Protocol Valid Paillier Public Key($\mathsf{PaillierPKPoK}$)

ZKP from [Lin17] of n being a Paillier public key for an undisclosed $\phi(n)$ s.t. $gcd(n, \phi(n)) = 1$, based on $\mathsf{NthRoot}$, a ZKPoK of N-th root of $n^n \mod n^2$

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

Inputs: $\mathcal{P}, \mathcal{V} \rightarrow pk \equiv n$, a Paillier public key,
$\mathcal{P} \rightarrow sk \equiv \phi(n)$, the corresponding Paillier private key.

```
$\mathcal{V}.\mathsf{Round1}(n) \dashrightarrow \boldsymbol{x}$
    Sample challenge $\boldsymbol{y} \leftarrow \{y_{(i)} \xleftarrow{\$} \mathbb{Z}_n\}_{\forall i\in[\sigma]}$
    $\boldsymbol{x} \leftarrow \{(y_{(i)})^n \mod n^2\}_{\forall i}$
    Run $\mathsf{NthRoot}(x_{(i)})$ $\forall i\in[\sigma]$ as prover with $\mathcal{P}$ as verifier. ABORT if it fails.
$\mathcal{P}.\mathsf{Round2}(n, \phi(n), \boldsymbol{x}) \dashrightarrow \boldsymbol{y'}$
    return challenge response $\boldsymbol{y'} = \{y'_{(i)}\}_{i\in[\sigma]}$ using $\phi(n)$ s.t. $y'_{(i)} \leftarrow (x_{(i)})^n$
$\mathcal{V}.\mathsf{Round3}(\boldsymbol{y'}) \dashrightarrow valid$
    Verify if every $y_{(i)} \stackrel{?}{=} y'_{(i)}$, ABORT if not.
    return $valid$
```

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.