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?

“Black-Hole Radiation Decoding is Quantum Cryptography.”

3) What does this mean?
You might be wondering...

1) What does this mean?

"Black-Hole Radiation Decoding is Quantum Cryptography."

2) What does this mean?

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

singularity

event horizon
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 \textit{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 \textit{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**.
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:

black hole

singularity

event horizon
[AMPS11] experiment:
1) Alice collects radiation until \(\frac{2}{3}\) 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.

Also maximally entangled!
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, $\text{poly}(n)$-size quantum circuit.
The Radiation Decoding Problem [HH13]

• Let $C$ be a public, $poly(n)$-size quantum circuit.
• $|\psi\rangle := C|0^n\rangle$ corresponds to final state of emitted radiation.
The Radiation Decoding Problem [HH13]

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

$|0^n\rangle$

\[
C \quad \Rightarrow \quad R = \frac{2n}{3} \text{ qubits (radiation emitted so far)}
\]

\[
B = 1 \text{ qubit (next qubit of radiation)}
\]

\[
H = \text{everything else}
\]
The Radiation Decoding Problem [HH13]

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

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

(promise that $R$ and $B$ are maximally entangled)
Radiation Decoding Problem:

Given $\mathbf{R}$ register of $|\psi\rangle_{\text{RBH}} = C|0^n\rangle$, 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 $\text{SZK} \not\subseteq \text{BQP}$, there exists $C$ s.t. radiation decoding is hard.

**Radiation Decoding Problem:**

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

"Hard" means no QPT adversary can win with probability $\geq \frac{1}{4} + \text{negl}(n)$

(formalized by [Brakerski23])

[HH13]: If SZK $\not\subseteq$ BQP, there exists $C$ s.t. radiation decoding is hard.
Radiation Decoding Problem:
Given $\mathbf{R}$ register of $|\psi\rangle_{\text{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ such that $(\mathbf{A}, \mathbf{B})$ is the EPR state $|00\rangle + |11\rangle$, promised this is possible.

Later works weakened the assumptions needed:
- [Aaronson16]: quantum-secure one-way functions
- [Brakerski23]: quantum bit commitment

[HH13]: If SZK $\not\subseteq$ BQP, there exists $C$ s.t. radiation decoding is hard.
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 $|\psi\rangle_{\text{RBH}} = C|0^n\rangle$, output a single qubit $\mathbf{A}$ s.t. $(\mathbf{A}, \mathbf{B})$ is the EPR state.
Radiation Decoding Problem:
Given $\mathbf{R}$ register of $|\psi\rangle_{RBH} = C |0^n\rangle$, 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 $R$ register of $|\psi\rangle_{RBH} = C|0^n\rangle$, output a single qubit $A$ s.t. $(A, B)$ is the EPR state.

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

The point:
$R$ and $B$ 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 $\varepsilon$. 
Radiation Decoding Problem:
Given $\mathbf{R}$ register of $|\psi\rangle_{\text{RBH}} = C|0^n\rangle$, 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 $\varepsilon$.

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 \((R, B)\) from \((R, B')\) where \(B'\) 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.
Distinguish $|0^n\rangle$ 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 $(R, B)$ from $(R, B')$ where $B'$ 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 $\psi$, with the ability to reveal $\psi$ later.
Quantum State Commitments

[Gunn-Ju-M-Zhandry23]

Protocol that lets a sender commit to a (possibly entangled) quantum state $\psi$, with the ability to reveal $\psi$ later.
Quantum State Commitments

[Gun-Ju-M-Zhandry23]

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

$\psi$ (commitment)

Verifier

$\psi$ (opening)

Receive

Verify $|\bar{\psi}\rangle$ is an opening for $|\psi\rangle$ and recover $\psi$. 
Quantum State Commitments

[Gun-Ju-M-Zhandry23]

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

- **Hiding**: $|\top\rangle$ hides message from receiver.
- **Binding**: After sending $|\top\rangle$, sender can't change $\psi$.

Verify $|\top\rangle$ is an opening for $|\bot\rangle$ and recover $\psi$. 
Quantum State Commitments

[Gunn-Ju-M-Zhandry23]

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

$\psi$ (commitment) $(\text{opening})$ $\psi$

Sender Receiver

Hiding: $\ket{\text{box}}$ hides message from receiver.

Binding: after sending $\ket{\text{box}}$, sender can’t change $\psi$.

Verify $\ket{\text{key}}$ is an opening for $\ket{\text{box}}$ and recover $\psi$. 
Quantum State Commitments

[Gunn-Ju-M-Zhandry23]

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

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

(sender) $\psi$ $\rightarrow$ (commitment) $|\psi\rangle$ $\rightarrow$ (opening) $|\psi\rangle$ (receiver)

Verify $|\psi\rangle$ is an opening for $|\psi\rangle$ and recover $\psi$. 

Commitment Syntax

\( \psi \)  

Sender

Receiver
Commitment Syntax

\[ \psi \rightarrow \text{Com} \]

\[ |0^\lambda\rangle \rightarrow C \quad (\text{commitment}) \]

\[ D \quad (\text{decommitment}) \]

Sender

Receiver
Commitment Syntax

ψ → Com → C (commitment) D (decommitment)

ψ

|0^λ⟩

Sender

Receiver
Commitment Syntax

\[ \psi \quad \text{Com} \quad (\text{commitment}) \]

\[ |0^\lambda\rangle \quad \text{D} \quad (\text{decommitment}) \]

Sender \[\psi\] \quad \text{Com} \quad \text{C} \quad \text{D} \quad \text{Receiver}
Commitment Syntax

To verify \((C, D)\), receiver applies \(\text{Com}^\dagger\) and checks if last \(\lambda\) bits are 0.
Security: Binding and Hiding

\[ \psi \quad \text{Com} \quad C \text{ (commitment)} \]

\[ \left| 0^\lambda \right> \quad D \text{ (decommitment)} \]
Security: Binding and Hiding

Statistical binding: $C$ info-theoretically determines/contains $\psi$. 
Security: Binding and Hiding

Statistical binding: \( C \) info-theoretically determines/contains \( \psi \).

Exists an inefficient unitary \( U_C \) that recovers \( \psi \) from \( C \) alone.
Security: Binding and Hiding

Statistical binding: \( C \) info-theoretically determines/contains \( \psi \).

Computational hiding: no QPT adversary can distinguish:
(1) commitment to \( \psi \) 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 \( \psi \).

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

Crucial point: since adversary picks \( \psi \), indistinguishability holds even if the adversary has a state entangled with \( \psi \).
Commitments to the EPR State

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

$|\text{EPR}\rangle \leftarrow B \quad B \quad A \quad A \quad \text{Com} \quad C \quad (\text{commitment}) \quad D \quad (\text{decommitment})$
Commitments to the EPR State

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

$|\text{EPR}\rangle$

\[
\begin{array}{c}
  B \\
  A \\
\end{array}
\overrightarrow{\text{Com}}
\begin{array}{c}
  C \\
  D \\
\end{array}

(Commitment)

(Decommitment)

Statistical Binding: $B$ and $C$ are maximally entangled.
Commitments to the EPR State

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

|EPR⟩ \[ \begin{array}{c} \text{B} \\ \text{A} \end{array} \] \[ \begin{array}{c} \text{B} \\ \text{C} \end{array} \] \[ \begin{array}{c} \text{C} \approx \text{Com} \text{ (commitment)} \\ \text{D} \approx \text{Com} \text{ (decommitment)} \end{array} \]

**Statistical Binding:** $B$ and $C$ are maximally entangled.

**Computational Hiding:** $(B, C)$ indistinguishable from $(B, C')$ where $C'$ is a commitment to a maximally mixed state $|\text{EPR}\rangle_B$.
Commitments to the EPR State

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

$|\text{EPR}\rangle_{AB}$

- $B$ (commitment)
- $C$ (decommitment)
- $|0^\lambda\rangle$
- $D$

**Statistical Binding:** $B$ and $C$ are maximally entangled.

**Computational Hiding:** $(B, C)$ indistinguishable from $(B, C')$ where $C'$ is a commitment to a maximally mixed state.

**Fact:** $(B, C')$ is distributed as $(B', C)$ for $B'$ maximally mixed.
Breaking Hiding of EPR Commitment:

Promised that $\mathbf{B}$ and $\mathbf{C}$ are maximally entangled, distinguish $(\mathbf{B}, \mathbf{C})$ from $(\mathbf{B}', \mathbf{C})$ where $\mathbf{B}'$ 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 $\rightarrow$ hard radiation distinguishing.
One last thing: to show hard radiation distinguishing → crypto, need to show EPR commitments → commitments to any state.
EPR Commitments $\rightarrow$ Commitment to Any State

\[ |\text{EPR}\rangle \left\{ \begin{array}{c} B \\ A \\ 0^k \end{array} \right\} \rightarrow \text{Com} \]
EPR Commitments → Commitment to Any State

Just teleport $\psi$ into $C$: to commit to $\psi$, measure $(\psi, B)$ in the Bell basis to get classical bits $(x, z)$, and send $(C, x, z)$. 
EPR Commitments → Commitment to Any State

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

- **Statistical Binding**: $C$ determines $A$. $(A, x, z)$ determines $\psi$. 
EPR Commitments $\rightarrow$ Commitment to Any State

Just teleport $\psi$ into $\mathbf{C}$: to commit to $\psi$, 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 $\psi$.

- **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 $\psi$. 
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 $\text{poly}(n)$-size circuit.
- Plausible crypto assumption: random quantum circuits give secure commitments.
Tight relationship between a problem from black hole physics and quantum cryptography.

• In black hole physics, $\mathcal{C}$ is a random $\text{poly}(n)$-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 $\mathcal{C}$, how hard is it to distinguish $\mathcal{C}|0^n\rangle$ from $\mathcal{C}|1^n\rangle$ given $2n/3$ of the qubits?