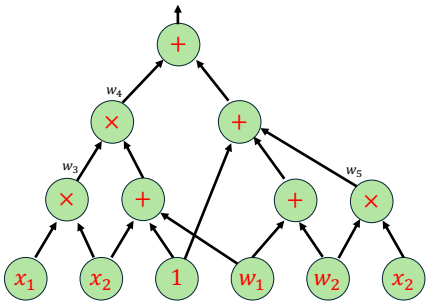
CS355: Applied Zero Knowledge Proofs **Spring 2025**

Assignment #2

Due: 11:59pm on Wed, Apr. 30, 2025, on Gradescope (each answer on a separate page)

Problem 1. (*R1CS*) Consider the following arithmetic circuit $\mathcal{C}(x_1, x_2, w_1, w_2)$ over a finite field $\mathbb{F}$:



Construct an R1CS program $A, B, C \in \mathbb{F}^{\ell \times m}$ that accepts exactly the same pairs $(x_1, x_2) \in \mathbb{F}^2$ as the circuit $\mathcal{C}$ above.
Hint: It is sufficient to use only $\ell = 3$ constraints (i.e., the matrices A, B, C have only three rows). Try to define $\bar{z} = (1, x_1, x_2, w_1, w_2, w_3, w_4, w_5) \in \mathbb{F}^8$, where w_3, w_4, w_5 are defined as the output of the multiplication gates in the figure above.

Problem 2. (*An R1CS for a range check*) Let $\mathbb{F}_p$ be a prime finite field, where $p \gg 2^\ell$. Design an R1CS program $A, B, C \in \mathbb{F}_p^{k \times m}$ that accepts exactly the set of elements $\{0, 1, \ldots, 2^\ell - 1\} \subset \mathbb{F}_p$. More precisely, your R1CS program A, B, C takes only one public input $x_1 \in \mathbb{F}_p$, and the language accepted by the program is $L(R_{A,B,C}) = \{0, 1, \ldots, 2^\ell - 1\}$. Your program should have at most $\ell + 1$ constraints.
Hint: Observe that $x \in \mathbb{F}_p$ satisfies $0 \le x < 2^\ell$ if and only if the binary representation of x has at most ℓ bits. Try to provide the bits in the binary representation of x as the witness to your R1CS program.
Discussion: Your R1CS program can be used to construct a non-interactive zero-knowledge proof that a given ElGamal ciphertext is an encryption of an integer in the interval $[0, 2^\ell)$. We saw in the lecture the tools needed to use your R1CS program to derive a Σ-protocol for this relation. This Σ-protocol can be made non-interactive using the Fiat-Shamir transformation. The proof size is $\ell + 2$ field elements. Using Bulletproofs one can give a proof of size $O(\log \ell)$ for this relation.

Problem 3. (*Collision resistance of the Pedersen hash*) Let $\mathbb{G}$ be a cyclic group of prime order q and let $g_1, \ldots, g_n \xleftarrow{R} \mathbb{G}$ be generators of $\mathbb{G}$. Define a hash function $H : \mathbb{Z}_q^n \to \mathbb{G}$ as

$$H(\alpha_1, \ldots, \alpha_n) := g_1^{\alpha_1} \cdots g_n^{\alpha_n}.$$

Our goal is to prove that if DLOG is difficult in $\mathbb{G}$ then H is collision resistant. Suppose towards a contradiction that there is an efficient algorithm $\mathcal{A}$ that takes as input $(g_1, \ldots, g_n)$, and outputs

a collision for H. That is, $\mathcal{A}(g_1, \ldots, g_n)$ outputs $\bar{\alpha}, \bar{\beta} \in \mathbb{Z}_q^n$ such that

$$g_1^{\alpha_1} \cdots g_n^{\alpha_n} = H(\bar{\alpha}) = H(\bar{\beta}) = g_1^{\beta_1} \cdots g_n^{\beta_n}.$$

Show that $\mathcal{A}$ can be used to efficiently compute discrete log in $\mathbb{G}$, which contradicts the assumption the DLOG is difficult in $\mathbb{G}$.

Hint: Your goal is to construct an efficient algorithm $\mathcal{B}$ that takes as input generators $u, v \in \mathbb{G}$ and outputs $\delta \in \mathbb{Z}_q$ such that $v = u^\delta$. Your algorithm $\mathcal{B}(u, v)$ could operate as follows: (i) sample random $\rho_1, \ldots, \rho_n \xleftarrow{R} \mathbb{Z}_q$ and $\nu_1, \ldots, \nu_n \xleftarrow{R} \mathbb{Z}_q$, (ii) set $g_i := u^{\rho_i} v^{\nu_i}$ for $i = 1, \ldots, n$, (iii) run $\mathcal{A}(g_1, \ldots, g_n)$, and (iv) use the resulting collision $\bar{\alpha}, \bar{\beta} \in \mathbb{Z}_q^n$ to compute the required $\delta \in \mathbb{Z}_q$. Make sure to explain why your $\mathcal{B}$ will output δ with high probability over the choice of $\bar{\rho}, \bar{\nu}$.