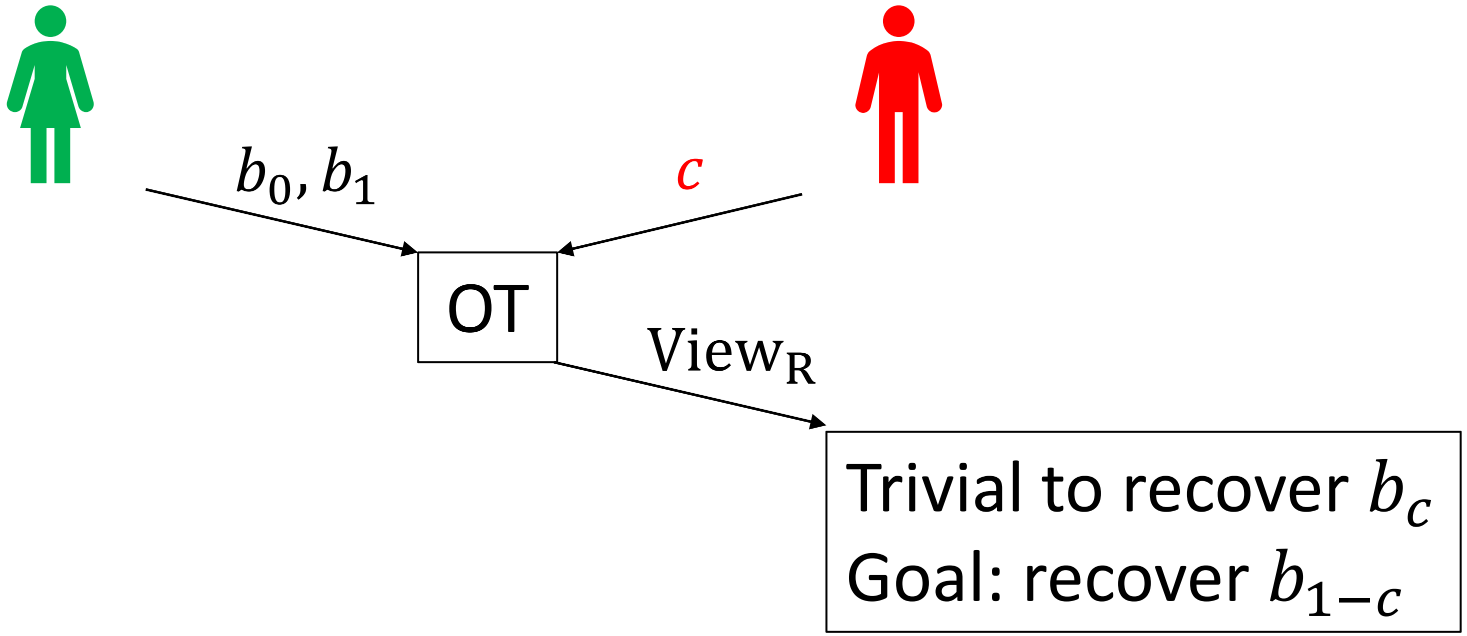
Oblivious transfer



Semi-honest security:

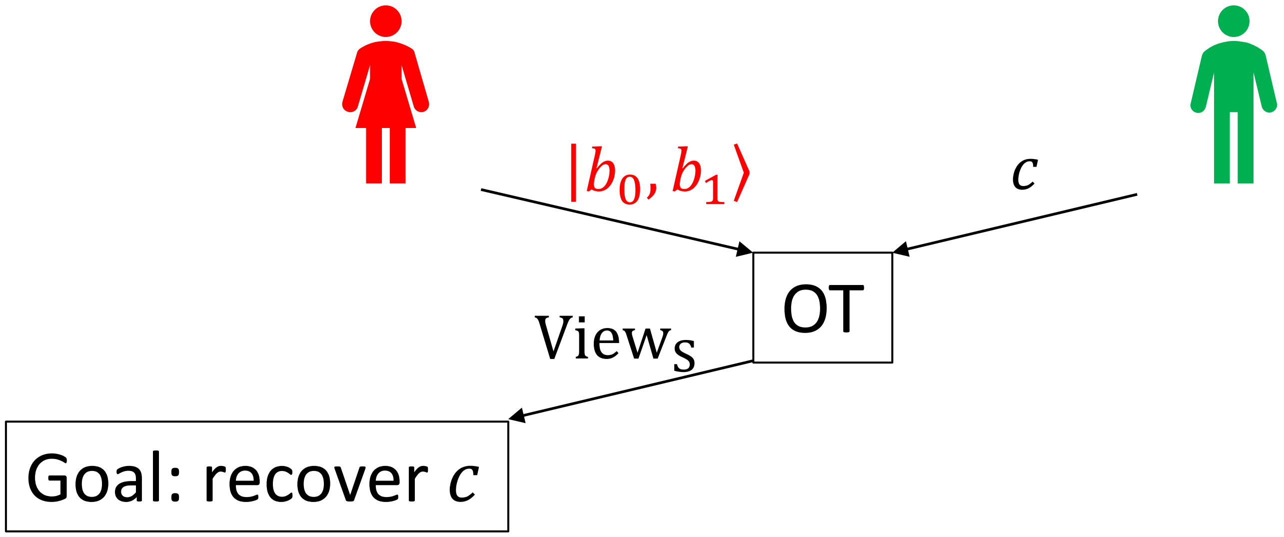
During protocol execution,
everyone is honest up to purifications
(details to come)

Oblivious transfer (semi-honest receiver)



Equivalent formulation as distinguishing:
Distinguish $\mathrm{View}_\mathrm{R} | b_{1-c} = 0$ vs $\mathrm{View}_\mathrm{R} | b_{1-c} = 1$

Oblivious transfer (semi-honest sender)

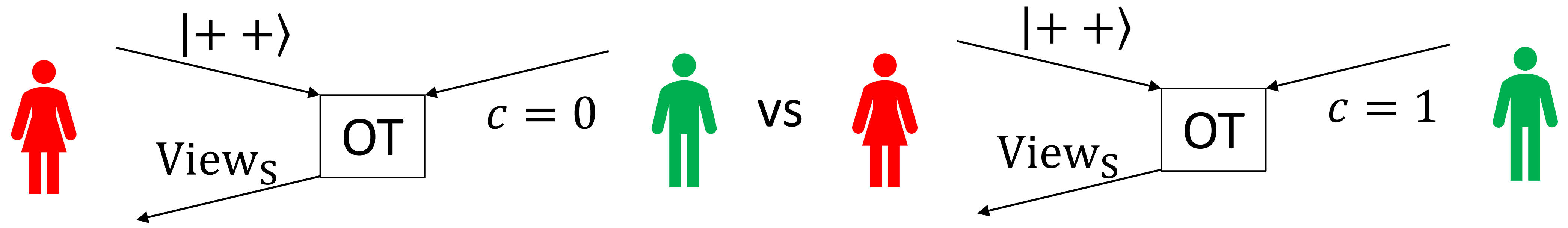


Equivalent formulation as distinguishing:
Distinguish $\text{View}_S | c = 0$ vs $\text{View}_s | c = 1$

EFI from semi-honest oblivious transfer

For every OT, either a semi-honest sender or a semi-honest receiver can (inefficiently) break security [Chailloux, Gutoski, Sikora'16]

1. If a semi-honest sender can break it,



- Computational indistinguishability $\Leftarrow$ Computational semi-honest security against sender
- Statistical farness $\Leftarrow$ by assumption

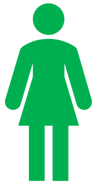
2. Similar argument for receiver case

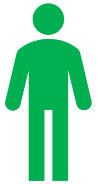
Oblivious transfer from commitment

- Well known [CK88; …; Crépeau, Légaré, Salvail’01; Fang, Unruh, Yan, Zhou’20, Yan22]
- Subtlety: computational binding for quantum commitments is harder to use
  - Solution: Yan’s computational collapse theorem [Yan22] suffices for semi-honest security

Next: a simple 2-round semi-honest OT

1-round honest oblivious transfer





$$|b_0\rangle, H|b_1\rangle \longrightarrow$$

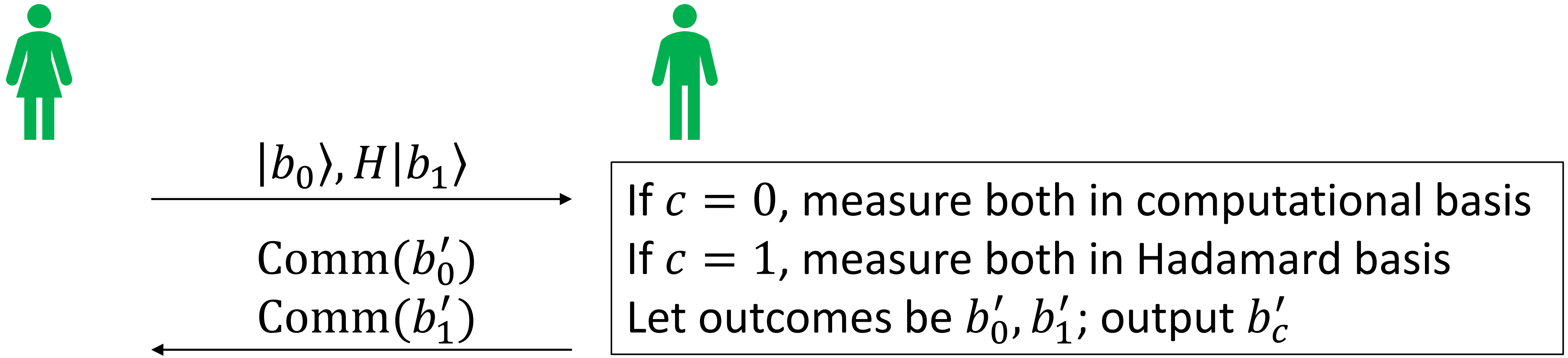
If $c = 0$, measure both in computational basis
If $c = 1$, measure both in Hadamard basis
Let outcomes be b_0', b_1'; output b_c'

Security against honest receiver: b_{1-c}' is independently random
Security against semi-honest receiver?

- A purified measurement on b_{1-c}' can be uncomputed $\times$

Force measurement via reporting measurement to sender
(tracing out sender's view will cause the collapse)

2-round semi-honest oblivious transfer



(b_0' and b_1' reveals some information about c, so cannot send in clear)

Semi-honest security against sender: hiding of commitment

Semi-honest security against receiver: state collapsed due to binding [Yan22]

Secure multiparty computation

- Sufficient with quantum statistically-binding commitments and thus EFI pairs [BCKM21, AQY22]
  - One-sided statistical security
  - Extension to quantum functionalities [Dupius, Nielsen, Salvail'12]
  - Extension to reactive functionalities [Crépeau, van de Graaf, Tapp'95; Ishai, Prabhakaran, Sahai'08]
- EFI pairs are necessary for semi-honest 2PC for non-trivial classical functionality
  - Classically this implies semi-honest oblivious transfer [Beimel, Malkin, Micali'99]
  - Generalizes to quantum "semi-honest"
  - Semi-honest oblivious transfer implies EFI pairs

Zero knowledge proofs

- EFI $\Rightarrow$ QCZK proof for QMA with an efficient prover having a single copy of witness state
  - It is a special case of statistical 2PC for quantum functionalities [Broadbent, Ji, Song, Watrous'20]
- EFI $\Rightarrow$ QCZK proof for QIP $=$ PSPACE
  - Wrap the IP protocol inside a reactive 2PC functionality, similar to classically [Ben-Or, Goldreich, Goldwasser, Håstad, Kilian, Micali, Rogaway'88]
  - The functionality simulates the real IP verifier for the verifier
- EFI $\Leftarrow$ QCZK proof for languages hard-on-average against BQP
  - QCZK proof gives an "instance-dependent" EFI (IDEFI) pair [Watrous'02; Vadhan'06; Ong, Vadhan'08; YWLQ15]
  - Average-case hardness + IDEFI pair $\Rightarrow$ EFI

Summary: minimality of EFI pairs

- We point out that the existence of EFI pairs are robustly equivalent to that of commitments, OT, MPC, and QCZK proofs
- EFI pairs seem somewhat minimal as EFI pairs are *immediately* implied by encryptions, pseudorandom states and unitaries, etc.
- Open: are EFI pairs necessary for the following?
  - Zero knowledge arguments
  - Signatures, money, "unforgeable security" in general (harder?)
- Open: any barriers for unconditionally proving the existence of EFI?

Enough of abstract nonsense, what are possible approaches to get EFI pairs without OWFs?

and what are the concrete EFI candidates?

EFI from complexity separations

- This work: If $\mathrm{BQP} \neq \mathrm{QCZK}$, then EFI pairs "exist"
- Chailloux, Kerenidis, Rosgen'11: If $\mathrm{QMA} \neq \mathrm{QIP}$, then EFI pairs "exist"

  (reductions are explicit)

Issues:

- Not concrete if the proof is not explicit
- Only get (quantum) auxiliary-input EFI pairs, especially in CKR11
- No evidence for being weaker than OWFs [Aaronson, Ingram, Kretschmer'22]

EFI from $\mathrm{QSCD_{ff}}$ [Kawachi, Koshiba, Nishimura, Yamakami'12]

- $\mathrm{QSCD_{ff}}$: Quantum state computational distinction with fully flipped permutations
- Nice properties: trapdoor, worst-case to average-case reduction, reduction to graph automorphism
- Issue: no evidence for being weaker than OWFs?

$$\rho_\pi^+(n) = \frac{1}{2n!} \sum_{\sigma \in S_n} \big(|\sigma\rangle + |\sigma\pi\rangle\big)\big(\langle\sigma| + \langle\sigma\pi|\big)$$

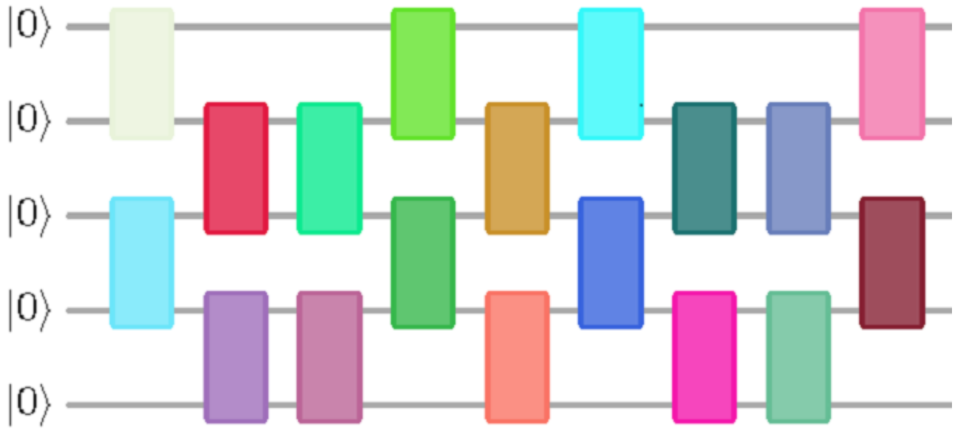
$$\rho_\pi^-(n) = \frac{1}{2n!} \sum_{\sigma \in S_n} \big(|\sigma\rangle - |\sigma\pi\rangle\big)\big(\langle\sigma| - \langle\sigma\pi|\big).$$

Kretschmer’s template

- Pseudorandom state (PRS) generator [Ji, Liu, Song’19]
  Like PRG, but outputs pure states that look “Haar random” even if given many copies
- Kretschmer’21: There exists a *quantum* oracle relative to which,
  - $\mathrm{BQP} = \mathrm{QMA}$, thus no quantum-secure one-way functions
  - Pseudorandom states exist, which implies the existence of EFI pairs
- Issues:
  - Quantum oracle separations are weaker than classical [Aaronson’09]
  - “Not concrete”: PRS is essentially generated by a Haar random unitary oracle

Candidate PRS from random quantum circuits

- Key describes a "sufficiently" large 2-local random unitary U_k
- Output: $U_k|0^n\rangle$
- Already studied in various contexts: quantum supremacy, black holes…
- Realizable on near-term quantum devices?



Candidate PRS from wormholes

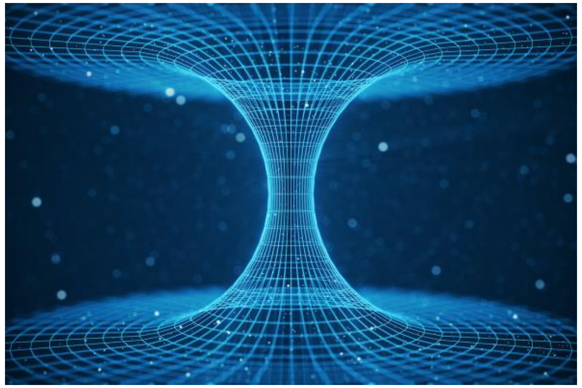
Wormhole: 2 black holes connecting 2 distinct regions of space-time

- Initial (Thermofield Double) state $|TFD\rangle$
- Highly "scrambling" evolution of black holes $U = e^{-iH_{CFT}t}$
- "Shock" O_i: (key) random Pauli operator applied on the first qubit

Conjecture: $UO_\ell UO_{\ell-1} \cdots O_1 U|TFD\rangle$ is PRS [Bouland, Fefferman, Vazirani'20]

BFV20: conjecture is true if U is a random black-box unitary

Evidence from black-hole physics?



Binary phase PRS

- Phase oracle for a Boolean function $f: \{0,1\}^n \to \{0,1\}$
$$U_f|x\rangle = (-1)^{f(x)}|x\rangle$$
- Binary phase PRS: $G(k) = U_{f_k} H^{\otimes n}|0^n\rangle$
- Proposed in [JLS18]; proven secure if $\{f_k\}$ is PRF [Brakerski, Shmueli'19]
- Kretschmer'21: If classical OWFs do not exist, then binary phase PRS is broken for all efficient $\{f_k\}$
    - A security proof for any binary PRS implies OWFs
- Inspired by Luby–Rackoff: do this for more than 1 rounds

2-Forrelation state [Kretschmer, Q, Sinha, Tal (forthcoming)]

- 2-Forrelation state: $G(k) = U_{f_{k,1}} H^{\otimes n} U_{f_{k,0}} H^{\otimes n} |0^n\rangle$
  (can extend to t-Forrelation state by repeating t rounds)
- Observation: still secure if $\{f_k\}$ is PRF
- KQST: this is a single-copy secure PRS against $\mathrm{BQP}^{\mathrm{PH}}$ adversaries if $\{f_{k,b}\}$ is instantiated by a random oracle
- Even if $\mathrm{P} = \mathrm{PH}$, this construction is still plausibly secure when instantiated by some efficient $\{f_{k,b}\}$ (like SHA-3)

Summary of EFI "candidates"

	Source of EFI pairs	Concrete?	Why is it weaker than OWF?
Complexity separations	$\mathrm{QMA} \neq \mathrm{QIP}$ [CKR11]	No*	Seems hard [AIK22]
	$\mathrm{BQP} \neq \mathrm{QCZK}$ [This work]	No*	?
	$\mathrm{QSCD}_{\mathrm{ff}}$ [KKNY12]	Yes	?
Candidate PRSs	Haar random unitary [K21]	No	Quantum oracle separation
	Random quantum circuits [AA13, AC17]	Yes	?
	Wormholes [BFV20]	It's a physics problem	Physical laws?
	2-Forrelation states [KQST, forthcoming]	Yes*	Random oracle separation

Thank you! Questions?