Protocol Lindell17.Sign

UC maliciously secure two-party 2-out-of-n ECDSA signing protocol from [Lin17, Section 3.3] for a group $\mathbb{G}(q, G)$. It is based on a Commitment scheme, a dlog PoK Fischlin, a hash to field $\mathsf{H}_{\mathbb{Z}_q}$ and Paillier encryption scheme.

Players: $\mathcal{P}_1\&\mathcal{P}_2$ hold a public key $Q \in \mathbb{G}$, a private key share $x_1, x_2 \in \mathbb{Z}_q$ and a Paillier public key pk

Inputs: a message m, a unique session id sid

$\mathcal{P}_1.\textsf{\textbf{Round1}}() \dashrightarrow c_1$

Sample $k_1 \xleftarrow{\$} \mathbb{Z}_q$ and compute $R_1 \leftarrow k_1 \cdot G$
Run $(c_1, w_1) \leftarrow \mathsf{Commit}(sid \mid\mid R_1)$
$\mathsf{Send}(c_1) \rightarrow \mathcal{P}_2$

$\mathcal{P}_2.\textsf{\textbf{Round2}}(c_1) \dashrightarrow (R_2, \pi_2^{dl})$

Sample $k_2 \xleftarrow{\$} \mathbb{Z}_q$ and compute $R_2 \leftarrow k_2 \cdot G$
Run $\pi_2^{dl} \leftarrow \mathsf{Fischlin.Prove}(k_2)$ as a dlog PoK of R_2
$\mathsf{Send}(R_2, \pi_2^{dl}) \rightarrow \mathcal{P}_1$

$\mathcal{P}_1.\textsf{\textbf{Round3}}(R_2, \pi_2^{dl}) \dashrightarrow (R_1, w_1, \pi_1^{dl})$

Run $\mathsf{Fischlin.Verify}(R_2, \pi_2^{dl})$; ABORT if it fails
Run $\pi_1^{dl} \leftarrow \mathsf{Fischlin.Prove}(k_1)$ as a dlog PoK of R_1
$R \leftarrow k_1 \cdot R_2$
$\mathsf{Send}(R_1, w_1, \pi_1^{dl}) \rightarrow \mathcal{P}_2$

$\mathcal{P}_2.\textsf{\textbf{Round4}}(R_1, w_1, \pi_1^{dl}) \dashrightarrow [\![c_3]\!]$

Run $\mathsf{Open}(sid \mid\mid R_1, c_1, w_1)$ and $\mathsf{Fischlin.Verify}(R1, \pi_1^{dl})$
$R \leftarrow k_2 \cdot R_1$
$m' \leftarrow \mathsf{H}_{\mathbb{Z}_q}(m)$
Sample $\rho \xleftarrow{\$} \mathbb{Z}_{q^2}$
Sample $\tilde{r} \xleftarrow{\$} \mathbb{Z}_q^*$ s.t. $\gcd(\tilde{r}, N) = 1$
$x_2^{SS} \leftarrow \mathsf{ShamirToAdditive}(x_2)$
$[\![c_3]\!] \leftarrow \mathsf{Paillier.Encrypt}(pk, \rho q + k_2^{-1}(m' + r \cdot x_2^{SS}))$
$\mathsf{Send}([\![c_3]\!]) \rightarrow \mathcal{P}_1$

$\mathcal{P}_1.\textsf{\textbf{Round5}}([\![c_3]\!]) \dashrightarrow \sigma = (r, s'', v)$

$s' \leftarrow Dec_{sk}([\![c3]\!])$
$s'' \leftarrow k_2^{-1} s' \mod q$
$v \leftarrow recoveryId(R)$
Verify (R, s'') is a valid ECDSA signature with the public key Q
return $\sigma = (R, s'', v)$

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.