Circuit for batching Groth16 proofs

May 10, 2019

For reference, recall the $\mathsf{Groth16}$ verification equation.

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

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

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

where $(a_1, \ldots, a_n)$ 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

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

We use ML to denote a miller loop and FE to denote the final exponetiation.

The private input for the circuit is a set of m $\mathsf{Groth16}$ proofs $S := \{\pi_{\mathsf{A,i}}, \pi_{\mathsf{B,i}}, \pi_{\mathsf{C,i}}\}_{i \in [m]}$

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. $r = \mathsf{Blake(P)}$, interperted as an element of $\mathbb{F}$.

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

$$F = \prod_{i \in m} \mathsf{PI}_i^{r^i}$$

The circut computes

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

The circuit checks that

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

References