Spisak ispitnih pitanja za Specijalni kurs deo Zero Knowledge proofs

Na ispitu biće kratka pitanja iz ovih tema. Nećete pisati sve što znate na ove teme već odgovoriti na 3 konkretna pitanja koja ćete dobiti. Imaćete i dva zadatka na ispitu.

1. Zero Knowledge proofs i illustrativni primeri
2. Primene ZKP-a
3. Merkle tree i ZK dokaz pripadnosti skupu
4. Completeness, soundness and ZK
5. Cyclic group (Zp*,·)
6. Problem diskretnog logaritma
7. Eliptičke krive nad konačnim poljem
8. Add and Double algoritam
9. Multi-Scalar-Multiplication (bucket metod)
10. Problem diskretnog logaritma nad eliptičkim krivama
11. Uparivanje na eliptičkim krivama
12. STARKs & SNARKs
13. Aritmetizacija i sistem ograničenja (system constraints) kod ZKP-a
14. Komitmenti pomoću polinoma (Polynomial Commitments) kod SNARK-ova
15. Trusted setups kod Groth16 i PLONK-a
16. Non-Interactive Preprocessing argument system
17. KZG
18. PLONK
19. Protokol Semafor