Oblivious Transfer (OT) and OT Extension

School on Secure Multiparty Computation

Arpita Patra
Roadmap

- Oblivious Transfer
  - Construction from `special’ PKE

- OT Extension
  - IKNP OT extension

- Tracing the journey of OT extension and some open questions
Oblivious Transfer

- **Complete** for MPC
- Used in both traditional approaches: Yao (per input) and GMW (per AND gate)
- OT forms the basis for most of the practical MPCs/2PCs, special purpose problems PSI
- OTs are **intrinsically expensive**- usually based on public key primitives
- AES Circuit: Millions of AND gates
Setting the stage for OT Extension

- X (task/object): executing/generating X is not very efficient
- Small no. X \( \rightarrow \) many no. X
  - **PRG**: Truly Random short Seed \( \rightarrow \) huge (pseudo-)random string
    
    \[
    s \in_R \{0,1\}^k \rightarrow \text{PRG} \rightarrow \text{PRG}(s) \in \{0,1\}^{p(k)}
    \]

- **Hybrid Encryption (HE)**: one instance of PKE \( \rightarrow \) many instances of PKE \( @ \) SKE operations
OT Extension: From small to many

OT\textsubscript{1} \quad OT\textsubscript{2} \quad OT\textsubscript{k}

OT Extension

SKE operations

OT\textsubscript{1} \quad OT\textsubscript{2} \quad OT\textsubscript{3} \quad OT\textsubscript{p(k)}

> OT Ext is not possible information theoretically [Bea96]
> OT Ext implies OWF [LZ13]

First work to tell us about OTExt

k: security parameter
Roadmap for Building OT Extension [IKNP03]

- **k bit inputs**
  - $OT_1$
  - $OT_2$
  - $OT_k$

- **m (poly(k)) > k bit inputs**
  - Domain Extension
    - $OT_1$
    - $OT_2$
    - $OT_k$

- **l bit inputs**
  - $OT_1$ with $b_1, x_{1b1}$
  - $OT_2$ with $b_2, x_{2b2}$
  - $OT_3$ with $b_3, x_{3b3}$
  - $OT_m$ with $b_m, x_{mbm}$

**OT Extension**

- $k$ OTs with $k$ bit inputs
- $k$ OTs with $m > k$ bit inputs
- $m$ OTs with $m > k$ bit inputs
Transformation I: Domain Extension

PRG \(G: \{0,1\}^k \rightarrow \{0,1\}^{m=p(k)}\)

- **k bit inputs**
  - \(k_0\)
  - \(k_1\)

- **m bit inputs**
  - \(m_0\)
  - \(m_1\)

\(y_0 = G(k_0) + m_0\)
\(y_1 = G(k_1) + m_1\)

\(m_b = G(k_b) + y_b\)
Roadmap for Building OT Extension [IKNP03]

Domain Extension:
- k OTs with k bit inputs
- k OTs with m > k bit inputs
- m OTs with m > k bit inputs

OT Extension:
- m OTs with m > k bit inputs
Transformation II: OT Extension

\[ B = [b_1, \ldots, b_m] \]

\[ \begin{align*}
Q &= Q_1 = T_1 \text{ (if } b_1 = 0) / T_1 + S \text{ (otherwise)} \\
Q_2 &= T_2 \text{ (if } b_2 = 0) / T_2 + S \text{ (otherwise)} \\
Q_m &= T_m \text{ (if } b_m = 0) / T_m + S \text{ (otherwise)}
\end{align*} \]

Random \( S \) is known to \( P_0 \) only
Transformation II: OT Extension

There's a Bug!

There's a Bug!

\[ \begin{align*}
Q &= \begin{cases}
Q_1 = T_1 (\text{if } b_1 = 0) / T_1 + S \ (\text{otherwise}) \\
Q_2 = T_2 (\text{if } b_2 = 0) / T_2 + S \ (\text{otherwise}) \\
Q_m = T_m (\text{if } b_m = 0) / T_m + S \ (\text{otherwise})
\end{cases} \\
\end{align*} \]

\[ \begin{align*}
x_{10} &= Q_1 + x_{10} \\
x_{11} &= Q_1 + S + x_{11} \\
x_{m0} &= Q_m + x_{m0} \\
x_{m1} &= Q_m + S + x_{m1}
\end{align*} \]

\[ \begin{align*}
x_{1} b_1 &= T_1 + y_{1} b_1 \\
x_{m} b_m &= T_m + y_{m} b_m
\end{align*} \]
Transformation II: OT Extension

Given random and independent $S$, $T_1$, ..., $T_m$, the joint distribution \{H(T_1 + S), ..., H(T_m + S), T_1, ..., T_m\} must be pseudo-random.

Cryptographic Hash function: SHA 1/2/3, RC4

\[
B = [b_1, ..., b_m]
\]

\[
P_0 \quad \begin{cases} 
  x_{10} = H(1, Q_1) + x_{10} \\
  x_{11} = H(1, Q_1 + S) + x_{11} \\
  x_{20} = H(1, Q_2) + x_{20} \\
  x_{21} = H(1, Q_2 + S) + x_{21} \\
  \vdots \\
  x_{m0} = H(m, Q_m) + x_{m0} \\
  x_{m1} = H(m, Q_m + S) + x_{m1}
\end{cases}
\]

\[
P_1 \quad \begin{cases} 
  y_{10} = H(1, Q_1) + x_{10} \\
  y_{11} = H(1, Q_1 + S) + x_{11} \\
  y_{20} = H(1, Q_2) + x_{20} \\
  y_{21} = H(1, Q_2 + S) + x_{21} \\
  \vdots \\
  y_{m0} = H(m, Q_m) + x_{m0} \\
  y_{m1} = H(m, Q_m + S) + x_{m1}
\end{cases}
\]

\[
\begin{align*}
  T &= T_1 \\ 
  &\quad T_2 \\
  &\quad \ldots \\ 
  &\quad T_m \\
  Q &= Q_1 \\
  &\quad T_1 \quad (if \, b_1 = 0) / T_1 + S \quad (otherwise) \\
  &\quad Q_2 = T_2 \quad (if \, b_2 = 0) / T_2 + S \quad (otherwise) \\
  &\quad Q_m = T_m \quad (if \, b_m = 0) / T_m + S \quad (otherwise) \\
\end{align*}
\]

Correlation Robust H: $[m] \times \{0,1\}^k \rightarrow \{0,1\}^l$
Transformation II: OT Extension

\[ B = [b_1, \ldots, b_m] \]

\[ Q = \begin{cases} 
Q_1 = \frac{T_1}{T_1 + S} \text{ (if } b_1 = 0) \\
Q_2 = \frac{T_2}{T_2 + S} \text{ (if } b_2 = 0) \\
Q_m = \frac{T_m}{T_m + S} \text{ (otherwise)} 
\end{cases} \]

Random \( S \) is known to \( P_0 \) only

\[ |T_i| = k \]
Transformation II: OT Extension

\[ B = [b_1, \ldots, b_m] \]

\( T \) is a \( \{0,1\}^{m \times k} \) matrix

\( T = [T^1, \ldots, T^k] \)

\( Q \) is a \( \{0,1\}^{m \times k} \) matrix

\( Q = [Q^1, \ldots, Q^k] \)

\[ x_{10}, x_{11}, x_{20}, x_{21}, x_{m0}, x_{m1} \]
Transformation II: OT Extension

\[ P_0 \quad \text{T}[1,1] + s_1 \quad S_1 \quad Q^1 \quad \text{T}^1 \quad \text{T}^1 + B \]

\[ \text{T}[1,2] + s_2 \quad S_2 \quad Q^2 \quad \text{T}^2 \quad \text{T}^2 + B \]

\[ \text{T}[1,k] + s_k \quad S_k \quad Q^k \quad \text{T}^k \quad \text{T}^k + B \]

\[ Q = \begin{cases} Q_1 = T_1 \text{ (if } b_1 = 0) / T_1 + S \text{ (otherwise)} \\ Q_2 = T_2 \text{ (if } b_2 = 0) / T_2 + S \text{ (otherwise)} \\ Q_m = T_m \text{ (if } b_m = 0) / T_m + S \text{ (otherwise)} \end{cases} \]

\[ B = [b_1, \ldots, b_m] \]

\[ \text{T} \text{ is a } \{0,1\}^{m,k} \text{ matrix} \]

\[ T = \left[ \begin{array}{c} T_1 \\ T_2 \\ \vdots \\ T_m \end{array} \right] \]
Transformation II: Putting everything together

\[ y_{10} = H(1, Q_1) + x_{10} \]
\[ y_{11} = H(1, Q_1 + S) + x_{11} \]
\[ y_{m0} = H(m, Q_m) + x_{m0} \]
\[ y_{m1} = H(1, Q_m + S) + x_{m1} \]

\[ B = [b_1, \ldots, b_m] \]

\[ T \text{ is a } \{0,1\}^{m \cdot k} \text{ matrix} \]
\[ T = \begin{bmatrix} T_1 \\ T_2 \\ \vdots \\ T_k \end{bmatrix} \]

\[ x_{1\ b_1} = H(1, T_1) + y_{1\ b_1} \]

\[ x_{m\ b_m} = H(m, T_m) + y_{m\ b_m} \]
Roadmap for Building OT Extension [IKNP03]

- **Domain Extension**
  - k OTs with k bit inputs
  - OT₁
  - OT₂
  - OTₖ

- **OT Extension**
  - m (poly(k)) > k bit inputs
  - m OTs with m > k bit inputs
  - OT₁
  - OT₂
  - OT₃
  - OTₘ

- Inputs:
  - x₁₀, x₁₁, x₂₀, x₂₁, x₃₀, x₃₁, xₘ₀, xₘ₁
  - b₁, x₁b₁, b₂, x₂b₂, b₃, x₃b₃, bₘ, xₘbₘ
Security For Receiver

$S_1$  $OT_1$  $S_2$  $OT_2$  $S_k$  $OT_k$

$T^1$  $T^1 + B$  $T^2$  $T^2 + B$  $T^k$  $T^k + B$

$x_{10} = H(1, Q_1) + x_{10}$
$y_{10} = H(1, Q_1 + S) + x_{11}$
$y_{11} = H(1, Q_1 + S) + x_{11}$
$y_m = H(m, Q_m) + x_{m0}$
$y_{m1} = H(1, Q_m + S) + x_{m1}$

$x_{m0} = H(m, Q_m) + x_{m0}$
$y_{m1} = H(1, Q_m + S) + x_{m1}$

Reduces to the sender’s security of $OT_1 \ldots OT_k$

$(y_{10}, y_{11}) \ldots \ldots (y_{m0}, y_{m1})$

$x_{m bm} = H(m, T_m) + y_{m bm}$
Security For Sender

\[ \text{[IKNP03]: Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. In CRYPTO, pages 145–161, 2003.} \]

\[ P_0 \]

\[ x_{10}, x_{11}, x_{20}, x_{21}, x_{m0}, x_{m1} \]

\[ y_{10} = H(1, Q_1) + x_{10} \]

\[ y_{11} = H(1, Q_1 + S) + x_{11} \]

\[ y_{m0} = H(m, Q_m) + x_{m0} \]

\[ y_{m1} = H(1, Q_m + S) + x_{m1} \]

\[ Q = [Q_1, \ldots, Q^k] \]

\[ Q = \begin{pmatrix} Q_1 \\ Q_2 \\ \vdots \\ Q_k \end{pmatrix} \]

\[ B = [b_1, \ldots, b_m] \]

\[ T = [T^1, \ldots, T^k] \]

\[ T \]

\[ T_1, T_2, \ldots, T_k \]

\[ S_1, S_2, \ldots, S_k \]

\[ OT_1, OT_2, \ldots, OT_k \]

\[ T^1 + B, T^2 + B, \ldots, T^k + B \]

\[ (y_{10}, y_{11}) \ldots (y_{m0}, y_{m1}) \]

\[ x_{m_1 b_1} = H(1, T_1) + y_{1 b_1} \]

\[ x_{m_b m} = H(m, T_m) + y_{m_b m} \]

\[ \text{Reduces to the receiver's security of } OT_1 \]

\[ \text{...OT}_k \]

\[ \text{Reduces to the security of } H \]
IKNP and Its Successors

Semi-honest: IKNP, ALSZ13
Active: NNOB, ALSZ15, KOS15

k: security parameter
KK13 and Its Successors

$\binom{2}{1} OT_1$

$\binom{2}{1} OT_2$

$\binom{2}{1} OT_k$

OT Extension

$\binom{n}{1} OT_1$

$\binom{n}{1} OT_2$

$\binom{n}{1} OT_3$

$\binom{n}{1} OT_{p(k)}$

$r = ?$

$x_1$

$x_2$

$\ldots$

$x_n$

$x_r$

$x_{r'} = ?$

Used in PSI, PIR etc

Semi-honest: KK13

Active: PSS17, OOS17

k: security parameter
OT Study Group

The list will be updated as and when needed.

| Basic Definitions & Reductions | Meeting 1 (18.05.15; 11am -1pm) | Leaders: Abhishek, Ajith, Priyanka |

- 1-out-of-2 OT, Rabin OT, equivalence: [Ost_LN],[Cramer_LN], [Crepeau87]
- 1-out-of-n OT, k-out-of-n OT, Reduction to 1-out-of-2 OT [Katz_LN],[Cramer_LN]
- Reducing 1-out-of-2 OT to Random OT: [WW06], [Lin09],[Katz_LN]
- Symmetricity of 1-out-of-2 OT: [WW06]

| Various Security Notions | Meeting 2 (22.05.15; 3:30 - 5:50 pm),3 (25.05.15; 3:30 - 5:50 pm),4 (27.05.15; 3:30 - 5:50 pm) | Leaders: Dheeraj, Divya, Kuljeet |

- Privacy only Security & Constructions: Hazay & Lindell
- One-sided Simulation & Constructions: Hazay & Lindell
- Full Simulation & Constructions: Hazay & Lindell

| OT from Generic Assumptions | Meeting 5 (29.05.15; 3:30 - 5:50 pm) | Leaders: Ajith, Anchita |

- OT from Enhanced TDF/ CPA-secure PKE with PK samplability (EGL): Chapter 3 of [Rothblum], [Katz_LN1],[Katz_LN2], Section 2 of [Hai08]
- OT from Homomorphic Encryption: Hazay & Lindell

| OT Extensions | Meeting 6 (09.06.15; 3:30 - 5:50 pm),7 (11.06.15; 3:30 - 5:50 pm),8 (12.06.15; 3:30 - 5:50 pm) | Leaders: Ajith, Dheeraj, Divya, Kuljeet |
Introduction

Indocrypt 2017 is the 18th International Conference on Cryptology in India. The conference will take place during 10-13 December 2017 at The Institute of Mathematical Sciences (IMSc), Chennai. Indocrypt 2017 is part of the Indocrypt series organized under the aegis of the Cryptology Research Society of India.

Important Dates

- Paper Submission Deadline: Aug 20 (12.00 GMT)
- Notification of Acceptance: Oct 5
- Final Manuscripts Due: Oct 15
- Conference: 10-13 December 2017

General chairs

C. Pandu Rangan
Indian Institute of Technology Madras, India

R. Balasubramanian
Institute of Mathematical Sciences, India

Program chairs

Arpita Patra
Indian Institute of Science, India

Nigel P. Smart
University of Bristol, UK
Thank you!
OT Extension - Recent Advances

[KK13]: From k 1-out-2 OTs to m 1-out-of-n OTs
    Most efficient in semi-honest setting
    Uses Walsh-Hadamard Code

[KOS15]: Most efficient maliciously secure IKNP

[PSS17]: Most efficient maliciously secure KK13
A public-key encryption scheme is a collection of 3 PPT algorithms \( \Pi = (\text{Gen}, \text{Enc}, \text{Dec}) \)

- **Gen**
  - Input: \( 1^k \)
  - Output: \( \text{pk}, \text{sk} \)
  - Syntax: \( (\text{pk}, \text{sk}) \leftarrow \text{Gen}(1^k) \)
  - Randomized Algo

- **Enc**
  - Input: \( \text{pk}, m \in M \)
  - Output: \( c \)
  - Syntax: \( c \leftarrow \text{Enc}_{\text{pk}}(m) \)
  - Randomized algo

- **Dec**
  - Input: \( c, \text{sk} \)
  - Output: \( m \)
  - Syntax: \( m := \text{Dec}_{\text{sk}}(c) \)
  - Deterministic (w.l.o.g)

Except with a negligible probability over \((\text{pk}, \text{sk})\) output by \(\text{Gen}(1^k)\), we require the following for every (legal) plaintext \(m\):

\[ \text{Dec}_{\text{sk}}(\text{Enc}_{\text{pk}}(m)) = m \]
**CPA Security**

Indistinguishability experiment

PPT A

I can break Π

**Game Output**

1 --- attacker won

0 --- attacker lost

Π is CPA-secure if for every PPT attacker A taking part in the above experiment, the probability that A wins the experiment is at most negligibly better than ½

\[
\Pr \left( \text{cpa PubK (k) } = 1 \right) \leq \frac{1}{2} + \text{negl}(k)
\]
A public-key encryption scheme is a collection of 5 PPT algorithms $\Pi = (\text{Gen}, \text{Enc}, \text{Dec}, \text{oGen}, \text{fGen})$

\begin{align*}
1^k &\quad \rightarrow \quad \text{oGen} \rightarrow \quad \text{pk, r} \\
\quad \quad \quad \text{Syntax: } (\text{pk}, \text{r}) &\quad \leftarrow \text{oGen}(1^k)
\end{align*}

\begin{align*}
\text{pk:} &\quad \rightarrow \quad \text{fGen} \rightarrow \quad \text{r'} \\
\quad \quad \quad \text{Syntax: } \text{r'} &\quad \leftarrow \text{fGen}(\text{pk})
\end{align*}

$(\text{pk}, \text{r'})$ and $(\text{pk}, \text{r})$ look indistinguishable
**Key Samplability**

Indistinguishability experiment

PPT A

I can break $\Pi$

1 --- attacker won

$\Pi$ is key-samplable if for every PPT attacker $A$ taking part in the above experiment, the probability that $A$ wins the experiment is at most negligibly better than $\frac{1}{2}$

$$\Pr\left(\left\{\begin{array}{l}
ksamp \\
PubK (k) \\
A, \Pi
\end{array}\right\} = 1\right) \leq \frac{1}{2} + \text{negl}(n)$$
1-out-of-2 Oblivious Transfer

\[ S \quad m_0 \quad m_1 \]

- \[ b = ? \]
- \[ m_{1-b} = ? \]

\[ c_0 \leftarrow \text{Enc}_{pk_0}(m_0) \]
\[ c_1 \leftarrow \text{Enc}_{pk_1}(m_1) \]

\[ (c_0, c_1) \]

- OTs are **intrinsically expensive** - usually based on public key primitives
- AES Circuit: Millions of AND gates
ElGamal PKE

Gen($1^k$)
(G, o, q, g)
h = $g^x$. For random x
pk = (G, o, q, g, h), sk = x

Enc$_{pk}$(m)
c$_1$ = $g^y$ for random y
c$_2$ = $h^y$. m
c = (c$_1$, c$_2$)

Dec$_{sk}$(c)
c$_2$ / (c$_1$)$^x$ = c$_2$ . [(c$_1$)$^x$]$^{-1}$
Transformation II: OT Extension

Every time query an input: same output
New input: output is completely random in the range
Every RO is Correlation-Robust (HR) Hash function

**Random Oracle**

\[ B = [b_1, \ldots, b_m] \]

\[ T = [T_1, T_2, \ldots, T_k] \]

\[ Q = [Q_1 = T_1 \text{ (if } b_1 = 0) / T_1 + S \text{ (otherwise)} \]
\[ Q_2 = T_2 \text{ (if } b_2 = 0) / T_2 + S \text{ (otherwise)} \]
\[ Q_m = T_m \text{ (if } b_m = 0) / T_m + S \text{ (otherwise)} \]

\[ r_{10} \]
\[ r_{11} \]
\[ r_{20} \]
\[ r_{21} \]
\[ r_{m0} \]
\[ r_{m1} \]

\[ y_{10} = H(1, Q_1) + r_{10} \]
\[ y_{11} = H(1, Q_1 + S) + r_{11} \]

\[ y_{m0} = H(m, Q_m) + r_{m0} \]
\[ y_{m1} = H(m, Q_m + S) + r_{m1} \]

\[ (y_{10}, y_{11}) \ldots \ldots (y_{m0}, y_{m1}) \]

Random Function \( H: [m] \times \{0,1\}^k \rightarrow \{0,1\}^l \)
A little diversion to RO Model

>> Love and hate relationship with this model

>> Many protocols have proof in RO model which otherwise does not have any proof.
   >> Real protocol: RO replaced with hash functions
   >> Proof is for any good?: Existence of such a proof implies the real protocol go wrong only when hash function does not simulate RO. Some proof better than no proof

>> Examples: RSA-OEAP (practically in use). CCA-secure extension of RSA

>> Finding proof under relatively realistic assumption (e.g. CR) than RO has been very challenging and considered to be great achievement!!

Random Function $H: [m] \times \{0,1\}^k \rightarrow \{0,1\}^l$