**Protocol** Paillier Decryption in Range (PaillierRange)

ZKP that $x \in \{\frac{q}{3}, ..., \frac{2q}{3}\}$ where $c = Enc_{pk}(x; r)$ from [Lin17] for statistical security parameter $t$ cheating prover success with probability $\leq 2^{-t}$ and prime $q$.

**Players:** A verifier $\mathcal{V}$, and a prover $\mathcal{P}$.
**Inputs:** $\mathcal{P}, \mathcal{V} \to pk \equiv n$, a Paillier public key,
$\mathcal{P} \to sk \equiv \phi(n)$, the corresponding Paillier private key.

$\mathcal{V}$.**Round1**$() \dashrightarrow$

$l \leftarrow \lfloor \frac{q}{3} \rfloor$
$c \leftarrow \leftarrow c \ominus l$ to shift $c$ to the range $[0, \frac{q}{3})$
Sample $e \xleftarrow{\$} \{0,1\}^t$
$com \leftarrow \mathsf{Commit}(e, sid)$ with $e = \{e_0, \ldots, e_{t-1}\}$.

$\mathcal{P}$.**Round2**$() \dashrightarrow$

$l \leftarrow \lfloor \frac{q}{3} \rfloor$
$x \leftarrow x - l$
Sample $w_1^1, ..., w_1^t \xleftarrow{\$} \{l, \ldots, 2l\}$ and compute $w_2^i = w_1^i - l \; \forall i \in [t]$.
For every $i \in [t]$, switch $w_1^i$ and $w_2^i$ with probability $\frac{1}{2}$.
For every $i \in [t]$, compute $c_1^i \leftarrow \mathsf{Enc}_{pk}(w_1^i; r_1^i)$ and $c_2^i \leftarrow \mathsf{Enc}_{pk}(w_2^i; r_2^i)$ where $r_1^i, r_2^i \xleftarrow{\$} \mathbb{Z}_N$.
$\mathsf{Send}(c_1^0, c_2^0, ..., c_1^{t-1}, c_2^{t-1}) \to \mathcal{V}$

$\mathcal{V}$.**Round3**$() \dashrightarrow$

$\mathsf{Send}(\mathsf{Open}(com)) \to \mathcal{P}$

$\mathcal{P}$.**Round4**$() \dashrightarrow$

**for** $i \in [t]$ **do**
    **if** $e_i = 0$ **then**
        $z_i \leftarrow (w_1^i, r_1^i, w_2^i, r_2^i)$
    **else**
        Let $j \in \{1, 2\}$ be the unique value such that $x + w_j^i \in \{l, ..., 2l\}$.
        $z_i \leftarrow (j, x + w_j^i, r \cdot r_j^i \mod N)$
    $\mathsf{Send}(z_i) \to \mathcal{V}$

$\mathcal{V}$.**Round5**$() \dashrightarrow valid$

**for** $i \in [t]$ **do**
    **if** $e_i = 0$ **then**
        Check that $c_1^i = \mathsf{Enc}_{pk}(w_1^i; r_1^i)$ and $c_2^i = \mathsf{Enc}_{pk}(w_2^i; r_2^i)$.
        Check that one of $w_1^i, w_2^i \in \{l, ..., 2l\}$ while the other is in $\{0, ..., l\}$.
    **else**
        Check that $c \oplus c_j^i = \mathsf{Enc}_{pk}(w^i; r^i)$ and $w^i \in \{l, ..., 2l\}$.

# References


[Lin17] Yehuda Lindell. Fast secure two-party ecdsa signing. In *Advances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Con-*

*ference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part II 37*, pages 613–644. Springer, 2017.