Scheme Transcript (T)

A transcript abstraction holding a state $s \in \mathbb{Z}_2^\kappa$, a condensed description of the messages exchanged in a protocol execution. It is parametrized by a hash function H (we employ SHA3-256 [Dwo15]), a PRNG (we use Shake256 [Dwo15]). The state s is initialized to zero and updated upon each Append / Extract.

```
$\mathsf{T.Append}_l\,(m) \dashrightarrow$
  $\mathsf{T}.s \leftarrow \mathsf{H}(\mathsf{H}(\mathsf{T}.s \,||\, l) \,||\, m)$ with message $m$ and label $l$ to update $s$
$\mathsf{T.Extract}_l\,(k \in \mathbb{N}) \dashrightarrow r \in \mathbb{Z}_2^k$
  $\mathsf{T}.s \leftarrow \mathsf{H}(\mathsf{T}.s \,||\, l)$ with label $l$ to update $s$
  Set $\mathsf{PRNG.Seed}(\mathsf{T}.s)$ and compute $r \leftarrow \mathsf{PRNG.Get}(k)$ to get the randomness.
  return $r$
```

References

[Dwo15] Morris Dworkin. Sha-3 standard: Permutation-based hash and extendable-output functions, 2015-08-04 2015.