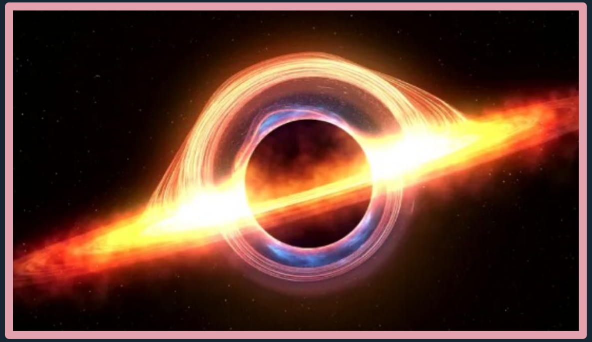
Quantum Commitments and Black Hole Radiation Decoding

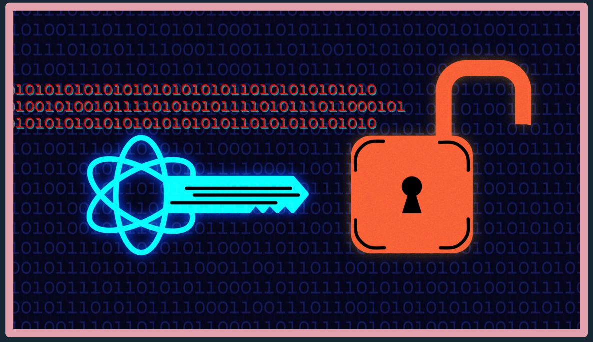
Fermi Ma

(Simons and Berkeley)

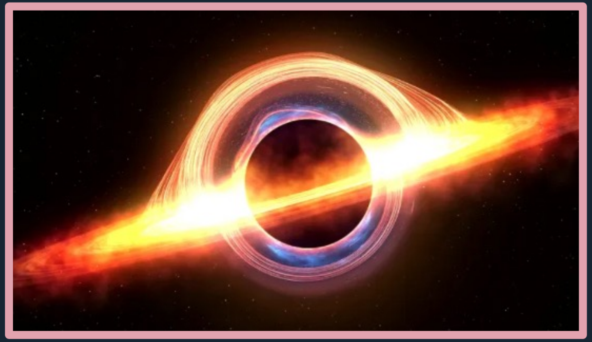
Based on discussions with Sam Gunn (Berkeley) and Alex Lombardi (Berkeley → Princeton)

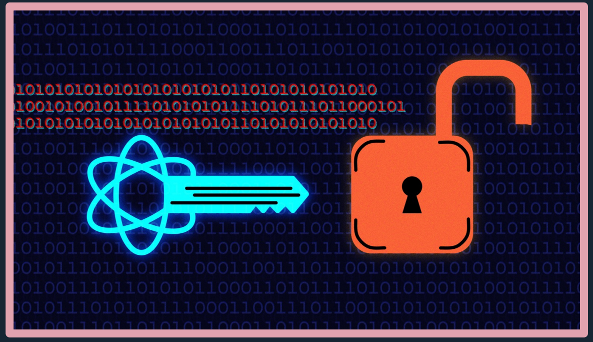
Question: What does black hole radiation decoding have to do with quantum cryptography?





Question: What does black hole radiation decoding have to do with quantum cryptography?





Answer:

Black-Hole Radiation Decoding is Quantum Cryptography

Zvika Brakerski*

Abstract

We propose to study equivalence relations between phenomena in high-energy physics and the existence of standard cryptographic primitives, and show the first example where such an

(building on [Harlow-Hayden13, Aaronson16])

You might be wondering…

“Black-Hole Radiation Decoding is Quantum Cryptography.”

You might be wondering…

1) What does this mean?

"Black-Hole Radiation Decoding is Quantum Cryptography."

You might be wondering...

1) What does this mean?

2) What does this mean?

"Black-Hole Radiation Decoding is Quantum Cryptography."

You might be wondering...

1) What does this mean?

2) What does this mean?

"Black-Hole Radiation Decoding is Quantum Cryptography."

3) What does this mean?

You might be wondering...

1) What does this mean?

2) What does this mean?

"Black-Hole Radiation Decoding is Quantum Cryptography."

3) What does this mean?

Goal: understand the title of Zvika's paper

Plan for this talk

(1) Background on black holes

Plan for this talk

(1) Background on black holes

(2) Radiation decoding problem [Harlow-Hayden13]

Plan for this talk

(1) Background on black holes

(2) Radiation decoding problem [Harlow-Hayden13]

(3) Radiation *distinguishing* problem

Plan for this talk

(1) Background on black holes

(2) Radiation decoding problem [Harlow-Hayden13]

(3) Radiation *distinguishing* problem

(4) Connection to quantum commitments

Plan for this talk

(1) Background on black holes

(2) Radiation decoding problem [Harlow-Hayden13]

(3) Radiation *distinguishing* problem

(4) Connection to quantum commitments

(3) + (4) is an alternative view of [Brakerski23].

Plan for this talk

(1) Background on black holes

(2) Radiation decoding problem [Harlow-Hayden13]

(3) Radiation *distinguishing* problem

(4) Connection to quantum commitments

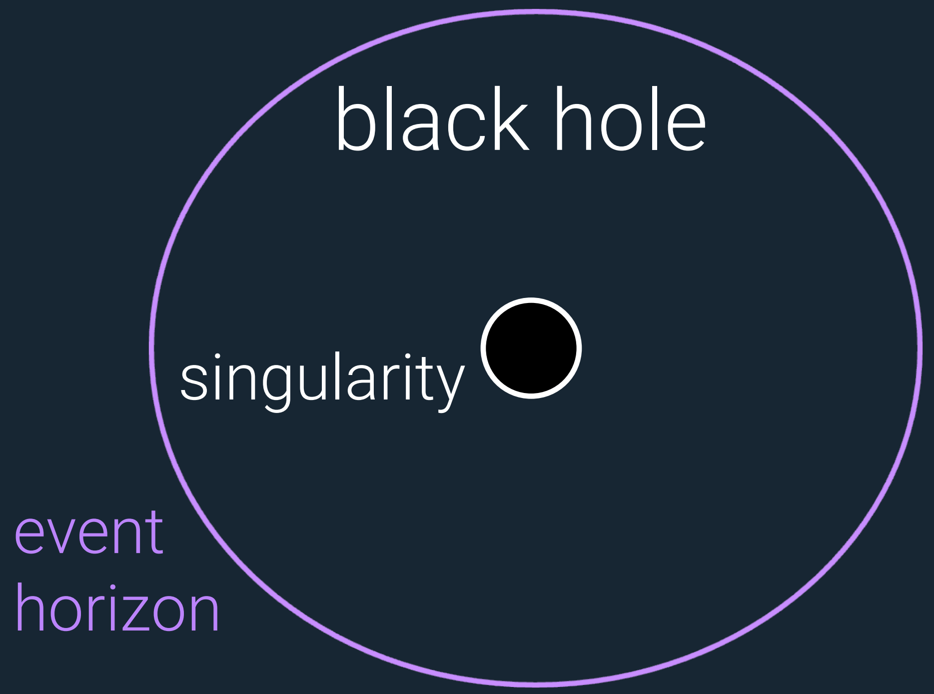
(3) + (4) is an alternative view of [Brakerski23].

Warning: I’m *not* a physicist.

Warning: I'm *not* a physicist.

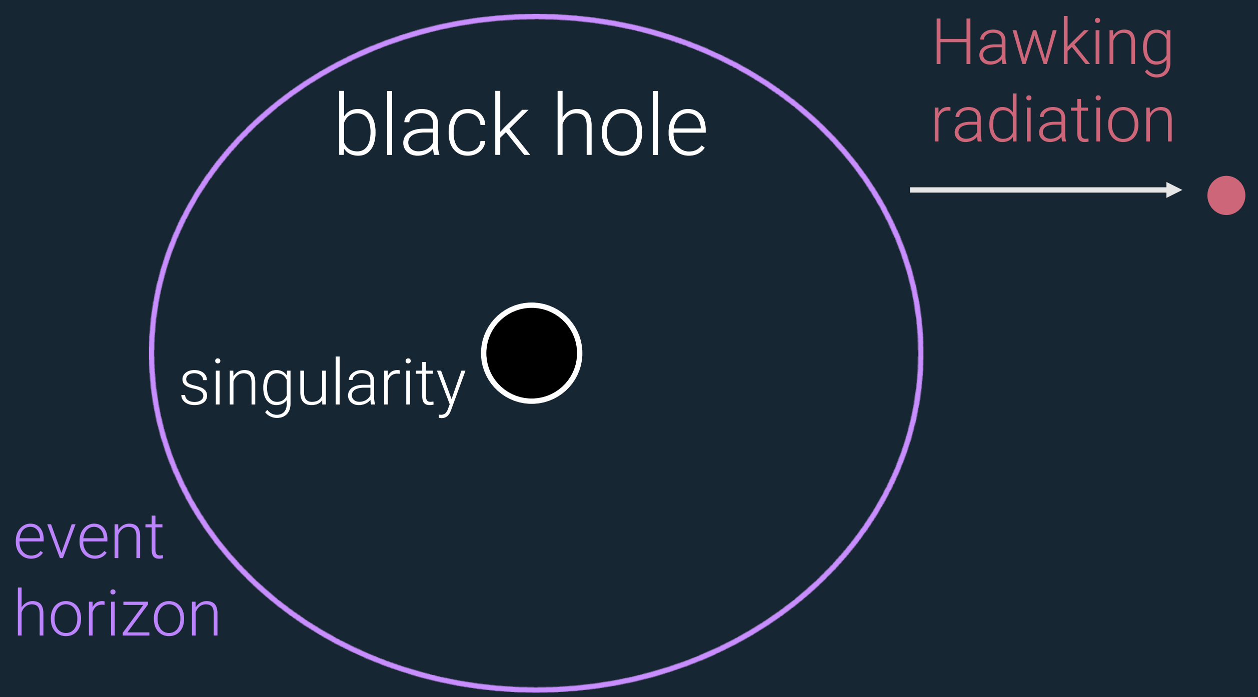
Everything I'm about to say about black hole physics is from Scott Aaronson's Barbados lecture notes (any mistakes are my own).

Black Hole Radiation



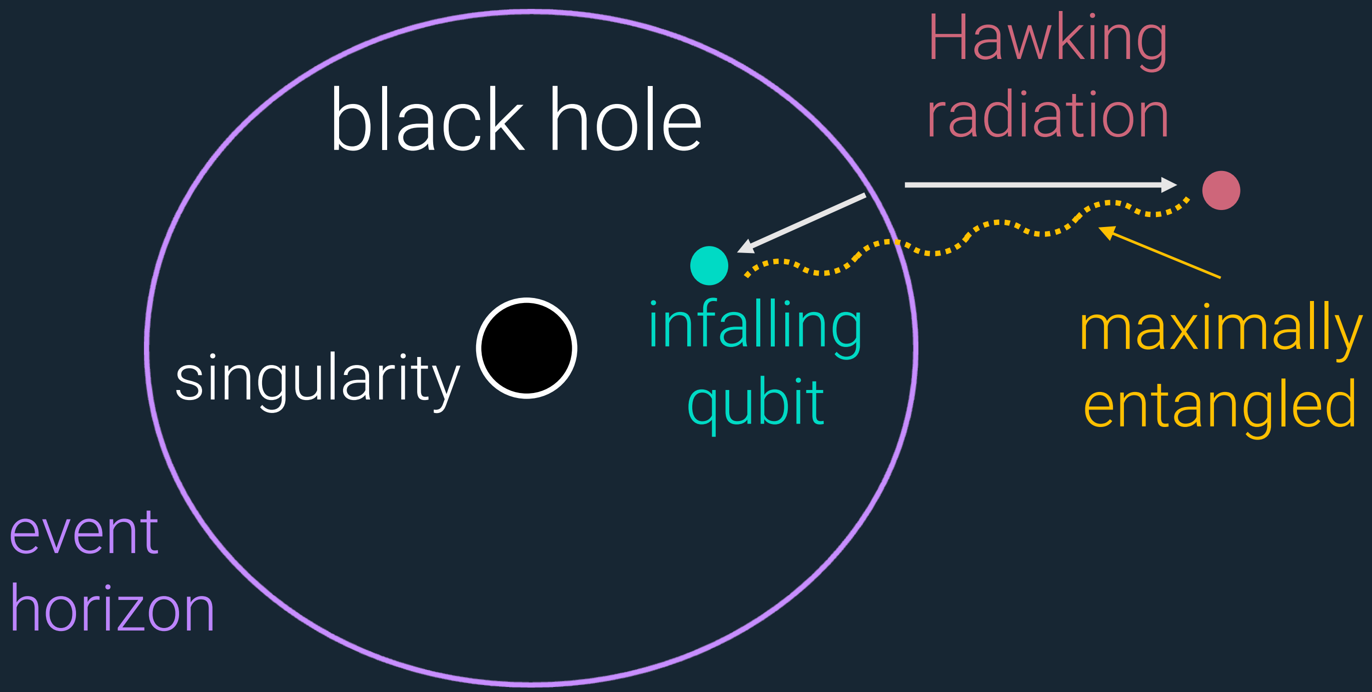
Black Hole Radiation

- Black holes emit qubits of Hawking radiation.



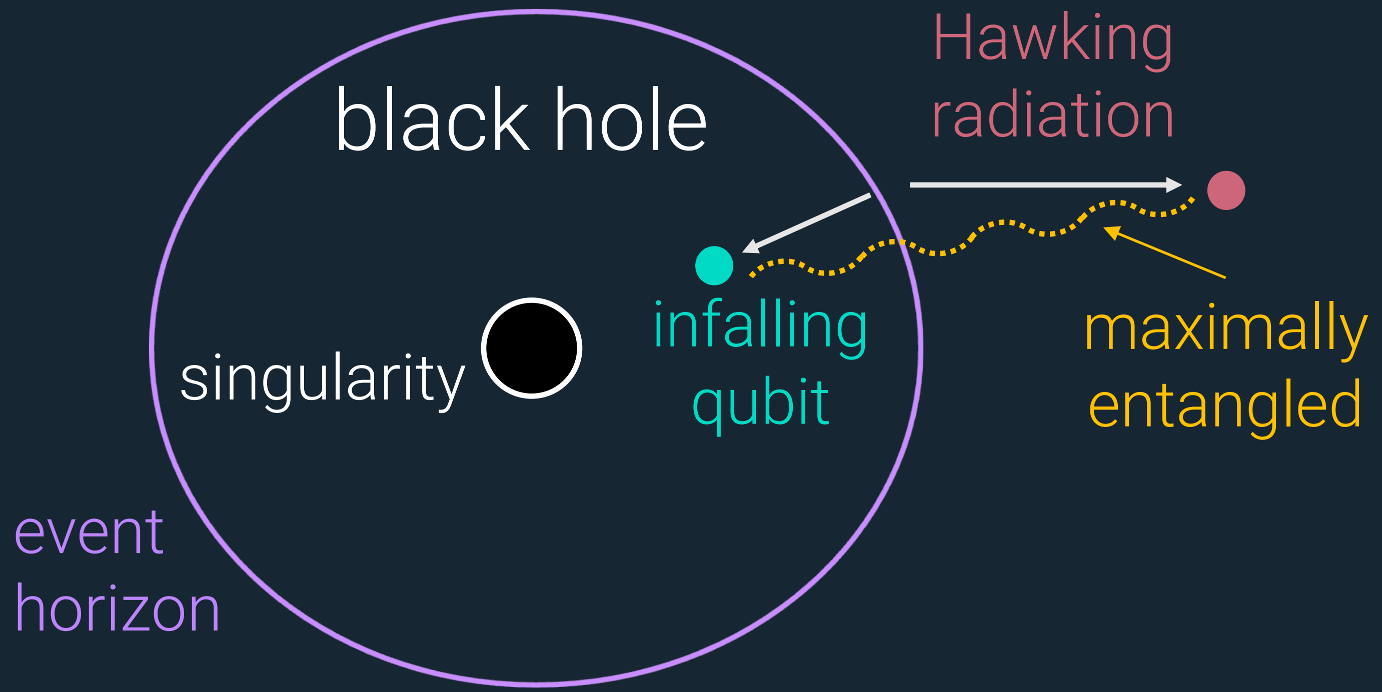
Black Hole Radiation

- Black holes emit qubits of Hawking radiation.
- Each outgoing qubit is maximally entangled with an infalling qubit.

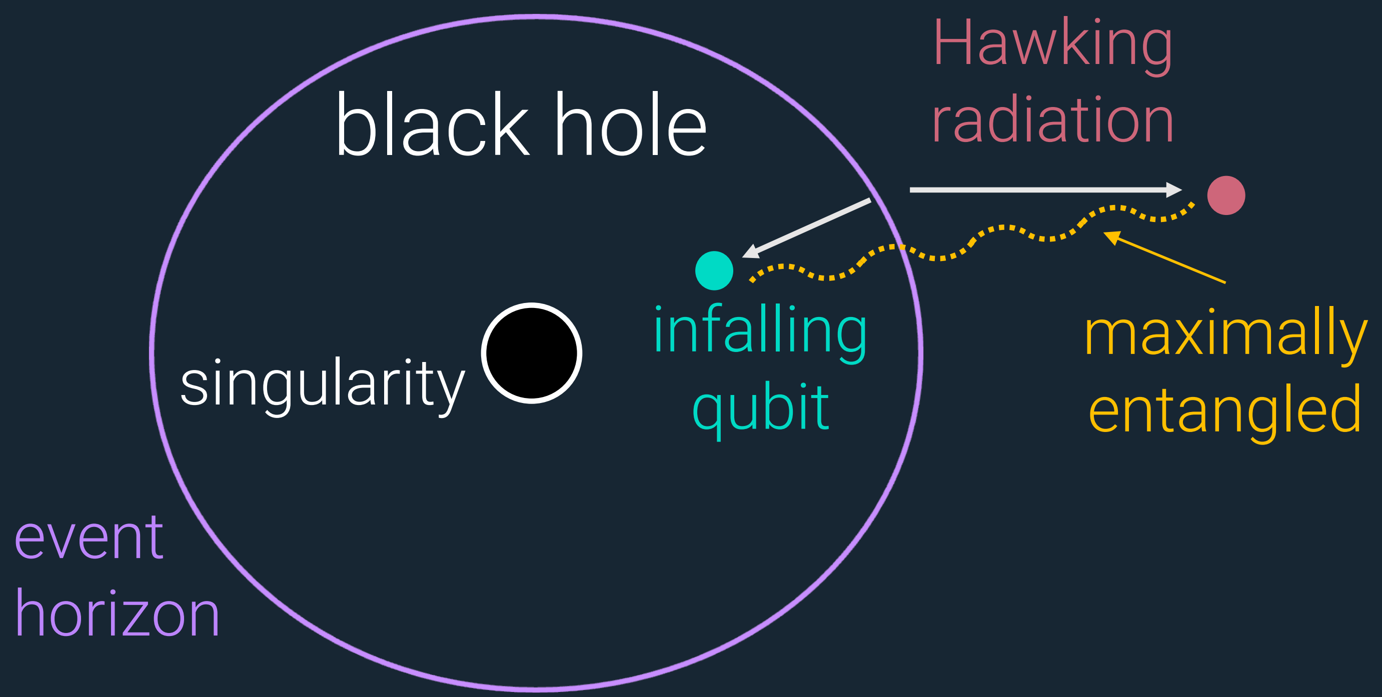


Black Hole Radiation

- Black holes emit qubits of Hawking radiation.
- Each outgoing qubit is maximally entangled with an infalling qubit.
- After long enough, black hole evaporates completely.

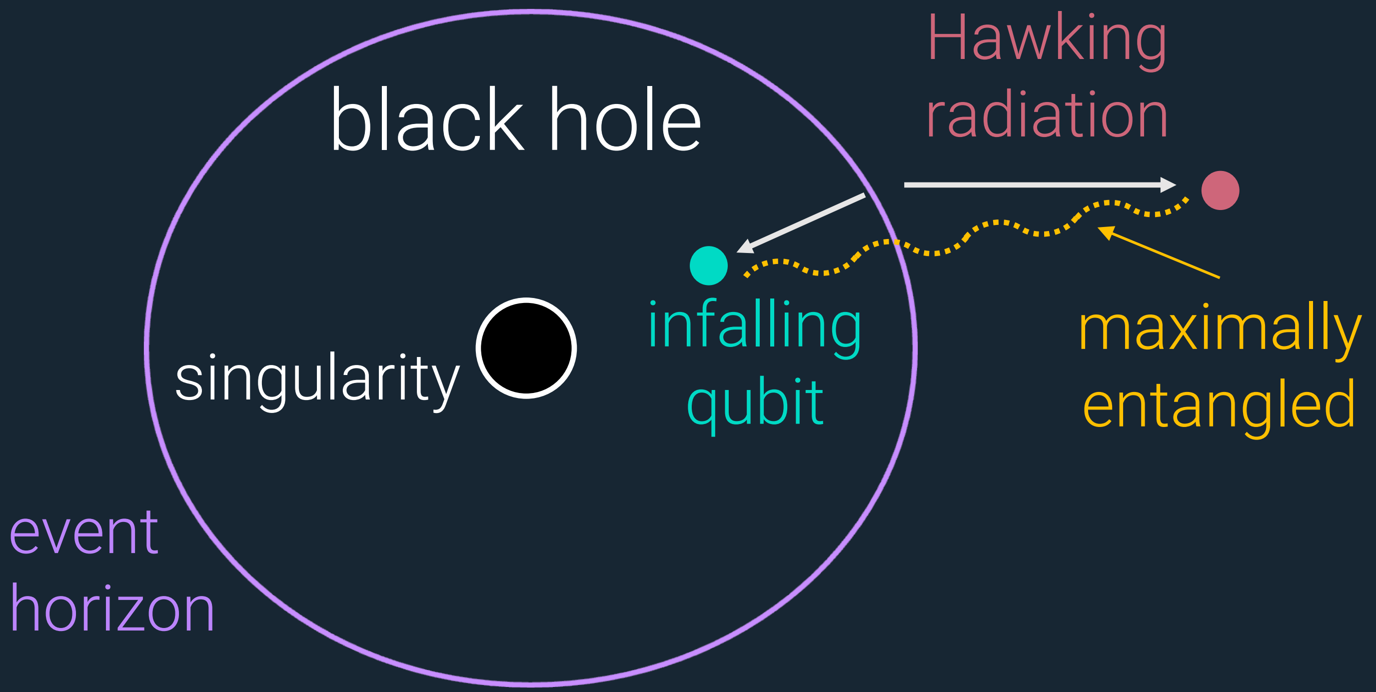


Emitted radiation comes out "scrambled."



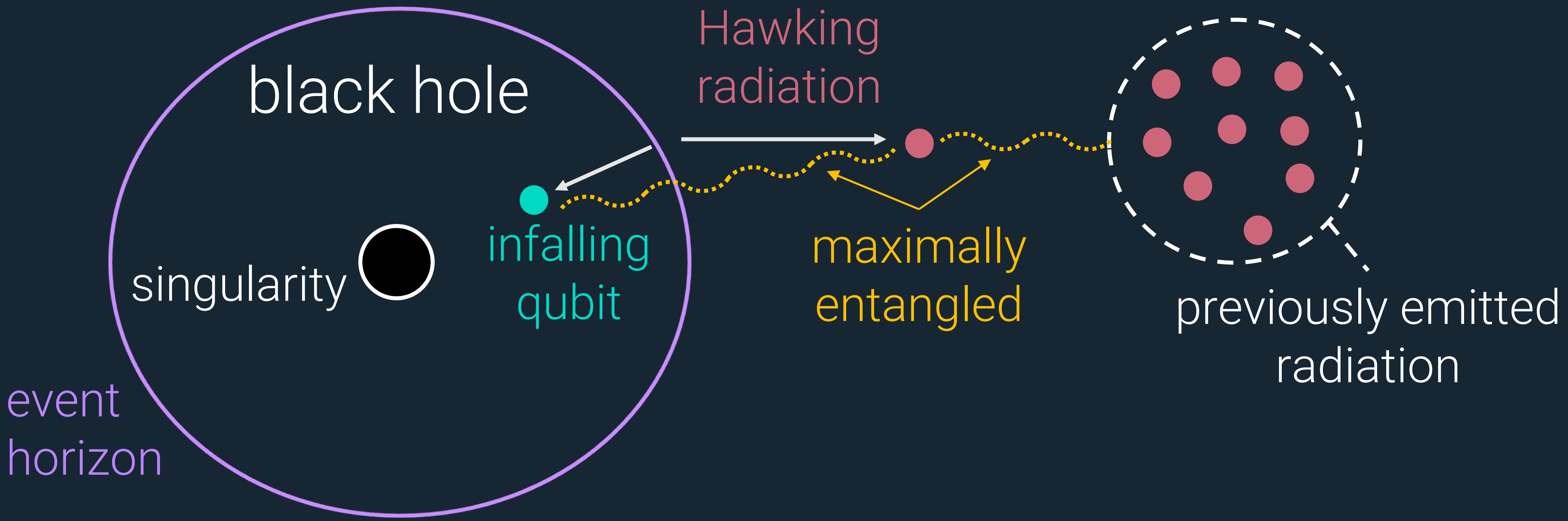
Emitted radiation comes out “scrambled.”

- Post-evaporation state is a (roughly) a random pure state.



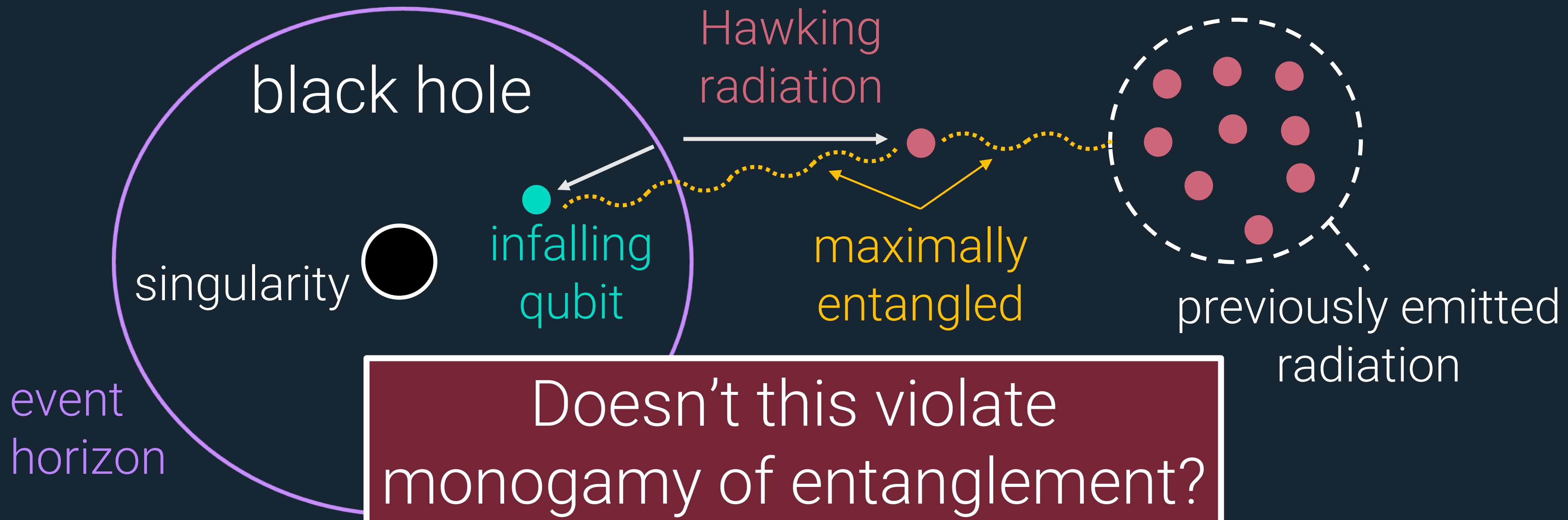
Emitted radiation comes out "scrambled."

- Post-evaporation state is a (roughly) a random pure state.
- Consequence: after $\sim 1/2$ of the black hole has evaporated, outgoing qubits are *maximally entangled* with previously emitted radiation.



Emitted radiation comes out "scrambled."

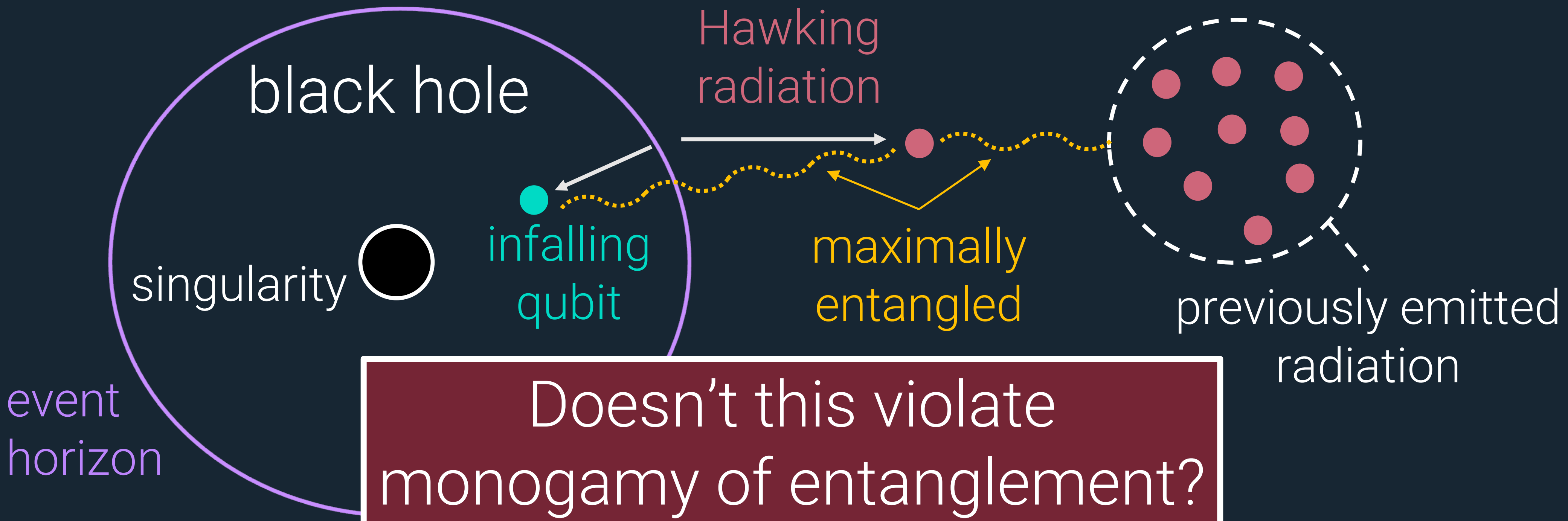
- Post-evaporation state is a (roughly) a random pure state.
- Consequence: after $\sim 1/2$ of the black hole has evaporated, outgoing qubits are *maximally entangled* with previously emitted radiation.



Doesn't this violate monogamy of entanglement?

Black hole complementarity [Susskind-'t Hooft, 90s]

If radiation is maximally entangled with two systems, they're the ***same system***.



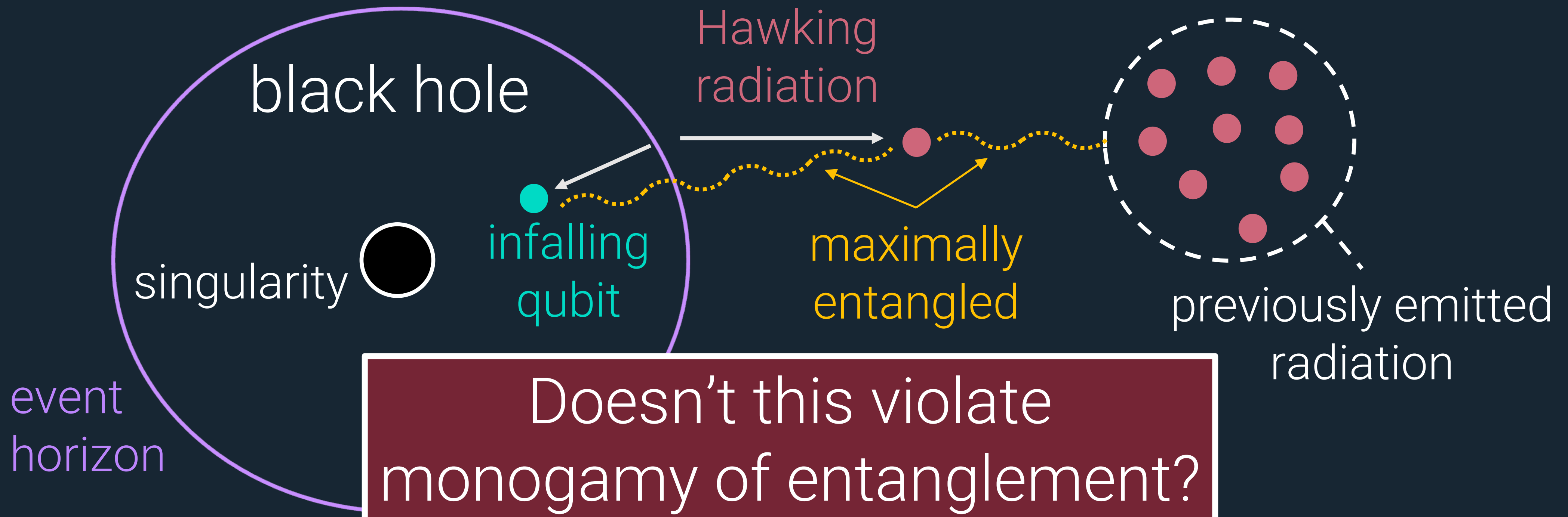
Doesn't this violate monogamy of entanglement?

Black hole complementarity [Susskind-'t Hooft, 90s]

If radiation is maximally entangled with two systems, they're the ***same system***.

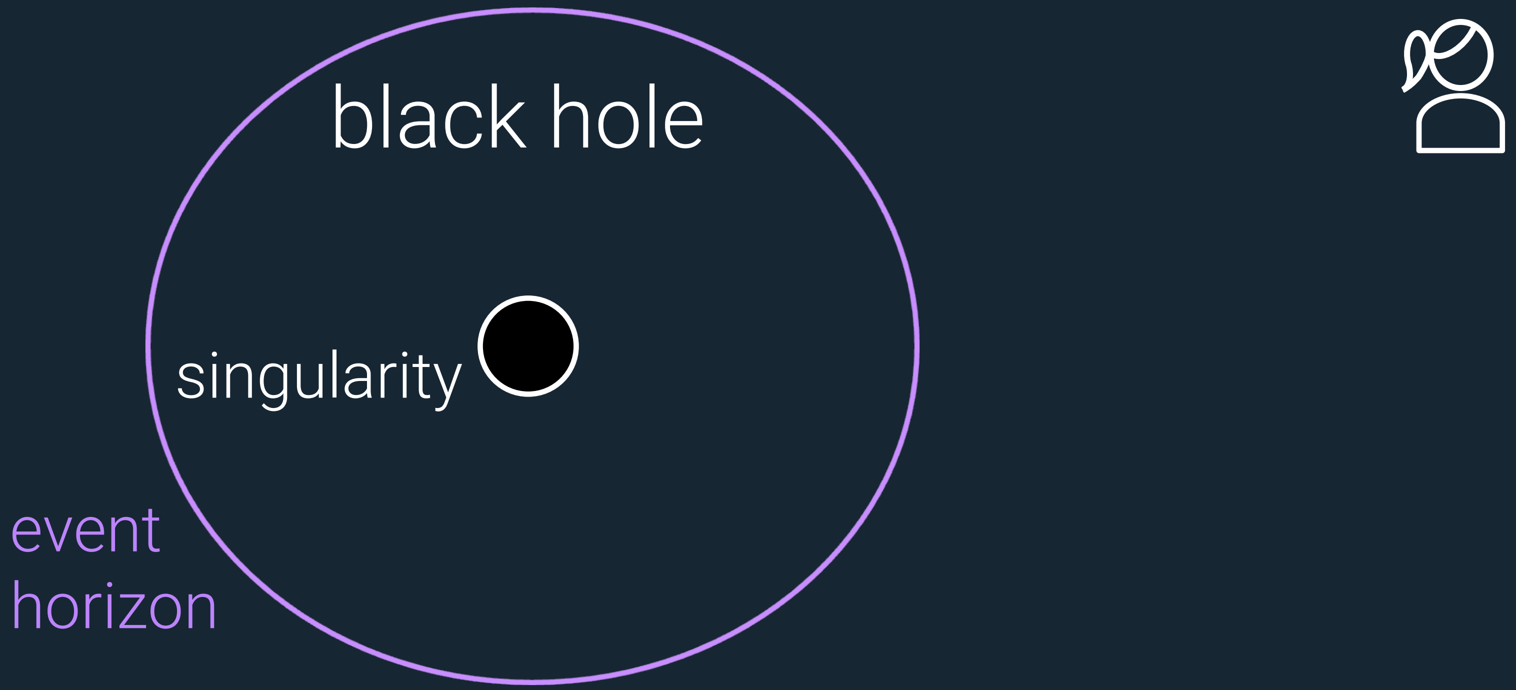
Firewall paradox [Almheiri-Marolf-Polchinski-Sully, 11]

Thought experiment in which an observer ***detects*** the monogamy violation.



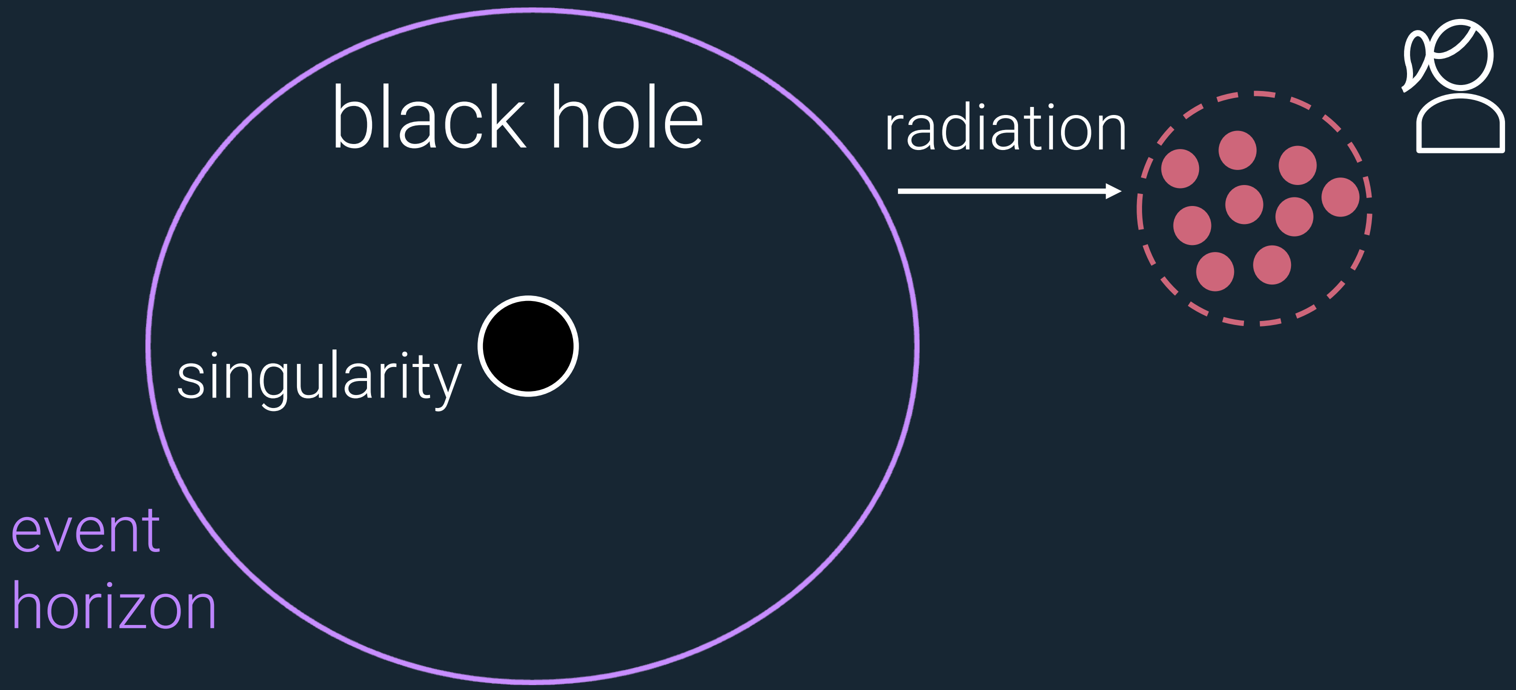
Doesn't this violate monogamy of entanglement?

[AMPS11] experiment:



[AMPS11] experiment:

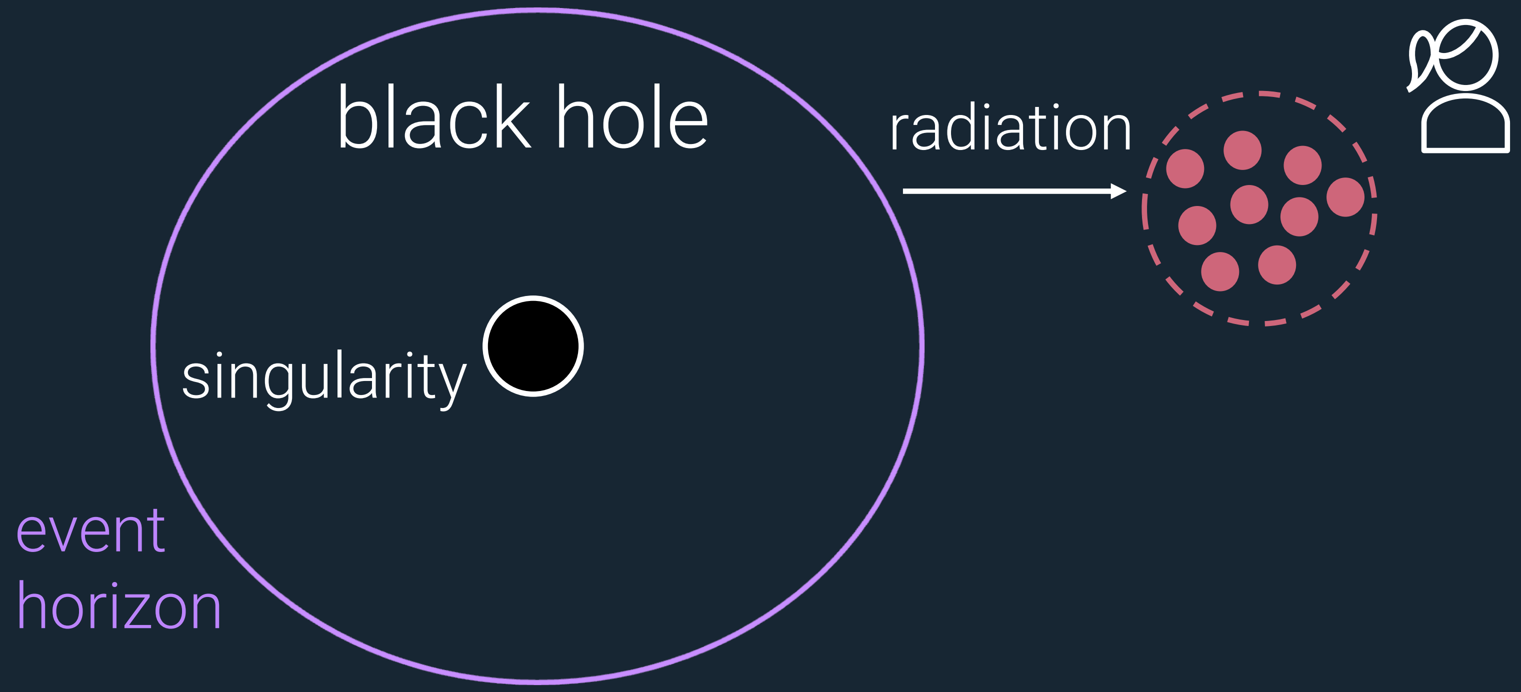
1) Alice collects radiation until 2/3 of black hole has evaporated.



[AMPS11] experiment:

1) Alice collects radiation until $2/3$ of black hole has evaporated.

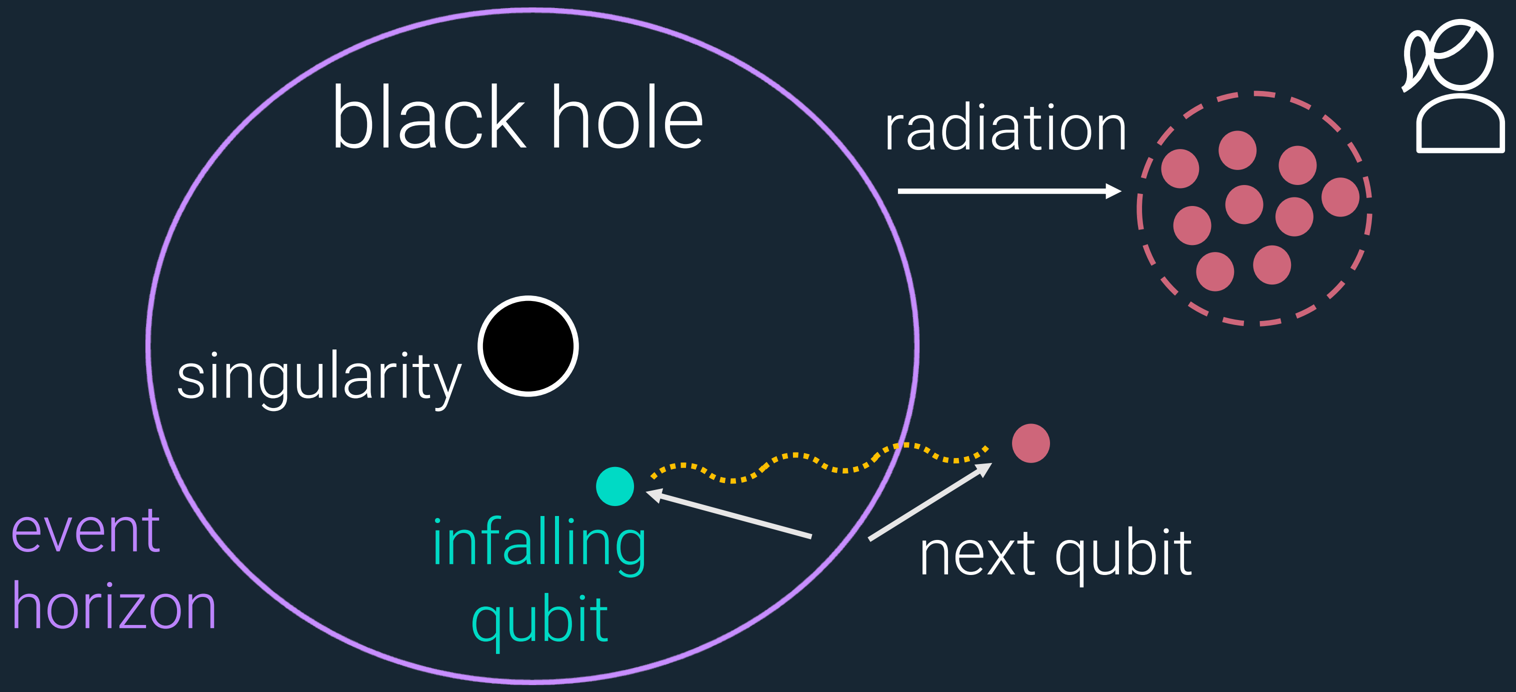
2) Alice uses a quantum computer to “check” that the next qubit is entangled with her collected radiation (e.g., distills an EPR pair).



[AMPS11] experiment:

1) Alice collects radiation until 2/3 of black hole has evaporated.

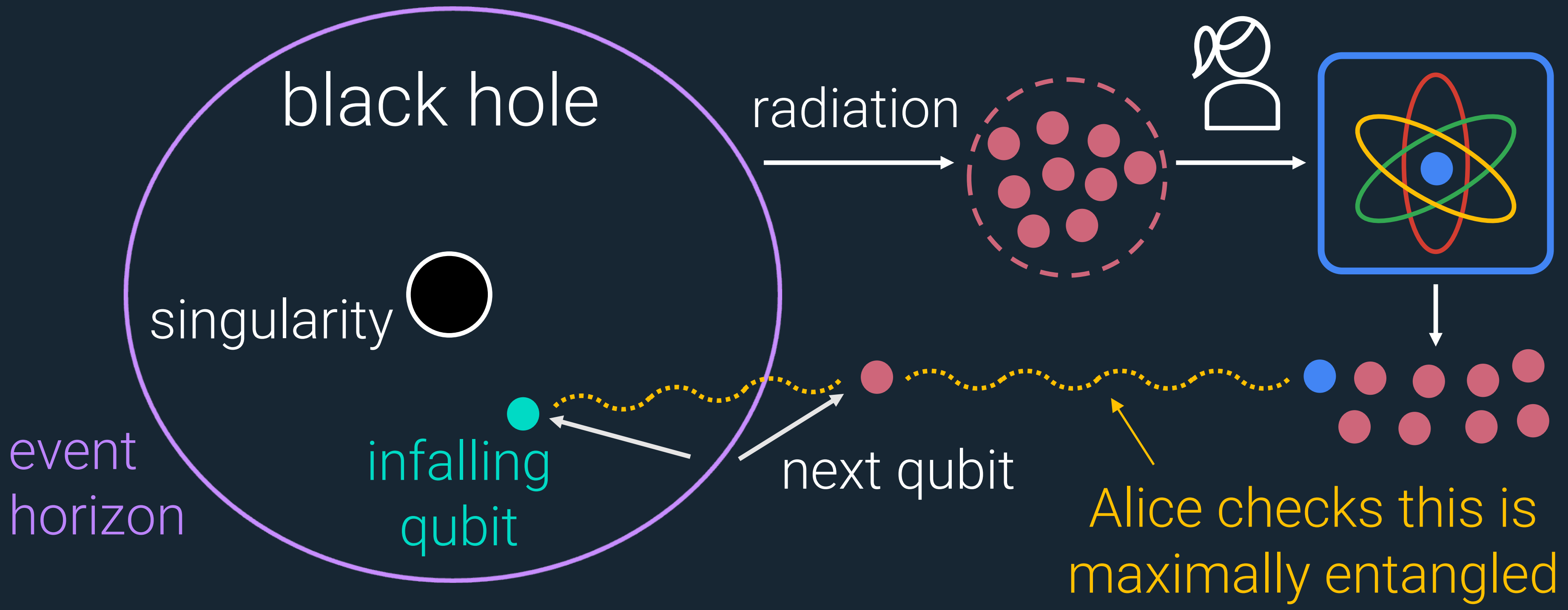
2) Alice uses a quantum computer to "check" that the next qubit is entangled with her collected radiation (e.g., distills an EPR pair).



[AMPS11] experiment:

1) Alice collects radiation until 2/3 of black hole has evaporated.

2) Alice uses a quantum computer to “check” that the next qubit is entangled with her collected radiation (e.g., distills an EPR pair).

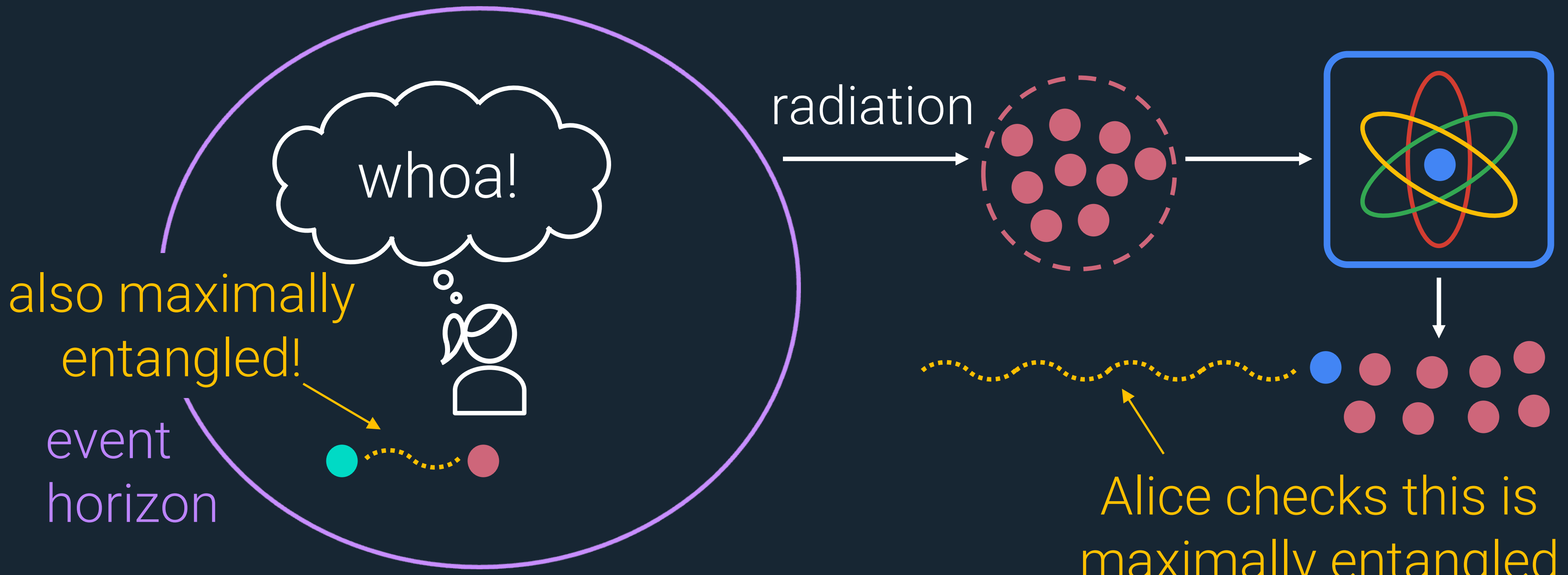


[AMPS11] experiment:

1) Alice collects radiation until 2/3 of black hole has evaporated.

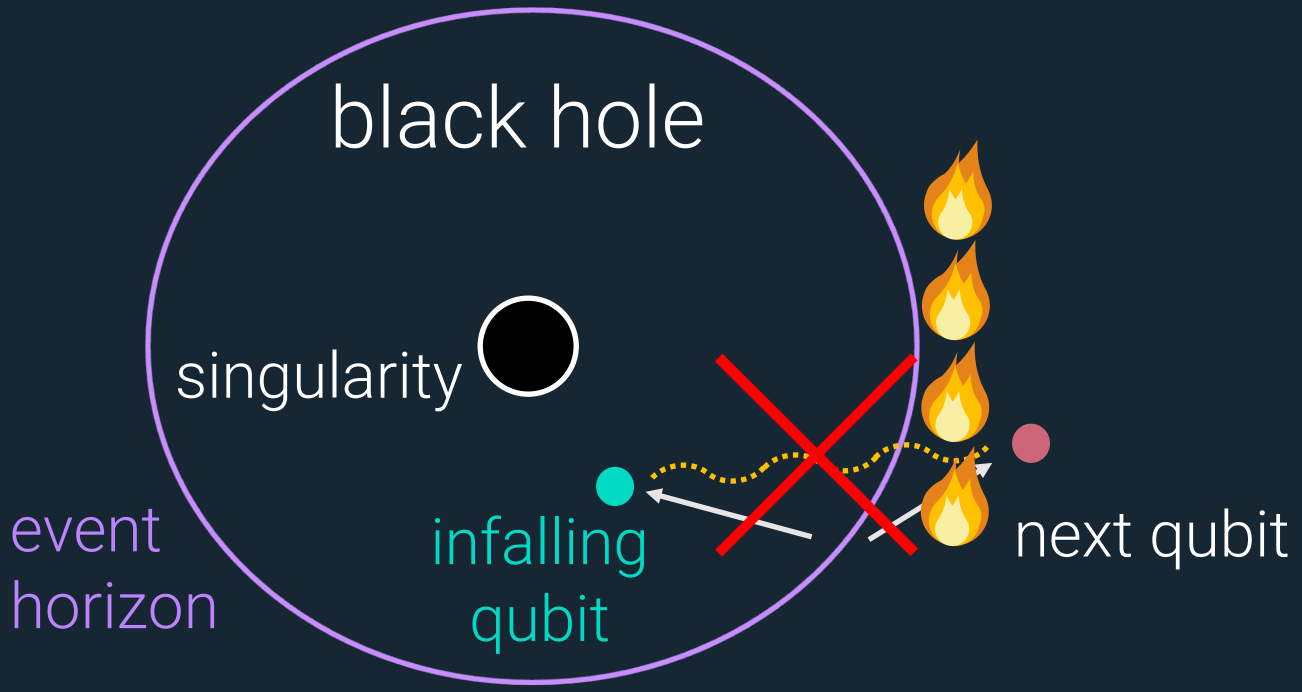
2) Alice uses a quantum computer to “check” that the next qubit is entangled with her collected radiation (e.g., distills an EPR pair).

3) Alice jumps into the black hole.



AMPS11 proposed resolution:

"Firewall" outside event horizon (breaking entanglement)



In 2013, Harlow and Hayden proposed a different resolution to the AMPS paradox based on ***computational complexity***.

In 2013, Harlow and Hayden proposed a different resolution to the AMPS paradox based on ***computational complexity***.

Very cool and surprising!!

[AMPS11] experiment:

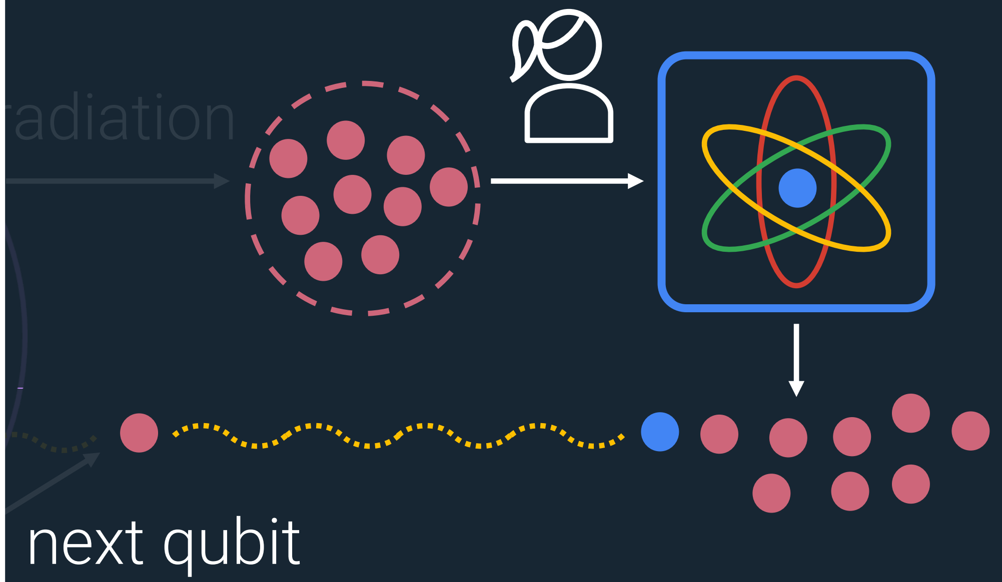
1) Alice collects radiation until 2/3 of black hole has evaporated.

2) Alice uses a quantum computer to “check” that the next qubit is entangled with her collected radiation (e.g., distills an EPR pair).

3) Alice jumps into the black hole.

[Harlow-Hayden 2013]

Under certain cryptographic assumptions, this step can require ***exponential*** time.



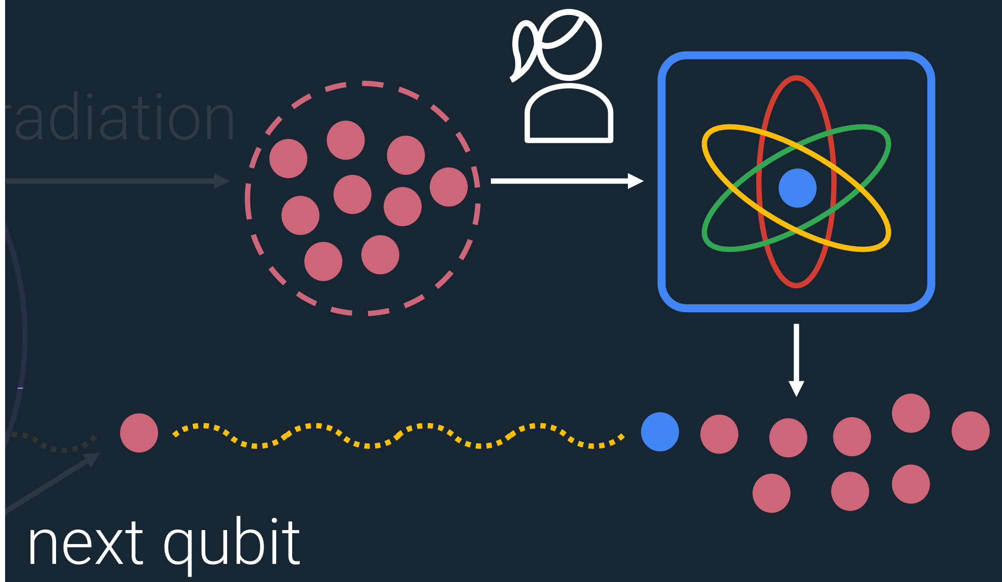
[AMPS11] experiment:

1) Alice collects radiation until 2/3 of black hole has evaporated.

2) Alice uses a quantum computer to "check" that the next qubit is entangled with her collected radiation (e.g., distills an EPR pair).

3) Alice jumps into the black hole.

> **[Harlow-Hayden 2013]**
>
> Under certain cryptographic assumptions, this step can require ***exponential*** time.
>
> By the time she's done decoding, the black hole will have evaporated!



Plan for this talk

(1) Background on black holes

(2) Radiation decoding problem [Harlow-Hayden13]

(3) Radiation *distinguishing* problem

(4) Connection to quantum commitments

(3) + (4) is an alternative view of [Brakerski23].

The Radiation Decoding Problem [HH13]

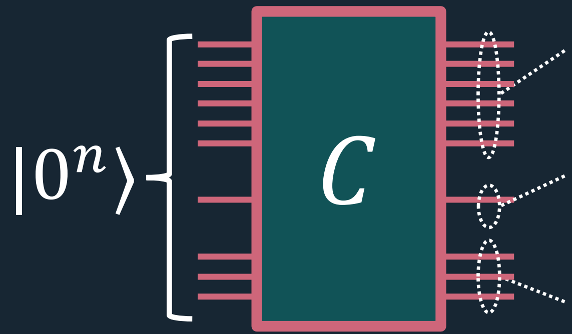
- Let C be a public, $poly(n)$-size quantum circuit.

The Radiation Decoding Problem [HH13]

- Let C be a public, $poly(n)$-size quantum circuit.
- $|\psi\rangle \coloneqq C|0^n\rangle$ corresponds to final state of emitted radiation.

The Radiation Decoding Problem [HH13]

- Let C be a public, $poly(n)$-size quantum circuit.
- $|\psi\rangle \coloneqq C|0^n\rangle$ corresponds to final state of emitted radiation.



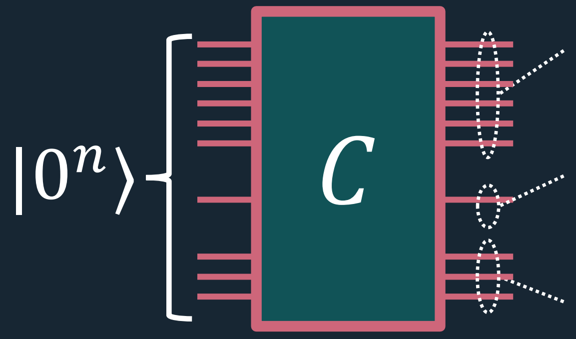
$\mathbf{R}$ = $2n/3$ qubits (radiation emitted so far)

$\mathbf{B}$ = 1 qubit (next qubit of radiation)

$\mathbf{H}$ = everything else

The Radiation Decoding Problem [HH13]

- Let C be a public, $poly(n)$-size quantum circuit.
- $|\psi\rangle \coloneqq C|0^n\rangle$ corresponds to final state of emitted radiation.



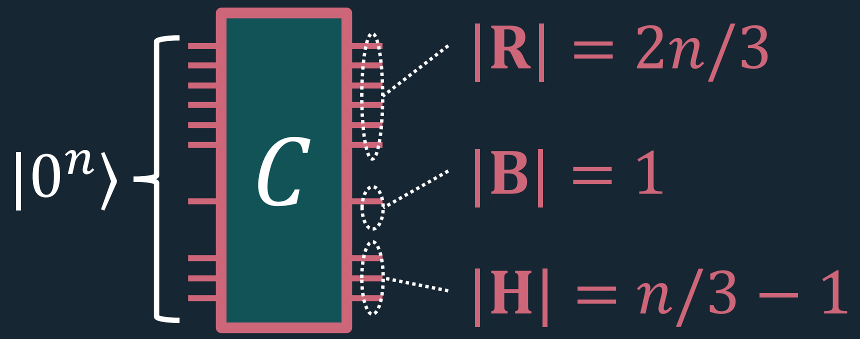
$\mathbf{R} = 2n/3$ qubits (radiation emitted so far)

$\mathbf{B} = 1$ qubit (next qubit of radiation)

$\mathbf{H} =$ everything else

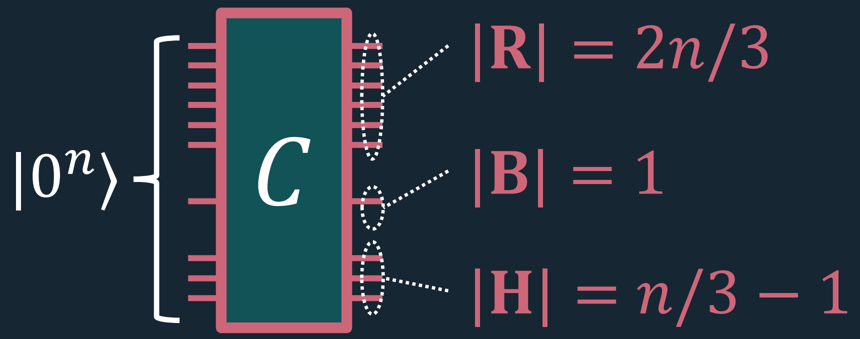
Task: Given $\mathbf{R}$ register of $|\psi\rangle_{\mathbf{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ such that $(\mathbf{A}, \mathbf{B})$ is the EPR state $|00\rangle + |11\rangle$.

(promised that $\mathbf{R}$ and $\mathbf{B}$ are maximally entangled)



Radiation Decoding Problem:

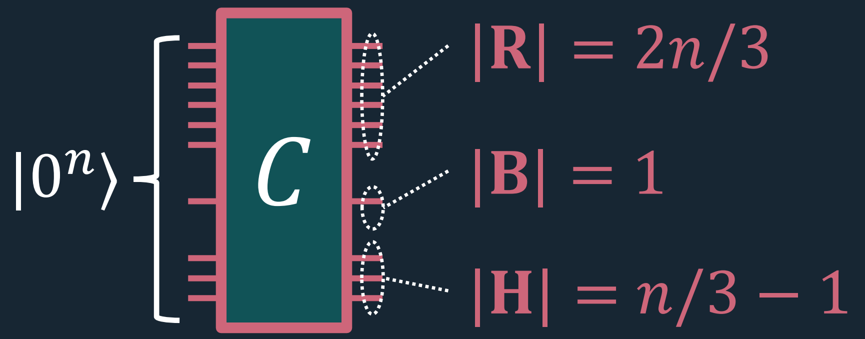
Given $\mathbf{R}$ register of $|\psi\rangle_{\mathbf{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ such that $(\mathbf{A}, \mathbf{B})$ is the EPR state $|00\rangle + |11\rangle$, promised this is possible.



Radiation Decoding Problem:

Given $\mathbf{R}$ register of $|\psi\rangle_{\mathbf{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ such that $(\mathbf{A}, \mathbf{B})$ is the EPR state $|00\rangle + |11\rangle$, promised this is possible.

[HH13]: If SZK $\not\subseteq$ BQP, there exists C s.t. radiation decoding is hard.

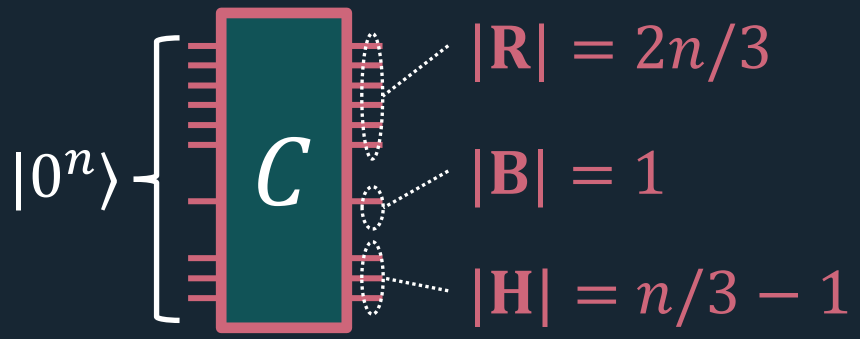


Radiation Decoding Problem:

Given $\mathbf{R}$ register of $|\psi\rangle_{\mathbf{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ such that $(\mathbf{A}, \mathbf{B})$ is the EPR state $|00\rangle + |11\rangle$, promised this is possible.

[HH13]: If SZK $\not\subseteq$ BQP, there exists C s.t. radiation decoding is hard.

"Hard" means no QPT adversary can win with probability $\geq \frac{1}{4} + \mathbf{negl}(n)$ (formalized by [Brakerski23])



Radiation Decoding Problem:

Given $\mathbf{R}$ register of $|\psi\rangle_{\mathbf{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ such that $(\mathbf{A}, \mathbf{B})$ is the EPR state $|00\rangle + |11\rangle$, promised this is possible.

[HH13]: If SZK $\not\subseteq$ BQP, there exists C s.t. radiation decoding is hard.

Later works *weakened* the assumptions needed:

- [Aaronson16]: quantum-secure one-way functions
- [Brakerski23]: quantum bit commitment

Brakerski also showed hardness of radiation decoding implies existence of quantum bit commitments. Thus:

Brakerski also showed hardness of radiation decoding implies existence of quantum bit commitments. Thus:

[Brakerski23]: Radiation decoding is hard **if and only** if quantum bit commitments exist.

Brakerski also showed hardness of radiation decoding implies existence of quantum bit commitments. Thus:

[Brakerski23]: Radiation decoding is hard **if and only** if quantum bit commitments exist.

Why cryptographers care: quantum commitments imply many important primitives, e.g., quantum oblivious transfer, multi-party computation, and zero knowledge.

Brakerski also showed hardness of radiation decoding implies existence of quantum bit commitments. Thus:

[Brakerski23]: Radiation decoding is hard **if and only** if quantum bit commitments exist.

Why cryptographers care: quantum commitments imply many important primitives, e.g., quantum oblivious transfer, multi-party computation, and zero knowledge.

"This can be viewed (with proper disclaimers, as we discuss) as providing a physical justification for the existence of secure cryptography" – [Brakerski23]

Rest of today: new perspective on Brakerski's result/proof.

Plan for this talk

(1) Background on black holes

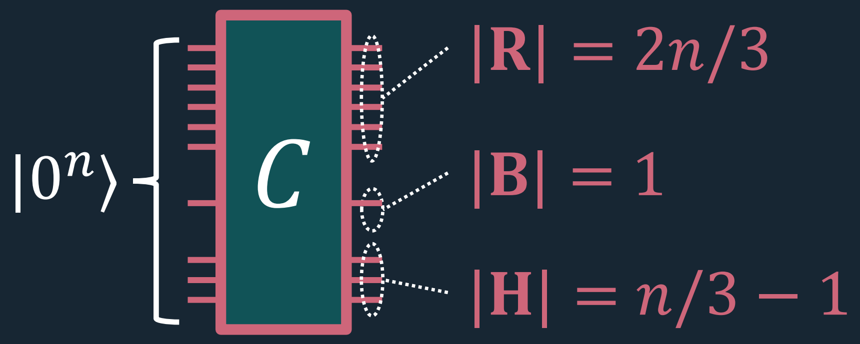
(2) Radiation decoding problem [Harlow-Hayden13]

(3) Radiation *distinguishing* problem

(4) Connection to quantum commitments

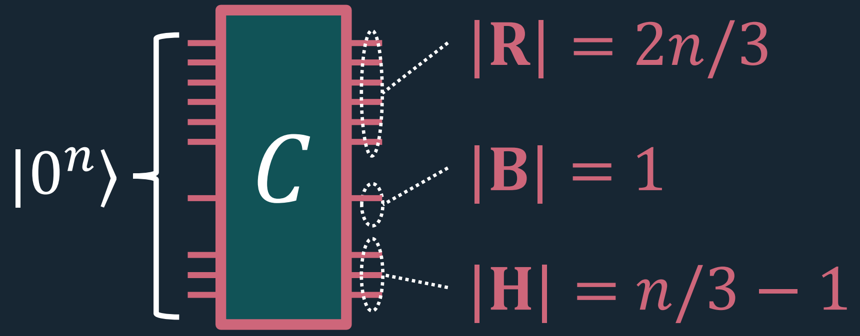
(3) + (4) is an alternative view of [Brakerski23].

Instead of studying the [HH13] radiation **decoding** problem, we'll define a new radiation **distinguishing** problem.



Radiation Decoding Problem:

Given $\mathbf{R}$ register of $|\psi\rangle_{\mathbf{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ s.t. $(\mathbf{A}, \mathbf{B})$ is the EPR state.

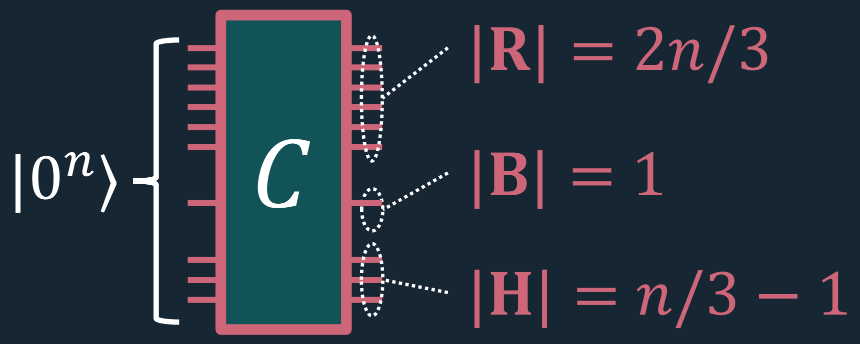


Radiation Decoding Problem:

Given $\mathbf{R}$ register of $|\psi\rangle_{\mathbf{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ s.t. $(\mathbf{A}, \mathbf{B})$ is the EPR state.

The point:

$\mathbf{R}$ and $\mathbf{B}$ are maximally entangled, but this entanglement isn't efficiently detectable.



Radiation Decoding Problem:

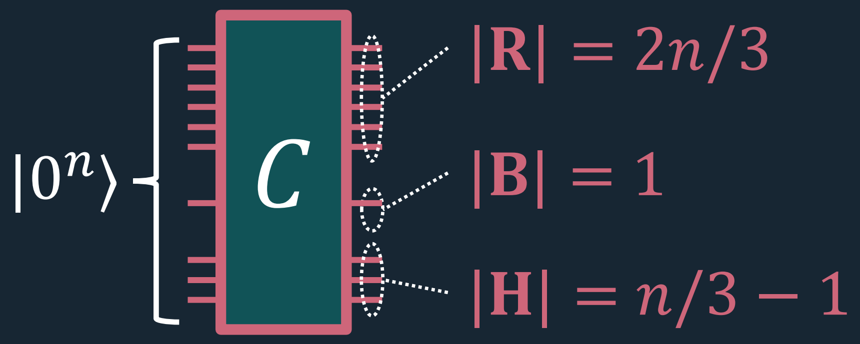
Given $\mathbf{R}$ register of $|\psi\rangle_{\mathbf{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ s.t. $(\mathbf{A}, \mathbf{B})$ is the EPR state.

Radiation Distinguishing Problem:

Distinguish $(\mathbf{R}, \mathbf{B})$ from $(\mathbf{R}, \mathbf{B}')$ where $\mathbf{B}'$ is an unentangled, maximally mixed qubit.

The point:

$\mathbf{R}$ and $\mathbf{B}$ are maximally entangled, but this entanglement isn't efficiently detectable.



Radiation Decoding Problem:

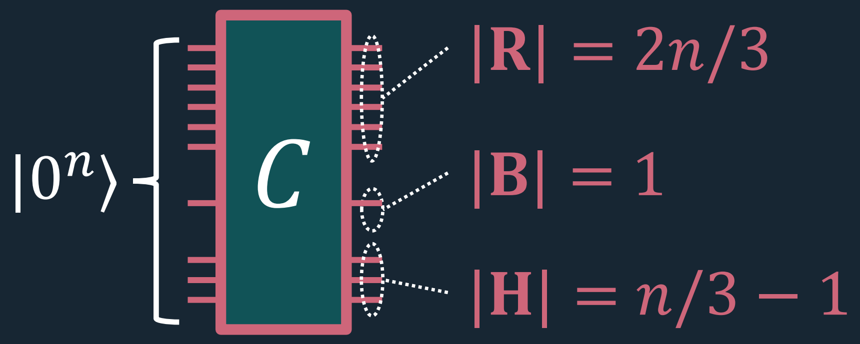
Given $\mathbf{R}$ register of $|\psi\rangle_{\mathbf{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ s.t. $(\mathbf{A}, \mathbf{B})$ is the EPR state.

Radiation Distinguishing Problem:

Distinguish $(\mathbf{R}, \mathbf{B})$ from $(\mathbf{R}, \mathbf{B}')$ where $\mathbf{B}'$ is an unentangled, maximally mixed qubit.

Claim 1: Distinguishing is easier than decoding.

If you can solve the decoding problem with advantage $1/4 + \varepsilon$, you can distinguish with advantage ε.



Radiation Decoding Problem:

Given $\mathbf{R}$ register of $|\psi\rangle_{\mathbf{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ s.t. $(\mathbf{A}, \mathbf{B})$ is the EPR state.

Radiation Distinguishing Problem:

Distinguish $(\mathbf{R}, \mathbf{B})$ from $(\mathbf{R}, \mathbf{B}')$ where $\mathbf{B}'$ is an unentangled, maximally mixed qubit.

Claim 1: Distinguishing is easier than decoding.

If you can solve the decoding problem with advantage $1/4 + \varepsilon$, you can distinguish with advantage ε.

Claim 2: Distinguishing should still be hard.

If Alice can't trigger a firewall, then she shouldn't be able to detect entanglement between $\mathbf{B}$ and $\mathbf{R}$ in the AMPS experiment.

Plan for this talk

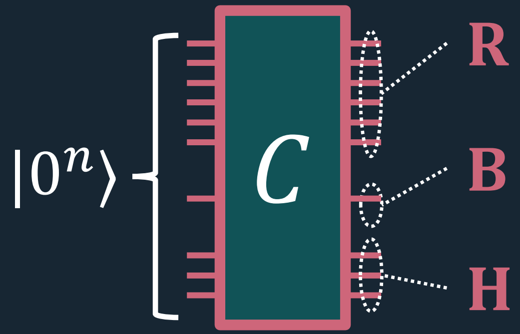
(1) Background on black holes

(2) Radiation decoding problem [Harlow-Hayden13]

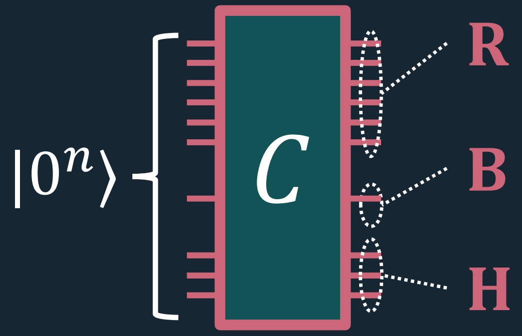
(3) Radiation ***distinguishing*** problem

(4) Connection to quantum commitments

(3) + (4) is an alternative view of [Brakerski23].

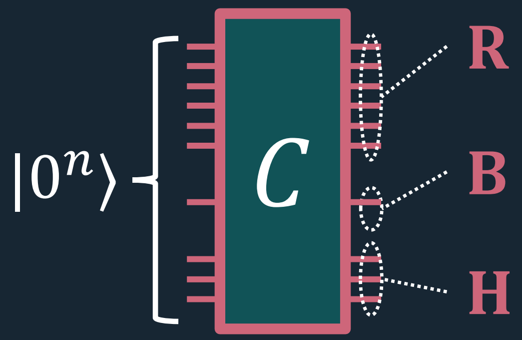


Radiation Distinguishing Problem:
Distinguish $(\mathbf{R}, \mathbf{B})$ from $(\mathbf{R}, \mathbf{B}')$ where $\mathbf{B}'$ is an unentangled, maximally mixed qubit.



Radiation Distinguishing Problem:
Distinguish $(\mathbf{R}, \mathbf{B})$ from $(\mathbf{R}, \mathbf{B}')$ where $\mathbf{B}'$ is an unentangled, maximally mixed qubit.

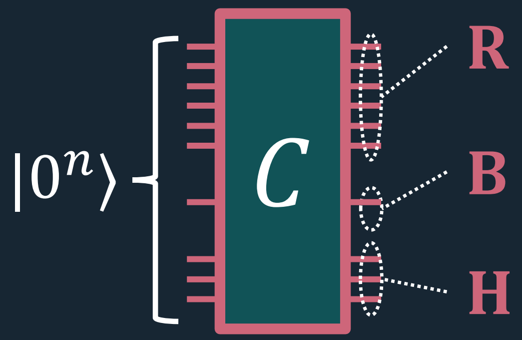
Claim: this is ***already*** a natural crypto assumption.



Radiation Distinguishing Problem:
Distinguish $(\mathbf{R}, \mathbf{B})$ from $(\mathbf{R}, \mathbf{B}')$ where $\mathbf{B}'$ is an unentangled, maximally mixed qubit.

Claim: this is ***already*** a natural crypto assumption.

Radiation Distinguishing is hard if and only if *quantum commitments to the EPR state* exist.



Radiation Distinguishing Problem:
Distinguish $(\mathbf{R}, \mathbf{B})$ from $(\mathbf{R}, \mathbf{B}')$ where $\mathbf{B}'$ is an unentangled, maximally mixed qubit.

Claim: this is ***already*** a natural crypto assumption.

Radiation Distinguishing is hard if and only if *quantum commitments to the EPR state* exist.

Up next: define commitments to quantum states

Quantum State Commitments

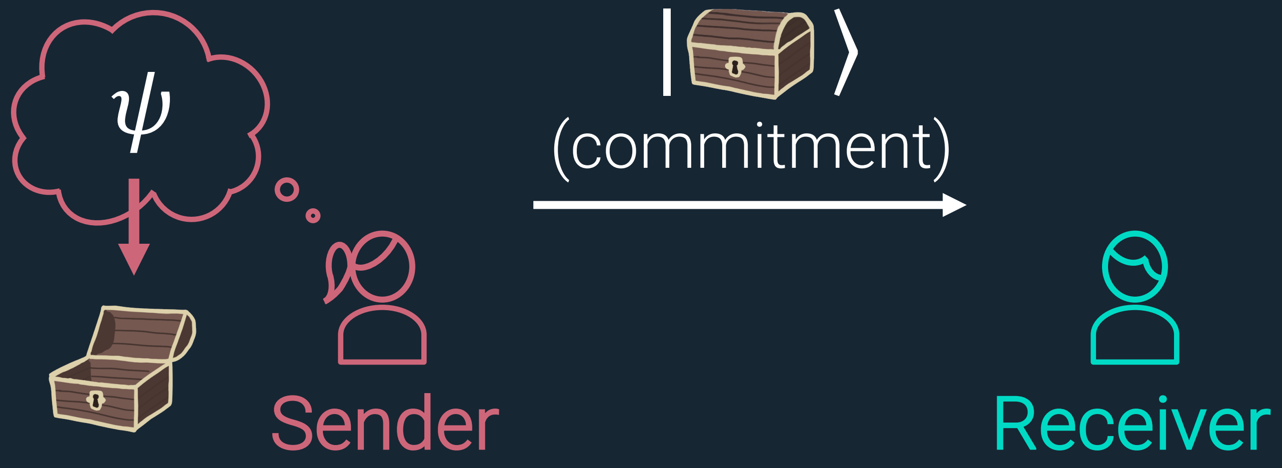
[Gunn-Ju-M-Zhandry23]

Protocol that lets a sender commit to a (possibly entangled) quantum state ψ, with the ability to reveal ψ later.

Quantum State Commitments

[Gunn-Ju-M-Zhandry23]

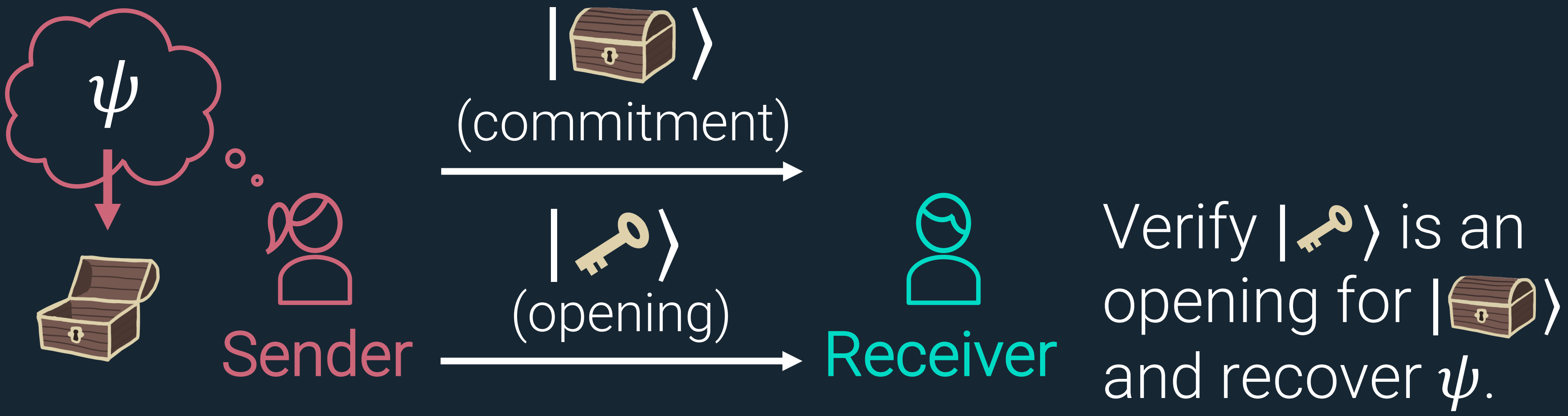
Protocol that lets a sender commit to a (possibly entangled) quantum state ψ, with the ability to reveal ψ later.



Quantum State Commitments

[Gunn-Ju-M-Zhandry23]

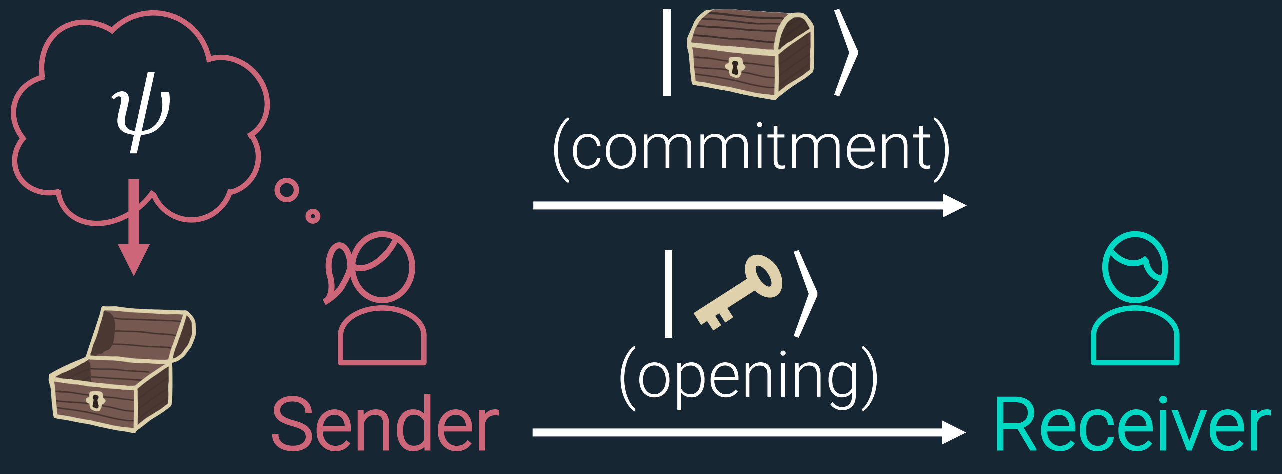
Protocol that lets a sender commit to a (possibly entangled) quantum state ψ, with the ability to reveal ψ later.



Quantum State Commitments

[Gunn-Ju-M-Zhandry23]

Protocol that lets a sender commit to a (possibly entangled) quantum state ψ, with the ability to reveal ψ later.



Verify |🔑⟩ is an opening for |🧰⟩ and recover ψ.

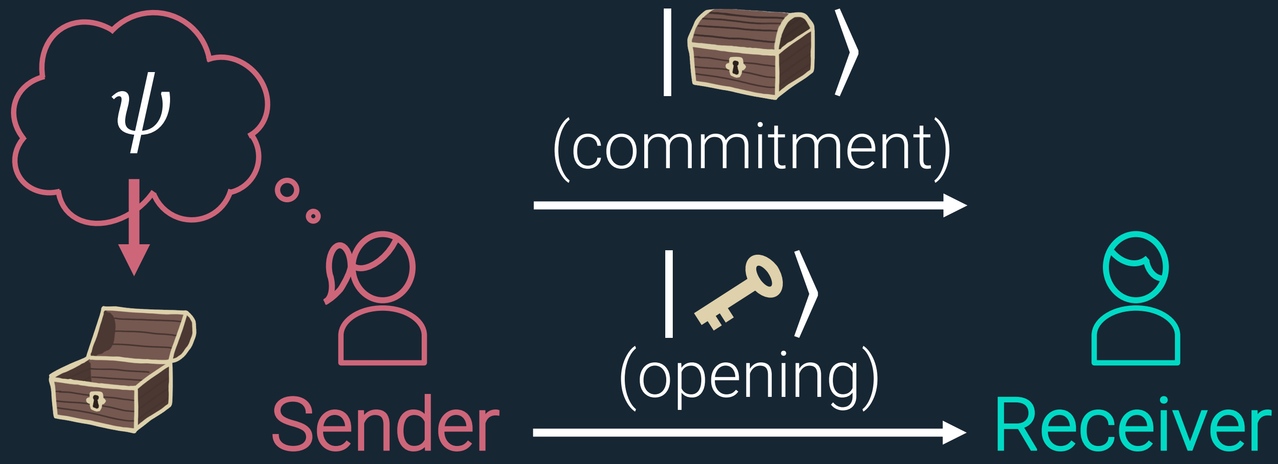
Hiding: |🧰⟩ hides message from receiver.

Binding: after sending |🧰⟩, sender can't change ψ.

Quantum State Commitments

[Gunn-Ju-M-Zhandry23]

Protocol that lets a sender commit to a (possibly entangled) quantum state ψ, with the ability to reveal ψ later.



Verify |⟩ is an opening for |⟩ and recover ψ.

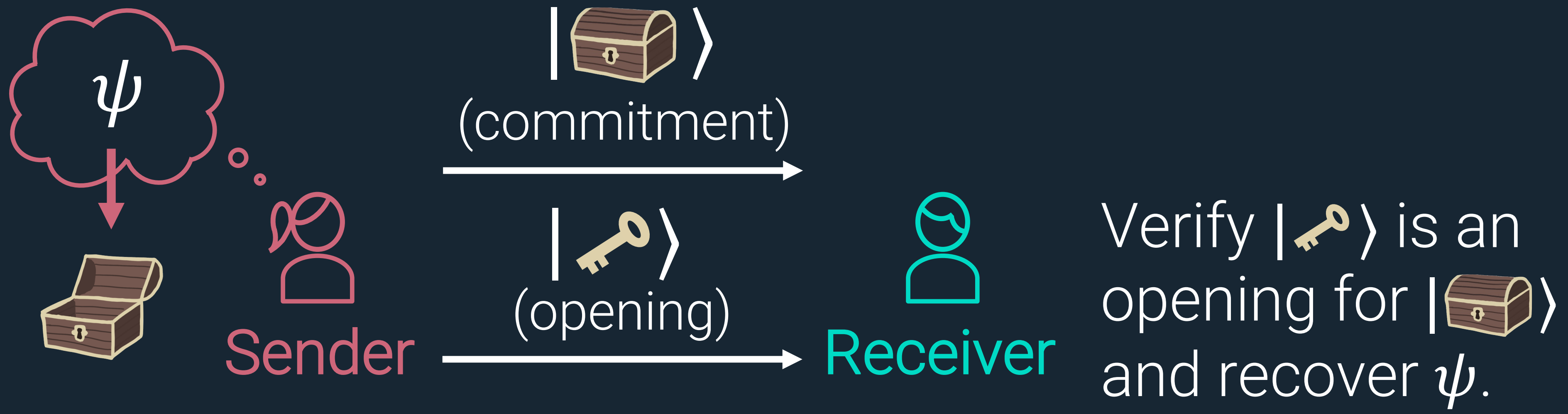
Hiding: |⟩ hides message from receiver.

Binding: after sending |⟩, sender can't change ψ.

Quantum State Commitments

[Gunn-Ju-M-Zhandry23]

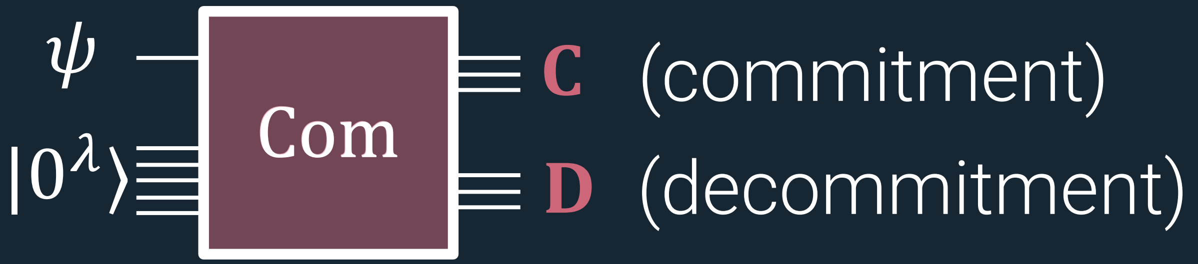
Protocol that lets a sender commit to a (possibly entangled) quantum state ψ, with the ability to reveal ψ later.



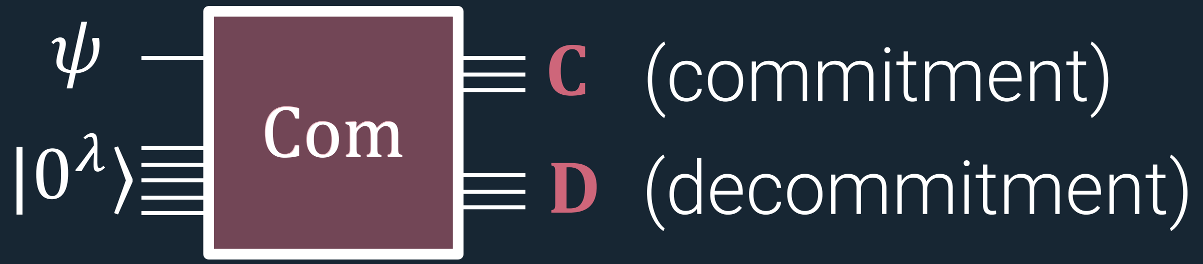
- Requires computational assumptions [M96, LC96].
- Exist if and only if quantum bit commitments exist.

Commitment Syntax

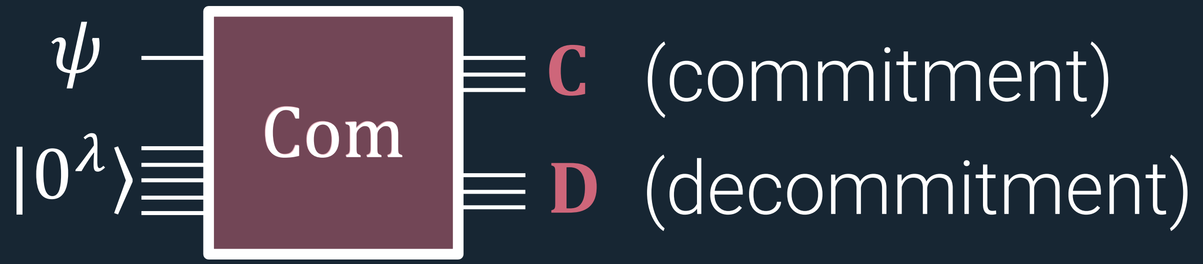
Commitment Syntax

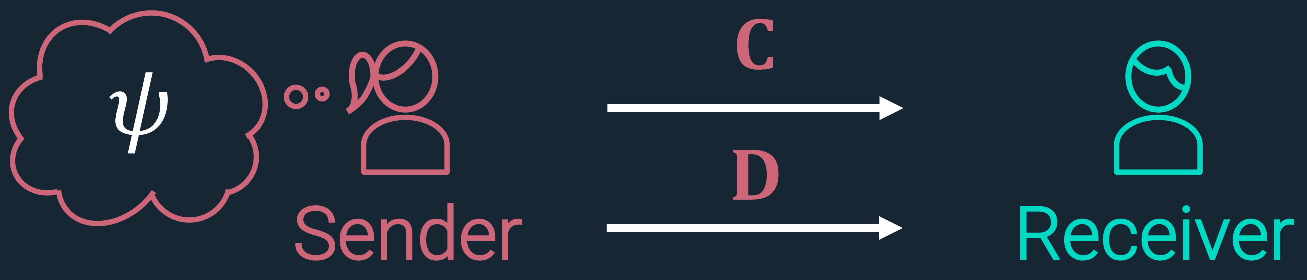


Commitment Syntax

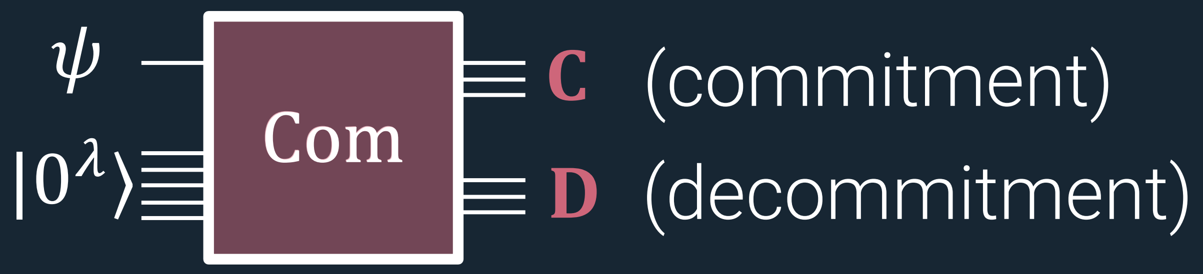


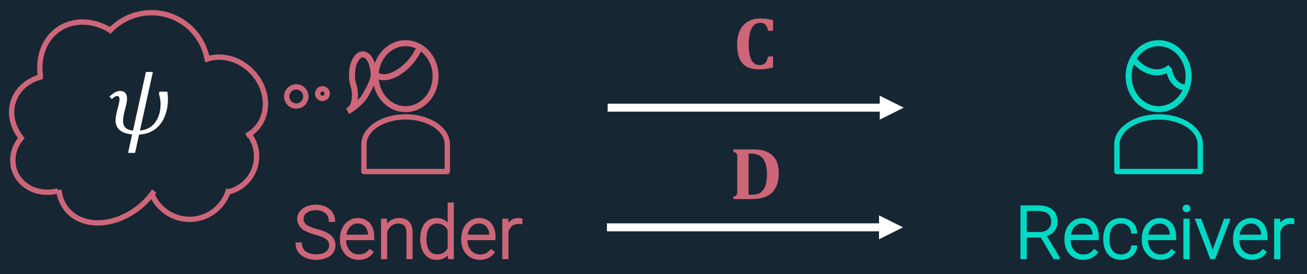
Commitment Syntax





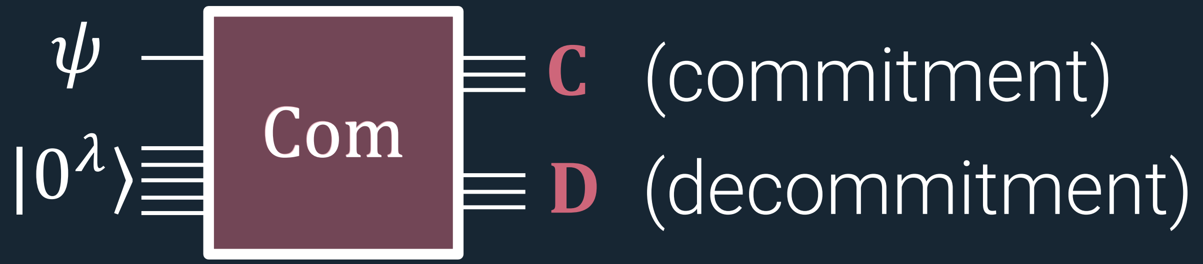
Commitment Syntax



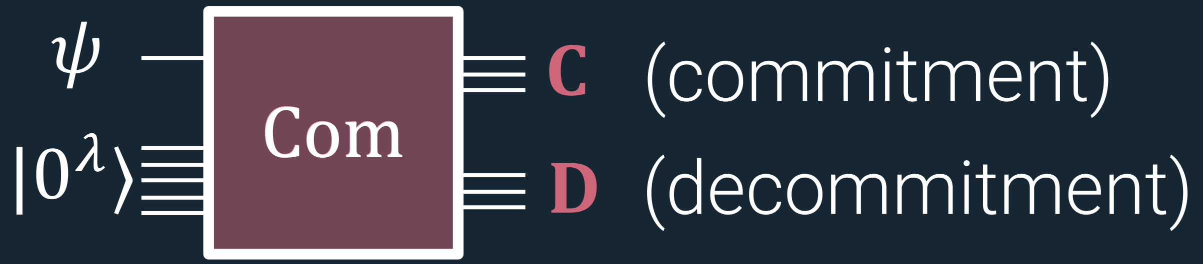


To verify $(\mathbf{C}, \mathbf{D})$, receiver applies $\mathtt{Com}^\dagger$ and checks if last λ bits are $\mathbf{0}$.

Security: Binding and Hiding

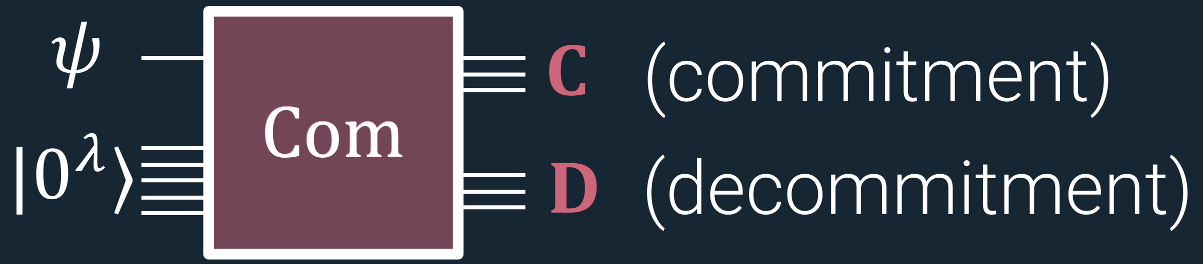


Security: Binding and Hiding



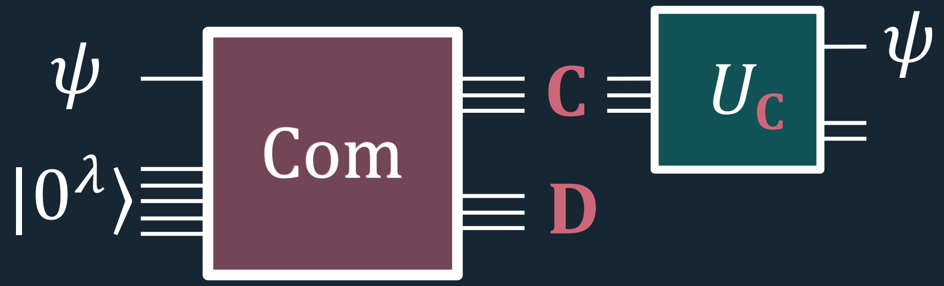
Statistical binding: **C** info-theoretically determines/contains ψ.

Security: Binding and Hiding

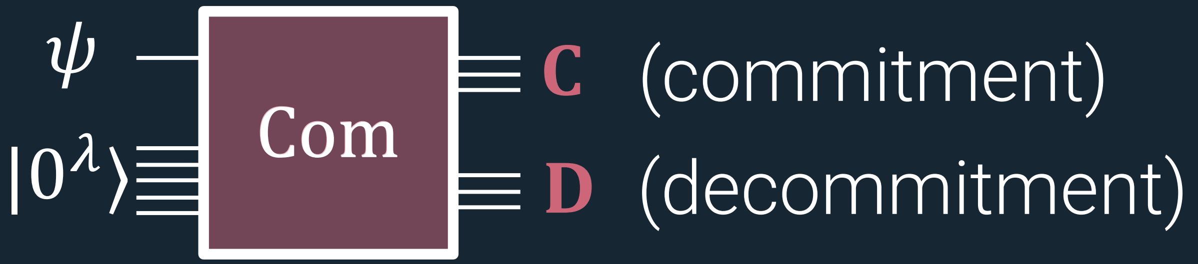


Statistical binding: C info-theoretically determines/contains ψ.

Exists an inefficient unitary $U_{\mathbf{C}}$ that recovers ψ from C alone.



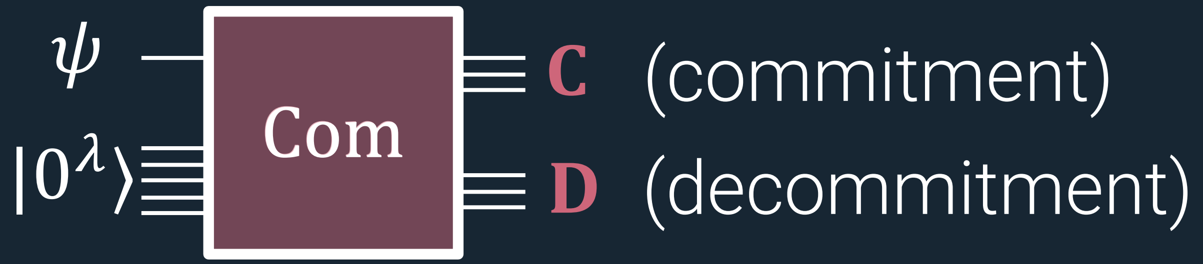
Security: Binding and Hiding



Statistical binding: **C** info-theoretically determines/contains ψ.

Computational hiding: no QPT adversary can distinguish:
(1) commitment to ψ of the adversary's choice
(2) commitment to junk (e.g., maximally mixed state)

Security: Binding and Hiding



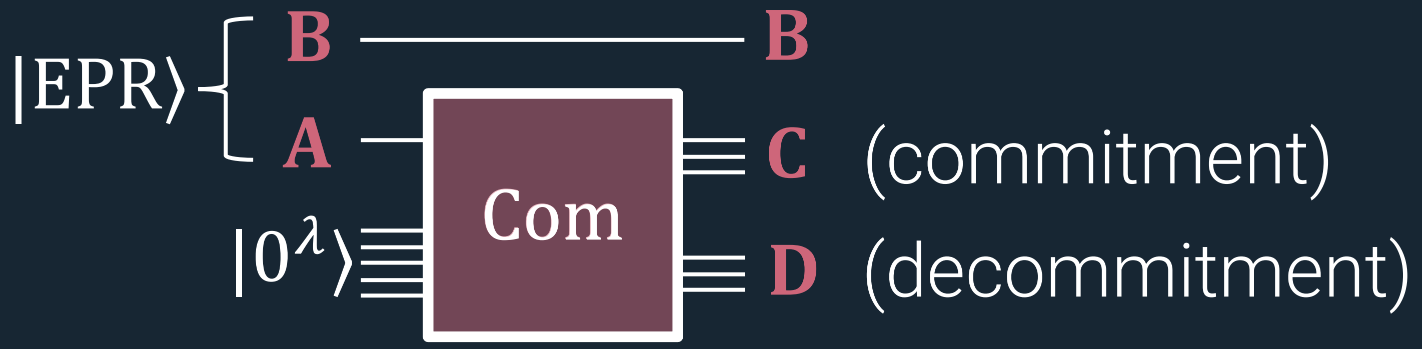
Statistical binding: C info-theoretically determines/contains ψ.

Computational hiding: no QPT adversary can distinguish:
(1) commitment to ψ of the adversary's choice
(2) commitment to junk (e.g., maximally mixed state)

Crucial point: since adversary picks ψ, indistinguishability holds even if the adversary has a state entangled with ψ.

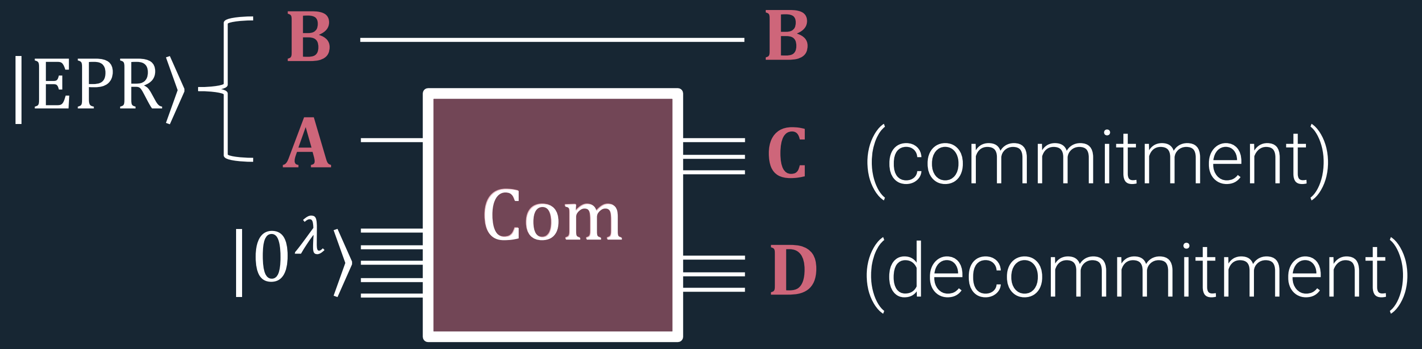
Commitments to the EPR State

Setup: Prepare $|\mathrm{EPR}\rangle_{\mathbf{AB}}$ and commit to $\mathbf{A}$.



Commitments to the EPR State

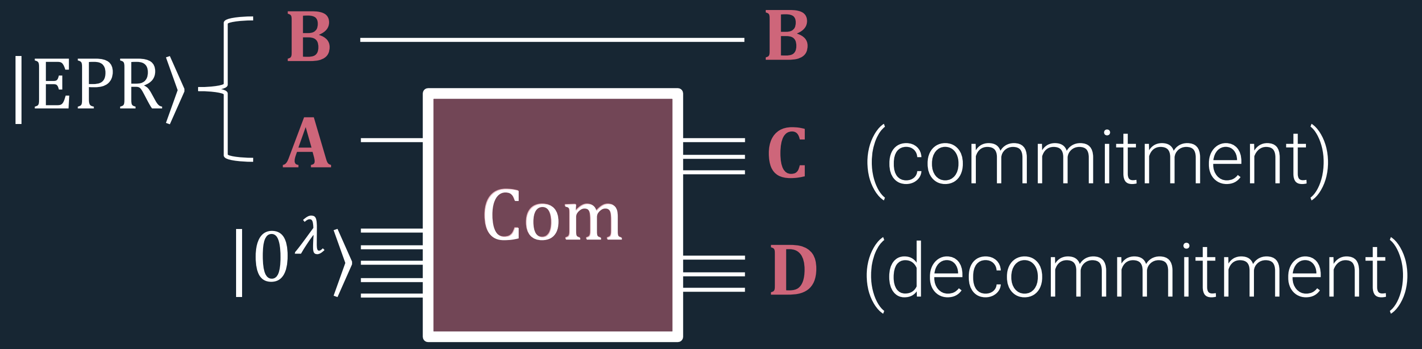
Setup: Prepare $|\mathrm{EPR}\rangle_{\mathbf{AB}}$ and commit to $\mathbf{A}$.



Statistical Binding: $\mathbf{B}$ and $\mathbf{C}$ are maximally entangled.

Commitments to the EPR State

Setup: Prepare $|\mathrm{EPR}\rangle_{\mathbf{AB}}$ and commit to $\mathbf{A}$.

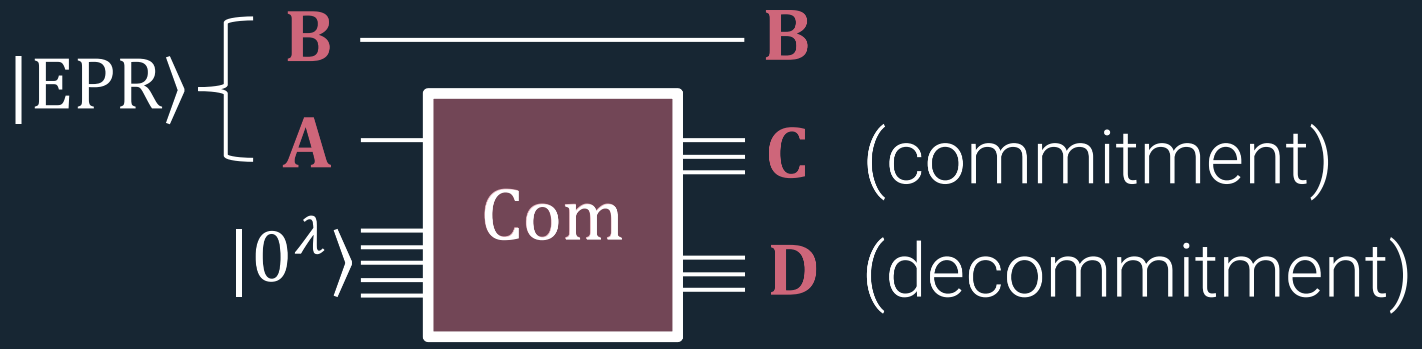


Statistical Binding: $\mathbf{B}$ and $\mathbf{C}$ are maximally entangled.

Computational Hiding: $(\mathbf{B}, \mathbf{C})$ indistinguishable from $(\mathbf{B}, \mathbf{C}')$ where $\mathbf{C}'$ is a commitment to a maximally mixed state

Commitments to the EPR State

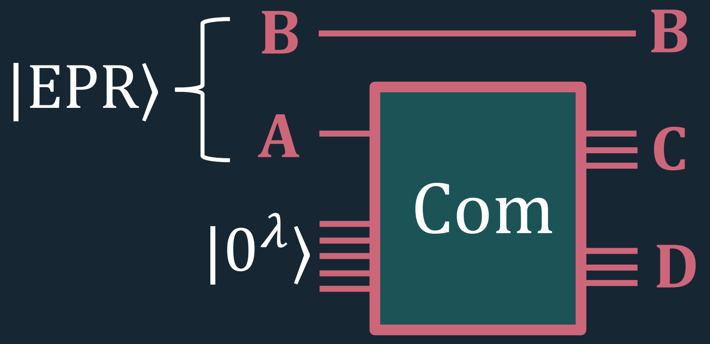
Setup: Prepare $|\mathrm{EPR}\rangle_{\mathbf{AB}}$ and commit to $\mathbf{A}$.



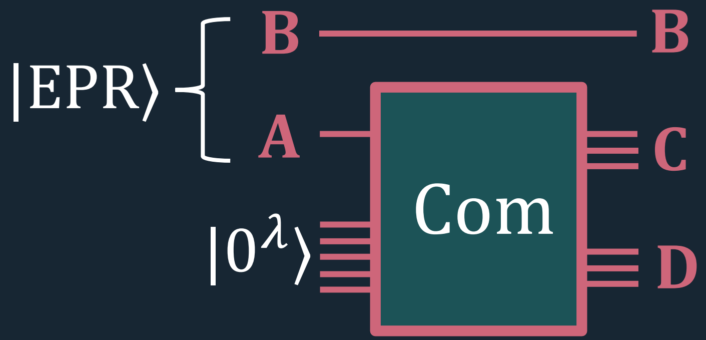
Statistical Binding: $\mathbf{B}$ and $\mathbf{C}$ are maximally entangled.

Computational Hiding: $(\mathbf{B}, \mathbf{C})$ indistinguishable from $(\mathbf{B}, \mathbf{C}')$ where $\mathbf{C}'$ is a commitment to a maximally mixed state

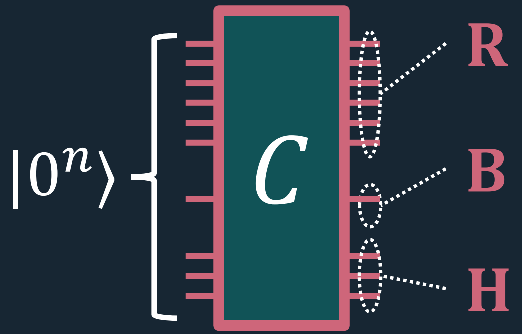
Fact: $(\mathbf{B}, \mathbf{C}')$ is distributed as $(\mathbf{B}', \mathbf{C})$ for $\mathbf{B}'$ maximally mixed.



Breaking Hiding of EPR Commitment:
Promised that **B** and **C** are maximally entangled, distinguish (**B**, **C**) from (**B′**, **C**) where **B′** is an unentangled, maximally mixed qubit.

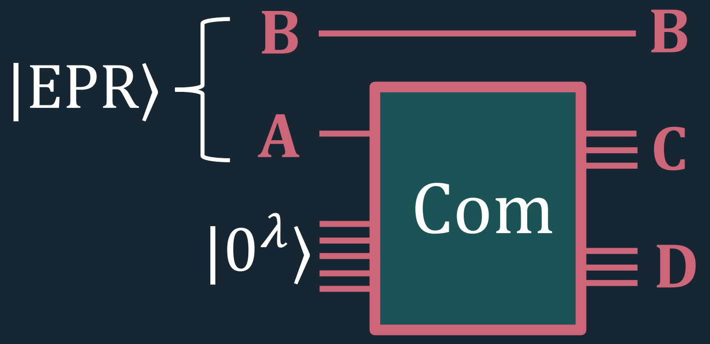


Breaking Hiding of EPR Commitment:
Promised that **B** and **C** are maximally entangled, distinguish (**B**, **C**) from (**B′**, **C**) where **B′** is an unentangled, maximally mixed qubit.

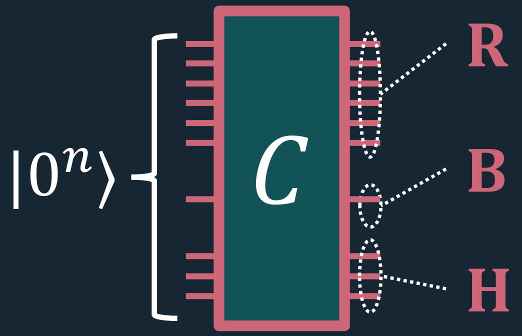


Radiation Distinguishing Problem:
Promised that **B** and R are maximally entangled, distinguish (**B**, **R**) from (**B′**, **R**) where **B′** is an unentangled, maximally mixed qubit.

Thus, quantum commitments → hard radiation distinguishing.



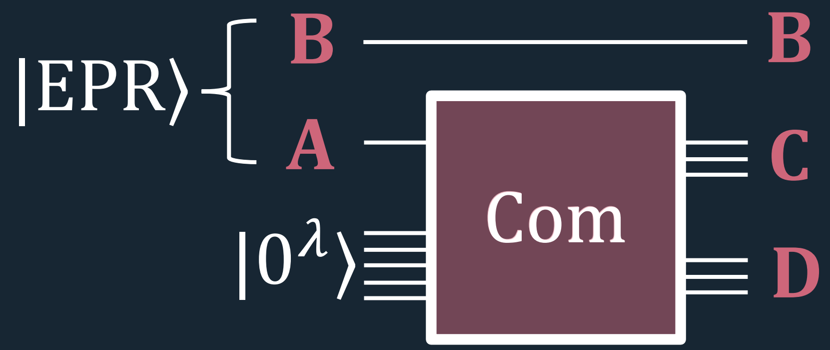
Breaking Hiding of EPR Commitment:
Promised that **B** and **C** are maximally entangled, distinguish (**B**, **C**) from (**B**′, **C**) where **B**′ is an unentangled, maximally mixed qubit.



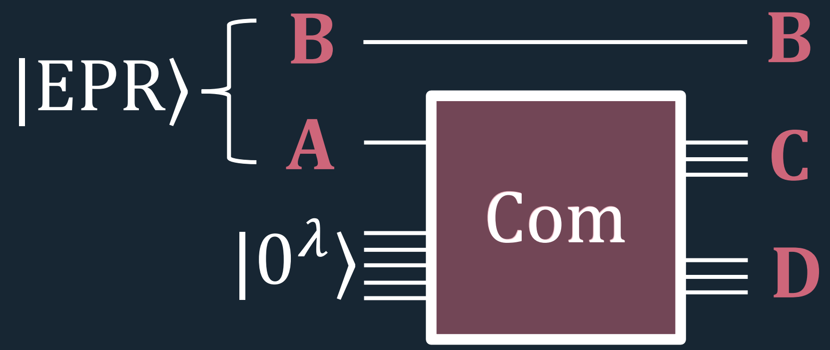
Radiation Distinguishing Problem:
Promised that **B** and **R** are maximally entangled, distinguish (**B**, **R**) from (**B**′, **R**) where **B**′ is an unentangled, maximally mixed qubit.

One last thing: to show hard radiation distinguishing → crypto, need to show EPR commitments → commitments to any state.

EPR Commitments → Commitment to Any State

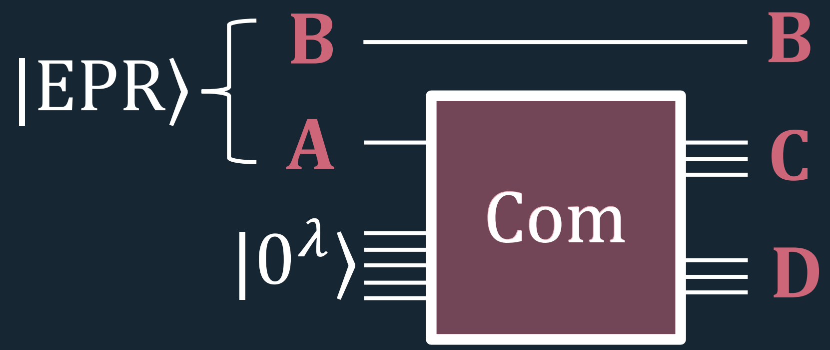


EPR Commitments → Commitment to Any State



Just teleport ψ into $\mathbf{C}$: to commit to ψ, measure $(\psi, \mathbf{B})$ in the Bell basis to get classical bits (x, z), and send $(\mathbf{C}, x, z)$.

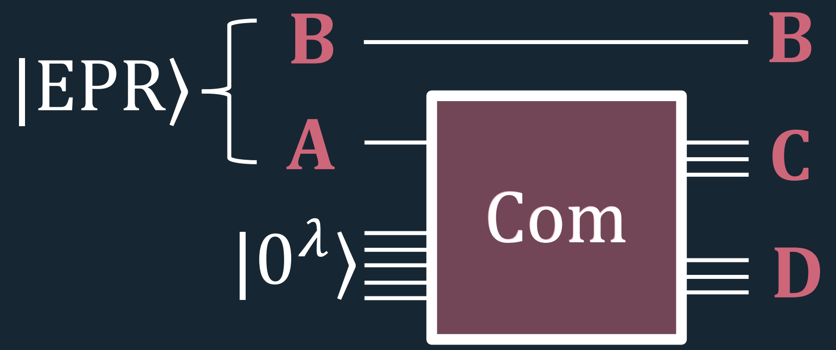
EPR Commitments → Commitment to Any State



Just teleport ψ into **C**: to commit to ψ, measure $(\psi, \mathbf{B})$ in the Bell basis to get classical bits (x, z), and send $(\mathbf{C}, x, z)$.

- **Statistical Binding:** **C** determines **A**. $(\mathbf{A}, x, z)$ determines ψ.

EPR Commitments → Commitment to Any State



Just teleport ψ into $\mathbf{C}$: to commit to ψ, measure $(\psi, \mathbf{B})$ in the Bell basis to get classical bits (x, z), and send $(\mathbf{C}, x, z)$.

- **Statistical Binding:** $\mathbf{C}$ determines $\mathbf{A}$. $(\mathbf{A}, x, z)$ determines ψ.
- **Computational Hiding:** $(\mathbf{C}, x, z)$ indistinguishable from $(\mathbf{C}', x, z)$ where $\mathbf{C}'$ is a commitment to junk, but this is independent of ψ.

Conclusion

Tight relationship between a problem from black hole physics and quantum cryptography.

Conclusion

Tight relationship between a problem from black hole physics and quantum cryptography.

- In black hole physics, C is a random $\mathbf{poly}(n)$-size circuit.
- Plausible crypto assumption: random quantum circuits give secure commitments.

Conclusion

Tight relationship between a problem from black hole physics and quantum cryptography.

- In black hole physics, C is a random $\mathbf{poly}(n)$-size circuit.
- Plausible crypto assumption: random quantum circuits give secure commitments.

Future research direction: give more evidence for hardness.

Given description of a random circuit C, how hard is it to distinguish $C|0^n\rangle$ from $C|1^n\rangle$ given $2n/3$ of the qubits?