Protocol Lindell17.DKG

An adaptation of the Distributed Key Generation (DKG) of [Lin17, Section 3.2], parametrized by a group $\mathbb{G}(q, G)$. The protocol is symmetric for all the n participants $\{\mathcal{P}_i\}_{i\in[n]}$

Players: $\mathcal{P}_1, \ldots, \mathcal{P}_i, \ldots, \mathcal{P}_n$.

```
$\mathcal{P}_i$.**Round1**$() \dashrightarrow Q_i^c$
    Sample $x_i \xleftarrow{\$} \mathbb{Z}_q$ as a private key share.    *(Or reuse $x_i$ from* GennaroDkg*)*
    Sample $x_i' \xleftarrow{\$} \mathbb{Z}_q$ and $x_i'' \xleftarrow{\$} \mathbb{Z}_q$ s.t. $x_i', x_i'' \in \left[\frac{q}{3}, \frac{2q}{3}\right]$ and $x_i = 3x_i' + x_i'' \mod q$
    $Q_i' \leftarrow x_i' \cdot G$ and $Q_i'' \leftarrow x_i'' \cdot G$
    $(Q_i^c, Q_i^w) \leftarrow \mathsf{Pedersen.Commit}(Q_i', Q_i'')$ to get a commitment to $Q_i'$ and $Q_i''$.
    $\mathcal{F}^{Broadcast}(Q_i^c)$

$\mathcal{P}_i$.**Round2**$(Q_j^c\ \forall j \in [n] \setminus \{i\}) \dashrightarrow Q_i^{dl'}, Q_i^{dl''}$
    $Q_i^{dl'} \leftarrow (Q_i')$ and $Q_i^{dl''} \leftarrow (Q_i'')$ as discrete log PoKs
    $\mathcal{F}^{Broadcast}(Q_i^w, Q_i', Q_i'', Q_i^{dl'}, Q_i^{dl''})$

$\mathcal{P}_i$.**Round3**$(Q_j^w, Q_j', Q_j'', Q_j^{dl'}, Q_j^{dl''}\ \forall j \in [n] \setminus \{i\}) \dashrightarrow pk_i, c'_{key_i}, c''_{key_i}$
    Verify opening of $Q_i^c$
    Verify $Q_i^{dl'}$ and $Q_i^{dl'}$
    Generate Paillier key pair $(pk_i, sk_i)$
    $c'_{key_i} = [\![x_i'; r_i']\!]pk_i$ and $c''_{key_i} = [\![x_i''; r_i'']\!]pk_i$
    Start the ZK proofs process with every other $\mathcal{P}_j$ (pairwise) that $pk_i$ was
      generated correctly ($L_P$) and that $c'_{key_i}$ and $c''_{key_i}$ encrypt dlogs of $Q_i'$ and
      $Q_i''$ respectively ($L_{PDL}$).
    $\mathcal{F}^{Broadcast}(pk_i, c'_{key_i}, c''_{key_i})$

$\mathcal{P}_i$.**Round4**$(pk_j, c'_{key_j}, c''_{key_j} \forall j \in [n] \setminus \{i\}) \dashrightarrow$
    $c_{key_j} = 3 \odot c'_{key_j} \oplus c''_{key_j}\ \forall j \in [n] \setminus \{i\}$
    $L_P$ and $L_{PDL}$ continue

$\mathcal{P}_i$.**Rounds5-8**$() \dashrightarrow$
    $L_P$ and $L_{PDL}$ continue. ABORT if any of the proofs fail
    **return** $(sk_i, pk_1, pk_2, ..., pk_n, c_{key_1}, c_{key_2}, ..., c_{key_n})$
```

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.