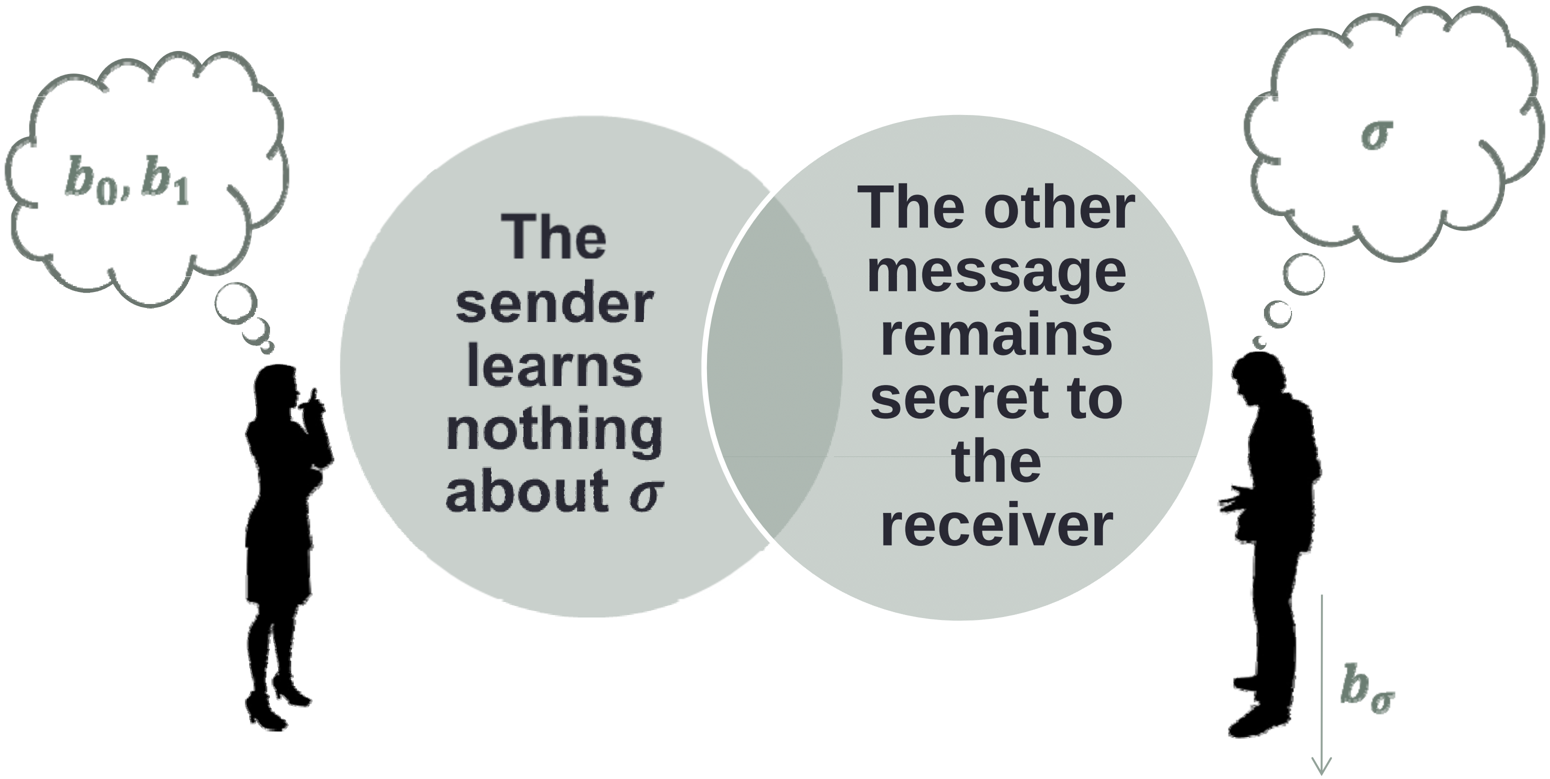
ON THE FEASIBILITY OF EXTENDING OBLIVIOUS TRANSFER

Yehuda Lindell — Bar-Ilan University, Tradition of Excellence

Hila Zarosim — Bar-Ilan University, Tradition of Excellence

TCC 2013

Oblivious Transfer



Oblivious Transfer

- One of the most important primitives in secure computation
  - Used in essentially all constructions of secure computation protocols

- Requires strong hardness assumptions
  - Enhanced TDP ; homomorphic encryption 
  - PKE ; OWF 

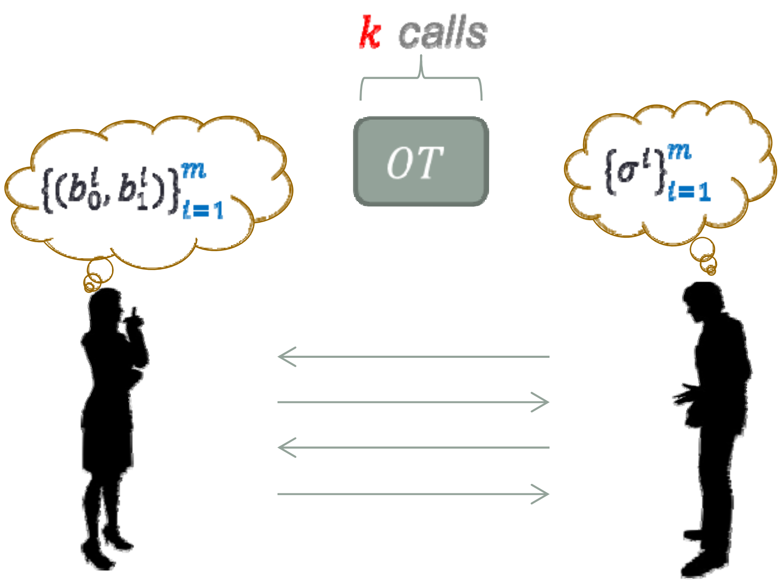
Oblivious Transfer

- OT is expensive and a secure protocol usually needs many executions of oblivious transfer

- In 1996 Beaver asked the following question:
  - Is it possible to use a small number of OT's and a weak assumption to obtain many OT's?

OT-Extensions

- [Beaver96]: It is possible to obtain *poly(n)* OT's given only *O(n)* OT's and **OWFs**
  - This concept is called an "***OT-extension***"
- Let $k < m$. An **OT-extension** from k to m securely computes m OT's given k calls to an ideal-box for computing OT



OT-Extensions

- [Beaver96]: It is possible to obtain *poly(n)* OT's given only *O(n)* OT's and **OWFs**
  - This concept is called an "***OT-extension***"
- Let $k < m$. An **OT-extension** from k to m securely computes m OT's given k calls to an ideal-box for computing OT

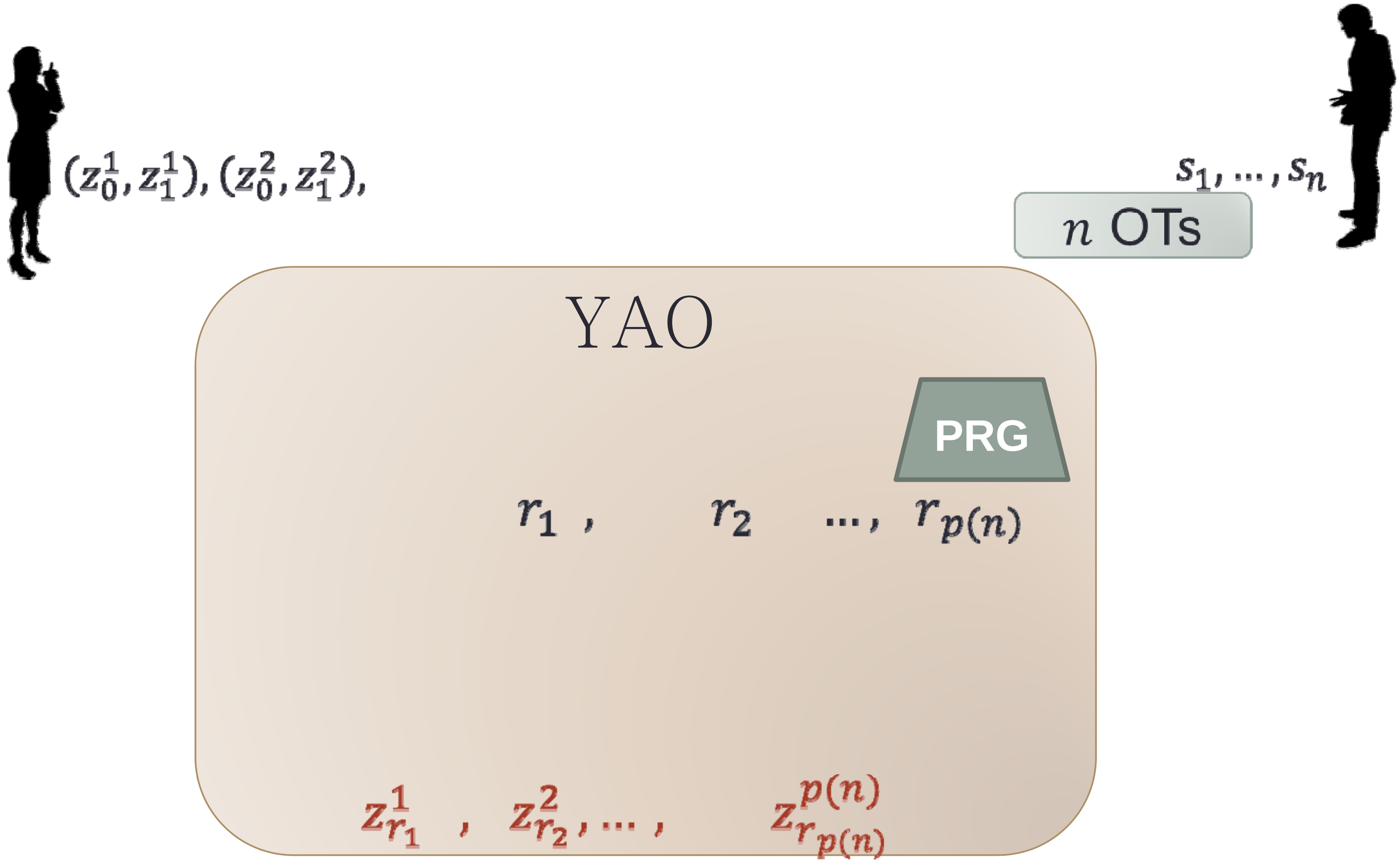
- Theorem [Beaver96]: OT cannot be extended information-theoretically

Efficient OT-Extension

- The original construction of Beaver is not efficient
- In 2003, an efficient OT-extension protocol was presented [IKNP03]
- Efficient OT-extension are widely used to speed-up protocols that use many OTs

OT Extensions - Background

- The protocol of Beaver uses Yao's garbled circuits
- In Yao's protocol:
  - Symmetric encryption for every gate of the Boolean circuit
  - Oblivious transfer for every bit of the P_2's (the receiver) input



$(z_0^1, z_1^1), (z_0^2, z_1^2),$
$s_1, \ldots, s_n$
n OTs
YAO
PRG
r_1 , r_2 ..., $r_{p(n)}$
$z_{r_1}^1$, $z_{r_2}^2, \ldots ,$ $z_{r_{p(n)}}^{p(n)}$

A Theoretical Study of OT Extension

- We know that OT extensions exist assuming OWFs
- We know that OT extensions cannot be computed information theoretically [B96]

- **WE DON'T KNOW ANYTHING ELSE!**

- This paper: we initiate a theoretical feasibility study of OT extensions
  - What can and cannot be achieved and under what assumptions?

On the feasibility of OT-extension

- We ask the following questions:

What is the minimal assumption required for constructing OT-extensions?

Is it possible to extend a ***logarithmic*** number of oblivious transfers?

Can oblivious transfer be extended with ***adaptive*** security?

On the feasibility of OT-extension

- We ask the following questions:

What is the minimal assumption required for constructing OT-extensions?

Is it possible to extend a ***logarithmic*** number of oblivious transfers?

Can oblivious transfer be extended with ***adaptive*** security?

Minimal Assumptions

<u>**Theorem:**</u> The existence of a secure OT-extension implies the existence of one-way functions.

- Corollary: One-way functions are sufficient and necessary for (statistically secure) OT-extensions

Proof Idea

- Given an OT-extension, we construct two ensembles D_1 and D_2 such that:
  - D_1 and D_2 are PPT constructible
  - D_1 and D_2 are computationally indistinguishable
  - D_1 and D_2 are statistically far

- The existence of such ensembles implies the existence of OWFs [Gol90]

Proof Idea

- Loosely speaking:
  - D_1 represents the real-world execution of the protocol on random inputs
  - D_2 represents the ideal-world execution on random inputs
- They are computationally indistinguishable
- We use a result of [WW10] on OT-extensions to show that the ensembles are statistically far apart

On the feasibility of OT-extension

- We ask the following questions:

What is the minimal assumption required for constructing OT-extensions?

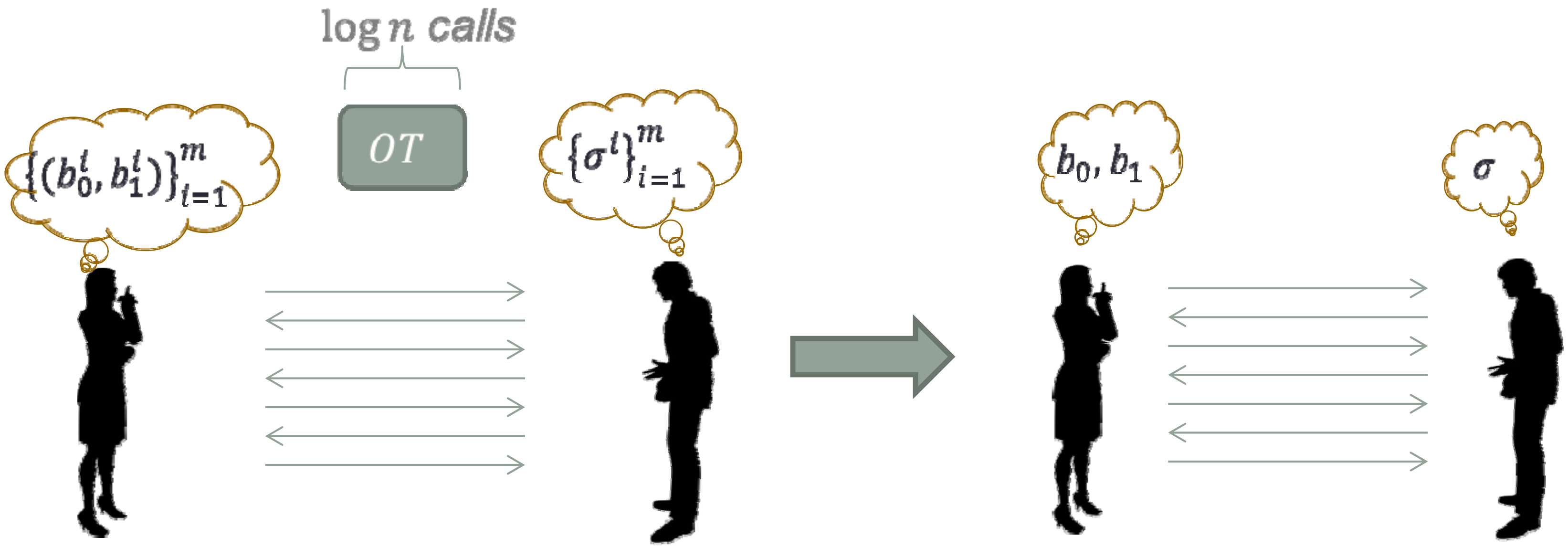
Is it possible to extend a ***logarithmic*** number of oblivious transfers?

Can oblivious transfer be extended with ***adaptive*** security?

On the number of initial OT's

Secure against **malicious adversaries**

Theorem: The existence of an **OT-extension** from $O(\log n)$ implies the existence of an **OT protocol**.



Proof Idea

- We use the OT-extension to construct an OT protocol.
  - The challenge is to eliminate the calls to ideal OT

- The receiver can guess the outputs it was supposed to obtain from the OTs

- There are only $O(\log n)$ calls, and so the probability that the receiver guesses correctly is $2^{O(\log n)} = \frac{1}{poly(n)}$
  - Our construction guarantees that when the receiver guesses incorrectly, it obtains the correct output with prob. $\frac{1}{2}$
  - Thus, overall it obtains correct output with prob. $\frac{1}{2} + \frac{1}{p(n)}$

Proof Idea

- We obtain OT with weak correctness
- Weak correctness can be amplified by multiple executions

- Malicious security guarantees that the receiver learns nothing
  - This is needed because the receiver “deviates” from the protocol
  - It guesses the output rather than taking the output from the OT calls

On the feasibility of OT-extension

- We ask the following questions:

What is the minimal assumption required for constructing OT-extensions?

Is it possible to extend a ***logarithmic*** number of oblivious transfers?

Can oblivious transfer be extended with ***adaptive*** security?

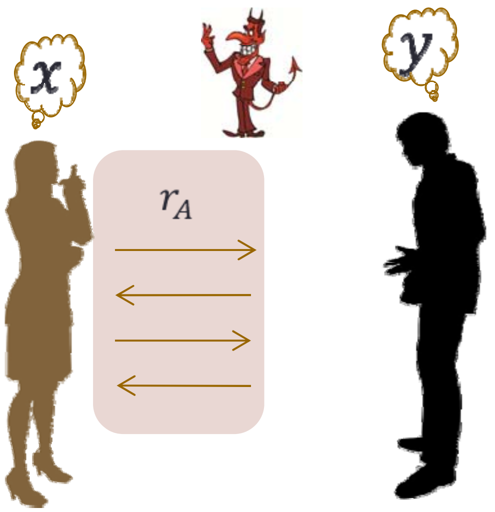
Adaptive Security

- The adversary chooses who to corrupt and when based on its view during the execution
- Corruptions can be made also at the end of the execution ("post-execution phase"), when the transcript is fixed
- Once a party is corrupted, the adversary receives its input and random tape

The Challenge in Adaptive Security

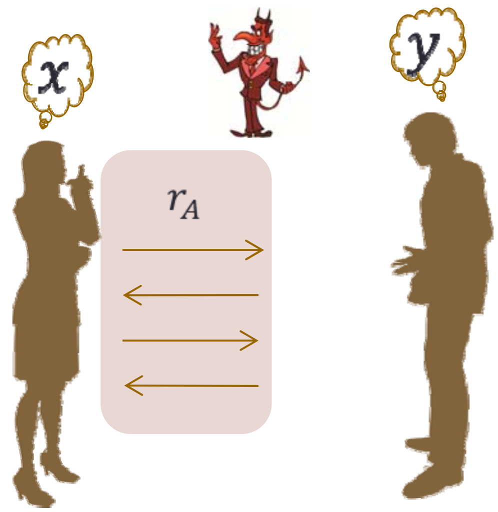
The Challenge in Adaptive Security

- Assume that Alice is corrupted at the outset.
  - The simulator has to generate a simulated view for Alice.



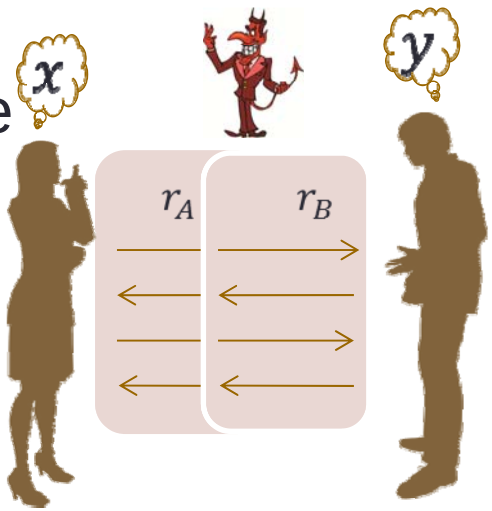
The Challenge in Adaptive Security

- Assume that Alice is corrupted at the outset.
  - The simulator has to generate a simulated view for Alice.
- Assume that Bob is corrupted at the post execution phase.



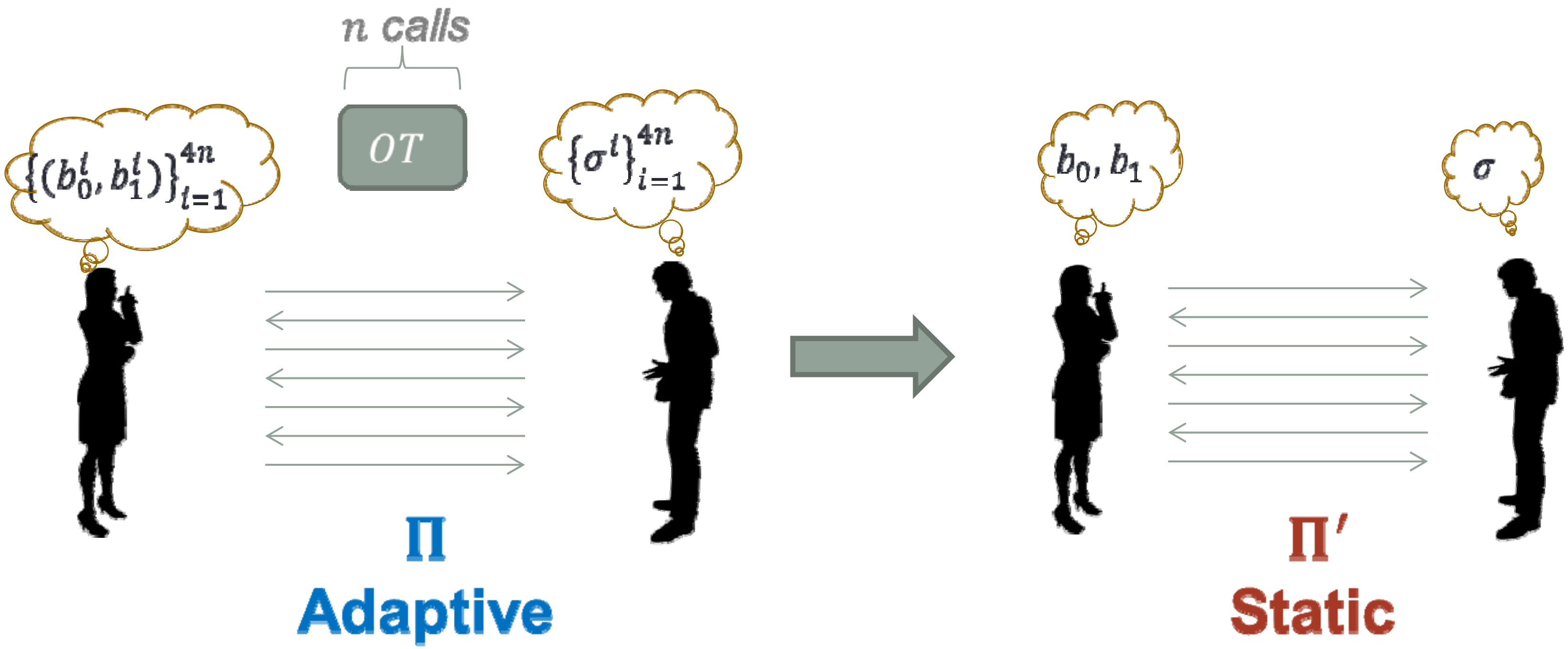
The Challenge in Adaptive Security

- Assume that Alice is corrupted at the outset.
  - The simulator has to generate a simulated view for Alice.
- Assume that Bob is corrupted at the post execution phase.
  - The simulator learns the input of Bob and has to generate a view for Bob that is consistent with the input of Bob and the **already fixed view of Alice**.
- Hence, the simulated view of Alice should be such that **it can later be "explained"** as consistent with **any possible input of Bob**.



Extensions with Adaptive Security

Theorem: The existence of an **adaptively secure OT-extension** implies the existence of a **statically secure OT protocol**.



Π'

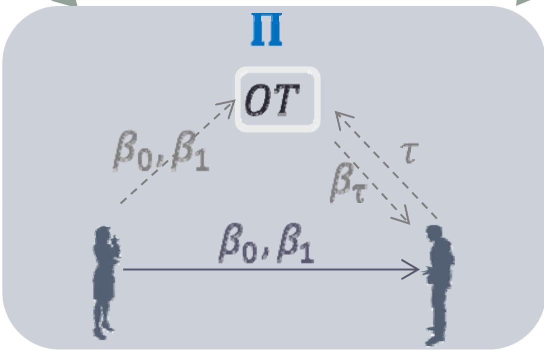
Sender thought: b_0, b_1

Receiver thought: σ

- Choose two random strings $\alpha_0, \alpha_1 \in_R \{0,1\}^{4n}$

Sender's input : α_0, α_1

Receiver's input : σ^{4n}



Receiver's output: α_σ

- Choose random $h_0, h_1 : \{0,1\}^{4n} \to \{0,1\}$
- $z_0 = h(\alpha_0) \oplus b_0$
- $z_1 = h(\alpha_1) \oplus b_1$

$(h_0, z_0), (h_1, z_1) \rightarrow$

Output: $z_\sigma \oplus h_\sigma(\alpha_\sigma)$

Proof Idea

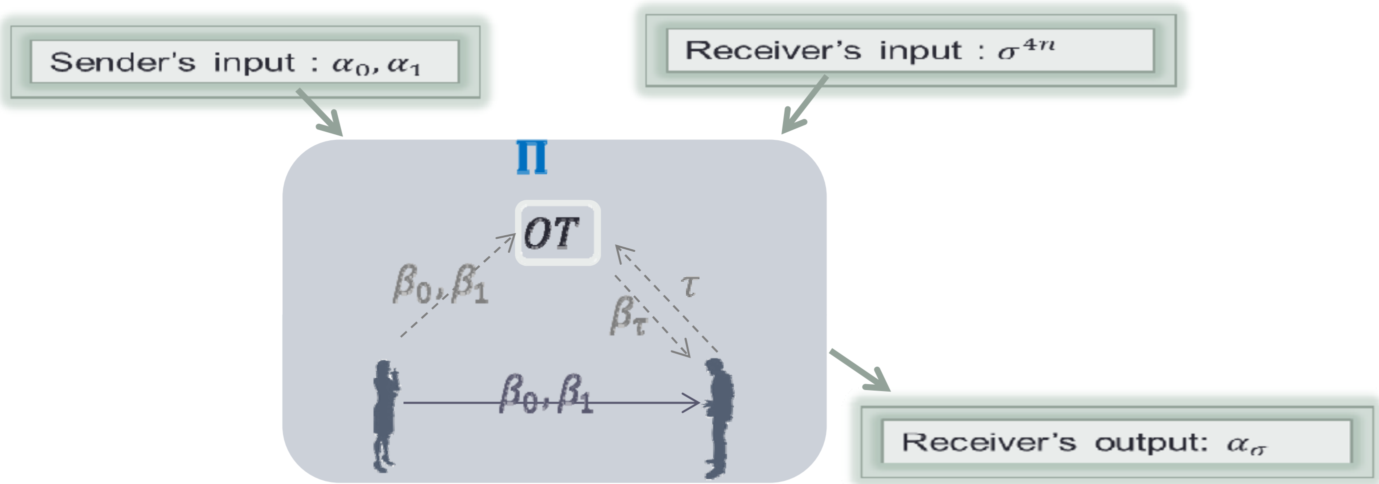
- For each ideal-OT in Π:
  - The receiver in $\boldsymbol{\Pi}$ learns one of the sender's inputs.
  - In $\boldsymbol{\Pi}'$, the receiver leans both of the sender's inputs.

- This gives the receiver n additional bits of information.
  - This might leak information about $\alpha_{1-\sigma}$ and hence about $b_{1-\sigma}$.

- However, $\alpha_{1-\sigma}$ is $4n$ bits long.
  - Hence, there is still enough entropy in $h(\alpha_{1-\sigma})$.

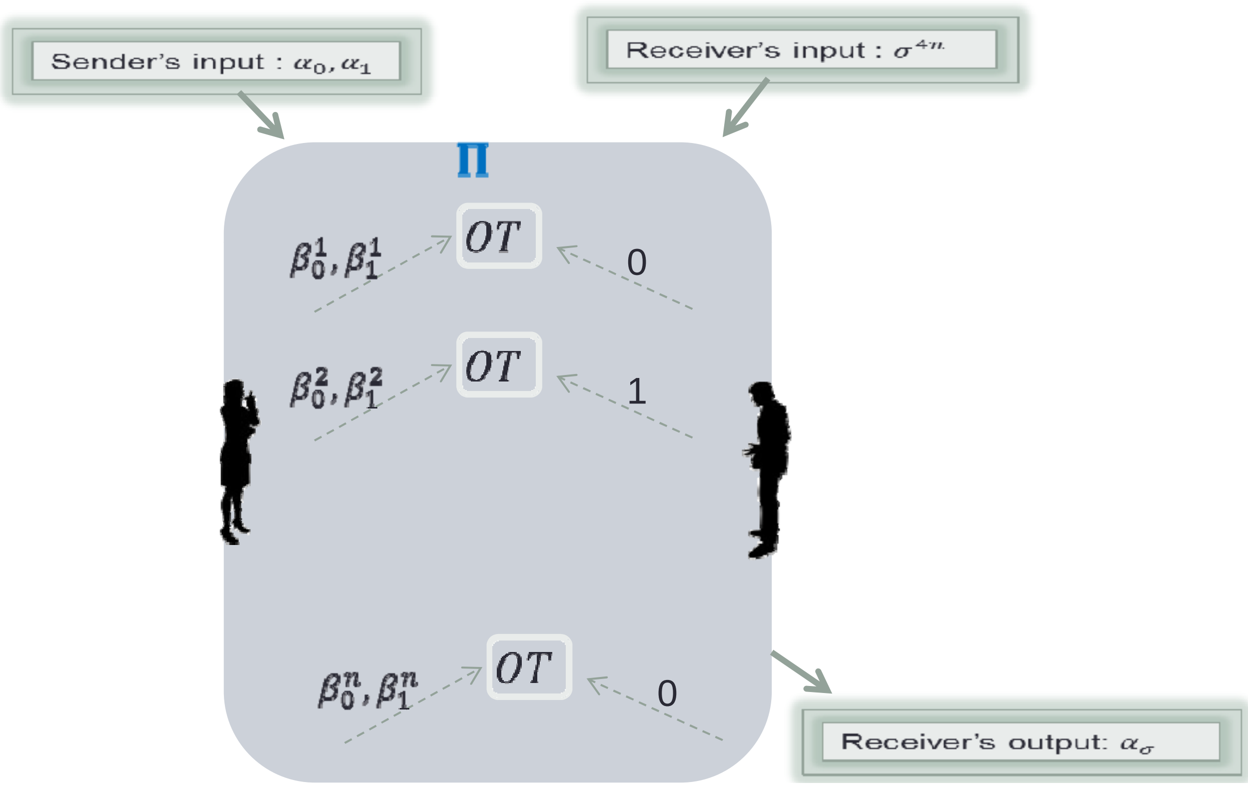
Proof Idea

- The main technical challenge is to simulate the view of the receiver in Π'
  - We would like to use the simulator guaranteed to exist for Π



  - A simulated view of the receiver in Π contains **one of** (β_0, β_1) for each ideal-OT
  - A simulated view for the receiver in Π' must contain **both** (β_0, β_1)

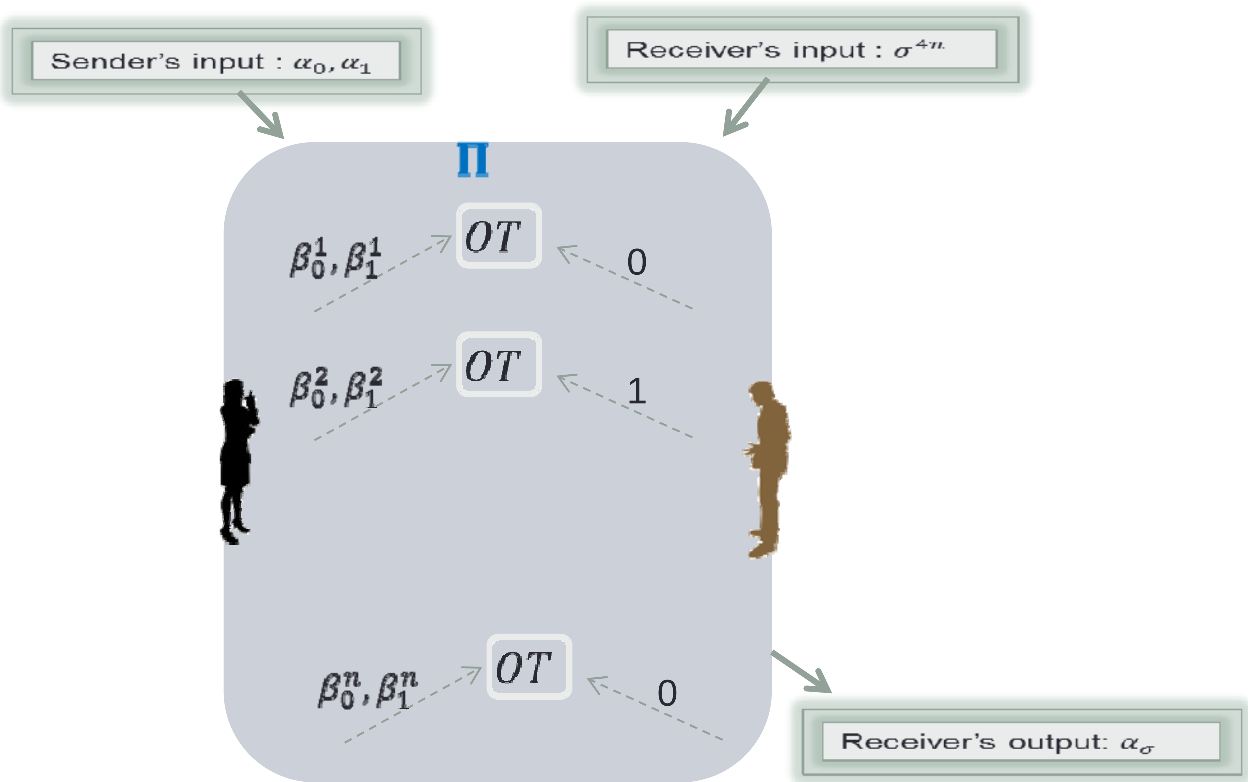
Proof Idea



Sender's input : α_0, α_1
Receiver's input : σ^{4n}
Π
β_0^1, β_1^1
OT
0
β_0^2, β_1^2
OT
1
β_0^n, β_1^n
OT
0
Receiver's output: α_σ

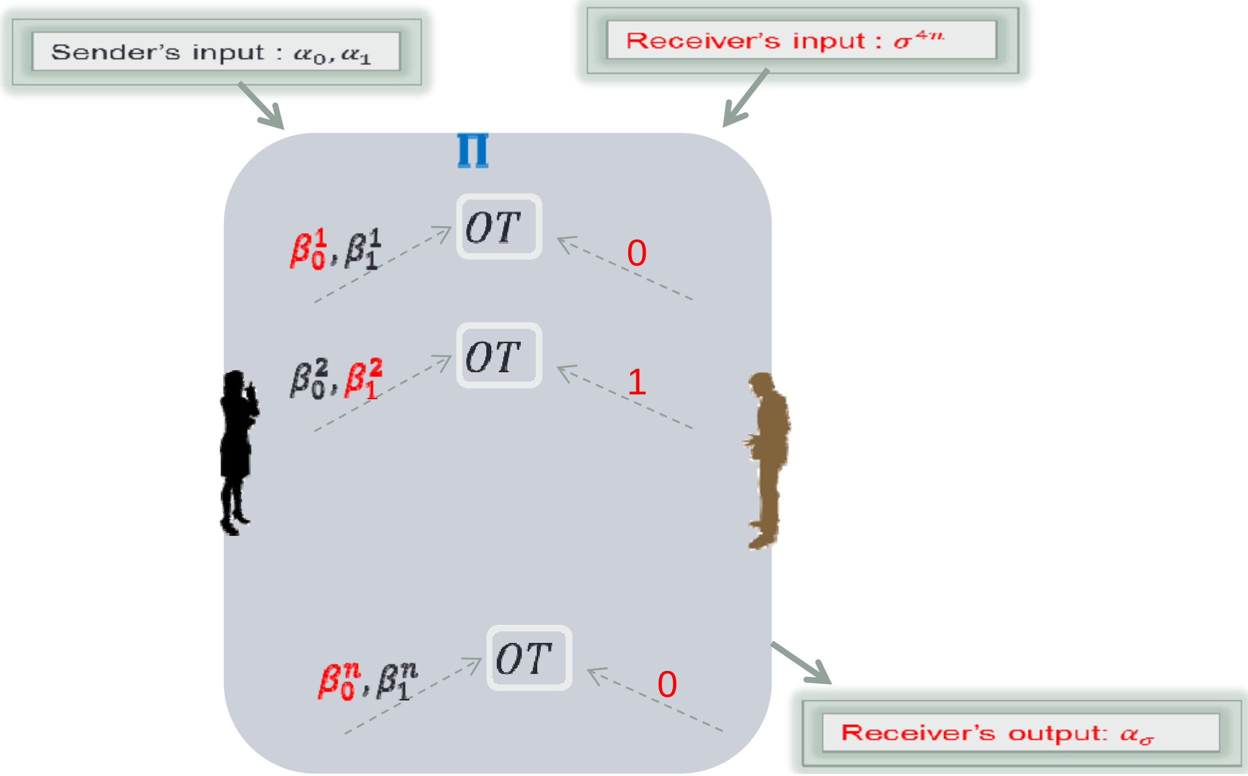
Proof Idea

- Assume that the receiver in Π is corrupted at the beginning of the protocol



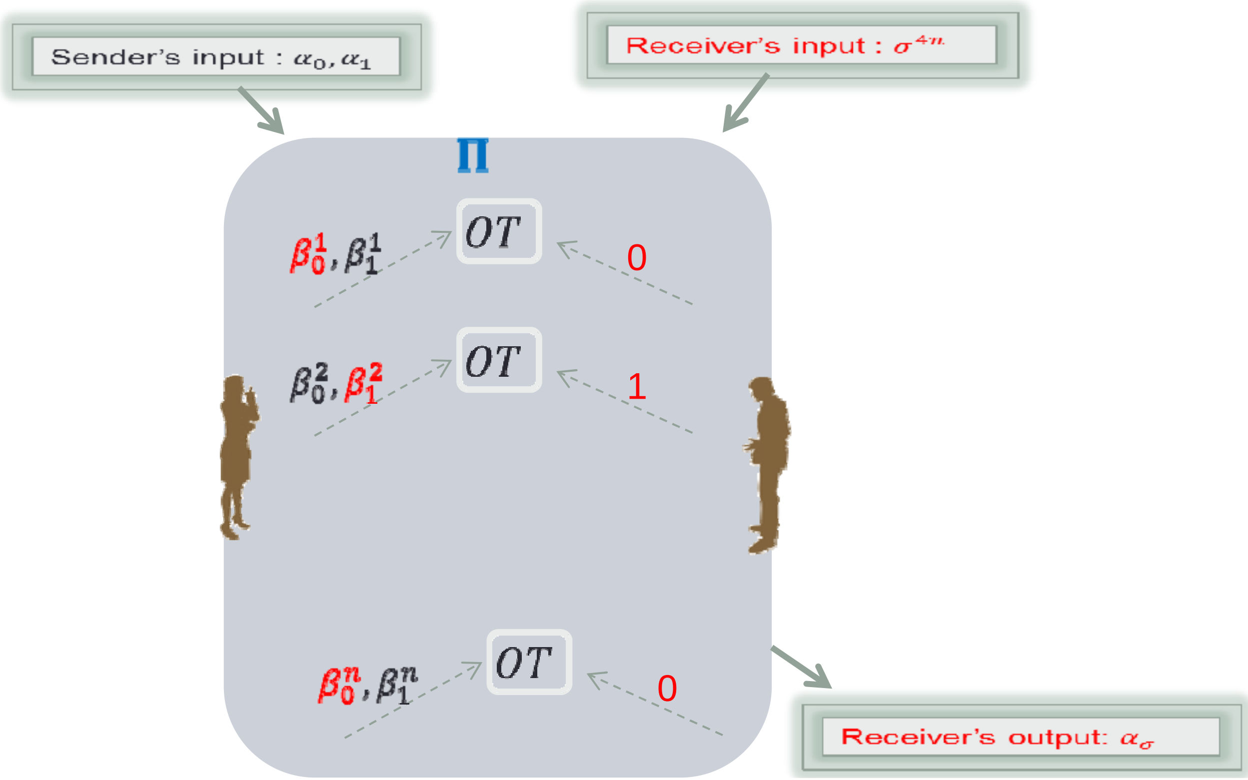
Proof Idea

- Assume that the receiver in Π is corrupted at the beginning of the protocol
  - Fix a simulated view for the receiver
  - This view contains n outputs of the ideal-OTs



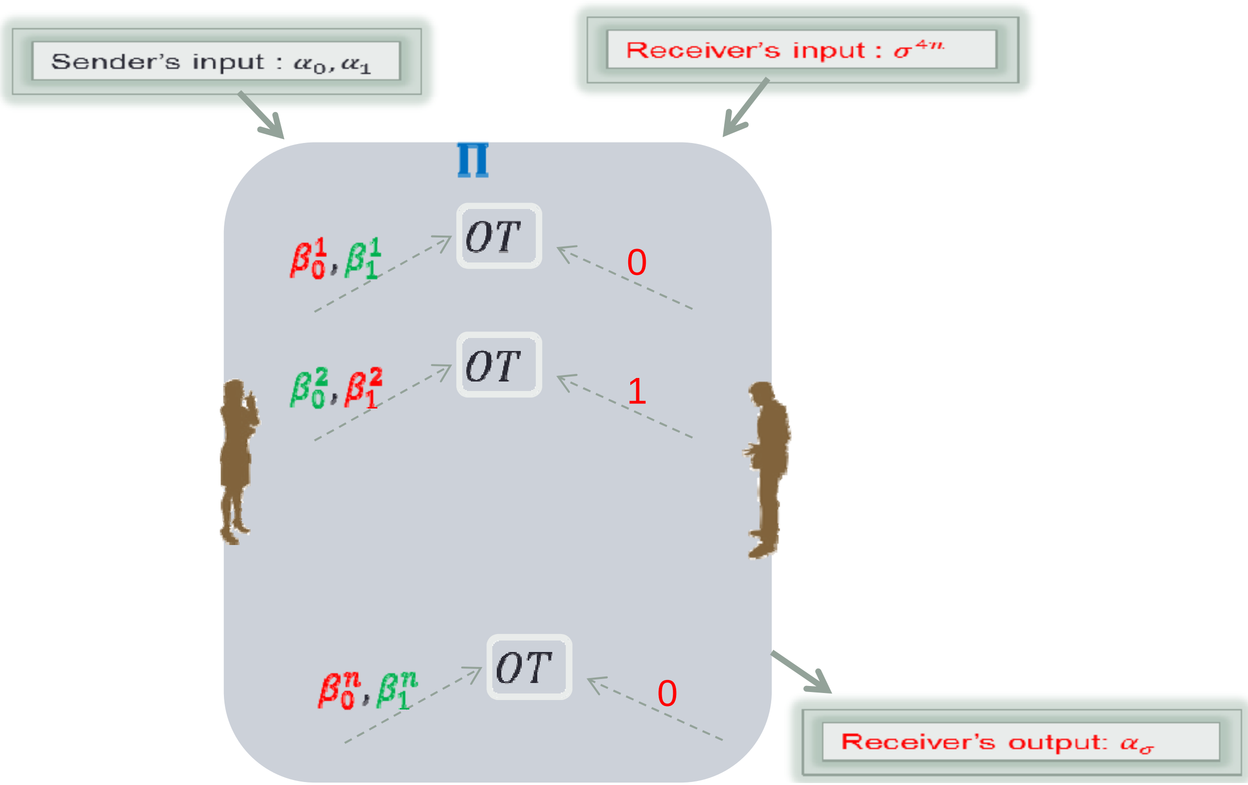
Proof Idea

- Now, assume that the sender is corrupted at the post-execution phase
  - The simulator generates a sender-view that is consistent with $\alpha_{1-\sigma}$ and the receiver-view



Proof Idea

- Append the inputs of the n ideal-OTs to the already-fixed receiver-view
  - We call this an "*extended receiver-view*"



Proof Idea

- Given the input $\alpha_{1-\sigma}$ of the sender, the simulator generates an extended receiver-view
- The new extended receiver-view contains n more bits of information
  - For every fixed receiver-view, there are 2^n *extended views*
- However, there are 2^{4n} possible $\alpha_{1-\sigma}$
- Hence, for "many" possible $\alpha_{1-\sigma}$, we obtain the same extended receiver-view

- We conclude that the extended view does not leak too much information on $\alpha_{1-\sigma}$
  - There is still enough entropy in $h(\alpha_{1-\sigma})$ to hide $b_{1-\sigma}$

Summary

- In this work, we study the feasibility of extending OT
- We show that OWF are necessary for extending OT
- To extend only a logarithmic number of oblivious transfers, one has to construct an OT protocol from scratch
- Adaptive OT extensions based on a weaker assumption than static oblivious transfer do not exist

Open Questions

- We showed that an adaptively secure OT-extension implies statically secure OT
  - Can adaptively secure OT-extension be based on assumption weaker than needed for adaptively secure OT?
- Is it possible to construct a semi-honest OT-extension from $O(\log n)$ from assumptions weaker that the existence of OT?
- Extending other primitives?


Thank You!