UCSB CS 291D: Blockchains and Cryptocurrencies **Fall 2020**

Lecture 13: zkSNARK Internal III

Lecturer: Shumo Chu *Scribes: Atefeh Mohseni-Ejiyeh*

13.1 Pinocchio Protocol: PHGR13

The Pinocchio protocol is a practical, usable implementation of a zk-Snark. Arithmetic circuit redefines as QAP: L, R, C, P as follows:

$$\text{L} := \Sigma_{i=1}^{m} c_i.L_i,$$

$$\text{R} := \Sigma_{i=1}^{m} c_i.R_i \ ,$$

$$\text{O} := \Sigma_{i=1}^{m} c_i.O_i \ ,$$

$$\text{P} := L.R - O,$$

$$P := H.T \ \forall s \in F_p \ P(s) = H(s).T(s)$$

Lemma 13.1 *schwartz-zipped lemma $E(P(s))$ $s \in F_p$ and $p >> d$ so, why this scheme is secure?*

Proof: We need to have (d+1) points to define a d-degree polynomial. Alice has to find a polynomial $P(s) = H(s).T(s)$ such that $P := L.R - O$. So, if Bob really picks a random number then the chance of Alice cheating is really small ■

13.1.1 Sketch Protocol

Goal: test whether Alice has a fulfillment assignment of a NP-statement.

1. Alice chooses poly. L, R, O, H of degree d.
2. Bob choose $\sigma \leftarrow F_p$, computes $E(T(s))$ and sends $E(1), ..., E(s^d)$ to Alice.
3. Alice sends all the hidings $E(L(s)), E(R(s)), E(O(s)), E(H(s))$.
4. Bob checks $E(T(s).H(s)) = E(L(s).R(s) - O(s))$.

The question which is not yet clear here is that how Alice and Bob actually communicate? How they choose the MP statement?

13.1.2 Verifiability of Protocol

The problem with this version of pinaccho protocol is that it is not very hard for Alice to choose L, R, O that matches in $L : R - O := H.T$ (T is public). How to solve this problem?

We need to make sure L, R and O are separate from the coefficients. Therefore, we have $F := L + X^{d+1}.R + X^{2(d+1)} - O$

Extend idea to define F as a linear combination: $F := \Sigma_{i=1}^{m} c_i F_i$.
Bob asks Alice to prove that F is a linear combination of F_i or $F_i = L_i + X^{d+1}.R_i + X^{2(d+1)}.O_i$.

13.1.3 Linear Combination Proof

1. Bob chooses $\beta \leftarrow F_p$, sends $E(\beta.F_1(s)), ..., E(\beta.F_m(s))$ to Alice.
2. Alice sends back $E(\beta.F(s))$.

It's not any arbitrary L, R, O for Alice because Bob has already structured L, O, R in hidings sent to Alice. Therefore, Alice can just change $E(\beta.F(s))$.

13.1.4 Zero-knowledge proof

Concealing the assignment

Alice knows hidings $E(L(s)), E(R(s)), E(O(s)), E(H(s))$ so it still leaks some information.
Given $[c'_1, ..., c'_2]$, Bib can compute some polynomials L', R', O', H' and $E(L'(s)), E(R'(s)), E(O'(s)), E(H'(s))$.
So, Bob could fine something that is not Alice's assignment. Attention that Bob doesn't know what exactly is an assignment but it can find out what it is not. It is considered a leak of information because in some case the range of possible values for an assignment is limited.

How fix this problem?

Instead of computing L, R, O directly; Alice can choose $\sigma_1 \leftarrow F_p$, $\sigma_2 \leftarrow F_p$, $\sigma_3 \leftarrow F_p$
$L_z := L_1 + S_1.T_1$, $R_z := R + \sigma_2.T$, $O_z := O + \sigma_3.T$.