СПЕЦИЈАЛНИ КУРС - ZERO KNOWLEDGE PROOF

јун 1

1. (5 поена) Навести две практичне примене потпуно хомоморфне енкрипције (FHE) и за сваку објаснити који се проблем решава и како FHE доприноси решењу.

2. (5 поена) Које су предности MACI протокола у односу на Semaphore протокол?

3. (5 поена) Објаснити како се генерише Trusted setup у PLONK-у.

4. (5 поена) Шта представља корен (root) у Меркле стаблу? Објаснити како се проверава да ли дати елемент припада скупу представљеном тим кореном.

5. (5 поена) Која три својства ZK доказ мора да испуњава? Дефинисати свако од њих.

6. (5 поена) Посматрајмо следећи Circom код, где сигнал $s$ узима вредност 0 или 1:

```
template Example() {
signal input s;
signal input x;
signal input y;
signal output z;

if (s == 1) {
    z <== x;
} else {
    z <== y;
}
}
```

   Објаснити зашто овај код не може да се успешно компајлира у Circom-у и објаснити како би иста логика могла исправно да се моделује аритметичким ограничењима.

7. (5 поена) Написати псеудокод (или Circom код) за ЗК коло којим се проверава да ли особа зна preimage (тајну вредност чији је хеш једнак датој јавној вредности) за дати јавни Посејдон хеш. Обавезно навести који улази су приватни, а који јавни.