Claim Statement

Let $\ell_{\mathsf{Merkle}}^{\mathsf{Sapling}}, \ell_{\mathsf{PRFnfSapling}}, \ell_{\mathsf{scalar}}^{\mathsf{Sapling}}$, ValueCommit, SpendAuthSig, $\mathbb{J}, \mathbb{J}^{(r)}, \mathsf{repr}_{\mathbb{J}}, q_{\mathbb{J}}, r_{\mathbb{J}}, h_{\mathbb{J}}$, $\mathsf{Extract}_{\mathbb{J}^{(r)}} : \mathbb{J}^{(r)} \to \mathbb{B}^{[\ell_{\mathsf{MerkleSapling}}]}$ be defined as in the original Sapling specification.

Furthermore let:

$\ell_{\mathsf{PRFnfsAlt}} : \mathbb{N} := 256$

$\mathsf{PRF}^{\mathsf{nfsAlt}}_{\mathsf{nk}\star}(\rho\star) = \mathsf{BLAKE2s\text{-}256}(\text{'MASP\_alt'}, \boxed{\mathrm{LESBS2OP}_{256}(nk\star)}\boxed{\mathrm{LESBS2OP}_{256}(\rho\star)})$.

A valid instance of π_{Claim} assures that given a *primary input*:

$(\mathsf{rt} : \mathbb{B}^{[\ell_{\mathsf{Merkle}}^{\mathsf{Sapling}}]}$,

$\mathsf{cv}^{\mathsf{Sapling}}$: ValueCommitment.Output,

$\mathsf{nf}_{\mathsf{Alt}} : \mathbb{B}^{[\ell_{\mathsf{PRFnfsAlt}}]}$,

rk : SpendAuthSig.Public)

the prover knows an *auxiliary input*:

$(\mathsf{path} : \mathbb{B}^{[\ell_{\mathsf{Merkle}}^{\mathsf{Sapling}}][\mathsf{MerkleDepth}^{\mathsf{Sapling}}]}$,

$\mathsf{pos} : \{0..2^{\mathsf{MerkleDepth}^{\mathsf{Sapling}}} - 1\}$,

$\mathsf{g_d} : \mathbb{J}$,

$\mathsf{pk_d} : \mathbb{J}$,

$\mathsf{v}^{\mathsf{Sapling}} : \{0..2^{\ell_{\mathsf{value}}} - 1\}$,

$\mathsf{rcv}^{\mathsf{Sapling}} : \{0..2^{\ell_{\mathsf{scalar}}^{\mathsf{Sapling}}} - 1\}$,

$\mathsf{cm}^{\mathsf{Sapling}} : \mathbb{J}$,

$\mathsf{rcm}^{\mathsf{Sapling}} : \{0..2^{\ell_{\mathsf{scalar}}^{\mathsf{Sapling}}} - 1\}$,

$\alpha : \{0..2^{\ell_{\mathsf{scalar}}^{\mathsf{Sapling}}} - 1\}$,

ak : SpendAuthSig.Public,

$\mathsf{nsk} : \{0..2^{\ell_{\mathsf{scalar}}^{\mathsf{Sapling}}} - 1\}$,

$\mathsf{path}^{\mathsf{excl}} : \mathbb{B}^{[\ell_{\mathsf{Merkle}}^{\mathsf{Sapling}}][\mathsf{MerkleDepth}^{\mathsf{excl}}]}$,

$\mathsf{pos}^{\mathsf{excl}} : \{0..2^{\mathsf{MerkleDepth}^{\mathsf{excl}}} - 1\}$,

$\mathsf{start} : \{0..2^{\mathsf{MerkleDepth}^{\mathsf{Sapling}}} - 1\}$,

$\mathsf{end} : \{0..2^{\mathsf{MerkleDepth}^{\mathsf{Sapling}}} - 1\})$

Such that the following conditions hold:

- **Note commitment integrity** $\mathsf{NoteCommit}^{\mathsf{Sapling}}_{\mathsf{rcm}^{\mathsf{Sapling}}}(\mathsf{repr}_{\mathbb{J}}(\mathsf{g_d}), \mathsf{repr}_{\mathbb{J}}(\mathsf{pk_d}), \mathsf{v}^{\mathsf{Sapling}})$.

- **Merkle path validity** Either $\mathsf{v}^{\mathsf{Sapling}} = 0$, or $(\mathsf{path}, \mathsf{pos})$ is a valid *Merkle Path* of depth $\mathsf{MerkleDepth}^{\mathsf{Sapling}}$, as defined in the original Sapling specification, from $\mathsf{cm_u} = \mathsf{Extract}_{\mathbb{J}^{(r)}}(\mathsf{cm}^{\mathsf{Sapling}})$ to the *anchor* rt

- **Value commitment integrity** $\mathsf{cv}^{\mathsf{Sapling}} = \mathsf{ValueCommit}^{\mathsf{Sapling}}_{\mathsf{rcv}}(\mathsf{v}^{\mathsf{Sapling}})$.

- **Small order checks** $\mathsf{g_d}$ and ak are not of small order, i.e. $[h_{\mathbb{J}}]\mathsf{g_d} \neq \mathcal{O}_{\mathbb{J}}$ and $[h_{\mathbb{J}}]\mathsf{ak} \neq \mathcal{O}_{\mathbb{J}}$.

- **Nullifier Integrity** $\mathsf{nf}^{\mathsf{Sapling}} = \mathsf{PRF}^{\mathsf{nfSapling}}_{\mathsf{nk}\star}(\rho\star)$ where

  $\mathsf{nk}\star = \mathsf{repr}_{\mathbb{J}}([\mathsf{nsk}]\mathcal{H})$

  $\rho\star = \mathsf{repr}_{\mathbb{J}}(\mathsf{MixingPedersenHash}(\mathsf{cm}^{\mathsf{Sapling}}, \mathsf{pos}))$

- **Alternate Nullifier Integrity** $\mathsf{nf}_{\mathsf{Alt}} = \mathsf{PRF}^{\mathsf{nfsAlt}}_{\mathsf{nk}\star}(\rho\star)$

- **Spend authority** $\mathsf{rk} = \mathsf{SpendAuthoritySig.RandomizePublic}(\alpha, \mathsf{ak})$.

- **Diversifier address integrity** $\mathsf{pk_d} = [\mathsf{ivk}]\mathsf{g_d}$ where

  $\mathsf{ivk} = \mathsf{CRH}^{\mathsf{ivk}}(\mathsf{ak}\star, \mathsf{nk}\star)$

  $\mathsf{ak}\star = \mathsf{repr}_{\mathbb{J}}(\mathsf{ak})$

- **Merkle path validity for** $(\mathsf{start}, \mathsf{end})$ $(\mathsf{path}^{\mathsf{excl}}, \mathsf{pos}^{\mathsf{excl}})$ is a valid Merkle path of depth $\mathsf{MerkleDepth}^{\mathsf{excl}}$, as defined in § 4.9 'Merkle Path Validity', from excl to the anchor $\mathsf{rt}^{\mathsf{excl}}$, where $\mathsf{excl} = \mathsf{MerkleCRH}^{\mathsf{Sapling}}(\mathsf{MerkleDepth}^{\mathsf{excl}}, \mathsf{start}, \mathsf{end})$.

- **Nullifier in excluded range** $\mathsf{start} \leq \mathsf{nf}^{\mathsf{Sapling}} \leq \mathsf{end}$.

Output Statement

The *Output Circuit* is defined in § 0.12.3 'Output Statement (MASP)' of the Multi-Asset Shielded Pool Specification.

Convert Statement

The *Convert Circuit* is defined in § 0.12.5 'Convert Statement' of the Multi-Asset Shielded Pool Specification.