

The results collected from running different SMPC methods, to calculate the average of randomly selected numbers, provided very comprehensive information about computational efficiency, scalability, and accuracy.

For the no-privacy setting, the results yielded low runtime across all values for n (number of randomly generated integers). This indicates that in a setting that doesn't require privacy this method is highly efficient, with precise accuracy. But we can also learn that efficiency comes at the expense of privacy.

When it comes to Paillier, the runtime was at its highest, and it demonstrated a high rate of runtime increase as the value of n increased. That is from around 4s when $n=5$ it rose to 38s for $n=100$. However, Paillier resulted best accuracy similar to the no-privacy setting, so if runtime is not a problem then Paillier offers security in addition to accuracy.

Shamir method offered a middle ground between the three methods. The runtime was slightly above the no-privacy setting and Differential Privacy, but significantly less than Paillier method. This means that Shamir method offers a balance between efficiency and privacy. But, the accuracy got skewed as data increased, so Shamir might not be the best option with big datasets.

As for Differential privacy, the runtime was lower than Shamir with a more linear horizontal line. However, accuracy seems to be issue but not as much as with Shamir, because even as data increased the accuracy did not change significantly compared to previous n values. So if we have a large database and we need the most optimal solution with some privacy and relative accuracy, then Differential privacy is the best choice.

