Protocol NthRoot

ZKPoK of the value v such that $u = v^n \mod n^2$, from [Lin17].

Players: A a prover $\mathcal{P}$ and verifier $\mathcal{V}$.
Inputs: $\mathcal{P}$: v, such that $u = v^n \mod n^2$

$\mathcal{P}$.**Round1**()$\dashrightarrow r$
1: $\mathsf{Send}(r \xleftarrow{\$} \mathbb{Z}_{n^2}) \to \mathcal{V}$ as the commitment.

$\mathcal{V}$.**Round2**$(r)\dashrightarrow e$
1: $\mathsf{Send}(e \xleftarrow{\$} \mathbb{Z}_2^{2\sigma}) \to \mathcal{V}$ as a random 2σ-bit challenge

$\mathcal{P}$.**Round3**$(e, v)\dashrightarrow z$
1: $\mathsf{Send}(z \leftarrow rv^e \mod n^2) \to \mathcal{P}$ as the challenge response

$\mathcal{V}$.**Round4**$(z)\dashrightarrow valid$
1: Check if $z^n \stackrel{?}{=} ru^e \mod n^2$. ABORT otherwise.

References

[Lin17] Yehuda Lindell. Fast secure two-party ecdsa signing. In *Advances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part II 37*, pages 613–644. Springer, 2017.