# Bloom Filter-Based MPSI

## Weekly Progress Meeting 4 Dec 2025

Andra Alăzăroaie

Supervisor: Lilika Markatou

Daily Supervisor: Tjitske Koster

04-12-2025

# 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:

- Read [4].
- Understand Jelle's C++ code for [2]. Not all details, but for the most part.
- Understand [3]'s construction well. Not all details, but for the most part.
- Start an implementation of an existing protocol.
  - [3]'s idea is based on [2], but uses ElGamal instead of Paillier. I am thinking it would be a good candidate for a better baseline. Went for [4] since it was easier, and it can be adapted to [3] later.
- Continue on going though the attack and proofs in [1]. Focused on [2], [3] and [4] instead, will go back to [1] after finishing the implementation for [4].

# Progress

- Read [2], [3], [4]. Started to implement [4] – based on ElGamal, quite similar to [3] and slightly to [2].
- I believed [4] is an improvement to [3], but it turns out it is not.
  - [3] is for the unbalanced scenario, [4] is for the balanced scenario.
  - They are from the same authors, but they don't cite each other.
  - [4] has a single citation: the one from Jelle's attack paper [1] (where I found out about it).
  - [4] does not have a proof, but [3] does.
  - [4] uses only ElGamal, [3] also uses Shamir.
- Also investigated the 4$^{th}$ implementation candidate from my proposal: [5].
  - Did not read it yet, but I looked through its Rust code a bit (also Jelle's code).
  - They propose multiple protocols, also for union, not only intersection.
  - Since the code is already available, [3] and [4] are more valuable to implement.

# Progress

Description of the protocol of [4]:

- Clients create and encrypt their BFs using ElGamal (for the “0” bins, they encrypt a random group element)
- Server combines them (multiplies them), obtains the combined encrypted BF
- Clients compute decryption shares using the combined encrypted BF and their secret keys
- Server combines them (multiplies them), obtains the combined BF
- Server checks its own elements against the combined BF and thus computes the intersection

# Progress

The code for [4]:

- I used the same BF code as the one from last week.
- Implemented ElGamal as described in the prerequisites.
- Implemented the protocol step-by-step, but left out some steps for now.
- Used the libraries that the paper uses (they don’t provide the implementation though) - Jelle also uses them in [2].
- Need to finish decryption share computation
- Need to handle details, left TODOs (key gen, prime number generation etc)
- Need to test and benchmark

# Challenges

- Understanding correctness of the protocols
- Reading proofs
- Working with mathematics in code

# Next Week

- Continue working on the code for [4].
  - When I get to benchmarking, I want to also research better ways of measuring time in C++ and of calculating communication costs (take inspiration from the APSI paper).
- Read [5] and inspect its implementation.
- Ongoing study: the attack and proofs in [1].

# Thank you!

04-12-2025