Fast Actively Secure OT Extension for Short Secrets

Ajith Suresh

IISc, Bangalore, India

Date : 28 February 2017

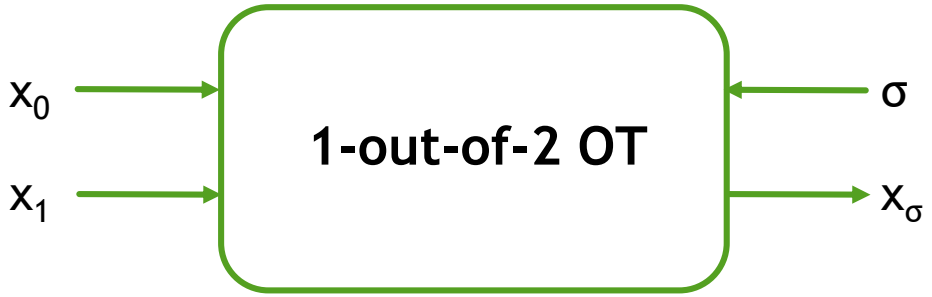
(Joint work with Arpita Patra and Pratik Sarkar (IISc))

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 σ
- ✓ Alice does not know $x_{1-\sigma}$



(x_0, x_1)

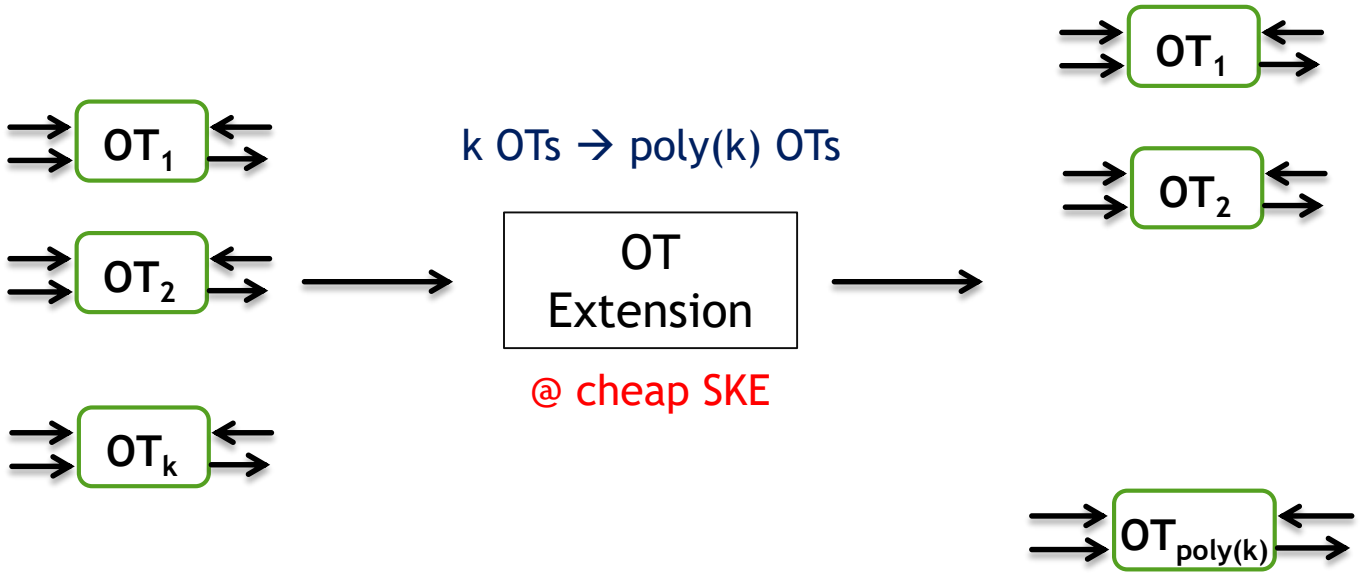
σ = 0 or 1

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

OT is complete for MPC (Kilian [88])

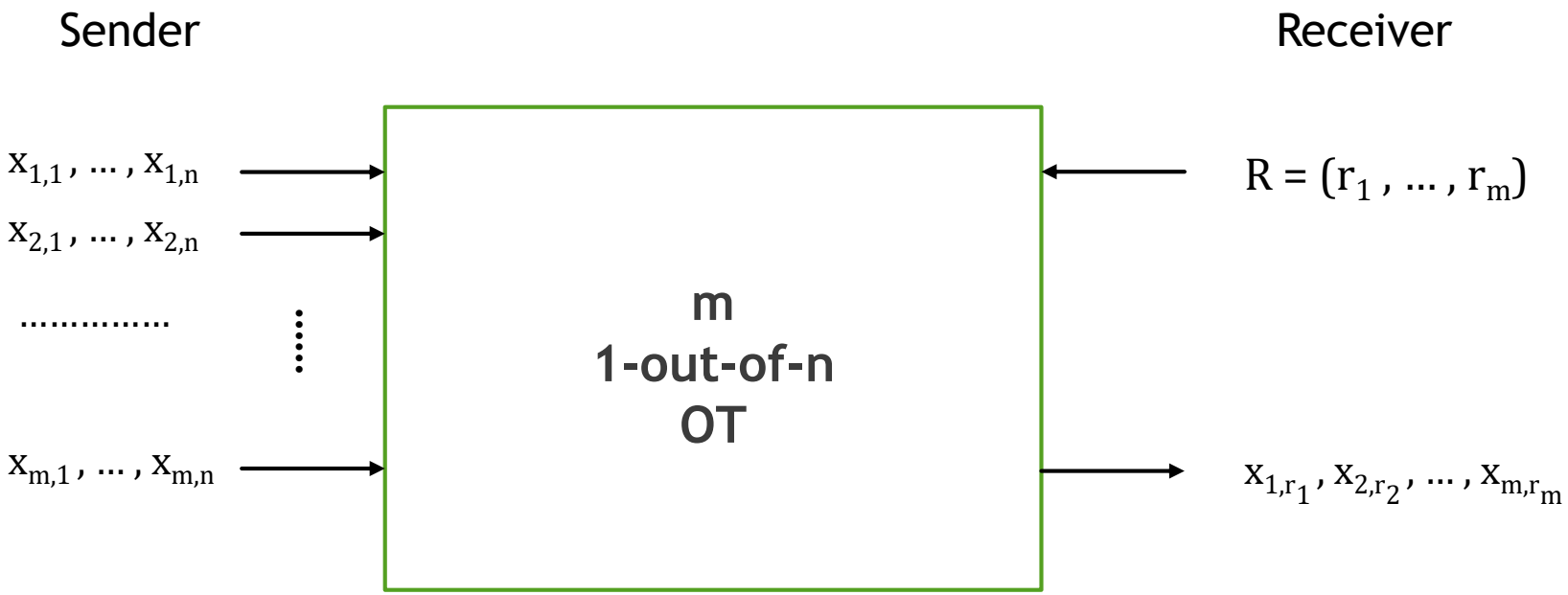
OT Extension [Beaver 96]

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

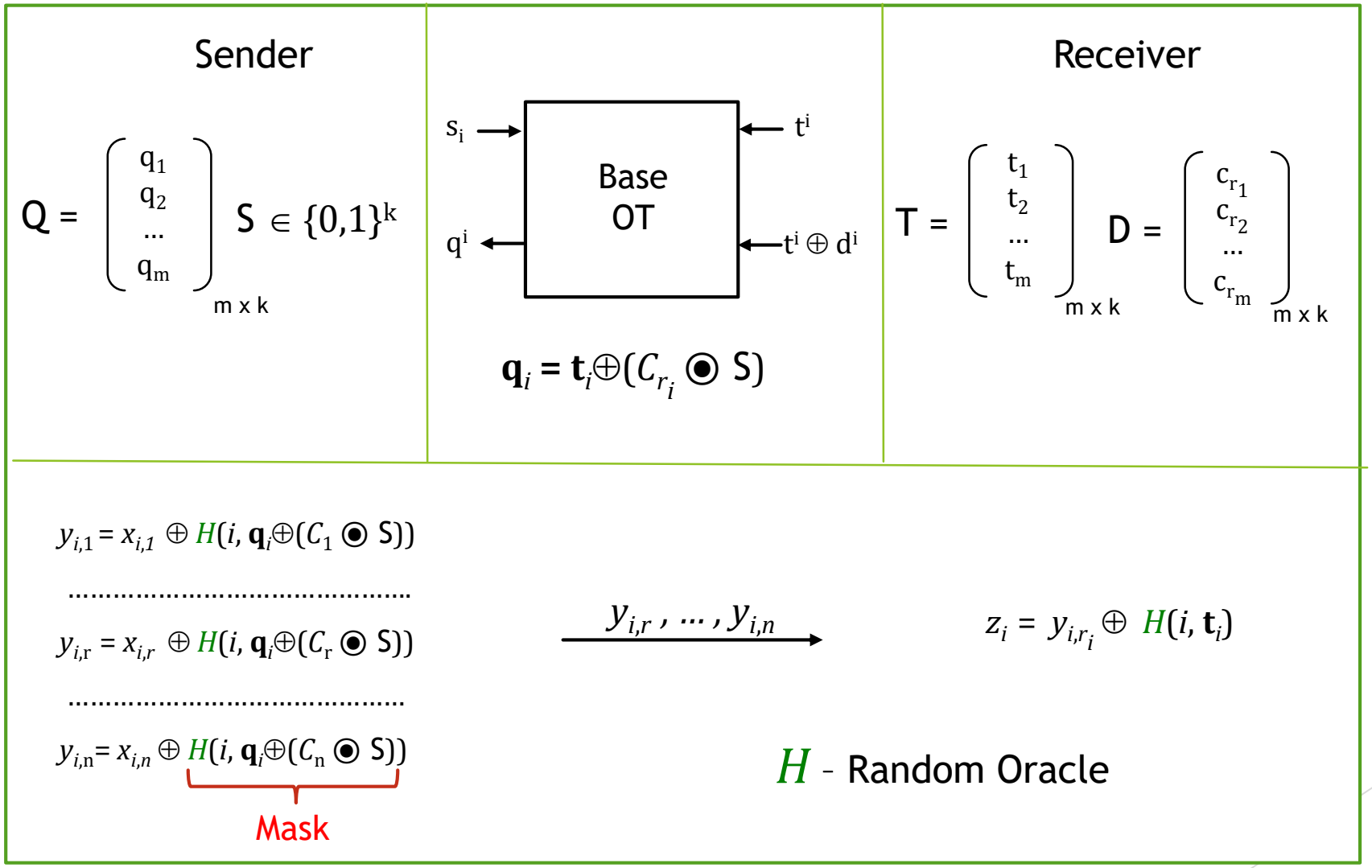


- ✓ Minimizes the cost of OT in an amortized sense.

KK13 OT Extension



KK13 OT Extension



$R = (r_1, \dots, r_m)$

C_i : i^{th} WH Codeword

Matrix **A**

a_i : i^{th} row

a^j : j^{th} column

Malicious Attack in KK13

- ✓ Adversary sets the D matrix as follows :

$$D = \begin{bmatrix} \bar{\mathbf{c}}_{11} & \mathbf{c}_{12} & \mathbf{c}_{13} & \cdots & \cdots & \cdots & \mathbf{c}_{1k} \\ \mathbf{c}_{21} & \bar{\mathbf{c}}_{22} & \mathbf{c}_{23} & \cdots & \cdots & \cdots & \mathbf{c}_{2k} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \mathbf{c}_{j1} & \mathbf{c}_{j2} & \mathbf{c}_{j3} & \cdots & \bar{\mathbf{c}}_{jj} & \cdots & \mathbf{c}_{jk} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \mathbf{c}_{m1} & \mathbf{c}_{m2} & \mathbf{c}_{m3} & \cdots & \cdots & \cdots & \mathbf{c}_{mk} \end{bmatrix} \rightarrow \mathbf{c}_1 \text{ with first bit flipped}$$

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

$$H(1, \mathbf{q}_1 \oplus (C_1 \odot S)) = H(1, \mathbf{t}_1 \oplus (D_1 \oplus C_1) \odot S)$$
$$= H(1, \mathbf{t}_1 \oplus ([1, 0, \ldots, 0] \odot S))$$
$$= H(1, \mathbf{t}_1 \oplus [s_1, 0, \ldots, 0])$$

- ✓ Given prior knowledge on $x_{1,1}$, adversary can find s_1 with two queries to H

$$\mathbf{q}_i = \mathbf{t}_i \oplus (C_{r_i} \odot S)$$

Formulating the problem

- 1st mask in the 1st 1-out-of-n OT :

$$H(1, \mathbf{q}_1 \oplus (C_1 \circledcirc S)) = H(1, \mathbf{t}_1 \oplus ((D_{r_1} \oplus C_1) \circledcirc S))$$

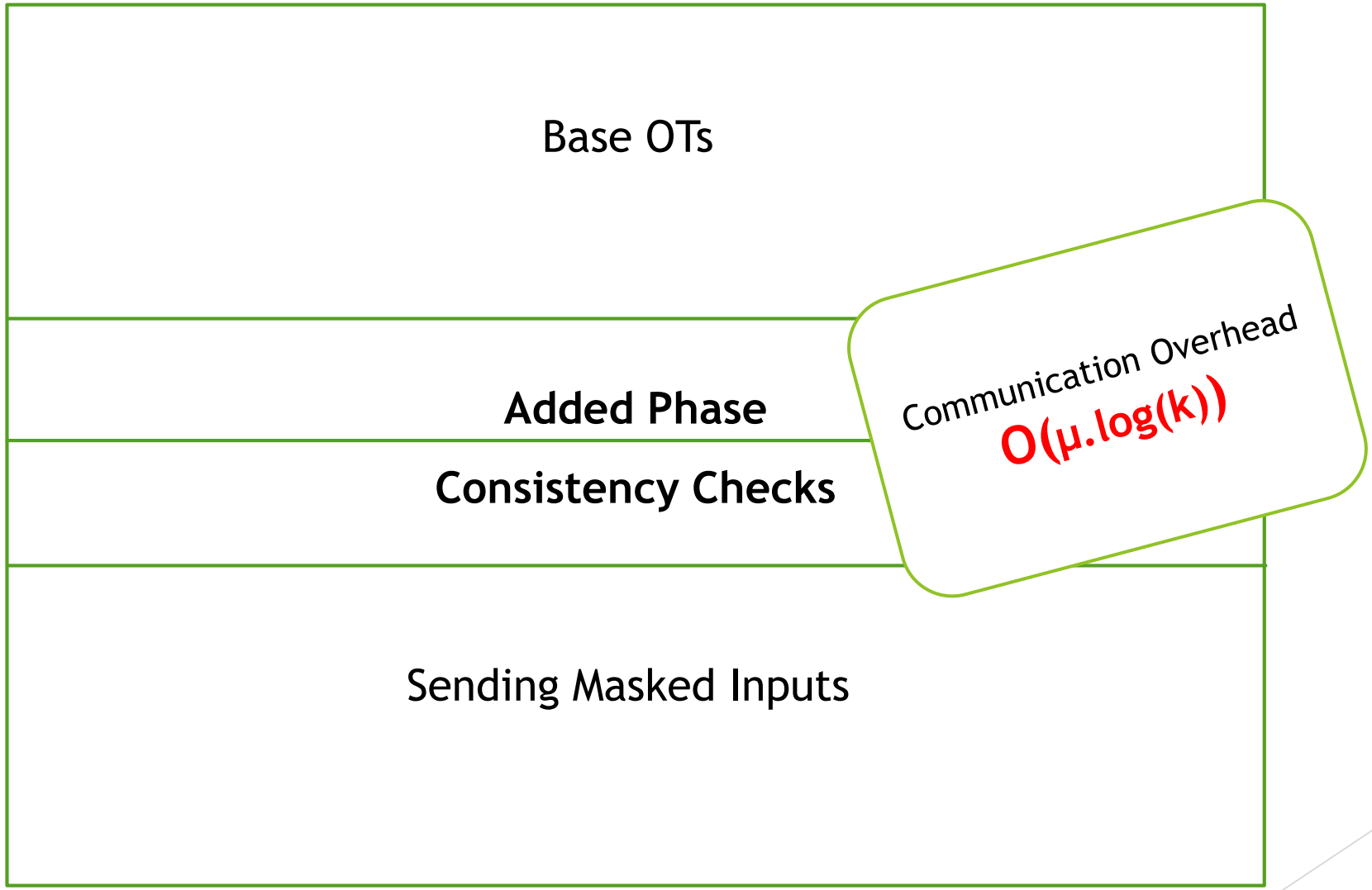
Hamming weight ≥ k/2

(Walsh - Hadamard Codes)

Requirement : Ensure that rows of **D** matrix are codewords

$$\mathbf{q}_i = \mathbf{t}_i \oplus (C_{r_i} \circledcirc S)$$

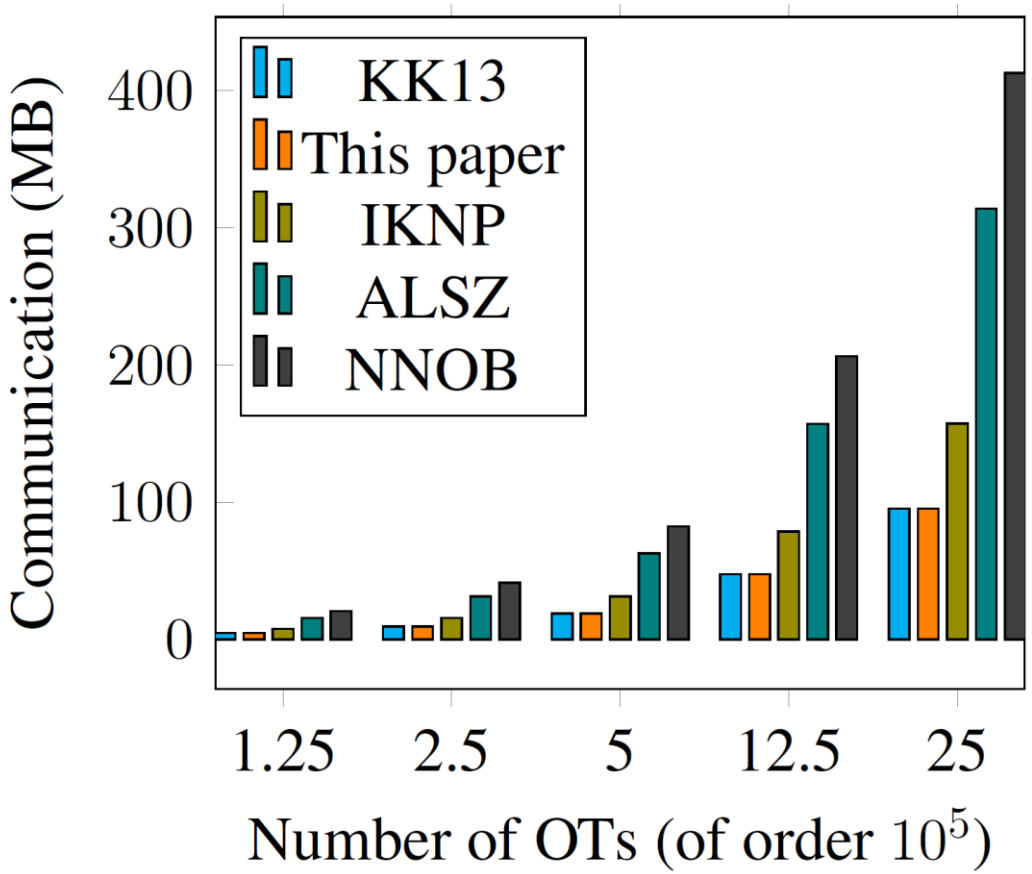
Our Actively Secure OT Extension Protocol



Implementation Results

Comparison with KK13

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



THANK YOU

Questions ??

References

1. G. Brassard, C. Crepeau, and J.M. Robert. *All-or-nothing disclosure of secrets*. In CRYPTO 86, pp. 234-238, 1987.
2. Donald Beaver. *Correlated pseudo randomness and the complexity of private computations*. In STOC, pages 479-488, 1996.
3. S. Even, O. Goldreich, and A. Lempel. *A randomized protocol for signing contracts*. C. ACM, 28:637-647, 1985.
4. Y. Ishai, J. Kilian, K. Nissim, and E. Petrank. *Extending oblivious transfers efficiently*. In Dan Boneh, editor, Advances in Cryptology - CRYPTO 2003, volume 2729 of Lecture Notes in Computer Science, pages 145-161. Springer, August 2003.Transfer (OT)
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
6. Marcel Keller, Emmanuela Orsini, and Peter Scholl. *Actively secure OT extension with optimal overhead*. In Thomas Ristenpart, Rosario Gennaro, and Matthew Robshaw, editors, CRYPTO 2015, Santa Barbara, CA, USA, August 16-20, 2015. Springer, Berlin, Germany.
7. Andrew Chi-Chi Yao. *Protocols for secure computations* (extended abstract). In FOCS, pages 160-164, 1982.