PIR – Homework

Please answer the following questions. **We don't expect rigorous formal proofs: rather, just a high-level argument from intuition.** Please submit your answers as a **PDF** to Gradescope. Collaboration is allowed and encouraged, but you must write up your own answers and acknowledge your collaborators in your submission.

Due Date: *Monday, April 20th*

1 (Extra Credit) GMW for Arithmetic Circuits

In this problem, we extend the GMW protocol to *arithmetic circuits* over the ring $\mathbb{Z}_{2^\ell}$. In particular, each wire w carries a value $v^w \in \mathbb{Z}_{2^\ell}$; the arithmetic circuit consists of ADD and MULT gates for addition and multiplication modulo 2^ℓ.

Throughout the protocol, we keep the invariant that for each wire w, the n parties hold additive secret shares for its value v^w over the ring $\mathbb{Z}_{2^\ell}$, namely, each party holds a random share $v_i^w \in \mathbb{Z}_{2^\ell}$ such that $\sum_{i\in[n]} v_i^w = v^w \mod 2^\ell$.

(1) **Inputs:** For each input wire w, say it carries an input from party P_k with input value $v^w \in \mathbb{Z}_{2^\ell}$, how does P_k generate additive secret shares of v^w and distribute them among all the parties?

(2) **ADD gates:** For each addition gate, the n parties hold additive secret shares $\{a_i\}_{i\in[n]}$ and $\{b_i\}_{i\in[n]}$ for the two input wires with values a and b, respectively. How can they generate additive secret shares $\{c_i\}_{i\in[n]}$ for the output wire with value $c = a + b \mod 2^\ell$?

(3) **MULT gates:** For each multiplication gate, the n parties hold additive secret shares $\{a_i\}_{i\in[n]}$ and $\{b_i\}_{i\in[n]}$ for the two input wires with values a and b, respectively. Now they want to generate additive secret shares $\{c_i\}_{i\in[n]}$ for the output wire with value $c = a \cdot b \mod 2^\ell$. Explain how this problem can be reduced to a **Reshare** protocol (between two parties over $\mathbb{Z}_{2^\ell}$). In the Reshare protocol, two parties hold inputs $x, y \in \mathbb{Z}_{2^\ell}$ respectively; from the protocol they learn random $r, s \in \mathbb{Z}_{2^\ell}$ respectively such that $r + s = x \cdot y \mod 2^\ell$.

(4) **Reshare:** Design such a Reshare protocol between two parties over $\mathbb{Z}_{2^\ell}$ using 1-out-of-2 OT.

Hint: Consider the bit decomposition of y.

2 Fully Homomorphic Encryption (FHE)

(1) In one sentence, what is fully homomorphic encryption?

(2) Give a potential application of FHE in practice. (Try to come up with one that was not covered in class!)

(3) Intuitively speaking, what's the main reason that all somewhat homomorphic encryption (SWHE) schemes only support a bounded number of homomorphic operations, especially homomorphic multiplications?

3 Private Information Retrieval (PIR)

(1) What are the similarities and differences between PIR and 1-out-of-n OT?

(2) We construct private information retrieval (PIR) from SWHE in this project. Let's look at the tradeoffs in choosing different values for d – the dimension of the hypercube that we use to store our data. What value should we choose to minimize the number of homomorphic multiplications (optimizing computation)? What value should we choose to minimize the size of the selection vector (optimizing communication)?