

TLS-Encrypted

TLS-Encrypted

TLS-Encrypted

OP

OR1

OR2

OR<sub>i</sub>Create C1  $\text{Enc}(K_{\text{or1}}, g^{x1})$ Created C1  $g^{y1} \text{Hash}(g^{x1y1})$ C1  $\text{Enc}(g^{x1y1}, [\text{Extend}, \text{OR2 } \text{Enc}(K_{\text{or2}}, g^{x2})])$ Create C2  $\text{Enc}(K_{\text{or2}}, g^{x2})$ Created C2  $g^{y2} \text{Hash}(g^{x2y2})$ C1  $\text{Enc}(g^{x1y1}, [\text{Extended}, g^{y2} \text{Hash}(g^{x2y2})])$ C1  $\text{Enc}(g^{x1y1}, \text{Enc}(g^{x2y2}, [\text{Extend}, \text{OR3 } \text{Enc}(K_{\text{or3}}, g^{x3})]))$ C2  $\text{Enc}(g^{x2y2}, [\text{Extend}, \text{OR3 } \text{Enc}(K_{\text{or3}}, g^{x3})])$ Create C3  $\text{Enc}(K_{\text{or3}}, g^{x3})$ Created C3  $g^{y3} \text{Hash}(g^{x3y3})$ C2  $\text{Enc}(g^{x2y2}, [\text{Extended}, g^{y3} \text{Hash}(g^{x3y3})])$ C1  $\text{Enc}(g^{x1y1}, \text{Enc}(g^{x2y2}, [\text{Extended}, g^{y3} \text{Hash}(g^{x3y3})]))$