
Scheme Fischlin

A transformation from an Interactive Sigma Protocol Σ_R into a Non-Interactive (NI) proof system following [Fis05], parametrized by a hash function¹ $H_\ell : \{0, 1\}^* \mapsto \mathbb{Z}_2^\ell$ with digest length of ℓ bits (we set $\ell=8$).

Prove(R, w) $\dashrightarrow \pi$

- 1: **for** $i \in [\lambda/\ell]$ **do**
 - 2: $(a_i, \text{state}_i) \leftarrow \Sigma_R.\text{Commitment}(w, R)$ commits witness w for relation R
 - 3: **for** $i \in [\lambda/\ell]$ **do**
 - 4: Sample a challenge $e_i \xleftarrow{\$} \{0, 1\}^{\ell \log_2(\lambda)}$
 - 5: $z_i \leftarrow \Sigma_R.\text{Response}(\text{state}_i, e_i)$ as the response to that challenge.
 - 6: Check if $H_\ell(\{a_i\}_{\forall i} \parallel i \parallel e_i \parallel z_i) \stackrel{?}{=} \mathbf{0}_{\mathbb{Z}_2^\ell}$, otherwise go back to step 6
- return** ($\pi = \{a_i, e_i, z_i\}_{\forall i}$)

Verify(R, $\pi = \{a_i, e_i, z_i\}_{i \in [\lambda/\ell]}$) $\dashrightarrow valid$

- 1: **for** $i \in [\lambda/\ell]$ **do**
 - 2: Check if $H_\ell(\{a_i\}_{\forall i} \parallel i \parallel e_i \parallel z_i) \stackrel{?}{=} \mathbf{0}_{\mathbb{Z}_2^\ell}$, otherwise **ABORT**
 - 3: Check if $\Sigma_R.\text{Verify}(x, z_i, e_i)$, otherwise **ABORT**
- return** *valid*
-

References

- [Fis05] Marc Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In *Annual International Cryptology Conference*, pages 152–168. Springer, 2005.

¹Typically instantiated via a standard hash function with truncated output, e.g., SHA-256.