
Protocol $\text{ROTe}_{\xi,\ell}(\mathbf{x}) \rightarrow (\mathbf{m}_0, \mathbf{m}_1, \mathbf{m}_x)$

Maliciously secure ROT extension protocol from SoftSpokenOT [Roy22] for a batch with ξ messages of $\ell \times \kappa$ bits each, setting $\eta = \xi \times \ell \times \kappa$ and $\mu = \eta/\sigma$. It uses a pseudo-random generator $\text{PRG}: \mathbb{Z}_2^\kappa \mapsto \mathbb{Z}_2^{\eta'}$ for $\eta' = \eta + \sigma$ (e.g., $\text{TmmoHash}_{\eta'}$), a transcript T (e.g., Scheme ??), a base OT (BBOT) and a hash $\mathsf{H}: \mathbb{Z}_2^\kappa \mapsto \mathbb{Z}_2^\kappa$

Players: sender \mathcal{S} , and receiver \mathcal{R}

Inputs: $\mathcal{R}: \mathbf{x} \in \mathbb{Z}_2^\xi$, the choice bits

Outputs: $\mathcal{S}: \mathbf{m}_0, \mathbf{m}_1 \in \mathbb{Z}_2^\eta$, pairs of random messages

$\mathcal{R}: \mathbf{m}_x \in \mathbb{Z}_2^\eta$, chosen messages such that

$$m_{x(i,j)} = m_{0(i,j)}x_{(i)} \oplus m_{1(i,j)}(1 - x_{(i)}) \quad \forall i \in [\xi] \quad \forall j \in [\ell]$$

$\mathcal{S} \& \mathcal{R}. \text{Setup}() \dashrightarrow \mathcal{S}: (\mathbf{k}_0, \mathbf{k}_1); \mathcal{R}: \mathbf{k}_b$

- 1: \mathcal{S} samples $\mathbf{b} \stackrel{\$}{\leftarrow} \mathbb{Z}_2^\kappa$ as the base OT choice bits
- 2: \mathcal{R} runs $\text{BBOT}_\kappa()$ as the base OT sender, obtaining $\mathbf{k}_0, \mathbf{k}_1 \in \mathbb{Z}_2^{\kappa \times \kappa}$
- 3: \mathcal{S} runs $\text{BBOT}_\kappa(\mathbf{b})$ as the base OT receiver, receiving $\mathbf{k}_b \in \mathbb{Z}_2^{\kappa \times \kappa}$

$\mathcal{R}. \text{Round1}(\mathbf{x} \in \mathbb{Z}_2^\xi) \dashrightarrow \mathcal{U}, \dot{\mathbf{x}}, \dot{\mathbf{t}}, \mathbf{m}_x$

- 1: Set $\mathbf{x}_{\text{rep}} \leftarrow \{\{x_{(i)}, x_{(i)}, \dots, x_{(i)}\}_{\ell}\}_{i \in [\xi]}$ by repeating ℓ times \mathbf{x}
 - 2: Sample $\mathbf{x}_\sigma \stackrel{\$}{\leftarrow} \mathbb{Z}_2^\sigma$ and concatenate $\mathbf{x}' \leftarrow \mathbf{x}_{\text{rep}} \parallel \mathbf{x}_\sigma$
 - 3: Extend $(\mathbf{t}_0, \mathbf{t}_1) \leftarrow \{\text{PRG}(k_{0(i)}), \text{PRG}(k_{1(i)})\}_{i \in [\kappa]}$ with $\mathbf{t}_0, \mathbf{t}_1 \in \mathbb{Z}_2^{\kappa \times \eta'}$
 - 4: $\mathbf{u} \leftarrow \{\{t_{0(i,j)} \oplus t_{1(i,j)} \oplus x'_{(j)}\}_{j \in [\eta']}_{i \in [\kappa]}$ with $\mathbf{u} \in \mathbb{Z}_2^{\kappa \times \eta'}$
 - 5: Run $\mathsf{T}. \text{Append}(\mathbf{u})$ and $\chi \leftarrow \mathsf{T}. \text{Extract}(\eta)$ to get the challenge $\chi \in \mathbb{Z}_2^{\mu \times \sigma}$
 - 6: Compute the challenge response $(\dot{\mathbf{x}}, \dot{\mathbf{t}})$ as:
 - 6.a: $\dot{\mathbf{x}} \leftarrow \{x_{\sigma(k)} \oplus \bigoplus_{m=1}^\mu \chi_{(m,k)} \cdot x_{\text{rep}(\sigma m+k)}\}_{k \in [\sigma]}$ with $\dot{\mathbf{x}} \in \mathbb{Z}_2^\sigma$
 - 6.b: $\dot{\mathbf{t}} \leftarrow \{\{t_{0(i,\eta+k)} \oplus \bigoplus_{m=1}^\mu \chi_{(m,k)} \cdot t_{0(i,\sigma m+k)}\}_{k \in [\sigma]}\}_{i \in [\kappa]}$ with $\dot{\mathbf{t}} \in \mathbb{Z}_2^{\kappa \times \sigma}$
 - 7: Transpose $\mathbf{t}'_0 \leftarrow \{\{t_{0(i,j)}\}_{i \in [\kappa]}\}_{j \in [\eta']}$ with $\mathbf{t}'_0 \in \mathbb{Z}_2^{\eta' \times \kappa}$
 - 8: $\text{Send}(\mathbf{u}, \dot{\mathbf{x}}, \dot{\mathbf{t}}) \rightarrow \mathcal{S}$
 - 9: $\mathbf{m}_x \leftarrow \{\{\mathsf{H}(j \parallel t'_{0(j\ell+l)})\}_{l \in [\ell]}\}_{j \in [\eta]}$
- return** \mathbf{m}_x

$\mathcal{S}. \text{Round2}(\mathbf{u}, \dot{\mathbf{x}}, \dot{\mathbf{t}}) \dashrightarrow (\mathbf{m}_0, \mathbf{m}_1)$

- 1: Extend $\mathbf{t}_b \leftarrow \{\text{PRG}(k_{b(i)})\}_{i \in [\kappa]}$ with $\mathbf{t}_b \in \mathbb{Z}_2^{\kappa \times \eta'}$
 - 2: $\mathbf{q} \leftarrow \{\{b_{(i)} \cdot u_{(i,j)} \oplus t_{b(i,j)}\}_{j \in [\eta']}\}_{i \in [\kappa]}$ with $\mathbf{q} \in \mathbb{Z}_2^{\kappa \times \eta'}$
 - 3: Run $\mathsf{T}. \text{Append}(\mathbf{u})$ and $\chi \leftarrow \mathsf{T}. \text{Extract}(\eta)$ to get the challenge $\chi \in \mathbb{Z}_2^{\mu \times \sigma}$
 - 4: Verify the challenge response:
 - 4.a: $\dot{\mathbf{q}} \leftarrow \{\{q_{(i,\eta+k)} \oplus \bigoplus_{m=1}^\mu \chi_{(m,k)} \cdot q_{(i,\sigma m+k)}\}_{k \in [\sigma]}\}_{i \in [\kappa]}$ with $\dot{\mathbf{q}} \in \mathbb{Z}_2^{\kappa \times \sigma}$
 - 4.b: Check $q_{(i,k)} \stackrel{?}{=} \dot{q}_{(i,k)} \quad \forall i \in [\kappa] \quad \forall k \in [\eta']$; otherwise **ABORT**
 - 5: Transpose $\mathbf{q}' \leftarrow \{\{q_{(i,j)}\}_{i \in [\kappa]}\}_{j \in [\eta']}$ with $\mathbf{q}' \in \mathbb{Z}_2^{\eta' \times \kappa}$
 - 6: $(\mathbf{m}_0, \mathbf{m}_1) \leftarrow \{\{\mathsf{H}(j \parallel q'_{(j)}) \parallel \mathsf{H}(j \parallel (q_{(j\ell+l)} \oplus b_{(j\ell+l)}))\}_{l \in [\ell]}\}_{j \in [\xi]}$
- return** $(\mathbf{m}_0, \mathbf{m}_1)$
-

References

- [Roy22] Lawrence Roy. Softspokenot: Quieter ot extension from small-field silent vole in the minicrypt model. In *Advances in Cryptology-CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part I*, pages 657–687. Springer, 2022.