Fast Actively Secure OT Extension for Short Secrets

Ajith Suresh
IISc, Bangalore, India
Date: 28 February 2017
(Joint work with Arpita Patra and Pratik Sarkar (IISc))
Outline of this presentation

- Oblivious Transfer (OT)
- OT Extension
- The protocol of KK13
- Our Actively Secure OT Extension Protocol
Oblivious Transfer (OT)

✓ Bob does not know $\sigma$

✓ Alice does not know $x_{1-\sigma}$

1 out of 2 OT:

$x_0$ → 1-out-of-2 OT → $\sigma$

$x_1$ → 1-out-of-2 OT → $x_{\sigma}$

σ = 0 or 1

✓ 1 out of n OT: The sender has n messages instead of two (Brassard et. al. [87])

OT is complete for MPC (Kilian [88])
OT Extension [Beaver 96]

- OT **cannot** be based on symmetric-key primitives alone [IR89]
- Small no. of “base” OTs + symmetric-key operations = Large no. of OTs

\[ \text{k OTs} \rightarrow \text{poly(k) OTs} \]

- Minimizes the cost of OT in an amortized sense.
KK13 OT Extension

Sender

\[ x_{1,1}, \ldots, x_{1,n} \]
\[ x_{2,1}, \ldots, x_{2,n} \]
\[ \vdots \]
\[ x_{m,1}, \ldots, x_{m,n} \]

1-out-of-n OT

Receiver

\[ R = (r_1, \ldots, r_m) \]
\[ x_{1,r_1}, x_{2,r_2}, \ldots, x_{m,r_m} \]
KK13 OT Extension

Sender

\[ Q = \begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_m \end{pmatrix} \quad S \in \{0,1\}^k \]

\[ q_i = t_i \oplus (C_{r_i} \otimes S) \]

\[ y_{i1} = x_{i1} \oplus H(i, q_i \oplus (C_1 \otimes S)) \]

\[ y_{ir} = x_{ir} \oplus H(i, q_i \oplus (C_r \otimes S)) \]

\[ y_{in} = x_{in} \oplus H(i, q_i \oplus (C_n \otimes S)) \]

\[ y_{i,r, \ldots, i,n} \rightarrow z_i = y_{i,r_i} \oplus H(i, t_i) \]

Receiver

\[ T = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_m \end{pmatrix} \quad m \times k \]

\[ D = \begin{pmatrix} c_{r_1} \\ c_{r_2} \\ \vdots \\ c_{r_m} \end{pmatrix} \quad m \times k \]

Matrix A

\[ a_i : i^{th} \text{ row} \]

\[ a_j : j^{th} \text{ column} \]

Mask

H - Random Oracle

\[ R = (r_1, \ldots, r_m) \]

\[ C_i : i^{th} \text{ WH Codeword} \]
Malicious Attack in KK13

✓ Adversary sets the D matrix as follows:

\[
\begin{bmatrix}
\overline{c}_{11} & c_{12} & c_{13} & \ldots & \ldots & \ldots & c_{1k} \\
c_{21} & \overline{c}_{22} & c_{23} & \ldots & \ldots & \ldots & c_{2k} \\
\vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
c_{j1} & c_{j2} & c_{j3} & \ldots & \overline{c}_{jj} & \ldots & c_{jk} \\
\vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
c_{m1} & c_{m2} & c_{m3} & \ldots & \ldots & \ldots & c_{mk}
\end{bmatrix}
\]

\[\rightarrow \quad \mathbf{c}_1 \text{ with first bit flipped}\]

✓ The 1st mask in the 1st OT will be of the form:

\[
H(1, q_i \oplus (C_1 \odot S)) = H(1, t_i \oplus (D_1 \oplus C_1) \odot S) = H(1, t_i \oplus [1, 0, \ldots, 0] \odot S) = H(1, t_i \oplus [s_1, 0, \ldots, 0])
\]

✓ Given prior knowledge on \(x_{1,1}\), adversary can find \(s_1\) with two queries to \(H\)
Formulating the problem

✓ 1\textsuperscript{st} mask in the 1\textsuperscript{st} 1-out-of-n OT:

\[ H(1, q_i \oplus (C_1 \otimes S)) = H(1, t_i \oplus ((D_{r_j} \oplus C_j) \otimes S)) \]

Hamming weight ≥ k/2
(Walsh - Hadamard Codes)

Requirement: Ensure that rows of D matrix are codewords

\[ q_i = t_i \oplus (C_{r_j} \otimes S) \]
Our Actively Secure OT Extension Protocol

Base OTs

Added Phase

Consistency Checks

Sending Masked Inputs

Communication Overhead $O(\mu \cdot \log(k))$
Comparison with KK13

- Communication Complexity: 0.028% overhead
- Runtime: 3% - 6% overhead (in both LAN and WAN)
THANK YOU

Questions ??
References


5. V. Kolesnikov and R. Kumaresan. *Improved OT Extension for Transferring Short Secrets.* In Advances in Cryptology-CRYPTO 2013 (pp. 54-70). Springer Berlin Heidelberg
