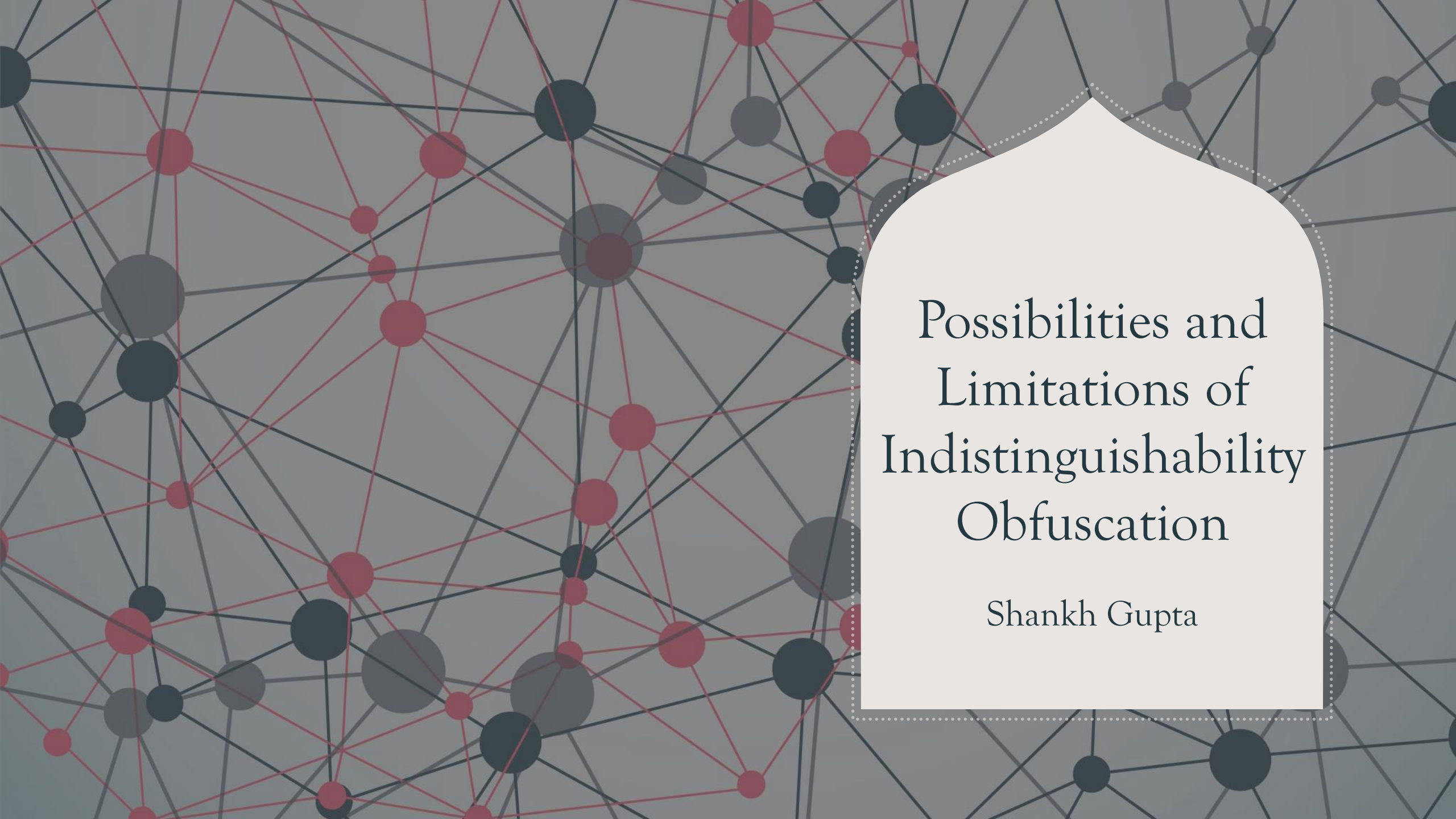
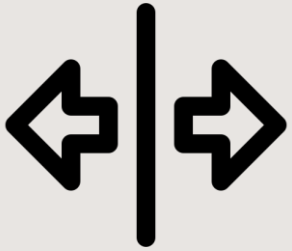


Possibilities and Limitations of Indistinguishability Obfuscation

Shankh Gupta

Contents

Preliminaries: IO and CRHFs

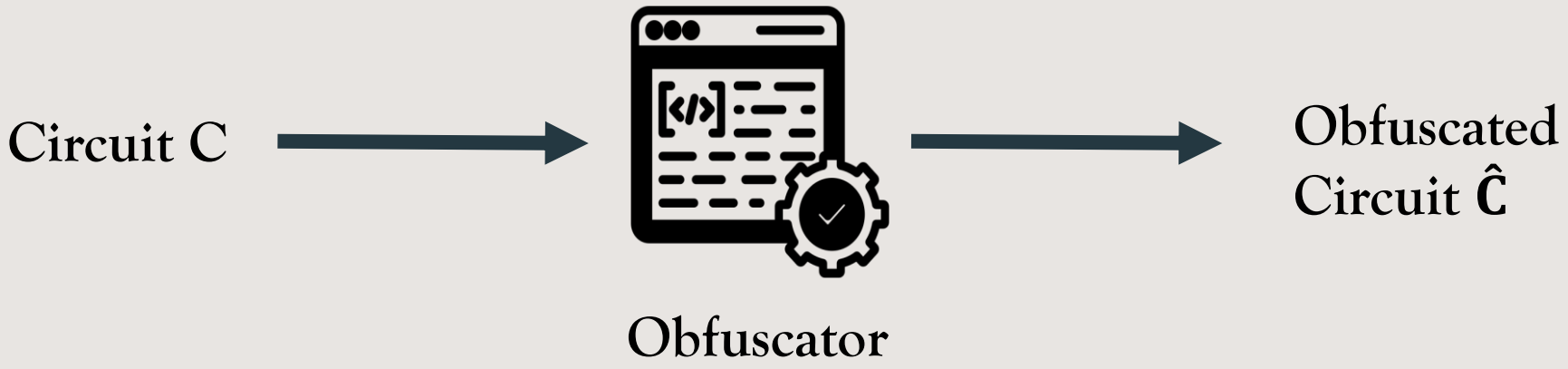


Overview of Black-Box Separations

Impossibility Result

Program Obfuscation

Goal : Make programs "hard to understand" while preserving functionality.



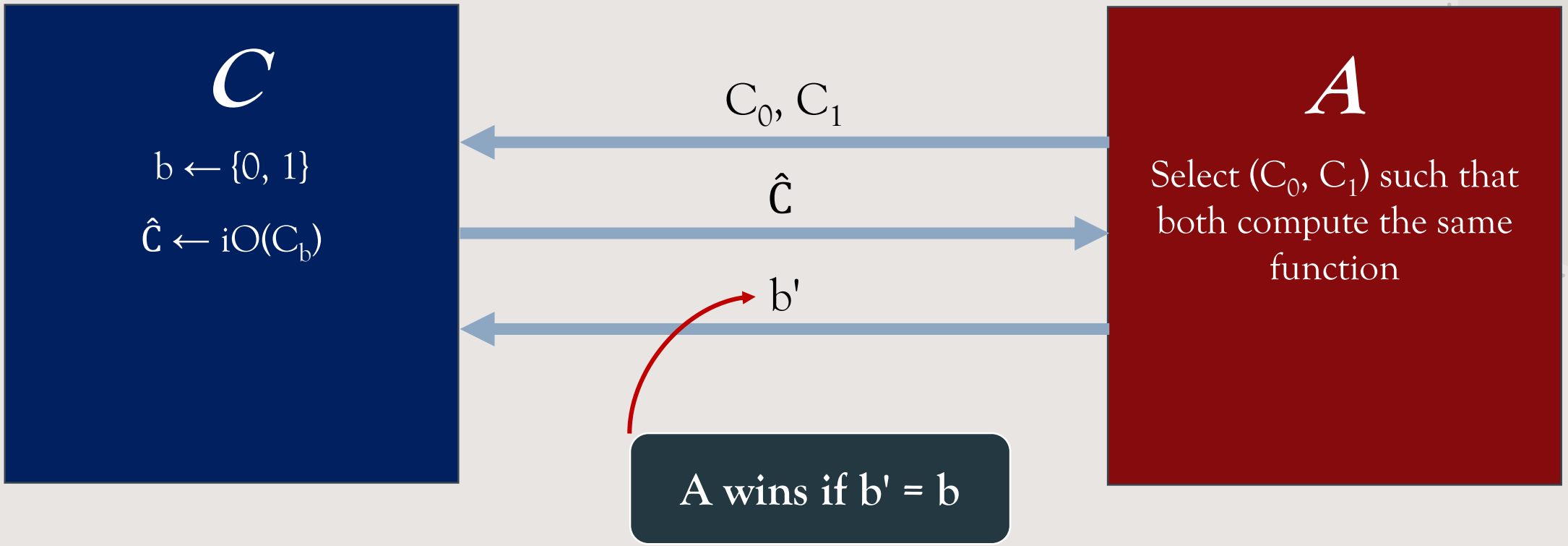
Correctness: Circuits C and Ĉ compute the same function.

Security: Ĉ reveals no more information than a black-box implementing circuit C

Impossible to achieve

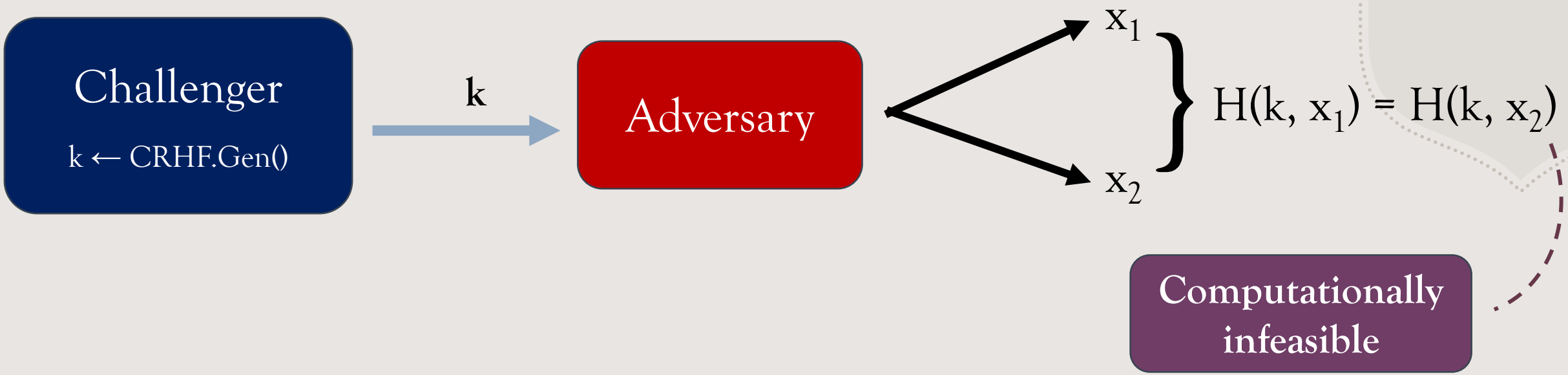
Indistinguishability Obfuscation

Modified Security: Obfuscation of two functionally-equivalent circuits are indistinguishable.

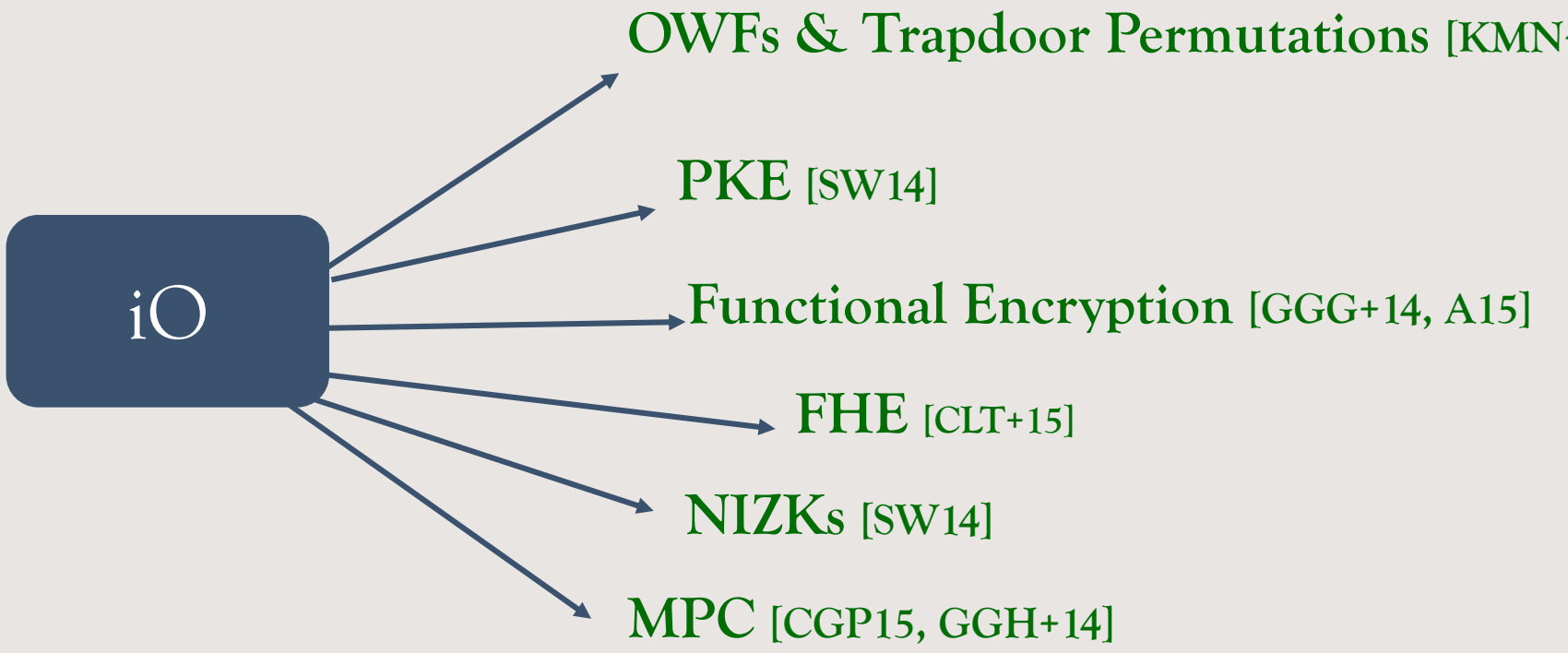


Collision-Resistant Hash Functions

Difficult to find two different inputs that hash to same output.



The Power of iO [SW14]



Is there a natural task that cannot be solved by iO?

CRHFs

Black-Box Constructions

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.

Black-Box Constructions

Construction of Q that uses only **oracle access** to P and guarantees that Q is secure given the security of P.

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

Relativizing Constructions

- First introduced by Impagliazzo and Rudich [IR89].
- BB Constructions ⇒ Relativizing Constructions.

Oracle Π

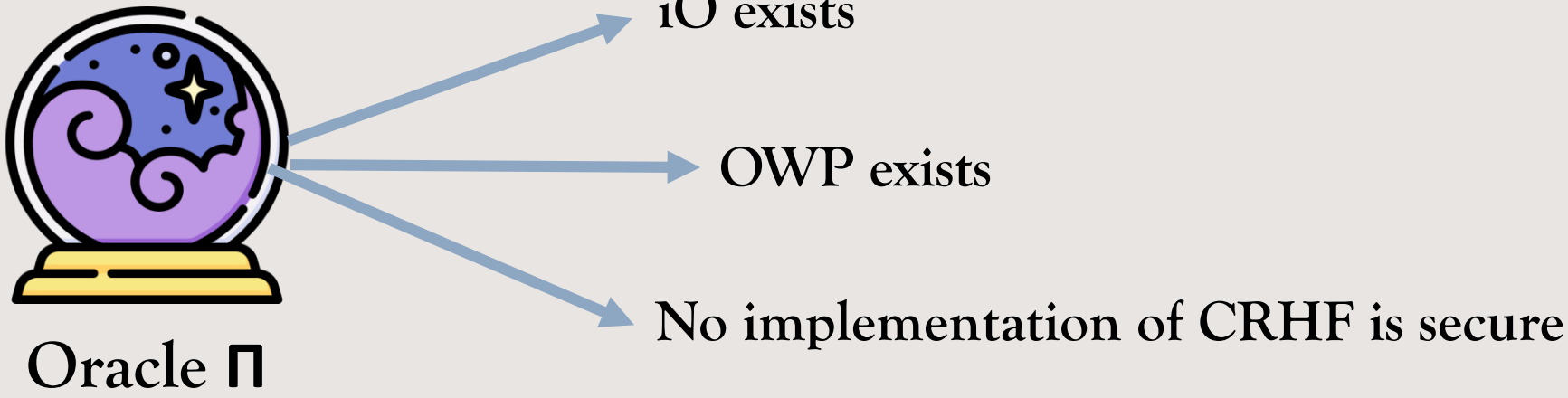
A^{Π} should not be able to break these primitives

then Q should also exist relative to Π

If P exists relative to Π

Limitations of iO [AS15]

Theorem: There is no fully black-box construction of a CRHF from an iO for oracle-aided circuits and One-way Permutations.



Oracle Construction

Oracle Π

$=$ OWP $+$ Indistinguishability Obfuscator $+$ Collision-Finder oracle

Circuit C

$\Downarrow$

Outputs a collision (w, w') w.r.t. C

Future work

- Study this separation result in the Post-Quantum setting (qROM model).

Challenges: Quantum reductions, Superposition oracle queries

- Understand the possibilities and limitations of the quantum analogue of indisitnguishibility obfuscation (**qsiO**).

Thank You!