Efficient Three-Party Shuffling Using Precomputation

TECHNISCHE UNIVERSITÄT DARMSTADT

Andreas Brüggemann, Thomas Schneider, Ajith Suresh, Hossein Yalame

Technical University of Darmstadt, Germany

{brueggemann, schneider, suresh, yalame}@encrypto.cs.tu-darmstadt.de

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

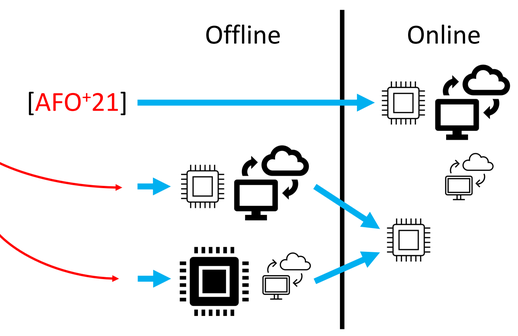
1. Secure Shuffling

- **Goal:** Shuffle private data according to a permutation that is known to no single party
- Applications: contact tracing (Graph Analysis) [AFO+21], metadata-hiding communication [EB22], private database joins [MRR20]
- Mixnets → MPC
- Recent: **RSS based 3PC shuffling [AFO+21],** Clarion: 2PC shuffling with helper [EB22]
- Existing 3PC protocols:

Protocol	Security	Messages per mult./AND	
		Offline	Online
RSS [AFL+16]	semi-honest	—	3
ASTRA [CCPS19]	semi-honest	1	2
SWIFT [PS20]	malicious	3	3

2. Our Contributions

- 3PC shuffling in the **semi-honest** setting
  - **2x online cost improvement** over [AFO+21]
  - Variant I: **Low offline computation**
  - Variant II: **Low offline communication**
- 3PC shuffling in the **malicious** setting
  - Up to **2x online cost improvement** over [AFO+21]
- Insights on **applications** to secure graph analysis



3. Problem Statement

- Input: Matrix $T \in \{0,1\}^{n \times m}$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ - & r_3 & - \\ - & r_4 & - \\ - & r_5 & - \end{pmatrix} \xrightarrow{\pi?} \begin{pmatrix} - & r_4 & - \\ - & r_3 & - \\ 0 & 1 & 1 \\ - & r_5 & - \\ 0 & 1 & 0 \end{pmatrix}$$

- Output: $\pi(T)$ for a random and unknown permutation π on the rows of T

4. General Idea

1. Encode permutation π by matrix M_π

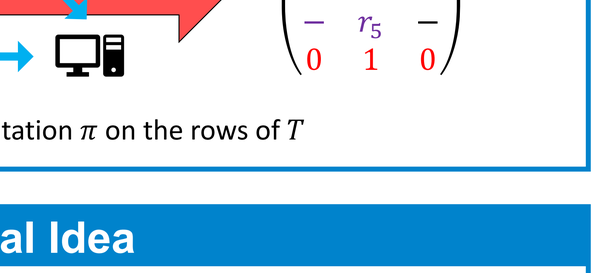
$$\pi = (1,4,5)(2,3) \quad \Rightarrow \quad M_\pi = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

2. Secure matrix multiplication

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ - & r_3 & - \\ - & r_4 & - \\ - & r_5 & - \end{pmatrix} = \begin{pmatrix} - & r_4 & - \\ - & r_3 & - \\ 0 & 1 & 1 \\ - & r_5 & - \\ 0 & 1 & 0 \end{pmatrix}$$

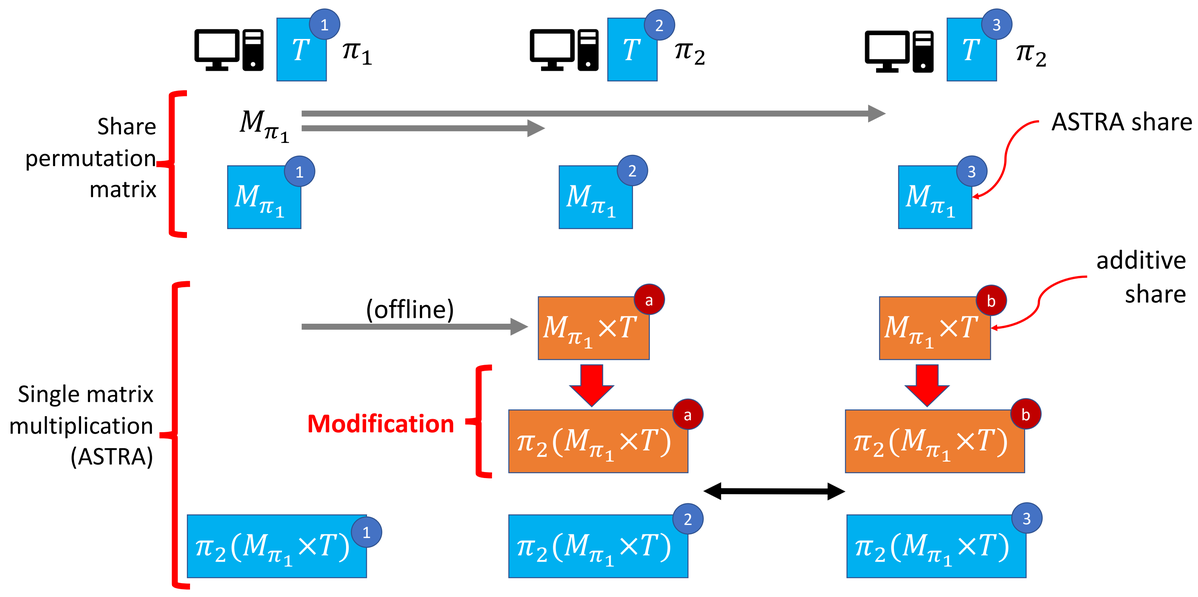
3. Parties generate and secret share multiple random permutation matrices so that no single party knows the product

$$\boldsymbol{M_{\pi_2} \times M_{\pi_1} \times T = (\pi_2 \circ \pi_1)(T)}$$



5. Optimizations

- In ASTRA [CCPS19], the second permutation comes for free



- Share sparse permutation matrix using distributed point functions (**DPF**s) [BGI16]
  - Transfer two keys per matrix row, key length is logarithmic in n

6. Performance

- Summary of permutation costs

Protocol	Communication [bits]		Online rounds
	offline	online	
Semi-honest			
[AFO+21]	—	$4nm$	2
[AFO+21] + offline	$2nm$	**2nm**	2
[EB22]	$2nm$	$3nm$	2
Our variant I	$n^2 + nm$	**2nm**	**1**
Our variant II	$\approx 2n \cdot \log_2(n/\kappa) \cdot \kappa + nm$	**2nm**	**1**
Malicious			
[AFO+21]	—	$> 24\sigma n + 6nm$	$> 9 + 3\log_2 \sigma$
Our variant III	$\approx 4n \cdot \log_2 n \cdot \kappa + 3n^2 + 3nm$	**3nm**	**1**
Our variant IV	$\approx 4n \cdot \log_2 n \cdot \kappa + 6nm$	$6nm$	2

κ/σ: comp./stat. security parameter — Comm. for matrix mult. — DPF key size

- E.g., graph analysis [AFO+21] heavily depends on applying the same permutation to k tables
- Better **amortization** in our protocol

Protocol	Communication [bits]		Online rounds
	offline	online	
[AFO+21]	—	$4knm$	$2k$
Our variant II	$\approx 2n \cdot \log_2(n/\kappa) \cdot \kappa + knm$	**2knm**	**k**

Comm. for matrix mult. — DPF key size — # shuffle runs

- **Open Question**: Efficient inverse of permutation?

References

[AFL+16] T. Araki, J. Furukawa, Y. Lindell, A. Nof, and K. Ohara. High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority. In ACM CCS, 2016.

[AFO+21] T. Araki, J.Furukawa, K. Ohara, B. Pinkas, H. Rosemarin, and H. Tsuchida. Secure Graph Analysis at Scale. In ACM CCS, 2021.

[BGI16] E. Boyle, N. Gilboa, and Y. Ishai. Function Secret Sharing: Improvements and Extensions. In ACM CCS, 2016.

[CCPS19] H. Chaudhari, A. Choudhury, A. Patra, and A. Suresh. ASTRA: High-Throughput 3PC over Rings with Applications to Secure Prediction. In CCSW@CCS, 2019.

[EB22] S. Eskandarian and D. Boneh. Clarion: Anonymous Communication from Multiparty Shuffling Protocols. NDSS, 2022.

[MRR20] P. Mohassel, P. Rindal, and M. Rosulek. Fast Database Joins and PSI for Secret Shared Data. In ACM CCS, 2020

[PS20] A. Patra and A. Suresh. BLAZE: Blazing Fast Privacy-Preserving Machine Learning. In NDSS, 2020.

European Research Council Established by the European Commission

DFG Deutsche Forschungsgemeinschaft German Research Foundation

Federal Ministry of Education and Research

HESSEN Hessisches Ministerium für Wissenschaft und Kunst