# Fast Actively Secure OT Extension for Short Secrets

Arpita Patra, Pratik Sarkar and Ajith Suresh
Department of Computer Science & Automation, Indian Institute of Science

## Introduction

**Oblivious Transfer (OT):** OT is a protocol between two parties: a sender and a receiver, where the sender holds a pair of strings and the receiver holds a selection bit. At the end of the protocol,

- The receiver should learn just the selected string.
- The sender should not gain any new information.

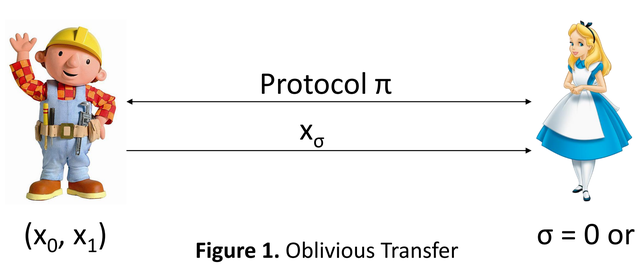


**Figure 1.** Oblivious Transfer

**1-out-of-n OT:** Sender has n messages instead of two and the receiver has a choice string instead of a bit.

**OT Extension :** A primitive that can generate a large number of OTs using a small number of OTs and relying on some extra cheap operations.

- Motivation: computing a large number of OTs is expensive since OTs cannot be based on symmetric key primitives alone.
- It is possible to obtain *poly(n)* OTs from *n* OT calls and using one-way functions (Beaver (STOC 1996) [2])
- It is impossible to extend OTs information theoretically (Beaver (STOC 1996) [2])
- Ishai et al. [3] showed how to practically extend OTs in the random oracle model assuming passive adversary.

## Our Protocol

| Sender | | Receiver |
|---|---|---|
| $x_{1,0}, \dots, x_{1,n}$ ..... $x_{m,0}, \dots, x_{m,n}$ | Inputs | $R = (r_1, \dots, r_m)$ $1 \le r_i \le n$ |
| $Q = \begin{pmatrix} \mathbf{q}_1 \\ \mathbf{q}_2 \\ \dots \\ \mathbf{q}_m \end{pmatrix}_{m \times k}$ $S \in \{0,1\}^k$ | Phase 1 – Base OTs: $s_i$, $q^i$ ← Base OT ← $t^i$, $t^i \oplus d^i$; $\mathbf{q}_i = \mathbf{t}_i \oplus (\mathbf{C}_{r_i} \circledcirc S)$ | $T = \begin{pmatrix} \mathbf{t}_1 \\ \mathbf{t}_2 \\ \dots \\ \mathbf{t}_m \end{pmatrix}_{m \times k}$ $D = \begin{pmatrix} \mathbf{c}_{r_1} \\ \mathbf{c}_{r_2} \\ \dots \\ \mathbf{c}_{r_m} \end{pmatrix}_{m \times k}$ |
| **Consistency Check**<br>• Sender and Receiver together generates randomness $w_1, w_2, \dots, w_m$.<br>$\mathbf{q} = \bigoplus_{i=1}^{m} w_i \cdot \mathbf{q}_i$ $q = \bigoplus_{i=1}^{k} q_i$ ← t , α → $\mathbf{t} = \bigoplus_{i=1}^{m} w_i \cdot \mathbf{t}_i$ $\mathbf{d} = \bigoplus_{i=1}^{m} w_i \cdot \mathbf{d}_i$<br>$\mathbf{p} = S \circledcirc \mathbf{c}_\alpha$ $p = \bigoplus_{i=1}^{k} \mathbf{p}_i$ $t = \bigoplus_{i=1}^{k} t_i$ $\mathbf{d} = \mathbf{c}_\alpha$<br>**Check:** $q \stackrel{?}{=} t \oplus p$ | | |
| Phase 2 – Sending Masked Inputs<br>$y_{i,1} = x_{i,1} \oplus H(i, \mathbf{q}_i \oplus (\mathbf{C}_1 \circledcirc S))$ .....<br>$y_{i,r} = x_{i,r} \oplus H(i, \mathbf{q}_i \oplus (\mathbf{C}_r \circledcirc S))$ → $y_{i,1}, \dots, y_{i,m}$ → $z_i = y_{i,r_i} \oplus H(i, \mathbf{t}_i)$<br>.....<br>$y_{i,m} = x_{i,m} \oplus H(i, \mathbf{q}_i \oplus (\mathbf{C}_m \circledcirc S))$ | | |
| **Notations :** H - Random Oracle $c_i$ - $i^{th}$ Walsh Hadamard Code Matrix A : $a_i$ - $i^{th}$ row $a^j$ - $j^{th}$ column | | |

**Algorithm 1.** Our Actively Secure Protocol

**Algorithm 1** describes our protocol for actively secure OT extension based on the passive KK13 [4] protocol.

- The protocol of KK13 [4] already provides security against a malicious Sender.
- For malicious Receiver, we added a consistency check.
- Consistency check ensures that Receiver inputs consistent values.

Below we compare our work with the existing protocols of KK13 [4], IKNP [3], ALSZ15 [1] and NNOB [5] in terms of communication and runtime in LAN and WAN settings.

## Results

| | KK13 | | Our Protocol | |
|---|---|---|---|---|
| Run Time (In seconds) | LAN | WAN | LAN | WAN |
| | 21.68 | 115.34 | 22.50 | 121.94 |
| Communication (In Bytes) | 47690 | | 47700 | |

**Table 1.** Comparison of our protocol (PSS) with KK13 ($1.25 \times 10^6$).

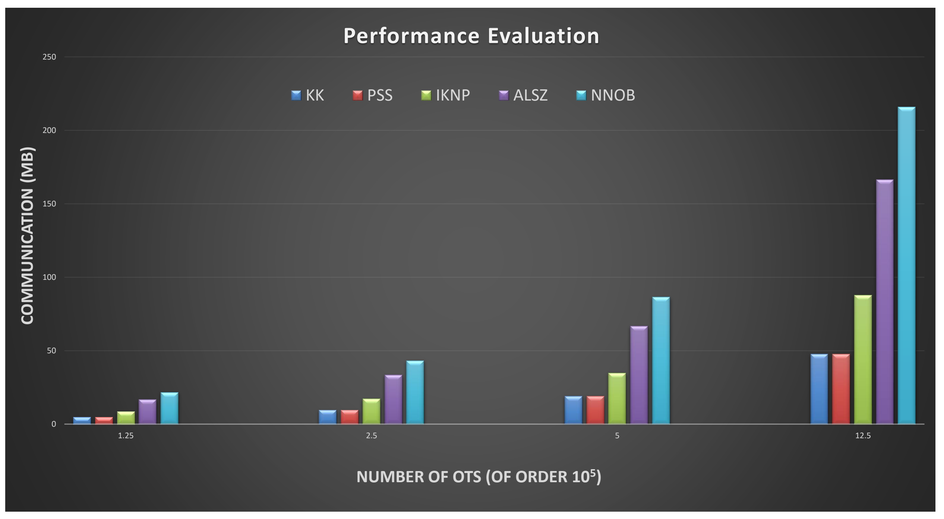


**Chart 1.** Performance Evaluation of OT Extension protocols.

## Discussion and Conclusion

The protocol of KK13 [4] provides a $O(log(k))$ factor improvement over IKNP [3] in both communication and computation for bit inputs. Upon comparing our actively secure protocol with that of KK13 [4] (**Table 1**),

- 4% computation overhead to KK13[4] in the LAN settings, and achieves active security
- Adds an overhead of only 0.028% over KK13 in terms of communication.

For the results in the local setting,

- Our protocol outperforms the ALSZ15 [1] protocol for all OTs tested on and scales better with increasing number of OTs (**Chart 1**).
- ALSZ15 [1] has an overhead of around 220% in comparison with our protocol.
- We outperforms the passive IKNP [3] protocol itself, reducing the overall communication by 62%.

To summarize,

- We present a fast OT extension protocol for small secrets in active setting.
- Our protocol outperforms all the known actively secure OT extensions (1-out-of-*n* OTs).
- Asymptotically, our protocol adds a communication overhead of $O(\mu.log(k))$ bits over KK13 protocol irrespective of the number of extended OTs, where $k$ and $\mu$ refer to computational and statistical security parameter respectively.
- Concretely, our protocol adds only 0.011-0.028% communication overhead and 4-6% runtime overhead both in LAN and WAN over KK13 extension.

## Contact

Ajith Suresh
Department of Computer Science & Automation
Indian Institute of Science
Email: ajith.s@csa.iisc.ernet.in
Phone: 08762049224

## References

1. [ALSZ15] Gilad Asharov, Yehuda Lindell, Thomas Schneider, and Michael Zohner. *More efficient oblivious transfer extensions with security for malicious adversaries*. In Elisabeth Oswald and Marc Fischlin, editors, EUROCRYPT 2015, Part I, volume 9056 of LNCS, pages 673-701, 2015. Springer, Berlin, Germany.
2. [Bea96] Donald Beaver. *Correlated pseudo randomness and the complexity of private computations*. In STOC, pages 479-488, 1996.
3. [IKNP03] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. *Extending oblivious transfers efficiently*. In Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, pages 145–161, 2003.
4. [KK13] Vladimir Kolesnikov and Ranjit Kumaresan. *Improved OT extension for transferring short secrets*. In Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II, pages 54–70, 2013.
5. [NNOB12] Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, and Sai Sheshank Burra. *A new approach to practical active-secure two-party computation*. In Reihaneh Safavi-Naini and Ran Canetti, editors, CRYPTO 2012, volume 7417 of LNCS, pages 681-700, Santa Barbara, CA, USA