

# Project 3: Secret Sharing

2025. 10. 8.

100 Points Possible

Attempt 3



In Progress

**NEXT UP: Submit Assignment**



의견 추가



## Unlimited Attempts Allowed

2025. 9. 26. 다음 요일로 2025. 10. 11.

### Details

The goal of this programming project is to expand your familiarity with secure multiparty computation through hands on experience. Projects should be completed individually.

Your project should compare the runtime of 2 different SMPC approaches with the non-private setting. Your code will compare the runtime required to compute the average of  $n$  different integer values (randomly generated by your code) using:

- No privacy protection.
- The additively homomorphic Paillier encryption scheme.
- Shamir's secret sharing. Assume each value is held by a different party ( $n$  total parties) and that at half of the parties are trusted (i.e.  $t = \lfloor n/2 \rfloor$ )

You should consider at least 5 different values of  $n$ . Choose your settings appropriately so that your results represent a wide variety of settings. Additionally, be careful to run your experiments in identical compute settings. This means the same machine should be used to generate all of your results **and** that this machine should not be actively conducting other work at the time which may lead to fewer compute resources being allocated to your project code.

Thinks to consider:

- Impact of set-up process for both Paillier and Shamir's secret sharing.
- Values of  $n$  which communicate the trade-offs of SMPC.
- Effectively communicating results via well formatted graphs.
- Is one run in each setting sufficient?

- Do not leave this project to the last minute! You will need to run your code many times to complete this project and therefore need to plan your time accordingly.

**Allowable Resources:** Due to the complexity of the set-up in the Paillier encryption scheme, you may use available packages such as python-paillier in Python 3 for the Paillier implementation. However, Shamir's secret sharing should be implemented by you.

**Deliverables:** Your submission should contain the following items:

1. PDF file containing:
  - A. Graphs presenting the results of your experiments.
  - B. Short ( $\leq 1$  page) discussion on the implications of your results.
2. Compressed folder containing:
  - A. Code which can reproduce your results.
  - B. A README file detailing how to run your code and reproduce your results.

#### ▽ 루브릭 보기

### Project 3

기준	등급		점
Completeness: Code <a href="#">view longer description</a>	<b>6 pts</b> <b>Full Marks</b>	<b>0 pts</b> <b>No Marks</b>	/ 6 pts
Completeness: README <a href="#">view longer description</a>	<b>6 pts</b> <b>Full Marks</b>	<b>0 pts</b> <b>No Marks</b>	/ 6 pts
Completeness: Implementation <a href="#">view longer description</a>	<b>6 pts</b> <b>Full Marks</b>	<b>0 pts</b> <b>No Marks</b>	/ 6 pts
Completeness: zip	<b>6 pts</b> <b>Full Marks</b>	<b>0 pts</b> <b>No Marks</b>	/ 6 pts

## Project 3

기준	등급		점
<a href="#">view longer</a> <a href="#">description</a>			
Code: Non-private setting <a href="#">view longer</a> <a href="#">description</a>	<b>6 pts</b> <b>Full Marks</b>	<b>0 pts</b> <b>No Marks</b>	/ 6 pts
Code: Paillier setting <a href="#">view longer</a> <a href="#">description</a>	<b>10 pts</b> <b>Full Marks</b>	<b>0 pts</b> <b>No Marks</b>	/ 10 pts
Code: Shamir setting <a href="#">view longer</a> <a href="#">description</a>	<b>15 pts</b> <b>Full Marks</b>	<b>0 pts</b> <b>No Marks</b>	/ 15 pts
Code: Reproducibility <a href="#">view longer</a> <a href="#">description</a>	<b>10 pts</b> <b>Full Marks</b>	<b>0 pts</b> <b>No Marks</b>	/ 10 pts
Code: Timing <a href="#">view longer</a> <a href="#">description</a>	<b>4 pts</b> <b>Full Marks</b>	<b>0 pts</b> <b>No Marks</b>	/ 4 pts
Write up: Details values of n	<b>6 pts</b> <b>Full Marks</b>	<b>0 pts</b> <b>No Marks</b>	/ 6 pts
Write up: Compare runtime to n <a href="#">view longer</a> <a href="#">description</a>	<b>10 pts</b> <b>Full Marks</b>	<b>0 pts</b> <b>No Marks</b>	/ 10 pts

Project 3

기준	등급		점
Write up: Discussion <a href="#">view longer description</a>	15 pts Full Marks	0 pts No Marks	/ 15 pts
			Total Points: 0

Choose a submission type

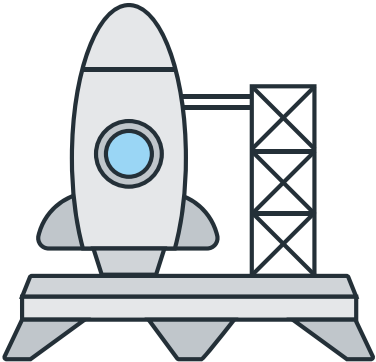
업로드



Office 365




외부 도구



Choose a file to upload

또는

 Webcam Photo