Protocol $\mathsf{VSOT}_{\xi,\ell,\mathbb{G}}$

Maliciously secure base OT protocol from [DKLs18, Protocol 7] for $\ell \times \kappa$-bit messages in a ξ-message batch, and a group $\mathbb{G}(q, G)$. Requires a hash H and a ZKPoK of the discrete log of a value $F_{ZK}^{R_{DL}}$ (e.g., Fischlin).

Players: a sender $\mathcal{S}$, and receiver $\mathcal{R}$.
Inputs: $\mathcal{R} : \boldsymbol{b} \in \mathbb{Z}_2^{\xi}$, the input choice bits.
Outputs: $\mathcal{R}: \boldsymbol{m_0}, \boldsymbol{m_1} \in \mathbb{Z}_2^{\xi\times\ell\times\kappa}$, pairs of messages
$\mathcal{S}: \boldsymbol{m_b} \in \mathbb{Z}_2^{\xi\times\ell\times\kappa}$, chosen messages s.t. $\boldsymbol{m_b} = \boldsymbol{m_1}\boldsymbol{b} + \boldsymbol{m_0}(1 - \boldsymbol{b})$

$\mathcal{S}.$**Round1**$() \dashrightarrow (\pi, B)$
Sample random $\beta \xleftarrow{\$} \mathbb{Z}_q$ as secret key
$B = \beta \cdot G$ as its public key
$\pi \leftarrow F_{ZK}^{R_{DL}}.\mathsf{Prove}_G(\beta, B)$ as a proof of knowledge of β
$\mathsf{Send}(\pi, B) \to \mathcal{R}$

$\mathcal{R}.$**Round2**$(\pi, B) \dashrightarrow (A)$
Check if $\mathcal{F}_{ZK}^{R_{DL}}.\mathsf{Verify}_G(\pi, B) \stackrel{?}{=} 1$, ABORT otherwise
for $i \in [\xi]$; $l \in [\ell]$ **do**
    Sample random $a \xleftarrow{\$} \mathbb{Z}_q$
    $m_{b(i,l)} \leftarrow \mathsf{H}(a_{(i,l)} \cdot B)$ as the pad
    $A_{(i,l)} \leftarrow \{\{a_{(i,l)} \cdot G + b_{(i)} \cdot B\}_{l\in[\ell]}\}_{i\in[\xi]}$ as a choice bit commitment
$\mathsf{Send}(\boldsymbol{A} = \{\{A_{i,l}\}_{l\in[\ell]}\}_{i\in[\xi]}) \to \mathcal{S}$

$\mathcal{S}.$**Round3**$(\boldsymbol{A}) \dashrightarrow (\boldsymbol{\chi})$
for $i \in [\xi]$; $l \in [\ell]$ **do**
    $m_{0(i,l)} \leftarrow \mathsf{H}(\beta \cdot A_{(i,l)})$ and $m_{1(i,l)} \leftarrow \mathsf{H}(\beta \cdot (A_{(i,l)} - B))$ as random pads
    $\chi_{(i,l)} \leftarrow \mathsf{H}(\mathsf{H}(m_{0(i,l)})) \oplus \mathsf{H}(\mathsf{H}(m_{1(i,l)}))$ as the challenge
$\mathsf{Send}(\boldsymbol{\chi} = \{\{\chi_{(i,l)}\}_{l\in[\ell]}\}_{i\in[\xi]}) \to \mathcal{R}$

$\mathcal{R}.$**Round4**$(\boldsymbol{\chi}) \dashrightarrow (\boldsymbol{\rho'})$
$\boldsymbol{\rho'} \leftarrow \{\{\mathsf{H}(\mathsf{H}(m_{b(i,l)})) \oplus (b_{(i)} \cdot \chi_{(i,l)})\}_{l\in[\ell]}\}_{i\in[\xi]}$
$\mathsf{Send}(\boldsymbol{\rho'}) \to \mathcal{S}$ as the challenge response

$\mathcal{S}.$**Round5**$(\boldsymbol{\rho'}) \dashrightarrow (\boldsymbol{\rho_0}, \boldsymbol{\rho_1}, \boldsymbol{m_0}, \boldsymbol{m_1})$
Check if ${\rho'}_{(i,l)} \stackrel{?}{=} m_{b(i,l)} \oplus \chi_{(i,l)}$ $\forall l{\in}[\ell]$ $\forall i{\in}[\xi]$, ABORT otherwise
$\mathsf{Send}(\boldsymbol{\rho_0} = \mathsf{H}(\boldsymbol{m_0}), \boldsymbol{\rho_1} = \mathsf{H}(\boldsymbol{m_1})) \to \mathcal{R}$
return $\boldsymbol{m_0}, \boldsymbol{m_1}$

$\mathcal{R}.$**Round6**$(\boldsymbol{\rho_0}, \boldsymbol{\rho_1}) \dashrightarrow (\boldsymbol{m_b})$
Check $\mathsf{H}(m_{b(i,l)}) \stackrel{?}{=} \rho_{1(i,l)} b_{(i)} \oplus \rho_{0(i,l)}(1\text{-}b_{(i)})$ $\forall l{\in}[\ell]$ $\forall i{\in}[\xi]$, else ABORT
Check $\chi_{(i,l)} \stackrel{?}{=} \mathsf{H}(\rho_{0(i,l)}) \oplus \mathsf{H}(\rho_{1(i,l)})$ $\forall l{\in}[\ell]$ $\forall i{\in}[\xi]$, else ABORT
return $\boldsymbol{m_b}$

References

[DKLs18] Jack Doerner, Yashvanth Kondi, Eysa Lee, and Abhi shelat. Secure two-party threshold ecdsa from ecdsa assumptions. In *2018 IEEE*

Symposium on Security and Privacy (SP), pages 980–997. IEEE, 2018.