Quantum Non-Committing Encryption

Anish Banerjee
Shankh Gupta

Contents

Overview of Non-Committing Encryption

Construction of [Nie02]

Extension to quantum adversaries

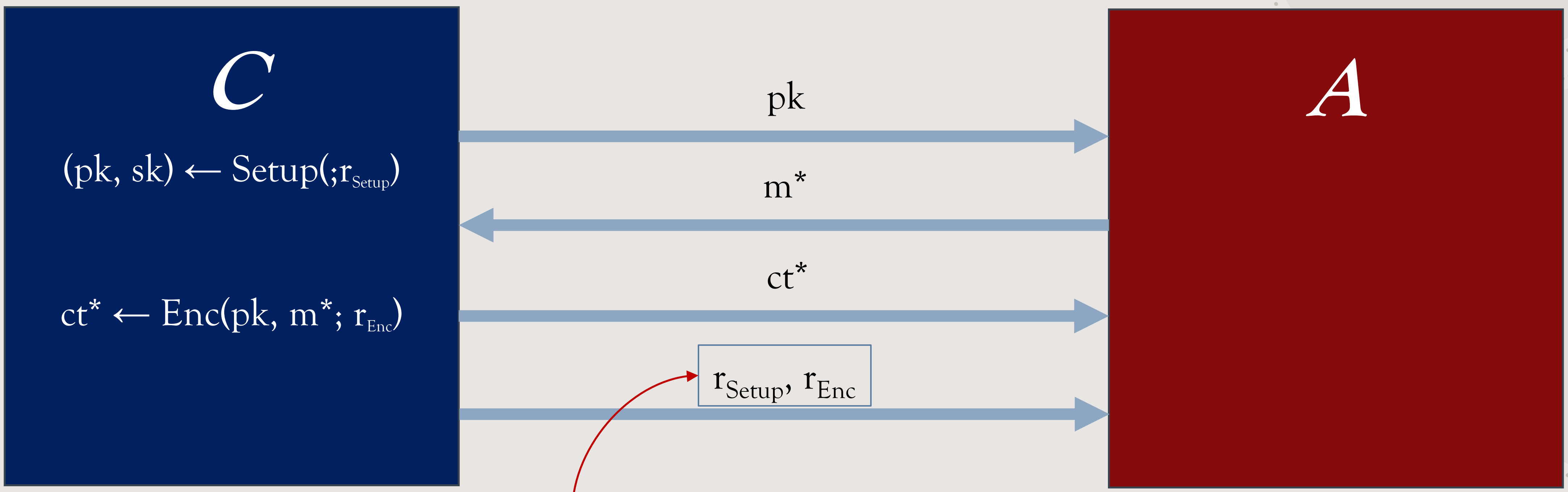
Non-Committing Encryption

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.

Real World (PKE)

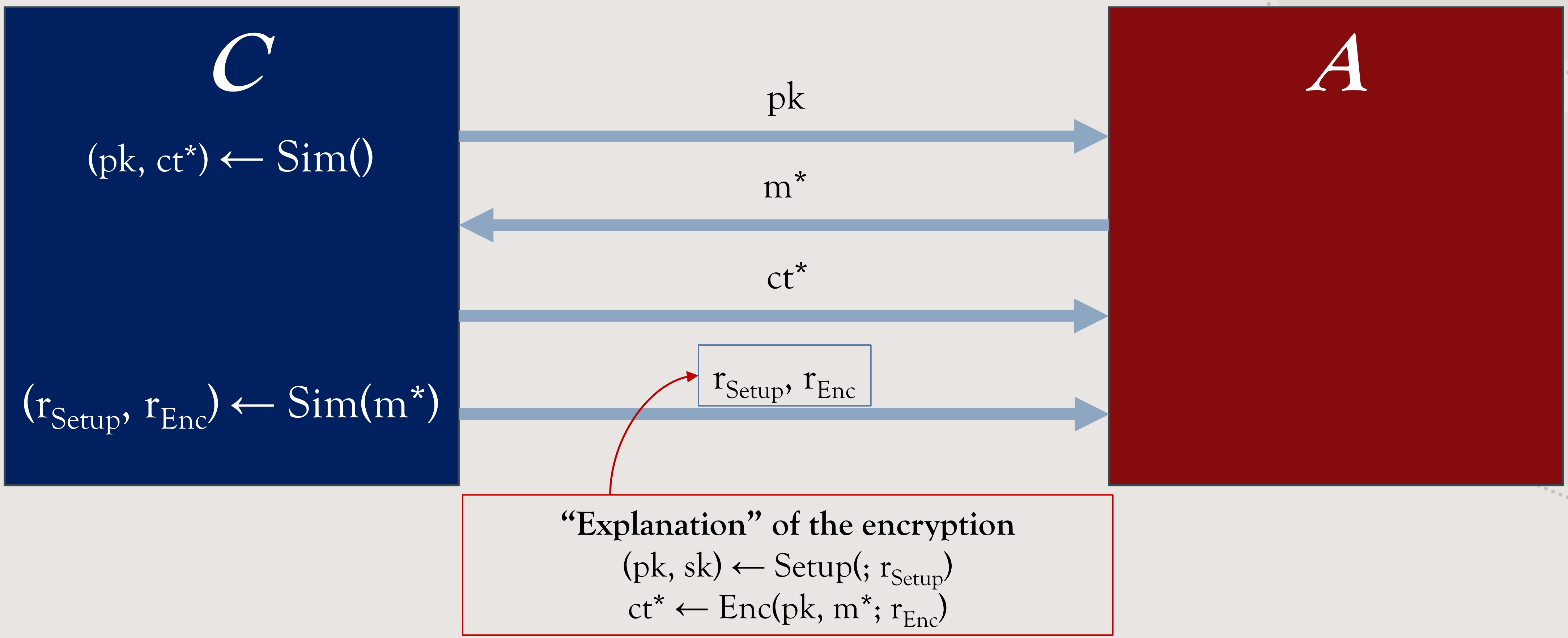


“Explanation” of the encryption

$(pk, sk) \leftarrow Setup(; r_{Setup})$

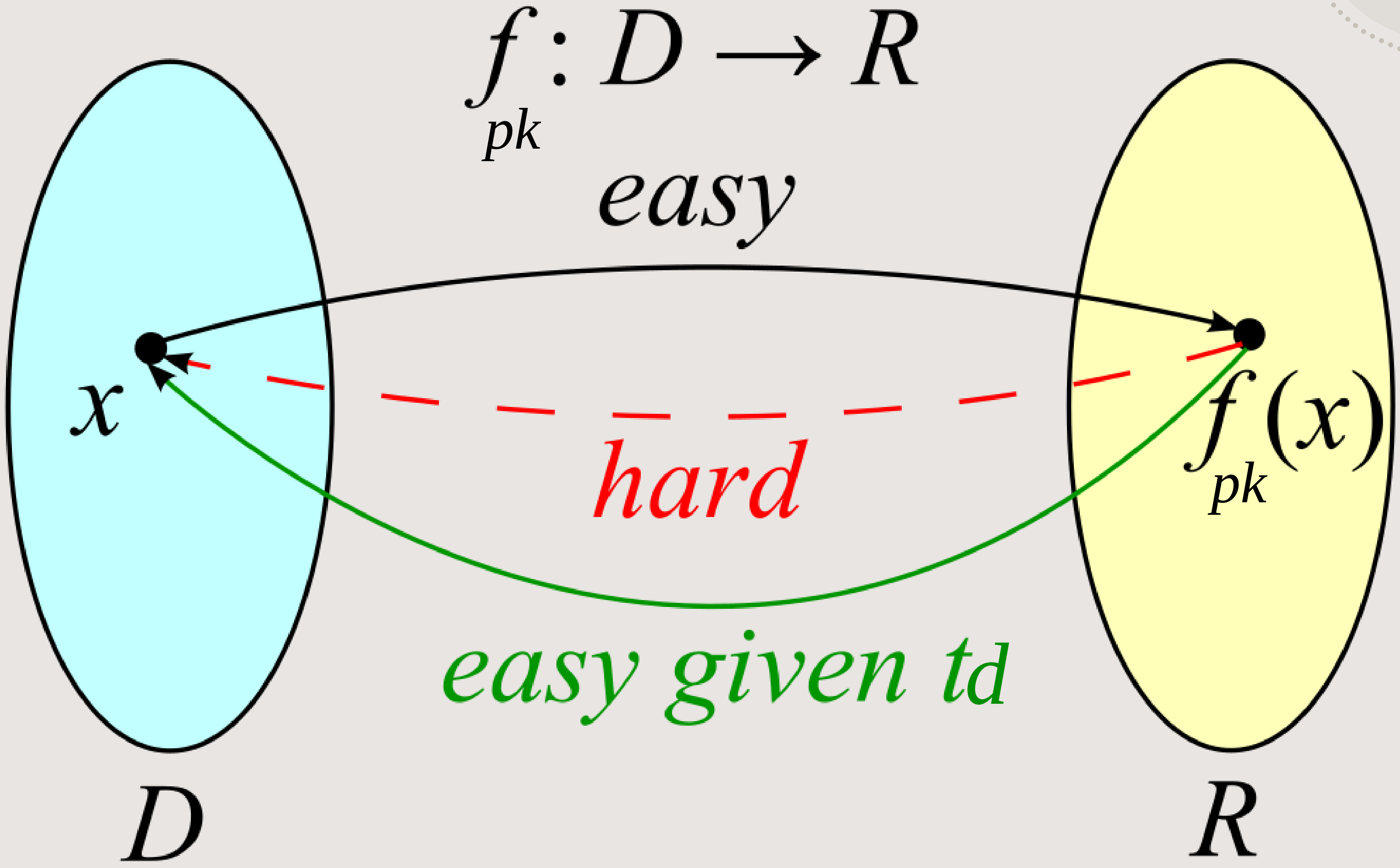
$ct^* \leftarrow Enc(pk, m^*; r_{Enc})$

Ideal World



Security: Real and Ideal worlds are computationally indistinguishable

Trapdoor Functions (TDF)

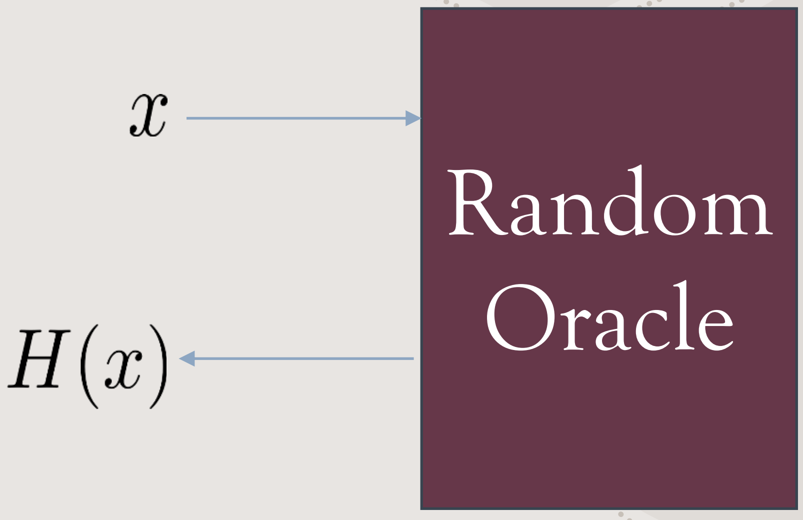


Source: Wikipedia (Edited)

The Random Oracle Model [BR93]

Model H as a **truly random function**

Only oracle access allowed



Real World: H is instantiated as a cryptographic hash function

Nielsen's Construction (Real World)

$\mathcal{C}$

$(pk, td) \leftarrow \text{TDF.Setup}(;r_{Setup})$

Sample random r

$ct^* \leftarrow (f_{pk}(r), H(r) \oplus m^*)$

pk

m^*

ct^*

$r_{Setup}, r_{Enc}{=}r$

$\mathcal{A}$

Nielsen's Construction (Ideal World)

$\mathcal{C}$

$(pk, td) \leftarrow \mathrm{TDF.Setup}(;r_{Setup})$

Sample random r and y

$ct^* \leftarrow (f_{pk}(r), y)$

Set $H(r) = y \oplus m^*$

$\mathcal{A}$

$\xrightarrow{pk}$

$\xleftarrow{m^*}$

$\xrightarrow{ct^*}$

$\xrightarrow{r_{Setup},\ r_{Enc}=r}$

Argue that probability of querying r is negligible (TDF)

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

The Quantum Random Oracle Model [BFD+11]

Why should we consider quantum access to the RO?

Adversary can make superposition queries!

Not clear how to make an analogous argument.

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

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

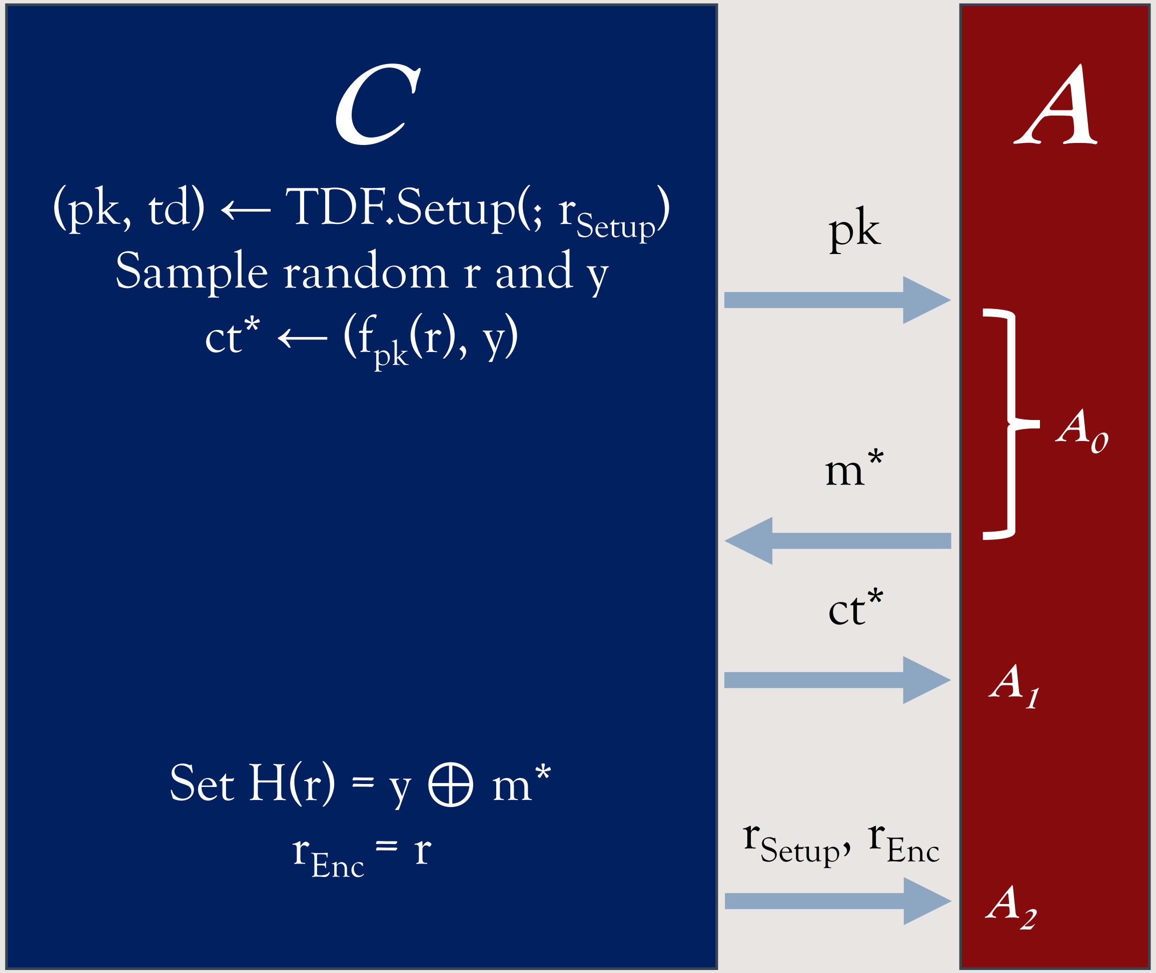
Quantum Random Oracle

One–Way to Hiding [Unr14]

- Suppose G and H only differ only on one x^*.
- Adversary cannot tell them apart without querying x^* with **some amplitude.**
- Simulator randomly chooses a query, stops $\boldsymbol{A}$ and measures its query register.
- Let **Guess** be the event that the measurement outcome is x^*.

$$|\Pr[1 \leftarrow \boldsymbol{A}^{H}] - \Pr[1 \leftarrow \boldsymbol{A}^{G}]| \leq 2q\,(\Pr[\mathrm{Guess}])^{1/2}$$

Proof Sketch



Observation: $\boldsymbol{A}$ can distinguish between the real and simulated worlds only if $\boldsymbol{A_0}$ or $\boldsymbol{A_1}$ query H on r.

Since the only information about r provided to $\boldsymbol{A}$ is in the form of $f_{pk}(r)$, using the one-way to hiding lemma we have

$$|P_{real} - P_{sim}| \leq 2q\,(P_{guess})^{1/2}$$

If $|P_{real} - P_{sim}| = \varepsilon$ is non-negligible then we break the security of the trapdoor function with probability $(\varepsilon/2q)^2$

Future Work

- Explore quantum NCEs
  - Formalize definitions and security notions
  - qNCEs from quantum secure one-way functions?
- Understand the security-loss in the quantum setting.
- Understanding the security of other ROM proofs in qROM

Thank You!