Many-to-One Private Set Intersection

We first define a new security problem, named mPSI (many-to-one private set interaction), which can find applications in many scenarios where the host of a big database may be queried by a large number of clients who have small-size queries and want to protect both the intentions and results of their queries. We also propose a new scheme to solve the $m$PSI problem. The scheme extends the state-of-the-art oblivious transfer-based one-to-one PSI schemes, but also embeds the innovative ideas of

1. leveraging the collaborations between clients to achieve high computational and communication efficiency, and
2. relying on server-aided secret encryption to hide each client’s private information from being exposed to either the server or any other client.

Extensive theoretical analysis and experiments have been conducted to evaluate the performance of the proposed scheme and compare the scheme with the state-of-the-art, and the results verify the efficiency of our proposed scheme.