

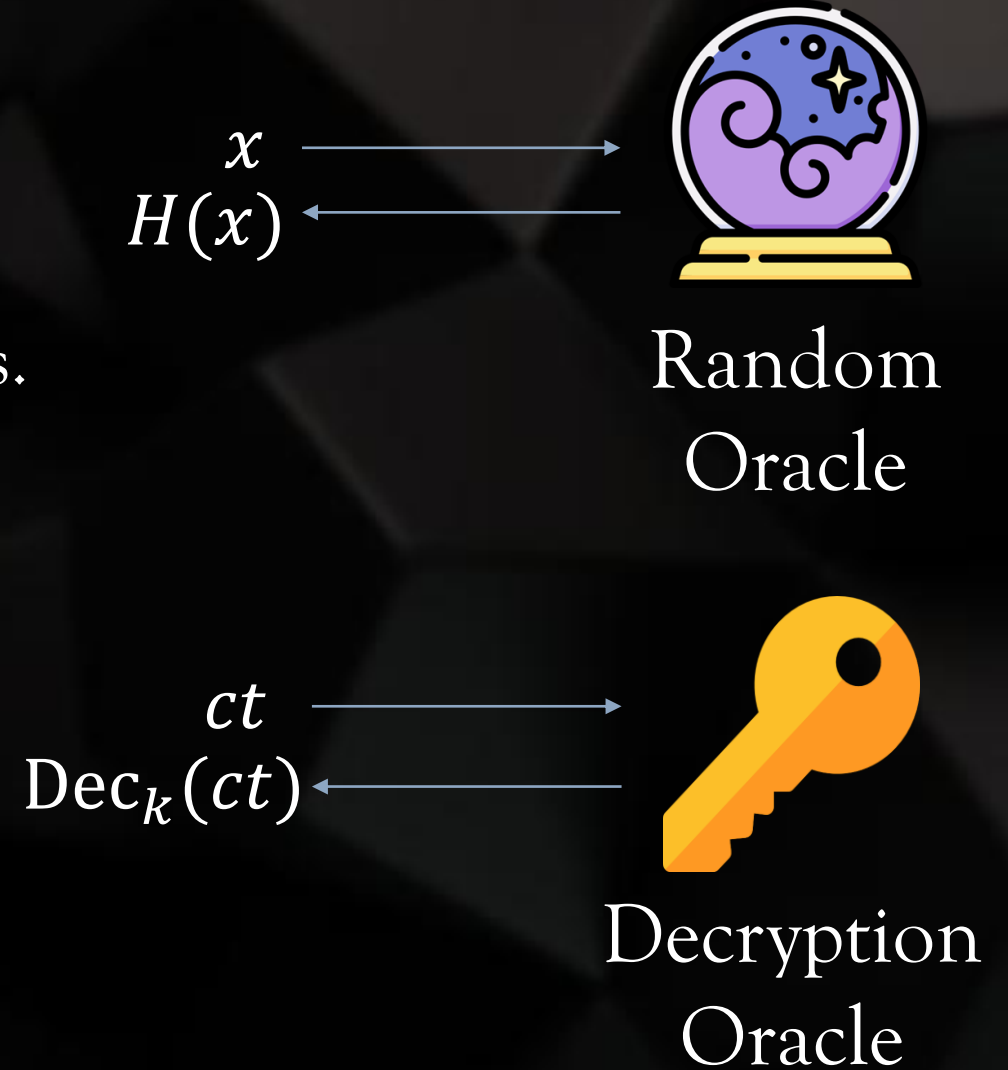
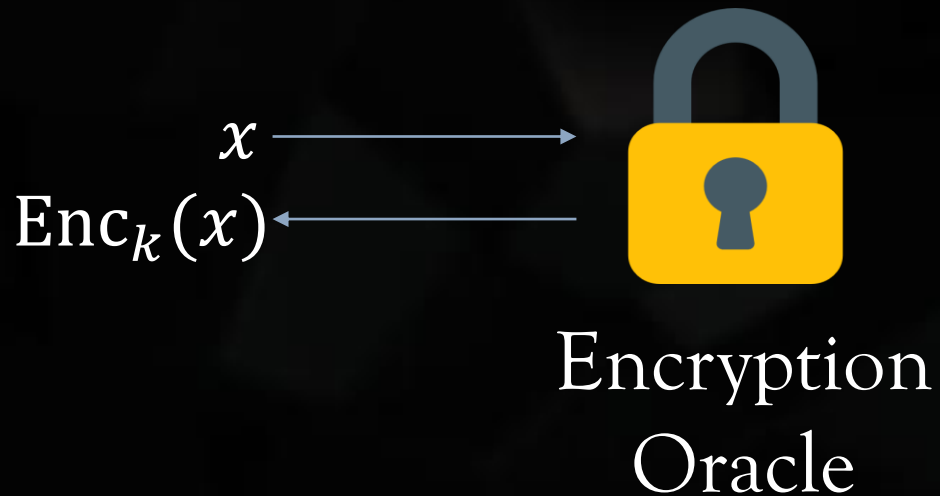
Cryptographic Proofs in the Quantum World

Anish Banerjee
Shankh Gupta



Queries

In classical cryptography, we often have to deal with queries made by the parties.



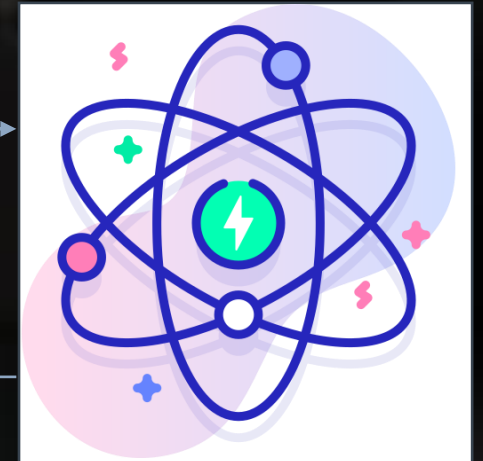
Quantum Queries

Adversary can make
superposition queries!

**Goal: Look at scenarios
where handling these
queries become non-trivial**

$$\sum_{x \in X} \alpha_x |x\rangle$$

$$\sum_{x \in X} \alpha_x |x\rangle |H(x)\rangle$$

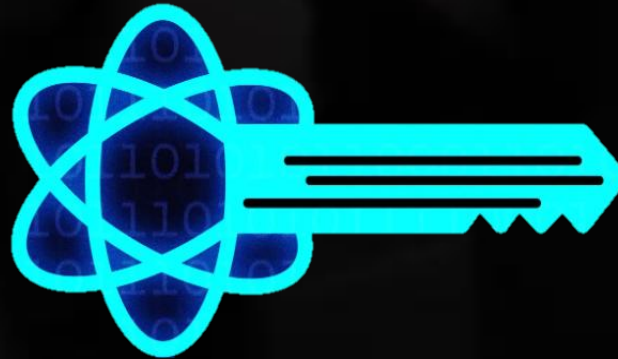


Quantum
Random
Oracle

Contents



Quantum Non-
Committing
Encryption



Quantum Public-Key
Encryption



Impossibility
Results

Non-Committing Encryption



Extensively studied in fields like **Multi-Party Computation (MPC)**.



Allows equivocation of ciphertexts.



Provides randomness that can "explain" a ciphertext as an encryption of any message.

Our result

- Nielsen's NCE construction is also secure in the **Quantum** Random Oracle Model.
- This construction suffers a security loss in the quantum realm.

A wins the NCE game with probability $\varepsilon \Rightarrow B$ breaks the security of the TDF with probability

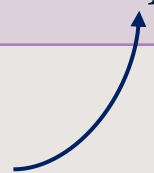
Classical

ε

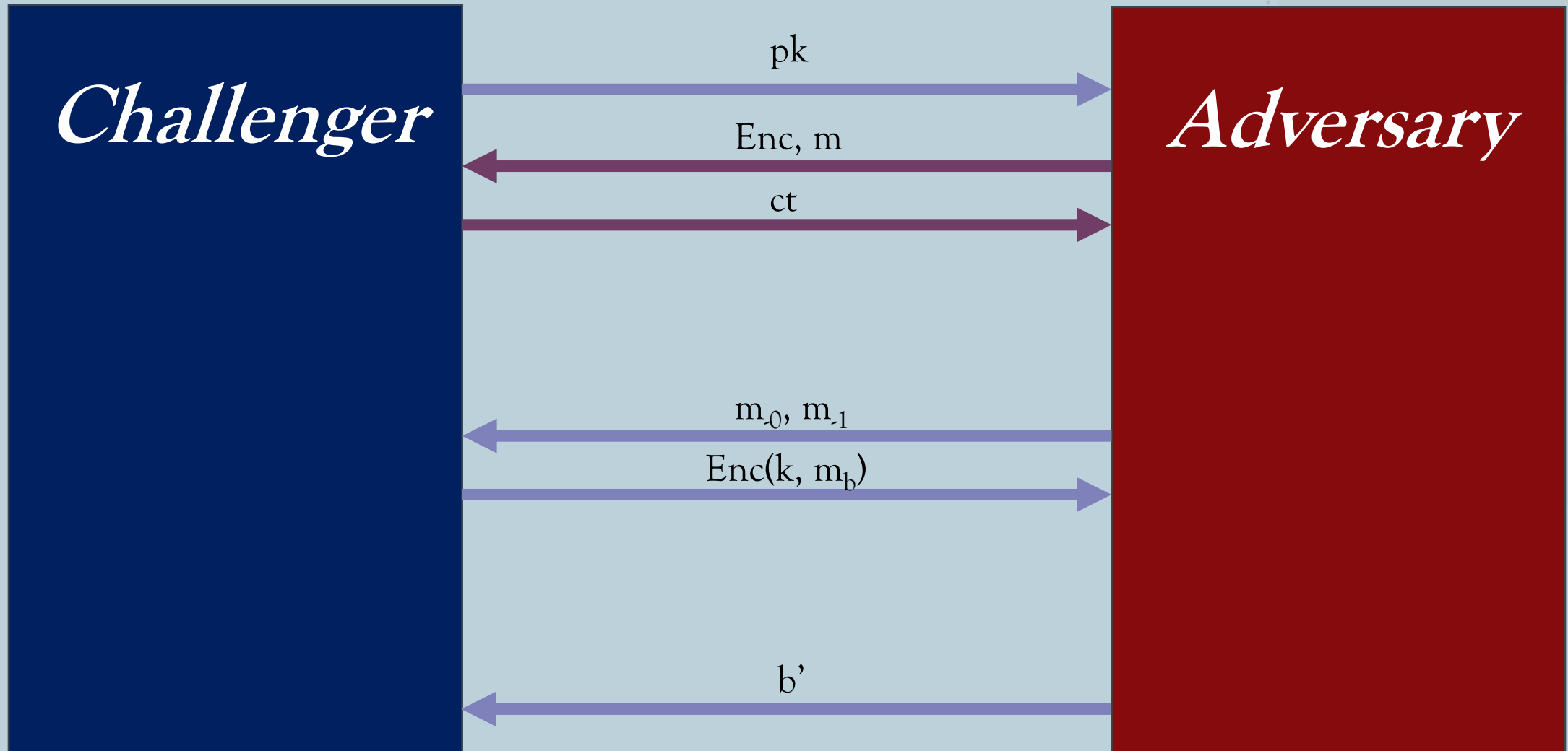
Quantum

$(\varepsilon/2q)^2$

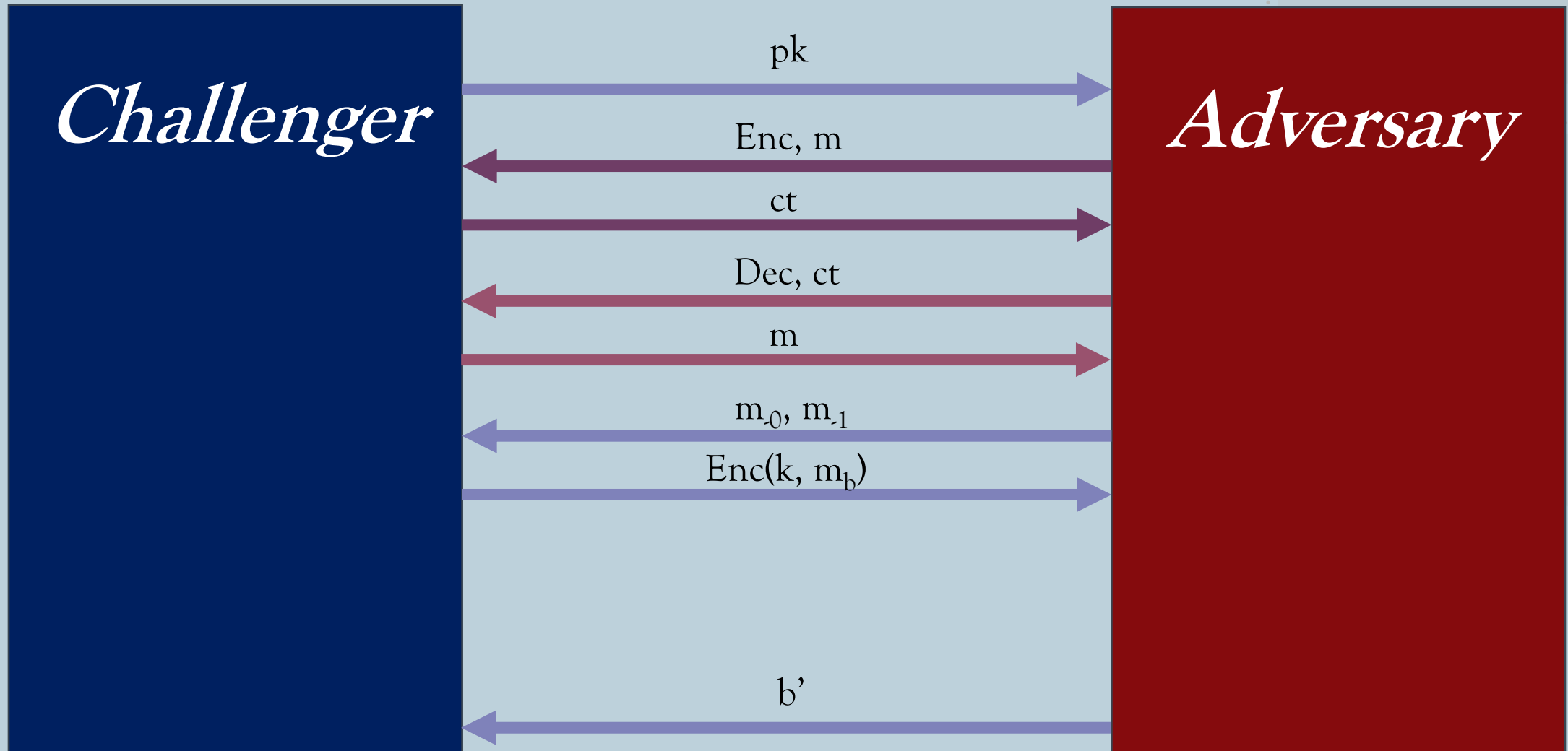
Number of queries made by A to the random oracle



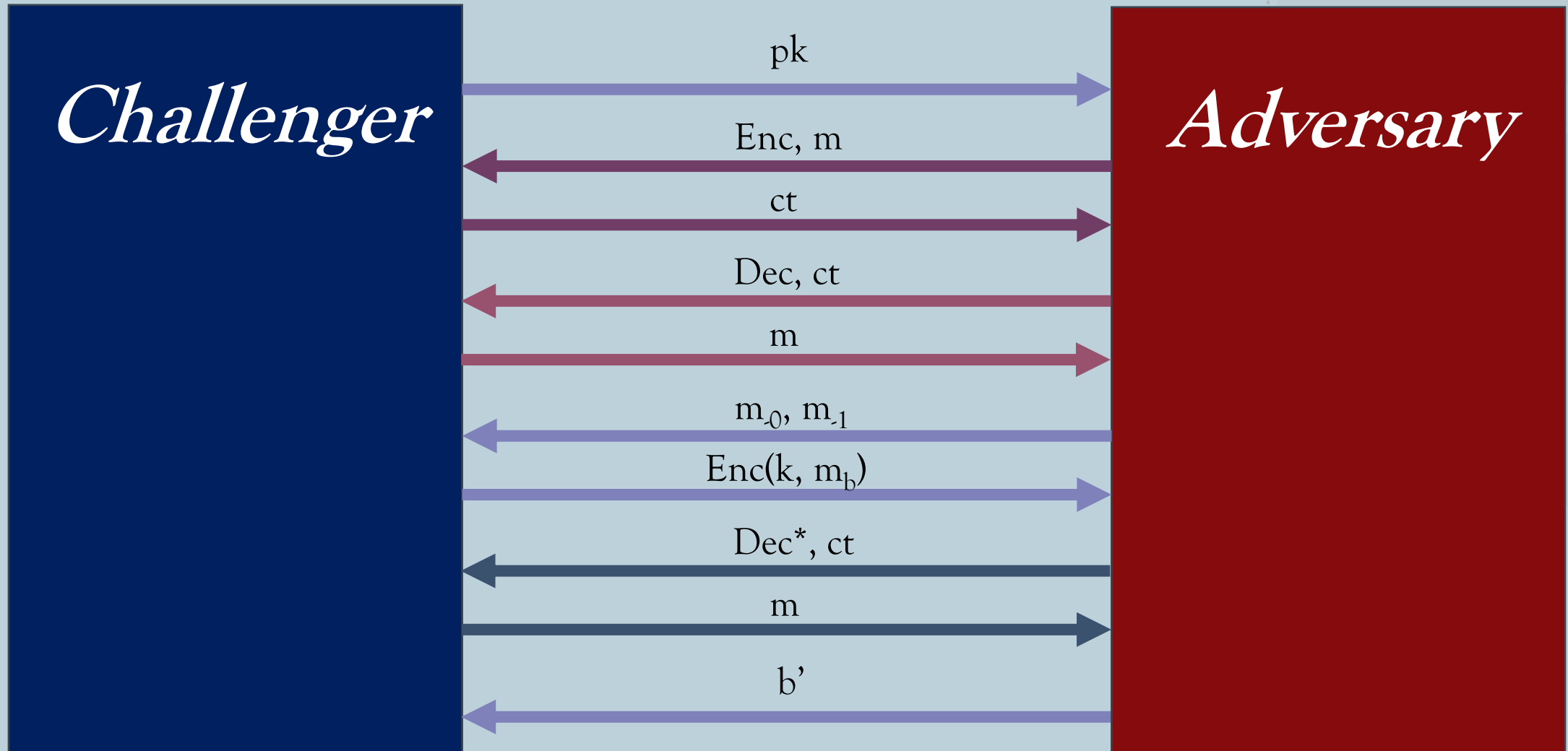
Cryptographic Security Definitions: CPA



Cryptographic Security Definitions: CCA1



Cryptographic Security Definitions: CCA2



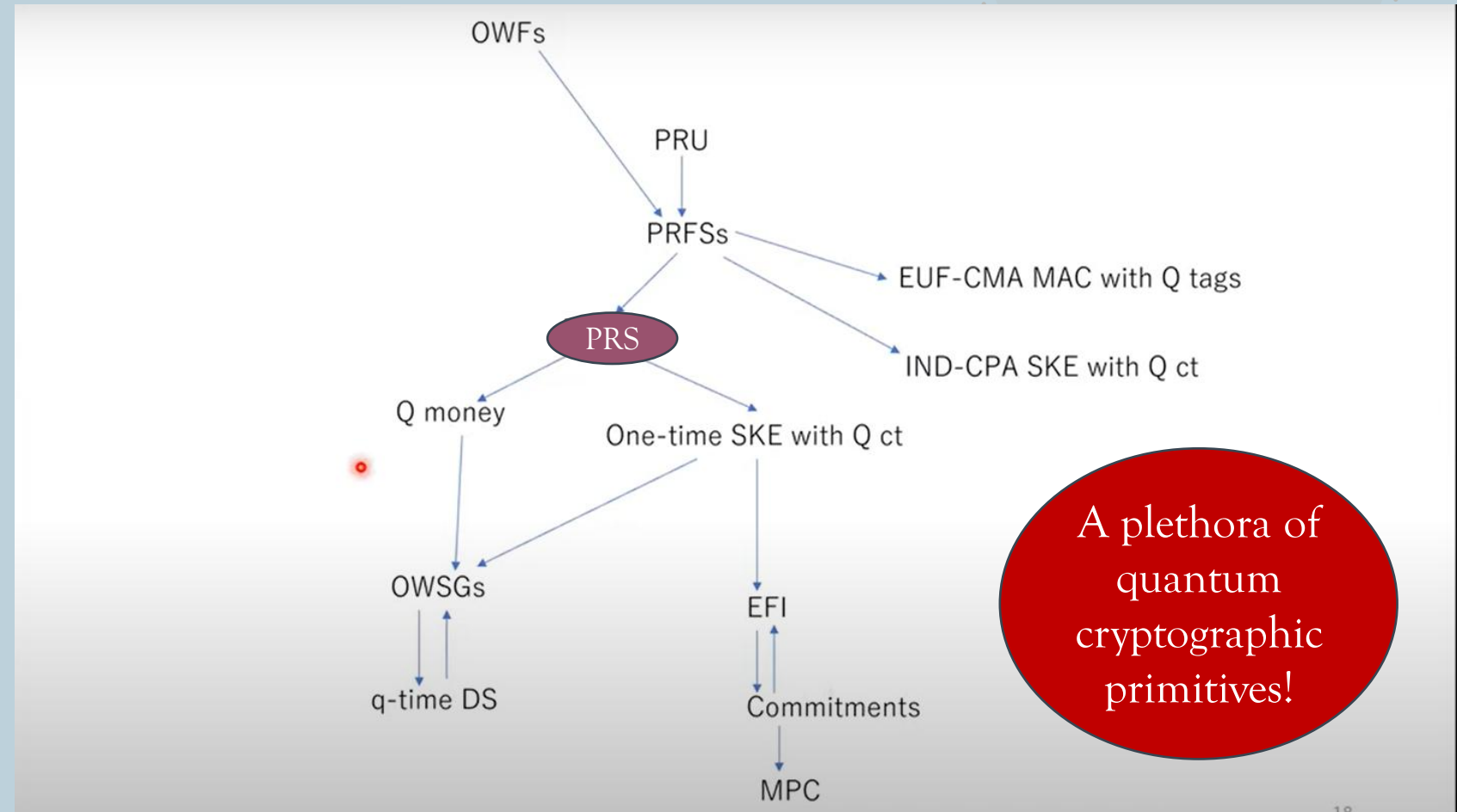
Minimal Assumption for Quantum Crypto

One-way functions:

Root of classical crypto

Q. Are qOWFs the minimal assumption for quantum crypto?

A. No!



Source: [Tomoyuki Morimae - Quantum cryptography without one-way functions](#) (Edited)

For more information, visit <https://sattath.github.io/microcrypt-zoo/>

Minimal Assumption for Quantum Crypto

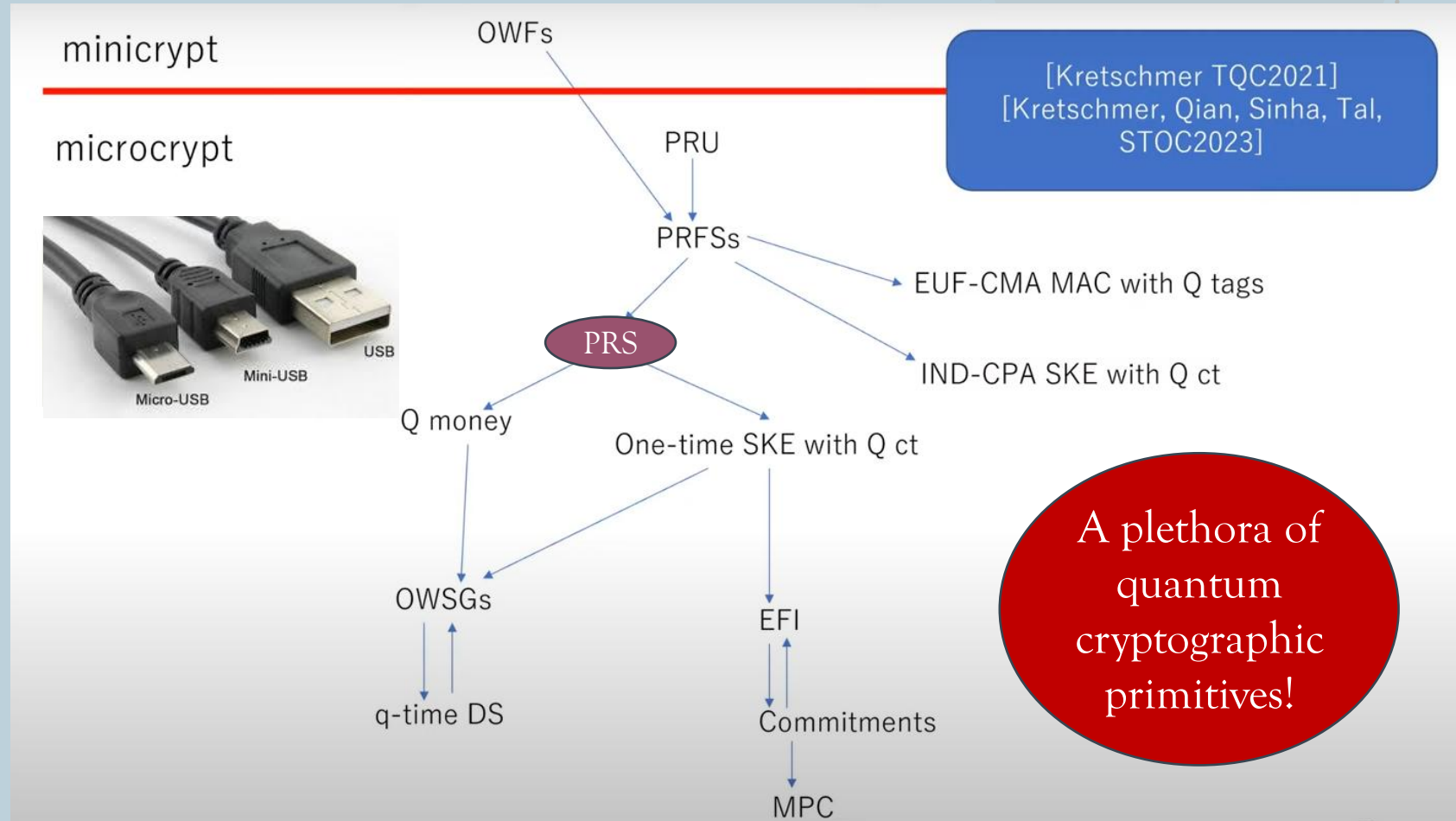
One-way functions:

Root of classical crypto

Q. Are qOWFs the minimal assumption for quantum crypto?

A. No!

Applications to
Black-hole physics!
[Brakerski,
CRYPTO23]



Source: [Tomoyuki Morimae - Quantum cryptography without one-way functions](#) (Edited)
For more information, visit <https://sattath.github.io/microcrypt-zoo/>

Pseudorandom States (PRS) [JLS19]

Haar random States

“Truly random” state

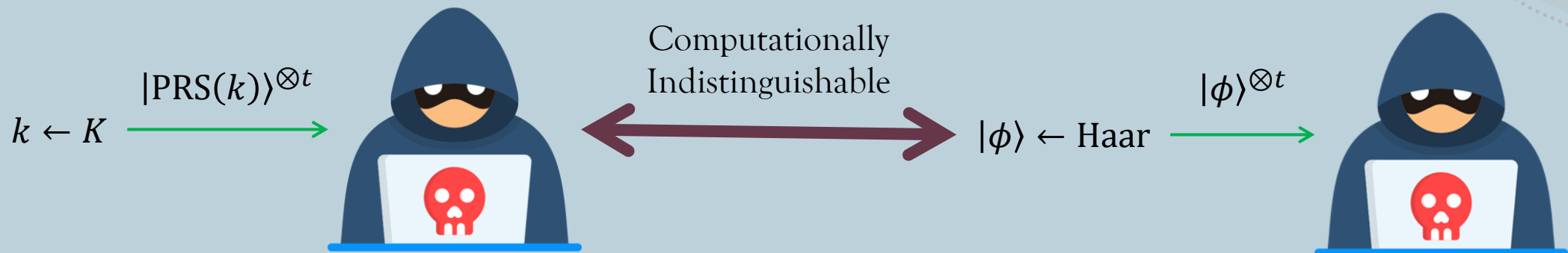
Pseudorandom States:

States indistinguishable from Haar random states

Example:

$$|\text{PRS}(k)\rangle = \frac{1}{\sqrt{|X|}} \sum_{x \in X} (-1)^{\text{PRF}_k(x)} |x\rangle$$

[BS19] : This is a PRS



Quantum Public-Key Encryption

[JLS21]

- $q\text{OWF} \rightarrow \text{PRS}$

[Kre21]

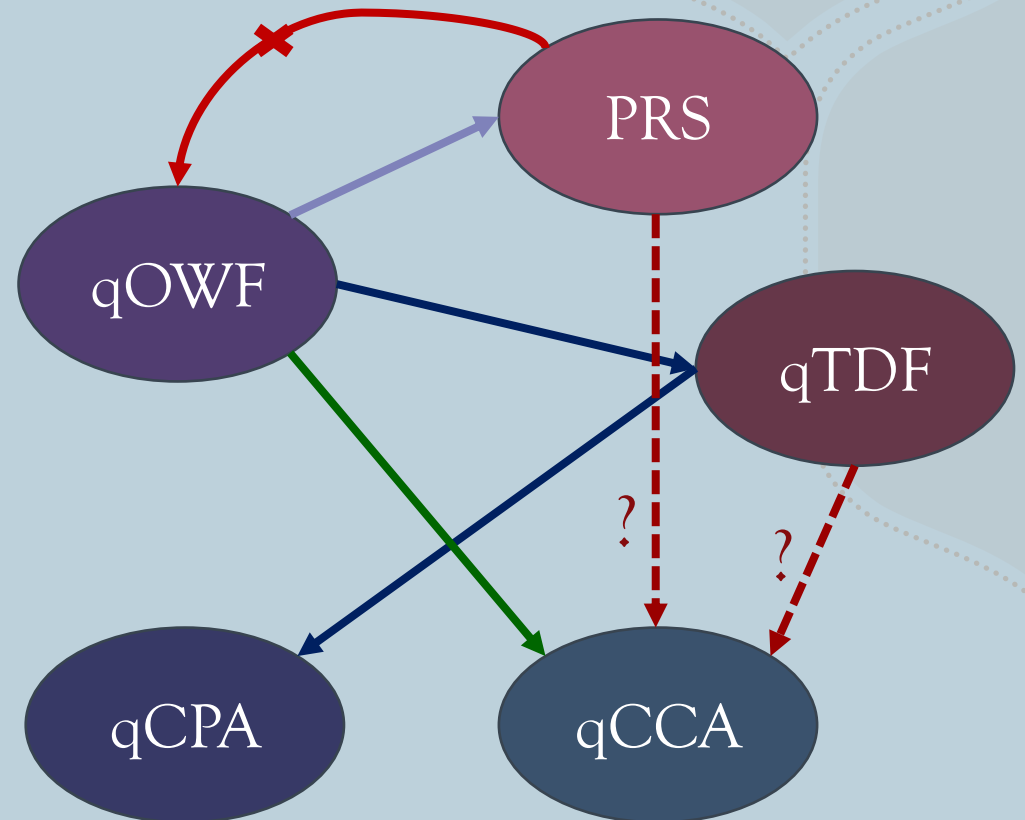
- There is a world where PRS exist but $q\text{OWF}$ don't

[Col23]

- $q\text{OWF} \rightarrow q\text{TDF}$
- $q\text{TDF} \rightarrow q\text{CPA}$

[BGH+23]

- $q\text{OWF} \rightarrow q\text{CCA}$



Questions

Q. Can we build PKE from One-Way Functions?

A. No!

qOWFs imply both qCPA and qCCA.

Q. Can we build CCA from CPA?

A. We don't know!

Q. Can we build qCCA from qCPA?

Q. Can we find some quantum cryptographic primitive which implies qCPA but not qCCA?





CCA from TDFs [HKW20]

Q. Can we do the same construction for the quantum case?

TDF \rightarrow CPA with (classical) RR : Can be done by modifying [Col23]'s construction.

Black-Box Reductions

An important question in Cryptography :

Whether existence of a primitive P is sufficient to construct primitive Q ?

- Often prove these reductions in a black-box way. For instance, take P as OWFs and Q to be PKE.

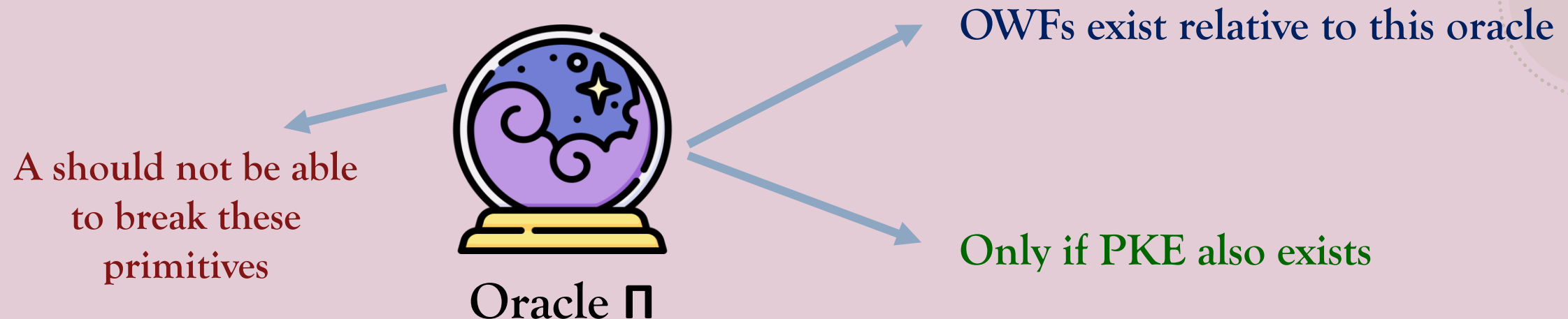
Black-Box Reductions

Construction of PKE that uses only oracle access to a function f and guarantees that PKE is secure given f is one-way.

- Doesn't use the internal structure of f .
- Well-defined even if f is not efficiently computable.
- If A breaks PKE, then $S^{A,f}$ can invert f .

Relativizing Reductions

- First introduced by Impagliazzo and Rudich [IR89].
- If PKE can be built from OWFs, then the construction still works if all parties are given access to some Oracle Π .



Black-Box Separations

Q. Can we build PKE from One-Way Functions?

A. PKE cannot be reduced to OWFs in a black-box way.

- We show a Black-Box separation between OWFs and PKE. [IR89 approach]
- Showed that any reduction from PKE to OWFs cannot relativize.



Oracle Π

OWFs exist relative to this oracle

PKE is impossible in this oracle-aided world

OWFs $\not\Rightarrow$ Public-Key Encryption



Oracle Π

$$= \text{Random Function Oracle} + \text{PSPACE-Complete oracle}$$

[IR89]

$P = NP \Rightarrow$ secure PKE does not exist relative to a RO

Black-Box
Separation

OWFs (or any other primitive implied by RO) will not suffice for Public-Key encryption in a Black-Box way.

PKE in Quantum World

Q. What if we allow Quantum Computations?

A. Quantum communication gives us secure PKE from OWFs alone.

↳ Downside : Prevents reusability of public-key

Q. But what if the communication is still classical?

- Public key, secret key, and ciphertexts are all classical.
- QCCC model (Quantum Computation, Classical Communication)

PKE Impossibility (Quantum Case)

[ACC⁺22] : PKE (in the QCCC setting) cannot be constructed in a black-box way from One-way functions. (Conditional result)

- Assuming **Polynomial Compatibility Conjecture (PCC)** to be true.
- Separation shown using the first technique.

- Various other black-box separation results in quantum world.
- E.g. PRS $\not\Rightarrow$ OWFs [Kre'21], OWFs $\not\Rightarrow$ CRH [HY18]

Future Work

- Studying whether the results about classical reductions can be translated to results in a quantum setting.
- Applying these techniques to obtain separation results for various other primitives.

Thank You!

