Two Round Oblivious Transfer from CDH or LPN

Eurocrypt 2020

Nico Döttling   Sanjam Garg   Mohammad Hajiabadi
Daniel Masny   Daniel Wichs

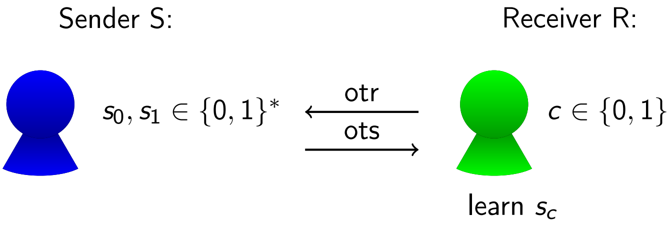
CISPA Helmholtz Center for Information Security

UC Berkeley

Visa Research

Northeastern University

Oblivious Transfer (OT)

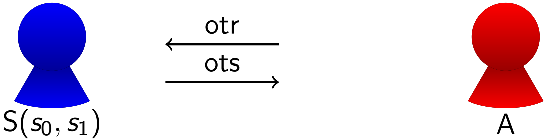


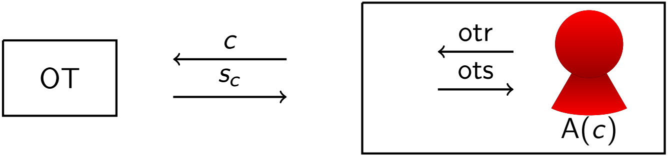
Security

- S does not learn c.
- R does not learn s_{1-c}

Simulation based Security (for Sender S)

For any A,





Security for Receiver R

Simulation based Security

- Same as for Sender
- A′ needs to extract s_0, s_1

Indistinguishability based Security

- weaker than simulation based
- malicious S cannot distinguish R(0) from R(1)

Our Results

Sim. Sender, Ind. Receiver Secure OT ($\tilde{\mathsf{OT}}$) $\Rightarrow$ Sim. Secure OT

- $\tilde{\mathsf{OT}}$ $\Rightarrow$ 2-round ZK
- $\tilde{\mathsf{OT}}$ + 2-round ZK $\Rightarrow$ Sim. Secure OT

CDH or LPN $\Rightarrow$ $\tilde{\mathsf{OT}}$

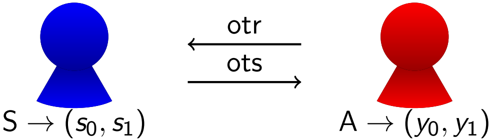
- weaker OT security notions for the sender
- CDH or LPN $\Rightarrow$ weaker notions
- generic transformation from weaker notions to $\tilde{\mathsf{OT}}$

Summary

$\tilde{OT}$ from CDH

1. CDH or LPN $\Rightarrow$ Elementary OT (eOT)
2. Elementary OT $\Rightarrow$ Search OT (sOT)
3. Search OT $\Rightarrow$ Indistinguishable OT (iOT)
4. Indistinguishable OT $\Rightarrow$ $\tilde{OT}$

CDH $\Rightarrow$ eOT $\Rightarrow$ sOT $\Rightarrow$ iOT $\Rightarrow$ $\tilde{\text{OT}}$



Elementary OT Security

$$\Pr[(y_0, y_1) = (s_0, s_1)] \leq \text{negl}$$

CDH ⇒ eOT ⇒ sOT ⇒ iOT ⇒ $\tilde{\text{OT}}$

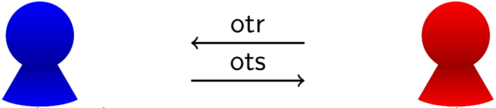
Bellare, Micali [BM90]:

Sender S:	CRS : $(X = g^x)$	Receiver R(c):
		$r \leftarrow \mathbb{Z}_p$
$h_1 = h_0 X$	$\xleftarrow{\text{otr} = h_0}$	$h_0 = g^r X^{-c}$
$s \leftarrow \mathbb{Z}_p$		
$S = g^s$	$\xrightarrow{\text{ots} = S}$	
		output S^r

Correctness and Security

- $s_c = h_c^s = (h_0 X^c)^s = (g^r X^{-c} X^c)^s = S^r$
- $s_{1-c} = h_{1-c}^s = (h_0 X^{1-c})^s = X^{(1-2c)s} S^r$
- computing $s_0 / s_1 = g^{xs}$ solves CDH for challenge X, S

$\mathsf{CDH} \Rightarrow \mathsf{eOT} \Rightarrow \mathsf{sOT} \Rightarrow \mathsf{iOT} \Rightarrow \tilde{\mathsf{OT}}$



$\mathsf{S} \to (s_0, s_1)$

$\mathsf{A}_1 \to (\mathsf{st}, \mathsf{otr})$

$\mathsf{A}_2(\mathsf{st}, \mathsf{ots}, w) \to y_w$

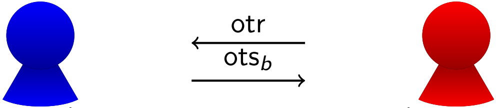
Search OT Security

With $1 - \mathsf{negl}$ probability over $(\mathsf{st}, \mathsf{otr})$,
$\exists w \in \{0, 1\}$ s.t. $\Pr_{\mathsf{ots}}[\mathsf{A}_2(\mathsf{st}, \mathsf{ots}, w) = s_w] \leq \mathsf{negl}$.

Elementary OT $\Rightarrow$ Search OT

$\Pr_{\mathsf{ots}}[\mathsf{A}_2(\mathsf{st}, \mathsf{ots}, w) = s_w] > \frac{3}{4} \Rightarrow$
$\Pr_{\mathsf{ots}}[\forall w, \mathsf{A}_2(\mathsf{st}, \mathsf{ots}, w) = s_w] > \mathsf{negl}$.
Solution: Amplify hardness (Canetti, Halevi, Steiner [CHS05])

CDH $\Rightarrow$ eOT $\Rightarrow$ <u>sOT $\Rightarrow$ iOT</u> $\Rightarrow$ $\widetilde{\text{OT}}$



$\mathsf{S}(\mathsf{otr}, m_0, m_1) \rightarrow \mathsf{ots}_0$
$\mathsf{S}(\mathsf{otr}, m_{1-w}, \mathsf{uniform}) \rightarrow \mathsf{ots}_1$

$\mathsf{A}_1 \rightarrow (\mathsf{st}, \mathsf{otr}, m_0, m_1)$
$\mathsf{A}_2(\mathsf{st}, \mathsf{ots}_b) \rightarrow b'$

Indistinguishable OT Security

With $1 - \mathsf{negl}$ probability over $(\mathsf{st}, \mathsf{otr})$, $\exists w \in \{0, 1\}$ s.t.
$|\Pr_{\mathsf{ots}}[\mathsf{A}_2(\mathsf{st}, \mathsf{ots}_0) = 1] - \Pr_{\mathsf{ots}}[\mathsf{A}_2(\mathsf{st}, \mathsf{ots}_1) = 1]| \leq \mathsf{negl}$.

Search OT $\Rightarrow$ Indistinguishable OT

Goldreich Levin hardcore predicates [GL89], hybrid argument.

CDH $\Rightarrow$ eOT $\Rightarrow$ sOT $\Rightarrow$ iOT $\Rightarrow$ $\tilde{\text{OT}}$

$\text{CRS} = (\text{CRS}_{\text{iOT}}, \text{pk})$

Sender $\mathsf{S}(m_0, m_1)$:

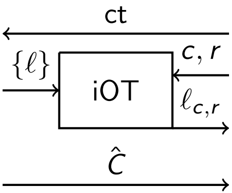
$C[\text{ct}, \text{CRS}, m_0, m_1](c, r)$:

  If $(\text{ct} = \text{Enc}(\text{pk}, c; r))$

  Then output m_c

  Else output $\perp$

$(\hat{C}, \{\ell\}) \leftarrow \text{Garble}(C)$



Receiver $\mathsf{R}(c)$:

$\text{ct} = \text{Enc}(\text{pk}, c; r)$

$m_c = \hat{C}(\ell_{c,r})$

Receiver Ind., Sender Sim. Security

- ct and iOT do not leak c
- Given sk, c can be extracted
- Can iOT and $\hat{C}$ be simulated without m_{1-c}?

Sender's Simulation based Security

Garbled Circuits; Yao [Yao82]

- $\{\ell\}$ and $\hat{C}$ leak m_0 and m_1.
- $\ell_{c,r}$, $\hat{C}$ only leak m_c.

Solution: Use independent $\{\ell\} \setminus \ell_{c,r}$ for $\hat{C}$ and iOT.

Distinguisher Dependent Simulation; Jain, Kalai, Khurana, Rothblum [JKKR17]

- Indistinguishable OT: $\exists w \in \{0,1\}$ s.t. $\ell_w \approx_c$ uniform.
- We test run the adversary to learn $w \in \{0,1\}$.
- In the actual simulation, w is consistent with good probability.
- We can replace $\ell_w \in \{\ell\} \setminus \ell_{c,r}$ with uniform.

Summary

Our Results, eprint.iacr.org/2019/414

1. CDH or LPN $\Rightarrow$ Elementary OT
2. Elementary OT $\Rightarrow$ Search OT
   (Hardness Amplification; Canetti, Halevi, Steiner [CHS05])
3. Search OT $\Rightarrow$ Indistinguishable OT
   (Hardcore Predicates; Goldreich, Levin [GL89])
4. Indistinguishable OT $\Rightarrow$ $\tilde{\text{OT}}$
   (Distinguisher Dependent Simulation; Jain, Kalai, Khurana, Rothblum [JKKR17], Garbled Circuits; Yao [Yao82])
5. $\tilde{\text{OT}}$ + 2-round ZK $\Rightarrow$ Sim. Secure OT
   ($\tilde{\text{OT}}$ $\Rightarrow$ 2-round ZK)