Protocol Paillier Decryption is Discrete Log (PDL)

ZKP from [Lin17] that a value encrypted in a given Paillier ciphertext c is the discrete log of a given Elliptic curve point Q.

Players: A verifier $\mathcal{V}$, and a prover $\mathcal{P}$.
Inputs: $\mathcal{P}, \mathcal{V} \rightarrow pk \equiv n$, a Paillier public key; Q, a public point.
$\mathcal{P} \rightarrow sk \equiv \phi(n)$, the corresponding Paillier private key; x, a scalar.
$\mathcal{V} \rightarrow c, r$, an encrypted value of x, such that $c = \mathsf{Enc}_{pk}(x; r)$.

$\mathcal{V}$.**Round1**$() \dashrightarrow c', c''$
1: Sample $a \xleftarrow{\$} \mathbb{Z}_q$ and $b \xleftarrow{\$} \mathbb{Z}_{q^2}$
2: Sample $r \in \mathbb{Z}_N^*$ verifying $\gcd(r, N) = 1$
3: $c' \leftarrow (a \odot c) \oplus \mathsf{Enc}_{pk}(b; r)$
4: $c'' \leftarrow \mathsf{Commit}(a, b)$
5: $Q' \leftarrow a \cdot Q + b \cdot G$
6: $\mathsf{Send}(c', c'') \rightarrow \mathcal{P}$

$\mathcal{P}$.**Round2**$(c', c'') \dashrightarrow \hat{c}$
1: $\alpha \leftarrow \mathsf{Dec}_{sk}(c')$ and compute $\hat{Q} \leftarrow \alpha \cdot G$
2: $\mathsf{Send}(\hat{c} \leftarrow \mathsf{Commit}(\hat{Q})) \rightarrow \mathcal{V}$

$\mathcal{V}$.**Round3**$(\hat{c}) \dashrightarrow (a, b)$
1: $(a, b) \leftarrow \mathsf{Open}(c'')$

$\mathcal{P}$.**Round4**$(a, b) \dashrightarrow$
1: Check that $\alpha \stackrel{?}{=} a \cdot x + b$, ABORT otherwise
2: Run PaillierRange proof: Prove that $x \in \mathbb{Z}_q$ (can be started in Round 1 and run concurrently).
3: $\mathsf{Send}(\hat{Q} \leftarrow \mathsf{Open}(\hat{c})) \rightarrow \mathcal{V}$

$\mathcal{V}$.**Round5**$() \dashrightarrow valid$
1: Check that $\hat{Q} \stackrel{?}{=} Q'$ and that the PaillierRange proof returns *valid*. 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.