CS65500: Advanced Cryptography	Instructor: Aarushi Goel

Homework 3

Due: February 27; 2025 (11:59 PM)

1 Secure Multiparty Computation

(20 points) Let Alice and Bob have inputs a and b, respectively. They want to securely send $(a+b)$ to a third-party Carol. Devise a protocol where Alice and Bob are only allowed to send **at most one message to each other** and **at most one message each to Carol**. Your protocol should satisfy all of the following security properties:

- *Security against Semi-honest Alice:* Alice should not learn b.
- *Security against Semi-honest Bob:* Bob should not learn a.
- *Security against Semi-honest Carol:* Carol should not learn a and b.

Formalize a simulation based security definition to capture the above requirements. Then formally argue that your protocol indeed satisfies this security definition, and gives the correct output to Carol.

2 Secret Sharing Schemes

1. **(20 points)** Consider a $(1,3)$-threshold secret sharing scheme described as follows:
   - $(s_1, s_2, s_3) \leftarrow \mathsf{Share}(m)$: On input a secret $m \in \mathbb{F}$, the share algorithm samples three random values $r_{1,2}, r_{3,1}, r_{2,3} \in \mathbb{F}$, such that $m = r_{1,2} + r_{3,1} + r_{2,3}$. It then assigns shares to the three parties as follows:
     - Party 1 receives $s_1 = \{r_{1,2}, r_{3,1}\}$.
     - Party 2 receives $s_2 = \{r_{1,2}, r_{2,3}\}$.
     - Party 3 receives $s_3 = \{r_{3,1}, r_{2,3}\}$.
   - $m \leftarrow \mathsf{Recon}(s_i, s_j)$: Any two parties i and j can reconstruct m as follows: parse $s_i = \{r_{i,k}, r_{j,i}\}$ and $s_j = \{r_{k,j}, r_{j,i}\}$, where $k \in [3]$ and $k \neq i \neq j$. Output $m = r_{j,i} + r_{i,k} + r_{k,j}$.

   This ensures that any two parties can reconstruct m, while an individual share provides no information about m (perfect secrecy).

   Design an algorithm $\mathsf{Conv}(i, s_i)$ that converts a given share s_i of the above scheme into a new share y_i, such that the transformed shares (y_1, y_2, y_3) form a $(1,3)$-Shamir secret sharing of m. Explain why your algorithm is correct.

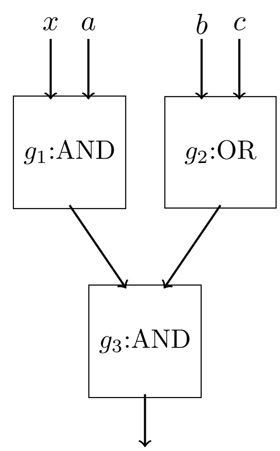
2. **(15 points)** In class, we discussed secret sharing schemes based on threshold access structures. This idea can be extended to more **general monotone access structures**, where certain subsets of parties can collectively reconstruct the secret, while other subsets gain no information about it.

   Design a secret sharing scheme over a finite field to distribute a secret m among four parties, ensuring the following conditions (and explain its correctness):

- Shares of parties 1 and 2 can be used together to reconstruct m.
- Shares of parties 2, 3 and 4 can be used together to reconstruct m.
- No individual party can learn anything about m.
- Shares of the following subsets of parties must also not leak any information about m:
  - Party 1 and 3
  - Party 2 and 3
  - Party 1 and 4
  - Party 3 and 4

3 Garbled Circuits

(15 points) Let C be a Boolean circuit as shown in the following figure.



Let (Garble, Eval) be the garbling scheme discussed in class. Recall that the $\mathsf{Garble}(\cdot)$ function, when given this Boolean circuit C as input, outputs the following:

$$(\hat{G} = \{\hat{g}_1, \hat{g}_2, \hat{g}_3\}, \hat{\mathsf{In}} = \{K_0^1, K_1^1, K_0^2, K_1^2, K_0^3, K_1^3, K_0^4, K_1^4\}) \leftarrow \mathsf{Garble}(C),$$

where $\hat{G}$ is the set of 3 garbled gates and $\hat{\mathsf{In}}$ is the set of wire keys for the 4 input wires in this circuit. In this question, we will see that the privacy of inputs in a garbled circuit does not hold if the adversary has both the keys for a wire.

Consider an adversary who knows the description of C, garbled gates $\hat{G}$ and input wire keys $\{K_0^1, K_1^1, K_a^2, K_b^3, K_c^4\}$. Note that the adversary gets both the input wire keys for the first input wire, and only one key for each of the remaining 3 input wires. Also note that the values a, b, c are not known to the adversary.

Show how this adversary can use this information to learn at least one out of a, b or c. (**Hint: Use the truth table of the gates to derive information.**)