

Circuit for batching Groth16 proofs

May 10, 2019

For reference, recall the **Groth16** verification equation.

$$e(\pi_A, \pi_B) = \epsilon(\pi_C, [\delta]_2) \cdot \text{PI}$$

Where PI is an element in \mathbb{G}_t derived by the verifier from the public input. Specifically,

$$\text{PI} = \left[\alpha\beta + K_0 + \sum_{i=1}^{\ell} a_i \cdot K_i \right]_t$$

where (a_1, \dots, a_n) is the public input, and $K_i = \beta u_i(x) + \alpha v_i(x) + w_i(x)$.

We move the second pairing to the LHS to receive

$$e(\pi_A, \pi_B) \cdot \epsilon(-\pi_C, [\delta]_2) = \text{PI}$$

We use **ML** to denote a miller loop and **FE** to denote the final exponentiation. We assume the verifier and prover both know the set of public inputs and thus the derived values $\{\text{PI}_i\}_{i \in [m]}$. The private input for the circuit is a set of m **Groth16** proofs $S := \{\pi_{A,i}, \pi_{B,i}, \pi_{C,i}\}_{i \in [m]}$

The public inputs of the circuit are

1. P - the alleged pedersen hash of all proof elements.
2. F - the alleged correct randomized combination of pairings of proof elements.
3. $r = \text{Blake}(P, (\text{PI}_1, \dots, \text{PI}_m))$, interpreted as an element of \mathbb{F} .

The verifier has the corresponding m public input elements $\text{PI}_1, \dots, \text{PI}_m$, and checks outside of the circuit that

$$F = \prod_{i \in [m]} \text{PI}_i^{r^i}$$

The circuit computes

1. $M := \prod_{i \in [m]} \text{ML}(\pi_{A,i}, \pi_{B,i})$.
2. $C' := - \sum_{i \in [m]} r^i \cdot \pi_{C,i}$
3. $C = \text{ML}(C', [\delta]_2)$

The circuit checks that

1. $F = \text{FE}(M \cdot C)$.
2. $P = \text{ped}(S)$.

Remark 0.1. *It is possible to not do **FE** inside the circuit and have the verifier do it outside; however since it's only once per batch it might be better to leave it in the circuit.*

References