Bloom Filter-Based MPSI

Weekly Progress Meeting 18 Dec 2025

Andra Alăzăroaie

Supervisor: Lilika Markatou

Daily Supervisor: Tjitske Koster

18-12-2025

Bibliography

[1] Jelle Vos, Jorrit van Assen, Tjitske Koster, Evangelia Anna Markatou, and Zekeriya Erkin. On the insecurity of bloom filter-based private set intersections. Cryptology ePrint Archive, 2024.

[2] Aslı Bay, Zekeriya Erkin, Jaap-Henk Hoepman, Simona Samardjiska, and Jelle Vos. Practical multi-party private set intersection protocols. IEEE Transactions on Information Forensics and Security, 17:1–15, 2021.

[3] Ou Ruan, Changwang Yan, Jing Zhou, and Chaohao Ai. A practical multiparty private set intersection protocol based on bloom filters for unbalanced scenarios. Applied Sciences, 13(24):13215, 2023.

[4] Ou Ruan and Chaohao Ai. An efficient multi-party private set intersection protocols based on bloom filter. In Second International Conference on Algorithms, Microchips, and Network Applications (AMNA 2023), volume 12635, pages 282–287. SPIE, 2023.

[5] Jelle Vos, MauroConti, and Zekeriya Erkin. Fast multi-party private set operations in the star topology from secure ands and ors. Cryptology ePrint Archive, 2022.

Progress

From the plan last week:

- Implement benchmarking for [4].
- Adapt the implementation to [3]?
- Ongoing study: the attack and proofs in [1].
- Revision of [2], [3], [5].

Progress

Benchmarking for [4]:

```
Benchmarking 2 parties
Format: (Mean Time ms, Std Dev ms)
Results for set size 2^4: (1132.7, 232.91),
Results for set size 2^6: (3668.8, 73.1707),
Results for set size 2^8: (15007.5, 327.245),
```

```
Benchmarking 5 parties
Format: (Mean Time ms, Std Dev ms)
Results for set size 2^4: (2368.7, 142.47),
Results for set size 2^6: (9441.6, 127.202),
Results for set size 2^8: (38087.4, 720.782),
```

Next Week

- Adapt the implementation to [3]?
- Ongoing study: the attack and proofs in [1].
- Start writing:
  - Why the attack in [1] works on my implementation
  - Parts of introduction and related work

Thank you!

18-12-2025