Bloom Filter-Based MPSI

Weekly Progress Meeting 15 Jan 2026

Andra Alăzăroaie

Supervisor: Lilika Markatou

Daily Supervisor: Tjitske Koster

15-01-2026

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, Mauro Conti, and Zekeriya Erkin. Fast multi-party private set operations in the star topology from secure ands and ors. Cryptology ePrint Archive, 2022.

[6] Vladimir Kolesnikov, Naor Matania, Benny Pinkas, Mike Rosulek, and Ni Trieu. Practical multi-party private set intersection from symmetric-key techniques.In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pages 1257–1272, 2017.

[7] Alireza Kavousi, Javad Mohajeri, and Mahmoud Salmasizadeh. Efficient scalable multi-party private set intersection using oblivious prf. In International Workshop on Security and Trust Management, pages 81–99. Springer, 2021.

Progress

From the plan last 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

Progress

- In [4], the server decrypts the combined Bloom filter and is supposed to test its own elements against it. However, they could test any element from the universe on that filter, therefore finding elements outside of the intersection.
- In [3], this is not the case. Here, we could explain why the protocol could be reduced to the idealized BF PSI, or we could show the practical attack.

Next Week

- Continue writing:
  - Why the attack in [1] works on my implementation.
  - Parts of introduction and related work.
- Get started on mitigations:
  - Read [6] and [7], learn about oblivious PRFs.

Thank you!

15-01-2026