Multi-Party Computation

Rohit Musti

CUNY - Hunter College

April 13, 2022

Motivating Examples

- How can we compute on encrypted data?
- How can Alice and Bob figure out who is wealthier without revealing their net worths?
- How can Signal learn if any of your contacts are using signal without Signal learning anything?
- How can two people check if their genome's share any characteristics without revealing any other information about their genomes?
- How could we share ML training data without revealing our underlying datasets?

Homework Example: Voting Problem

- Recall from HW 1, the challenge of computing the vote of the class
- This protocol had some notable security flaws (two actors could collaborate and discover someone else's vote) (someone could lie about their vote)
- However, it is a good example of multi-party computation as honest actors can collaborate to compute the collective vote
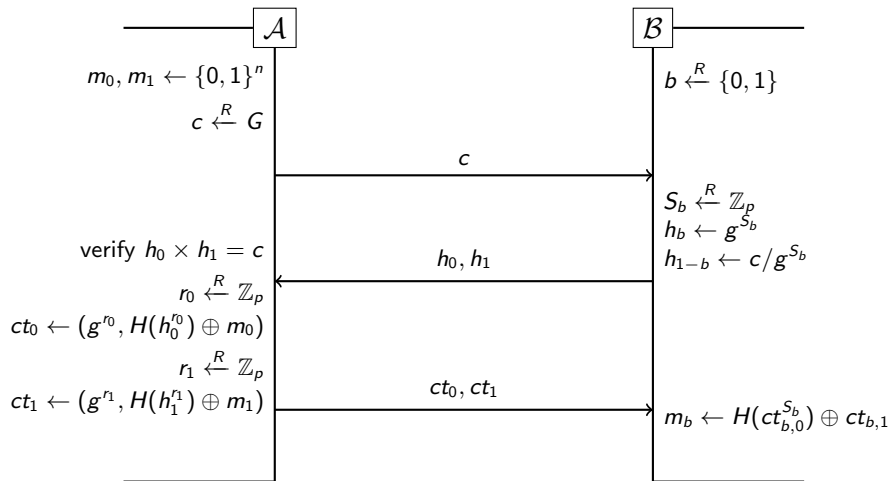
Warm Up

- Can we securely compute XOR?
- Can we securely compute OR?
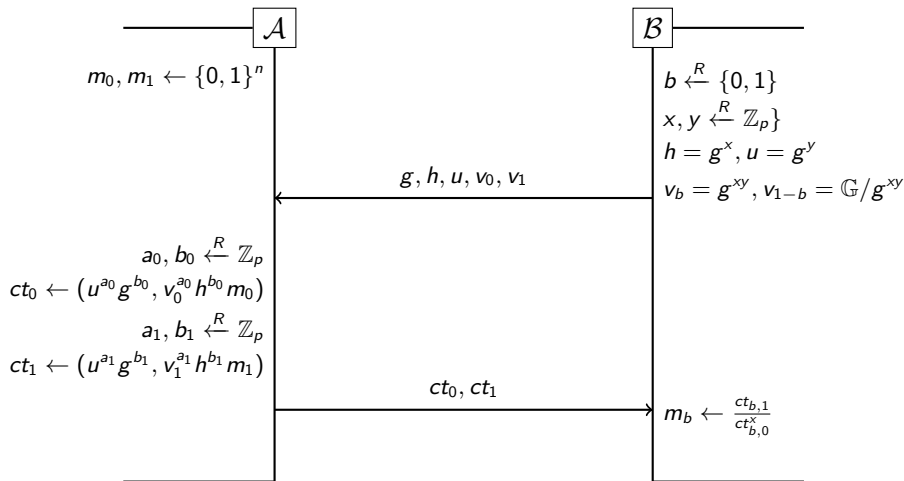- Can we securely compute AND?

2 Oblivious Transfer

Oblivious Transfer

- The most simple building block of multi-party computation
- The idea is to establish a portocol where the sender has two messages (m_0, m_1) and the receiver learns the details of one of the messages, but not the other, and the receiver doesn't know which one they learned

Oblivious Transfer: Random Oracles

$$\mathcal{A}$$ $$\mathcal{B}$$

$m_0, m_1 \leftarrow \{0,1\}^n$

$c \xleftarrow{R} G$

$b \xleftarrow{R} \{0,1\}$

$\xrightarrow{\quad c \quad}$

$S_b \xleftarrow{R} \mathbb{Z}_p$

$h_b \leftarrow g^{S_b}$

verify $h_0 \times h_1 = c$

$h_{1-b} \leftarrow c/g^{S_b}$

$\xleftarrow{\quad h_0, h_1 \quad}$

$r_0 \xleftarrow{R} \mathbb{Z}_p$

$ct_0 \leftarrow (g^{r_0}, H(h_0^{r_0}) \oplus m_0)$

$r_1 \xleftarrow{R} \mathbb{Z}_p$

$\xrightarrow{\quad ct_0, ct_1 \quad}$

$ct_1 \leftarrow (g^{r_1}, H(h_1^{r_1}) \oplus m_1)$

$m_b \leftarrow H(ct_{b,0}^{S_b}) \oplus ct_{b,1}$

Oblivious Transfer: No RO

$\mathcal{A}$

$m_0, m_1 \leftarrow \{0,1\}^n$

$\mathcal{B}$

$b \xleftarrow{R} \{0,1\}$

$x, y \xleftarrow{R} \mathbb{Z}_p\}$

$h = g^x, u = g^y$

$v_b = g^{xy}, v_{1-b} = \mathbb{G}/g^{xy}$

g, h, u, v_0, v_1

$a_0, b_0 \xleftarrow{R} \mathbb{Z}_p$

$ct_0 \leftarrow (u^{a_0} g^{b_0}, v_0^{a_0} h^{b_0} m_0)$

$a_1, b_1 \xleftarrow{R} \mathbb{Z}_p$

$ct_1 \leftarrow (u^{a_1} g^{b_1}, v_1^{a_1} h^{b_1} m_1)$

ct_0, ct_1

$m_b \leftarrow \frac{ct_{b,1}}{ct_{b,0}^x}$

3 Shamir Secret Key Sharing

Shamir Secret Sharing: Review

- Recall our discussion of Shamir Secret sharing during the public key encryption lecture
- Essentially, it allowed us to share a secret with an arbitrary number of people and allow any subset of them to come together to unlock the secret
- I got a little excited and put it there early, now we will discuss how to actually compute it!

Shamir Secret Sharing: Mechanism

$$shares = [(-3, 0), (2, 5), (-1, -4)]$$

$$f(x) = 0 \times \frac{(x - 2)(x - (-1))}{(-3 - 2)(-3 - (-1))} + 5 \times \frac{(x - (-3))(x - (-1))}{(2 - (-3))(2 - (-1))} +$$
$$- 4 \times \frac{(x - (-3))(x - 2)}{(-1 - (-3))(-1 - 2)}$$

$$f(0) = 0 \times \frac{(0 - 2)(0 - (-1))}{(-3 - 2)(-3 - (-1))} + 5 \times \frac{(0 - (-3))(0 - (-1))}{(2 - (-3))(2 - (-1))} +$$
$$- 4 \times \frac{(0 - (-3))(0 - 2)}{(-1 - (-3))(-1 - 2)}$$

$$f(0) = -3$$

4. Computing on Secret Shared Data

Computing on Secret Data

- Supposed Alice, Bob, and Charlie are friends and Charlie wants to know how many marbles Alice and Bob have!
- Alice gives two random numbers to Charlie and Bob. Bob gives two random numbers to Alice and Charlie
- Alice computes $(a_{total} - s_{ac} - s_{ab}) + s_{ba}$
- Bob computes $(b_{total} - s_{bc} - s_{ba}) + s_{ab}$
- Charlie computes $s_{ac} + s_{bc}$
- They all share their results and independently compute $(a_{total} - s_{ac} - s_{ab}) + s_{ba} + (b_{total} - s_{bc} - s_{ba}) + s_{ab} + s_{ac} + s_{bc}$