Protocol $\mathsf{RVOLE}_{\ell,q}$

A two-party protocol [DKLs23, Protocol 5.2] realizing the $\mathcal{F}^{RVOLE}_{q,\ell}$ random multiplicative to additive share generation with malicious security in a group $\mathbb{G}(q,G)$, based on a $\mathsf{ROTe}_{\xi,\ell}$ with batch-size $\xi = |q| + 2\sigma$, a hash function $\mathsf{H}_{2\kappa}: \{0,1\}^* \mapsto \mathbb{Z}_2^\kappa$ and a hash-to-field function $\mathsf{H}_{\mathbb{Z}_q^{\ell\times\rho}}: \{0,1\}^* \mapsto \mathbb{Z}_q^{\ell\times\rho}$ with $\rho = \lceil |q|/\kappa \rceil$

Players: Alice $\mathcal{P}_A$, and Bob $\mathcal{P}_B$
Inputs: $\mathcal{P}_A \to \boldsymbol{a} \in \mathbb{Z}_q^\ell$; $\mathcal{P}_A \& \mathcal{P}_B \to \mathrm{sid} \in \{0,1\}^*$ as session id
Outputs: $\mathcal{P}_A \leftarrow \boldsymbol{c} \in \mathbb{Z}_q^\ell$ $\mathcal{P}_B \leftarrow b \in \mathbb{Z}_q, \boldsymbol{d} \in \mathbb{Z}_q^\ell$ s.t. $a_{(i)} \cdot b = c_{(i)} + d_{(i)}$ $\forall i \in [\ell]$

$\mathcal{P}_A \& \mathcal{P}_B.\mathsf{Setup}() \dashrightarrow$
0: $\mathcal{P}_A \& \mathcal{P}_B$ run $\mathsf{ROTe.Setup}()$ to generate κ Base OT seeds for the $\binom{2}{1}$-ROTe functionality with $\mathcal{P}_A$ as sender $\mathcal{S}$ and $\mathcal{P}_B$ as receiver $\mathcal{R}$
1: Set an arbitrary public gadget vector $\boldsymbol{g} \in \mathbb{Z}_q^\ell$

$\mathcal{P}_B.\mathsf{Round1}() \dashrightarrow (\gamma, b)$
1: Sample $\boldsymbol{\beta} \xleftarrow{\$} \mathbb{Z}_2^\xi$ as bob's ROTe choice bits
2: Run $\boldsymbol{\gamma} \leftarrow \mathsf{ROTe.Round1}(\boldsymbol{\beta})$
3: $b \leftarrow \sum_{j=1}^{\xi} g_{(j)} \cdot \beta_{(i)}$
4: $\mathsf{Send}(\boldsymbol{\gamma}) \to \mathcal{P}_A$
return b as the multiplicative share of $\mathcal{P}_B$

$\mathcal{P}_A.\mathsf{Round2}(\boldsymbol{\gamma}, \boldsymbol{a}) \dashrightarrow (\tilde{\boldsymbol{a}}, \boldsymbol{\eta}, \mu, \boldsymbol{c})$
1: Run $(\boldsymbol{\alpha_0}, \boldsymbol{\alpha_1}) \leftarrow \mathsf{ROTe.Round2}(\boldsymbol{\gamma})$, where $\boldsymbol{\alpha_0}, \boldsymbol{\alpha_1} \in \mathbb{Z}_q^{\xi\times(\ell+\rho)}$
2: $\boldsymbol{c} \leftarrow \{c_{(i)} = -\sum_{j=1}^{\xi} \alpha_{0(j,i)} \cdot g_{(j)}\}_{i\in[\ell]}$
3: Sample $\hat{\boldsymbol{a}} \xleftarrow{\$} \mathbb{Z}_q^\rho$
4: $\tilde{\boldsymbol{a}} \leftarrow \{\{\alpha_{0(j,i)} - \alpha_{1(j,i)} + a_{(i)}\}_{i\in[\ell]} || \{\alpha_{0(j,\ell+k)} - \alpha_{1(j,\ell+k)} + \hat{a}_{(i)}\}_{k\in[\rho]}\}_{j\in[\xi]}$
5: $\boldsymbol{\theta} \leftarrow \mathsf{H}_{\mathbb{Z}_q^{\ell\times\rho}}(\mathrm{sid} \,||\, \tilde{\boldsymbol{a}})$
6: $\boldsymbol{\eta} \leftarrow \{\hat{a}_{(k)} + \sum_{i=1}^{\ell} \theta_{(i,k)} \cdot a_{(i)}\}_{k\in[\rho]}$
7: $\boldsymbol{\mu} \leftarrow \{\{\alpha_{0(j,\ell+k)} + \sum_{i=1}^{\ell} \theta_{(i,k)} \cdot \alpha_{0(j,i)}\}_{k\in[\rho]}\}_{j\in[\xi]}$
8: $\mu \leftarrow \mathsf{H}_{2\kappa}(\mathrm{sid} \,||\, \boldsymbol{\mu})$
9: $\mathsf{Send}(\tilde{\boldsymbol{a}}, \boldsymbol{\eta}, \mu) \to \mathcal{P}_B$
return $\boldsymbol{c}$ as the output share of $\mathcal{P}_A$

$\mathcal{P}_B.\mathsf{Round3}(\tilde{\boldsymbol{a}}, \boldsymbol{\eta}, \mu) \dashrightarrow (\boldsymbol{z_B})$
1: $\boldsymbol{\theta} \leftarrow \mathsf{H}_{\mathbb{Z}_q^{\ell\times\rho}}(\mathrm{sid} \,||\, \tilde{\boldsymbol{a}})$
2: $\dot{\boldsymbol{d}} \leftarrow \{\{\gamma_{(j,i)} + \beta_{(j)} \cdot \tilde{a}_{(j,i)}\}_{i\in[\ell]}\}_{j\in[\xi]}$
3: $\boldsymbol{d} \leftarrow \{\sum_{j=1}^{\xi} g_{(j)} \cdot \dot{d}_{(j,i)}\}_{i\in[\ell]}$
4: $\hat{\boldsymbol{d}} \leftarrow \{\{\gamma_{(j,\ell+k)} + \beta_{(j)} \cdot \tilde{a}_{(j,\ell+k)}\}_{k\in[\rho]}\}_{j\in[\xi]}$
5: $\boldsymbol{\mu'} \leftarrow \{\{\hat{d}_{(j,k)} + \sum_{i=1}^{\ell} \theta_{(i,k)} \cdot \dot{d}_{(j,i)} - \beta_{(j)} \cdot \eta_{(k)}\}_{k\in[\rho]}\}_{j\in[\xi]}$
6: $\mu' \leftarrow \mathsf{H}_{2\kappa}(\mathrm{sid} \,||\, \boldsymbol{\mu'})$
7: Check if $\mu' \stackrel{?}{=} \mu$, ABORT otherwise
return $\boldsymbol{d}$ as the output share of $\mathcal{P}_B$

References

[DKLs23] Jack Doerner, Yashvanth Kondi, Eysa Lee, and A. shelat. Threshold ecdsa in three rounds. *Cryptology ePrint Archive*, 2023.