Execute Circuit

Victor Lopez

Dusk Network

July 2021

1 Private Inputs

- $\mathbb{I}$ Set of input notes I
- c_v Crossover value
- c_b Crossover blinder
- $\mathbb{O}$ Set of output notes O

2 Public Inputs

- A Tree anchor / merkle tree root
- $\mathbb{N}$ Set of nullifiers of $\mathbb{I}$
- C Crossover value commitment
- F Fee value
- $\mathbb{V}$ Set of value commitments of $\mathbb{O}$
- T Transaction hash

3 Gadgets

$opening(r, b, h) \rightarrow O(b), b_{first} = h, b_{last} = r$

$k, K = k{\cdot}G, K' = k{\cdot}G^*, doubleSchnorr(\sigma, K, K', m) \rightarrow \sigma = doubleSchnorrSign(k, m)$

$commitment(P, v, b) \rightarrow P == v \cdot G + b \cdot G^*$

$range(v, s) \rightarrow v < 2^s$

4 Circuit

1. $\forall (i, N) \in (\mathbb{I}, \mathbb{N})$
   (a) $k := i_s \cdot G$
   (b) $k' := i_s \cdot G^*$
   (c) $opening(A, i_o, i_h)$
   (d) $i_h == H(i_t, i_c, i_n, k, i_r, i_p, i_\psi)$
   (e) $doubleSchnorr(i_\sigma, k, k', T)$
   (f) $N == H(k', i_p)$
   (g) $commitment(i_c, i_v, i_b)$
   (h) $range(i_v, 64)$
2. $commitment(C, c_v, c_b)$
3. $range(c_v, 64)$
4. $\forall (o, V) \in (\mathbb{O}, \mathbb{V})$
   (a) $commitment(V, o_v, o_b)$
   (b) $range(o_v, 64)$
5. $\sum(i_v \in \mathbb{I}) - \sum(o_v \in \mathbb{O}) - c_v - F = 0$

5 Structures

- $I = (t, v, b, c, n, s, r, p, \psi, h, o, \sigma)$ Input note
  - t Note type
  - v Value
  - b Blinder
  - c Value commitment
  - n Encryption nonce
  - s sk_r
  - r R
  - p Position
  - ψ Encryption cipher
  - h Hash
  - o Merkle path
  - σ Schnorr signature
- $O = (v, b)$ Output note
  - v Value
  - b Blinder

6 Constants

- G JubJub Generator
- G^* JubJub Generator Nums

7 Functions

- H Hash to BLS12-381
- O Merkle Opening over H