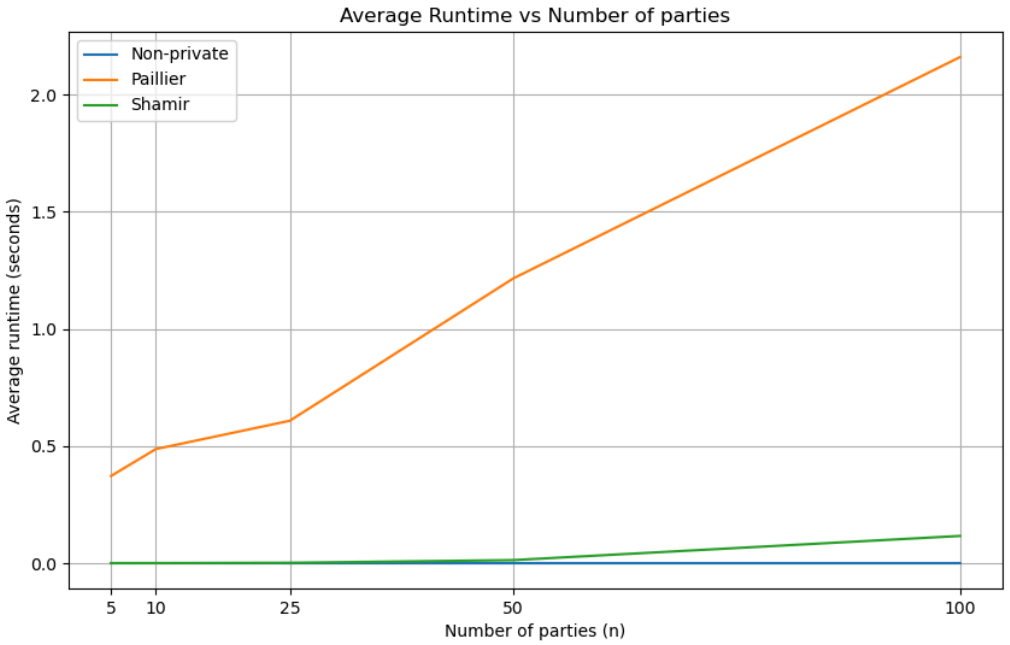
CS 323 Project 3 - Report

Hyeonseo Lee



This result illustrates the differences in runtime performance among the three methods (Non-private, Paillier, and Shamir).

The chosen values of n (5, 10, 25, 50, and 100) allow a clear comparison of how the runtime scales with the number of parties for each method. As n increases, the performance differences between the methods become more noticeable.

As shown in the graph, the runtime of the Paillier method is significantly higher than that of the other two, while the Non-private method remains almost flat near the bottom.
This indicates that as the number of parties increases, the runtime grows rapidly for the Paillier approach, whereas the Non-private and Shamir methods remain relatively efficient.

Furthermore, the results show that Shamir's Secret Sharing requires slightly more time than the Non-private method because it performs additional operations for splitting and reconstructing the secret. However, since it is a relatively lightweight cryptographic technique, it remains fairly efficient overall.

In contrast, the Paillier encryption method involves both encryption and decryption operations, which significantly increase computational cost compared to the other two methods.

Therefore, as the number of parties (n) increases, the runtime of the Paillier method grows rapidly. This demonstrates that achieving stronger privacy protection inevitably comes with

higher computational overhead — in other words, the stronger the privacy you aim to achieve, the longer you have to wait for the computation to complete.