

СПЕЦИЈАЛНИ КУРС - *ZERO KNOWLEDGE PROOF*

јануар 1

1. (5 поена) Која три својства ЗК доказ мора да испуњава? Дефинисати свако од њих.
2. (5 поена) Навести две примене ЗК доказа.
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) $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. 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 има тајну шифру. Ана има листу од 10 различитих вредности. Милица треба да докаже Ани да поседује шифру чији Poseidon хеш одговара једној од вредности из Анине листе, али без откривања тајне шифре. Написати Circom коло које Милице омогућава да пружи Ани одговарајући ЗК доказ.
5. (7.5 поена) Колорадо је једна од две америчке државе која је у облику правоугаоника. Колорадо је смештен у правоугаоник између 37. и 41. степена северне географске ширине и између 102. и 109. степена западне географске дужине. Написати Circom коло којим би неки становник Колорада могао да докаже да има пребивалиште у Колораду без откривања своје тачне адресе пребивалишта. Становник прослеђује своју северну географску ширину (број између 0 и 90) и западну географску дужину (број између 0 и 180), при чему се подразумева да се пре тога комитовао на блокчејну хеширањем своје адресе пребивалишта (која је потписана од стране полицијских службеника тј. проверена је истинитост података).