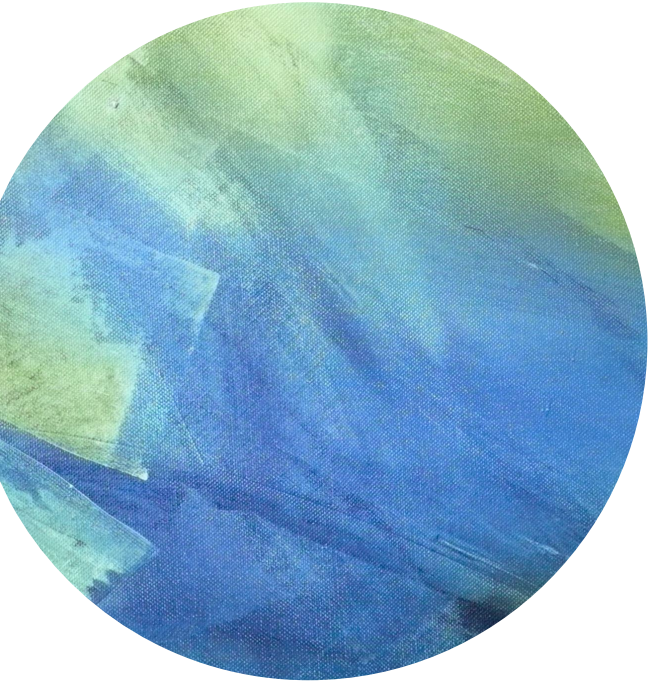

Lecture 20



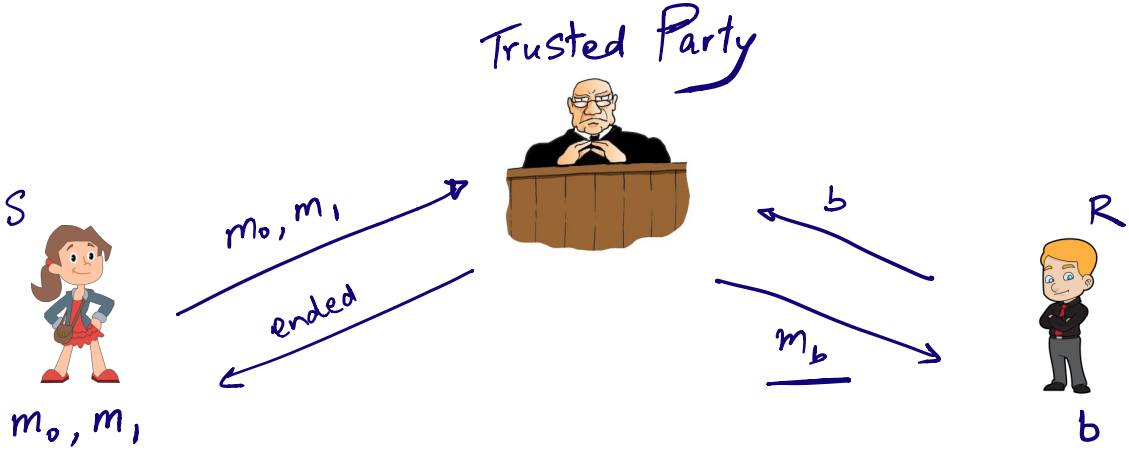
Outline

Secure Computation

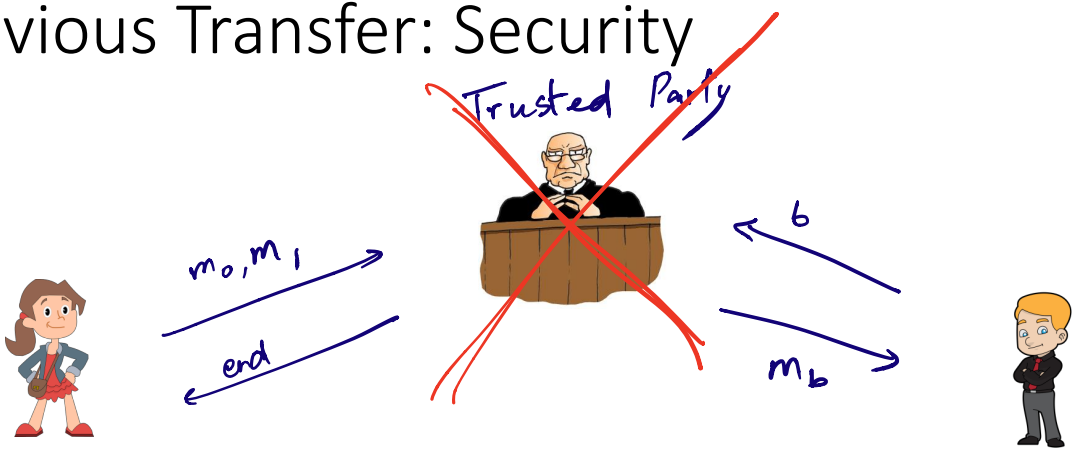
Garbled Circuits

Oblivious Transfer

Oblivious Transfer



Oblivious Transfer: Security



Alice doesn't learn b

Bob doesn't learn m_{1-b}

Oblivious Transfer: Construction

m_0, m_1

$g^{\alpha_0} = g$ $\quad g^{\alpha_1}$

pk_0, pk_1

$enc_{pk_0}(m_0)$, $enc_{pk_1}(m_1)$

$g^{\beta_0}, H(g^{\alpha_0\beta_0}) \oplus m_0$ $\quad$ $g^{\beta_1}, H(g^{\alpha_1\beta_1}) \oplus m_1$

b

m_b

For choice bit b,

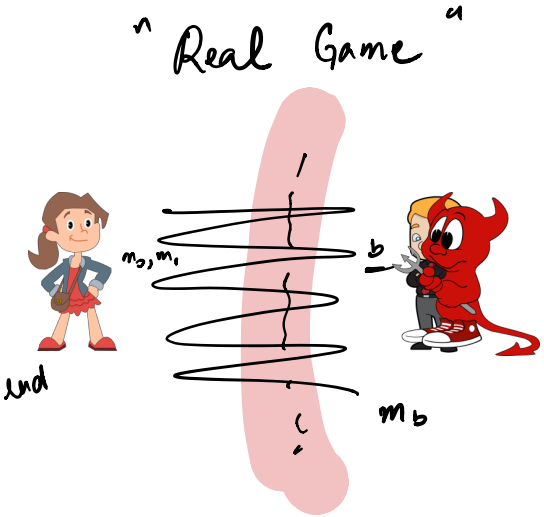
Sample $pk_b = g^{\alpha_b}$ $\quad$ $pk_{1-b} = g^{\alpha_{1-b}}$

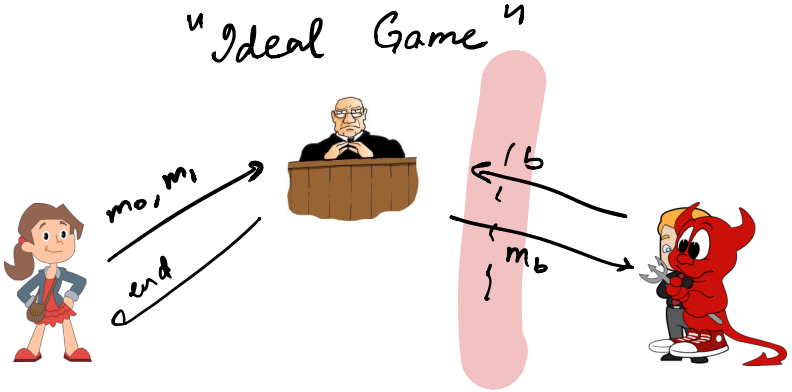
✗ Recover m_b

Types of adversaries

- Semi-honest/honest-but-curious adversary
  - Follows protocol specifications; already defined
- Malicious adversary
  - Does not follow protocol specifications
  - We will define this next

OT: Security against Malicious Receivers





OT: Security against Malicious Receivers

"Real World/Expmt"

$\text{View}_{\text{Bob}} = (\text{State}_{\text{Bob}}) + (\text{transcript})$

does not contain info. about m_{1-b}, by virtue of indistinguishability from the ideal view

"Ideal Expmt"

cannot contain info. about m_{1-b}!

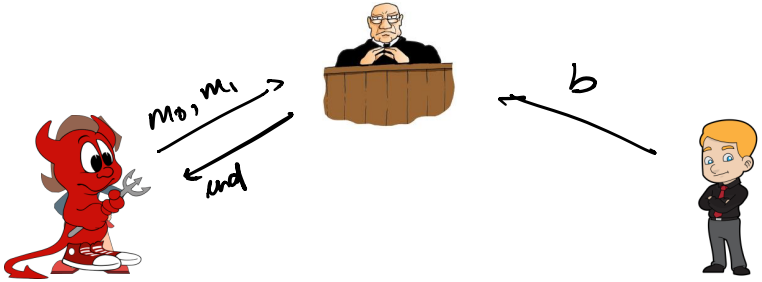
$\text{View}_{\text{Bob}} = (\text{State}_{\text{Bob}}) + (\text{transcript})$

(1) Sim has to pretend to be Alice

(2) Sim has to "find" implicit b that Bob uses.

(3) Sim must generate view w/o knowledge of m_{1-b}

OT: Security against Malicious Senders



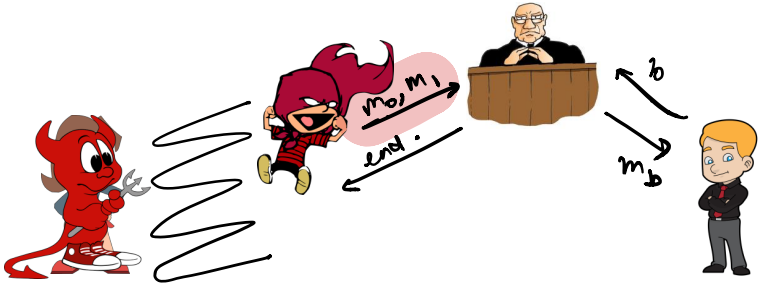
OT: Security against Malicious Senders

"Real World"

$\text{View}_{\text{Alice}}$

$\approx$

"Ideal World"



$\text{View}_{\text{Alice}}$

[2019]

Oblivious Transfer Secure Against Malicious Adversaries:

CONSTRUCTION

[PKE with pseudorandom public keys]

RANDOM ORACLE

Bob: Has input b

s_0, s_1

1) Sample $(pk, sk) \leftarrow Gen$

$pk_0 = H(s_0) \oplus s_1$

$pk_1 = H(s_1) \oplus s_0$

ct_0, ct_1

$ct_0 = Enc_{pk_0}(m_0)$

$ct_1 = Enc_{pk_1}(m_1)$

$m_b \leftarrow Dec_{sk}(ct_b)$

3) Sample $r_0 \xleftarrow{R} \{0,1\}^n$

Compute $H(r_0)$.

4) Set $r_1 = H(r_0) \oplus pk$

Note: $pk = r_1 \oplus H(r_0)$

5) Set $pk' = r_0 \oplus H(r_1)$

Bob doesn't know sk'.

6) If $b = 0$

$s_0 = r_0, s_1 = r_1$

If $b = 1$,

$s_1 = r_0, s_0 = r_1$

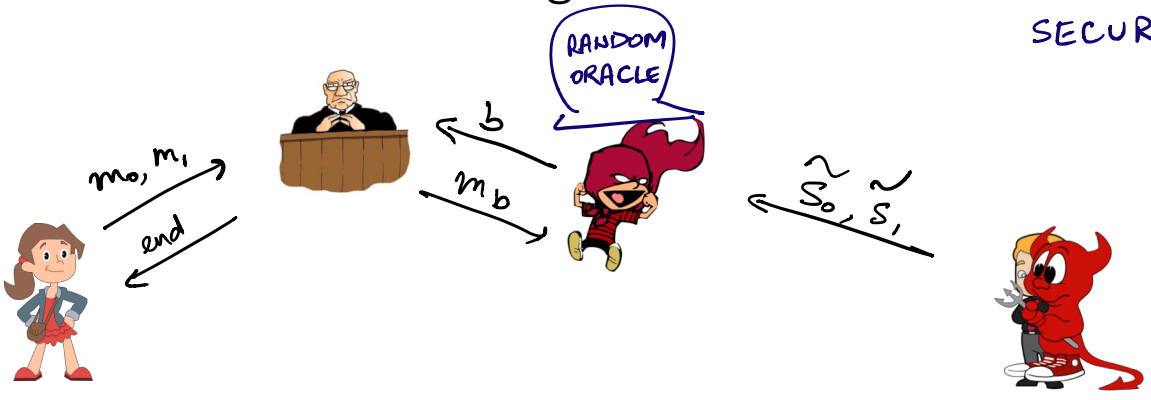
Oblivious Transfer Secure Against Malicious Adversaries :

CONSTRUCTION

RANDOM ORACLE

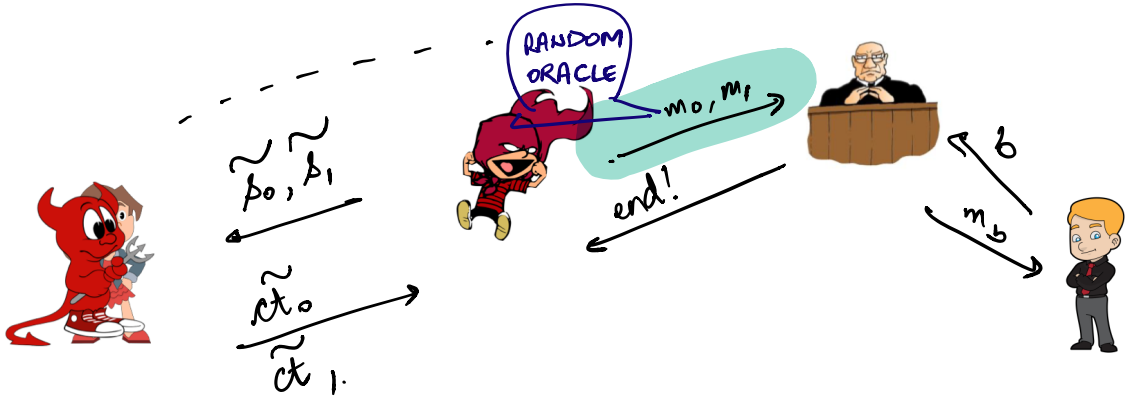
Oblivious Transfer Secure Against Malicious Adversaries :

SECURITY



Oblivious Transfer Secure Against Malicious Adversaries:

SECURITY



Simulator's goal: Sample $\tilde{s}_0, \tilde{s}_1$ s.t. they know (sk_0, sk_1) for (pk_0, pk_1) where $pk_0 = H(\tilde{s}_0) \oplus \tilde{s}_1$, $pk_1 = H(\tilde{s}_1) \oplus \tilde{s}_0$.

* Sim will first sample $(pk_0, sk_0) \leftarrow Gen$ $(pk_1, sk_1) \leftarrow Gen$. Sample $(\tilde{s}_0, \tilde{s}_1)$. Set $H(\tilde{s}_0) = pk_0 \oplus \tilde{s}_1$, $H(\tilde{s}_1) = pk_1 \oplus \tilde{s}_0$