Fundamentals of Cryptography: Project List

Instructor: Wenfei Wu

December 18, 2020

Rules to Play

1. We would profile a few crypto application libararies.
2. Choose a library from Homomorphic Encryption, Multi-Party Computation, or Zero-Knowledge Proof.
3. Profile its computation capability and performance.

Submission

1. A experiment report with the following element.
   - The library you choose and the environment you configure to run the experiment.
   - What computation does it support, including operators (addition, multiplication, etc.), data type (integer, string, etc.), control flow (loop, if-else, etc.), supporting functions or not, global/local variable or not? (Hint: Just think about the programs in your programming class, can you implement them?)
   - Compare its performance with a non-crypto piece of code (e.g., written in C or Python), describe your experiments (you can design several ones).
     - What logic is executed in your experiment (e.g., addition, vector inner product)?
     - What are the parameters you controlled for the experiment (crypto v.s. non-crypto, data type, data size, etc.) ?
     - What is the performance metric (completion time, memory consumption, etc.)?
     - Visualize the result if possible.
     - Describe the experiment result.
2. Your source code.

References