СПЕЦИЈАЛНИ КУРС - *ZERO KNOWLEDGE PROOF*

јун 1

1. (5 поена) Шта представља Merkle root и како се користи у верификацији припадности елемента скупу?

2. (5 поена) Објаснити како се генерише подешавање засновано на поверењу (trusted setup) код PLONK-а?

3. (5 поена) Нека је E елиптичка крива над коначним пољем K. Нека су $\mathbb{G}_1$ и $\mathbb{G}_2$ адитивне подгрупе тачака реда p, са криве E (p је прост број). Нека су њихови генератори редом g_1 и g_2. Дато је упаривање (pairing) $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Нека су f и h полиноми, док су $s, z \in K$ и нека важи $f(x) - f(z) = h(x)(x - z), \forall x \in K$. Подразумева се да је $com_f = f(s) * g_1$. Изменити једну страну следеће једнакости тако да постане тачна:

$$e(h(z) * g_1, (s - z) * g_2) = e(com_f - f(z) * g_1, g_2).$$

4. (7.5 поена) Милица и Јован играју следећу игру: Милица бира природан број између 1 и 500. Јован покушава да погоди да ли је тај број паран или непаран. Након сваког покушаја, Милица треба да пошаље ЗК доказ чији излаз даје 1 ако је погодио парност, а 0 ако није. Написати Circom коло које омогућава Милици да докаже исправност свог одговора.

5. (7.5 поена) Написати Circom код за коло којим се проверава да ли особа за дату јавну вредност Посејдон хеша зна број чијим се хеширањем добија та вредност.