Scheme Fiat-Shamir(FS)

A transformation from a public-coin Interactive-Proof (IP) IP_{R} into a Non-Interactive proof system following [FS86], parametrized by a hash function H.

Players: A prover $\mathcal{P}$ and a verifier $\mathcal{V}$.

$\mathcal{P}.\mathsf{Prove}(x, w) \dashrightarrow \pi$

1: Run all steps of the prover in $\pi \leftarrow \mathsf{IP}_{\mathrm{R}}.\mathsf{Prove}(x, w)$, replacing[1] the verifier's challenges with $e_i \leftarrow \mathsf{H}(x \mid\mid m_0 \ldots \mid\mid m_i)$ where m_i is $\mathcal{P}$ message at step i.
return π

$\mathcal{V}.\mathsf{Verify}(x, \pi) \dashrightarrow \mathit{valid}$

1: Run all steps of the verifier in $\mathsf{IP}_{\mathrm{R}}.\mathsf{Verify}(x, \pi)$, replacing the verifier's challenges with $e_i \leftarrow \mathsf{H}(x \mid\mid m_0 \ldots \mid\mid m_i)$ where m_i is $\mathcal{P}$ message at step i.

References

[FS86] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the theory and application of cryptographic techniques*, pages 186–194. Springer, 1986.

[1] In practice we employ a transcript T (Section **??**), replacing message concatenation with $\mathsf{T}.\mathsf{Append}$ and the final hashing with the hash-chaining of $\mathsf{T}.\mathsf{Extract}$.