| | Signature | PKE, Revised PKE | Pre-Shared Key |
|---|---|---|---|
| $prf_I$ | $\mathsf{PRF}_k(g^x, g^y, \mathsf{cky_I}, \mathsf{cky_R}, \overrightarrow{SA}, ID_I)$ | | |
| $prf_R$ | $\mathsf{PRF}_k(g^y, g^x, \mathsf{cky_R}, \mathsf{cky_I}, \overrightarrow{SA}, ID_R)$ | | |
| $\sigma_X$ | $\mathsf{Sign}(sk_X, prf_X)$ | - | - |
| $c_5$ | $\mathsf{Enc}(k_2; ID_I, cert_I, \sigma_I)$ | $\mathsf{Enc}(k_2; prf_I)$ | $\mathsf{Enc}(k_2; ID_I, prf_I)$ |
| $c_6$ | $\mathsf{Enc}(k_2; ID_R, cert_R, \sigma_R)$ | $\mathsf{Enc}(k_2; prf_R)$ | $\mathsf{Enc}(k_2; ID_R, prf_R)$ |