In this thesis, we first define a new security problem, named many-to-one private set interaction (PSI), 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 three new schemes to address the PSI problem from different perspectives:

1. HOM-PSI, a naive solution to PSI problem, which extends the state-of-the-art oblivious transfer-based one-to-one PSI schemes;
2. P-mPSI, an improvement based on HOM-PSI to strengthen the security property based on permutation;
3. PSI, which resolves brute force attack using a different indexing function.

Our schemes also embed 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 schemes with the state-of-the-art, and the results verify the efficiency of our proposed schemes.