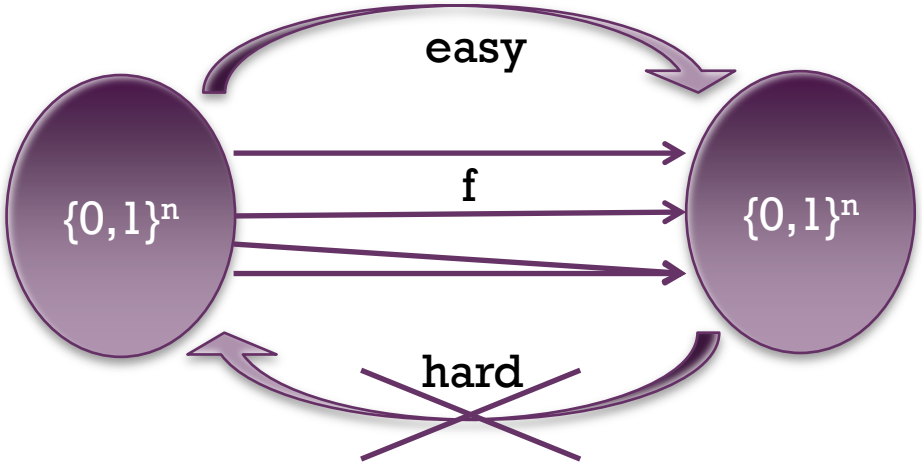
The Curious Case of Non-Interactive Commitments

Mohammad Mahmoody
Rafael Pass

Modern Cryptography and One-Way Functions

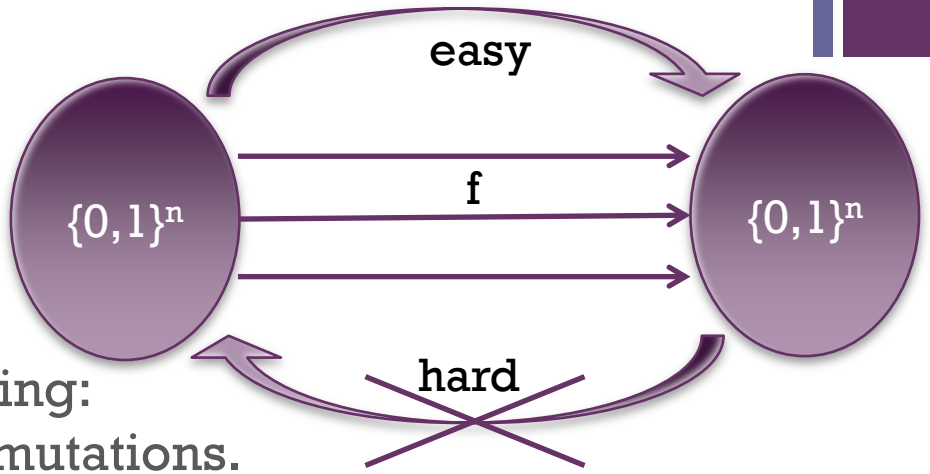
- Modern Cryptography is based on computational assumptions. [Shannon 1950s]
- OWFs, a central player:



Easy to compute $f(x)$
Hard to find $x \in f^{-1}(U_n)$

1. Almost all crypto "needs" one-way-ness [Impaliazzo-Luby'89]
2. We can do great things with it (Encryption, Signatures, etc).

A Success Story: OWF vs OWP



- One-Way *Permutation* **f**:
  f is OWF + it is a permutation (e.g. discrete logarithm).

- **Success Story**: To do something:
  1) Build it using one-way Permutations.
  2) Get rid of the structure: use injective, then regular, then….
  Eventually use any one-way function!

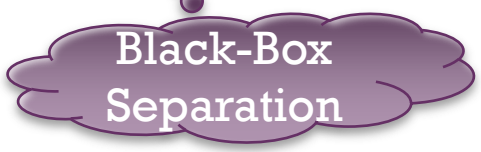
- **Examples**:
  Pseudorandom Generators [BM82, Yao82, Lev87, GKL93, GL89, HILL99]
  Statistical Zero Knowledge [BCC88, GMR88, BCY91, NOVY98, GK96, DPP98, HHKKMS05, NOV06, HR07, HNORV07, HRVW09] Signatures, etc.

- Interestingly: we know OWF $\not\Rightarrow$ OWP [BI87, HH87, Tar87, Rud88]

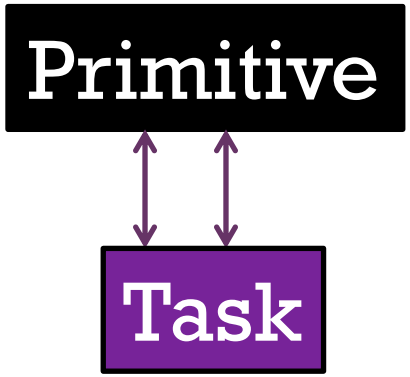
Question 1: Can we always use OWFs instead of OWPs in Natural Cryptographic Tasks?

→ Is there any natural task Q such that

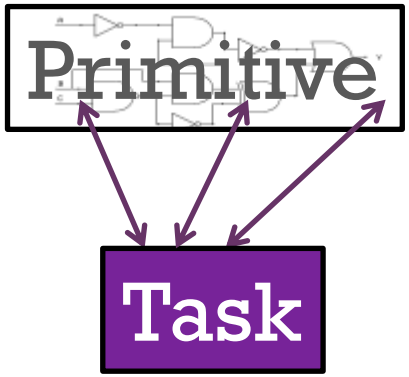
OWP → Q but OWF $\not\rightarrow$ Q ?



Black-Box Constructions (Separation: No Const. Exists)



Black-Box



Non-Black-Box

Black-Box Constructions

- The (perhaps inefficient) primitive is used only as an "oracle".
- Captures most known techniques
- Usually more efficient
- Can incorporate "physical" implementations and attacks

Another Success Story (from Non-Black-Box to Black-Box)

- For many Cryptographic Constructions :
  Start from a non-black-box const. → make it black-box.
  [HIKLP'11, CDSMW'09, WeePass'08, Wee'10, Goyal'10,…]

- Our Focus: Implementation (not the security reduction)
  Different from setting of [GK'90] vs [Barak'05].

Question 2: Can we always make non-black-box implementations black-box?

Any natural task Q and assumption A known that:

$A \not\Rightarrow Q$ black-box but $A \rightarrow Q$ non-black-box

Our Results

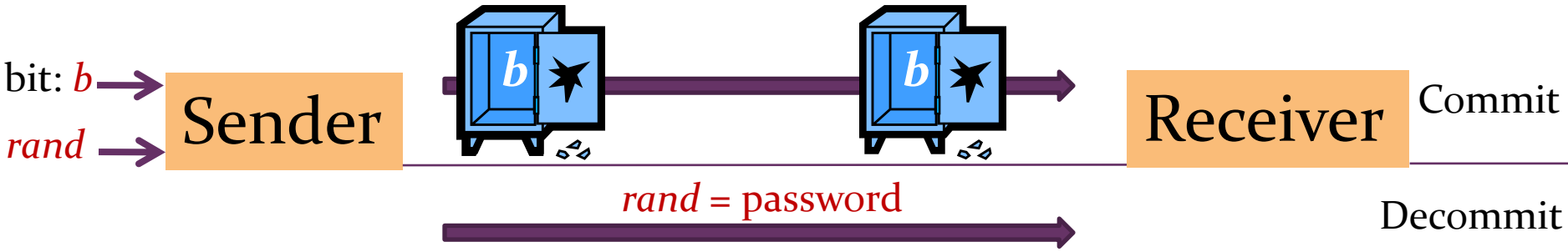
- NIC = Non-Interactive Commitments

1) OWP → NIC but OWF $\not\rightarrow$ NIC

2) There is a crypto assumption A such that:
NIC can be based on A using a **non**-black-box
NIC can**not** use A only as a black-box.

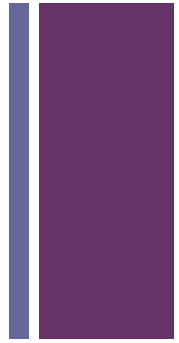
(Non-Interactive) Commitments

- digital analogue of a vault:



- **Hiding**: Receiver can't guess bit b in commit phase.
- **Binding**: Sender can't decommit to both 0 *and* 1 in decommit phase.
- Non-Interactive : Commit without interaction with receiver.
- **Application**: ZK, coin tossing, publicly verifiable secret predictions, etc.
- Blum-Micali'81 + Yao'82 : One-Way **Permutations** → NIC

Plan



- Black-Box Separation of NIC from OWF
- An inherently non-black-box assumption for NIC
- Extensions and Open Questions

Plan

- Black-Box Separation of NIC from OWF
- An inherently non-black-box assumption for NIC
- Extensions and Open Questions

A General Technique for Separation from OWF [IR'86]

- To get Black-Box Separation:
  1. Use Random Oracle instead of OWF in construction of NIC
  2. Break NIC with poly(n) queries to Random Oracle.

- Why it works?
  Such attack against NIC + Security Reduction for NIC:
  → invert Random Oracle with poly(n) queries (impossible).

Applying the General Technique?

- Hope: "break" any NIC with ``few queries'' in the *random oracle model.*
- But: relative to RO injective OWFs exist !
  (still sufficient for NIC).
- We will use a *partially-fixed* random oracles O:
  Fixed (with collisions) on poly(n) points, random elsewhere

High Level of Proof

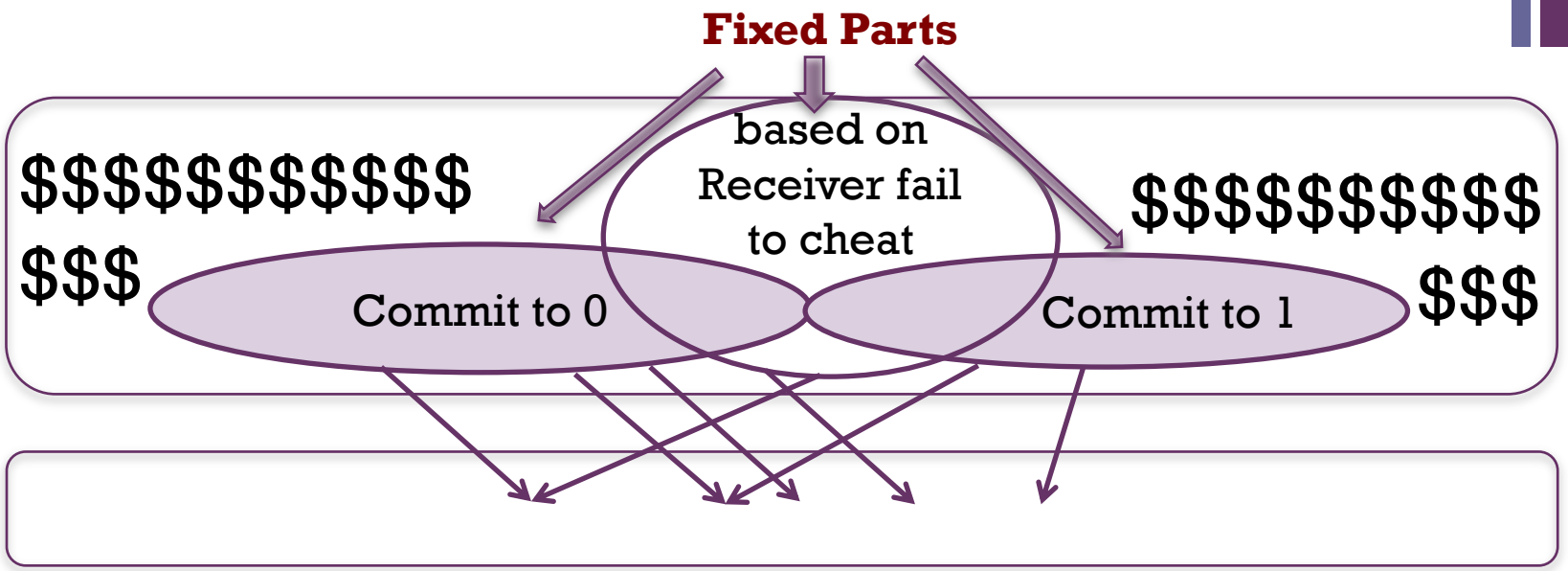
- **Theorem**
  There is no black-box construction of NICs from OWFs

- **Proof**: *Either* of the following holds:

1) Receiver can guess b in **Rand Oracle** by poly(n) queries.
   (Learn queries "likely" asked by Sender, then guess b).

2) If the cheating Receiver FAILS:
   Sender can decommit into b = 0 *and* 1 using a ***partially-fixed*** **Random Oracle** (fixed on poly(n) points, random elsewhere).

Cheating Sender's Partially-Fixed Random Oracle



- Oracle fixed only over poly(n) points and random elsewhere.
- So the oracle is strongly one-way.
- Yet, the sender can open the commitment C into both 0 and 1 *consistent* with the oracle.

■

Theorem [this work]
There **is no** black-box construction of NIC from OWFs.

Answers our first question:
OWP is indeed more useful than OWF to get NIC.

Plan

- Black-Box Separation of NIC from OWF
- An inherently non-black-box assumption for NIC
- Extensions and Open Questions

Black-Box vs Non-Black-Box Use of OWF – a Conditional Separation

Theorem [this work]
There **is no** black-box construction of NIC from OWFs.

Theorem [BOV'05].
Assuming certain (believable) circuit lower bounds:
There **is** a **non**-black-box construction of NIC from OWFs
(derandomize Naor's two-message protocol).

Conclusion:
Assuming the same circuit lower bounds:
NIC can be based on OWFs only by non-black-box construction.

Black-Box vs Non-Black-Box Use of OWF – Unconditional Separation ?

Theorem [this work]
There **is no** black-box construction of NIC from OWFs.
even if it is a "hitting" OWF.

Theorem [implicit in **BOV'05**].
There **is** a **non**-black-box construction of NIC from hitting OWFs
(no circuit lower-bound assumption!)

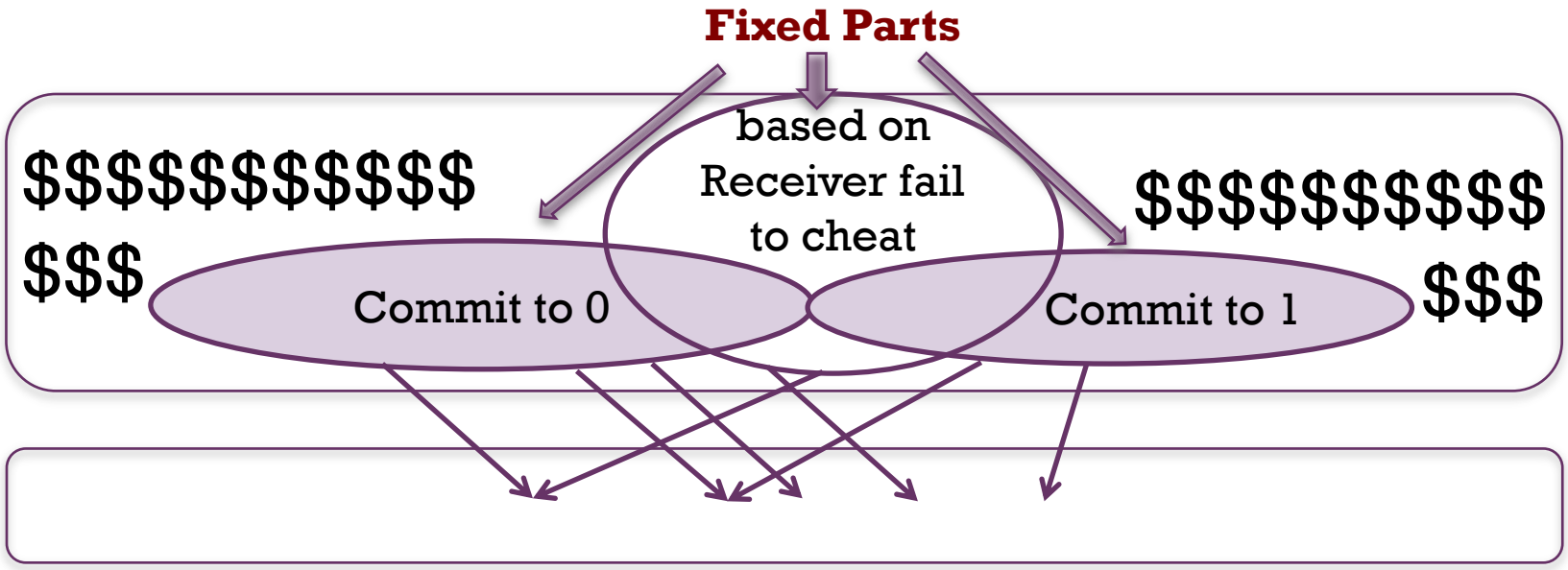
Conclusion:
NIC can be based on Hitting OWFs only through a non-black-box construction.

Hitting Functions

f is Hitting if $\{f(1), f(2), \ldots f(n^2)\}$ intersects "accepting inputs" of *all* poly(n)-sized non-deterministic circuits that accept most of their input.

Easy to show: Random Oracle is hitting with high probability.

How about our partially fixed random oracle?



Need technical tools: new concentration bounds using anti-concentration.

Plan

- Black-Box Separation of NIC from OWF
- An inherently non-black-box assumption for NIC
- Extensions and Open Questions

3-Message Zero-Knowledge Proofs

- NIC used for 3-message Honest-Verifier Zero-Knowledge

- **Theorem.** Use OWF as a black-box to get "certain" 3-message HVZK for NP
  → **NP** is "checkable" [BK'89]
  Same barrier as in [H**M**X10, **M**X10,GWXY10]

- Idea: Construct a proof system for **co-NP** with prover in BPP^{NP}

Open Questions

- Prove that **NP** is checkable based on *any* black-box construction of 3-message HVZK for NP from OWFs.

- Other natural pairs of cryptographic primitives that inherently require non-black-box constructions?

Thank You !