Updating zkSNARK Public Parameters

Vitalik Buterin
vitalik@ethereum.org

Christian Reitwießner
chris@ethereum.org

Abstract

1 GGPR

Remember that in the QSP (more specifically, strong QSPs) we are given polynomials $v_0, \ldots, v_m$, $w_0, \ldots, w_m$, a target polynomial t (of degree at most d) and a binary input string u. The prover finds $a_1, \ldots, a_m$, $b_1, \ldots, b_m$ (that are somewhat restricted depending on u) and a polynomial h such that

$$th = (v_0 + a_1 v_1 + \cdots + a_m v_m)(w_0 + b_1 w_1 + \cdots + b_m w_m).$$

In the previous section, we already explained how the common reference string (CRS) is set up. We choose secret numbers s and α and publish

$$E(s^0),\, E(s^1),\, \ldots,\, E(s^d) \quad \text{and} \quad E(\alpha s^0),\, E(\alpha s^1),\, \ldots,\, E(\alpha s^d)$$

Because we do not have a single polynomial, but sets of polynomials that are fixed for the problem, we also publish the evaluated polynomials right away:

- $E(t(s))$, $E(\alpha t(s))$,
- $E(v_0(s)), \ldots, E(v_m(s))$, $E(\alpha v_0(s)), \ldots, E(\alpha v_m(s))$,
- $E(w_0(s)), \ldots, E(w_m(s))$, $E(\alpha w_0(s)), \ldots, E(\alpha w_m(s))$,

and we need further secret numbers β_v, β_w, γ (they will be used to verify that those polynomials were evaluated and not some arbitrary polynomials) and publish

- $E(\gamma)$, $E(\beta_v \gamma)$, $E(\beta_w \gamma)$,
- $E(\beta_v v_1(s)), \ldots, E(\beta_v v_m(s))$
- $E(\beta_w w_1(s)), \ldots, E(\beta_w w_m(s))$
- $E(\beta_v t(s))$, $E(\beta_w t(s))$

This is the full common reference string. In practical implementations, some elements of the CRS are not needed, but that would complicate the presentation.

2 Generating the CRS

Assume we have already generated $E(\gamma)$, $E(s^0)$, $E(s^1)$, $\ldots$, $E(s^d)$. Then the remaining parts of the CRS can be generated in an associative way building on the fact that E is additive. More specifically, it is possible to generate the full CRS by combining the private parameters, α', β'_v and β'_w and α'', β''_v and β''_w from two CRS sets, marked by $'$ and $''$ in the following way:

α' and α'' are combined to $\alpha' + \alpha''$
β'_v and β''_v are combined to $\beta'_v + \beta''_v$
β'_w and β''_w are combined to $\beta'_w + \beta''_w$

The CRS can be computed without having access to the private parameters, because the private parameters are always a linear factor.