

Challenger

A

$(P, x, y, z) \leftarrow \text{Setup}(G, n);$

$\text{ID}_{\text{RP1}} = P; \text{ID}_{\text{RP2}} = xP$

$\xrightarrow{\text{ID}_{\text{RP1}}, \text{ID}_{\text{RP2}}}$

$(n_1, n_2, n_3) \leftarrow \text{Random}(n)$

$\xleftrightarrow[n_1, n_2, n_3]{\text{ID}_{\text{RP1}}, \text{ID}_{\text{RP2}}}$

if $\text{Verify}(\text{ID}_{\text{RP1}}, \text{PID}_{\text{RP1}}, n_1)$

then $\text{PID}_{\text{U1}} \leftarrow F_{\text{PIDu}}(y, \text{PID}_{\text{RP1}})$

$\xleftarrow{\text{PID}_{\text{RP1}}}$

$\xrightarrow{\text{PID}_{\text{U1}}}$

$(\text{PID}_{\text{RP1}}, \text{PID}_{\text{RP2}}, \text{PID}_{\text{RP3}}) \leftarrow$

$A_I(\text{ID}_{\text{RP1}}, \text{ID}_{\text{RP2}}, n_1, n_2, n_3)$

$\xleftarrow{\text{PID}_{\text{RP2}}}$

$\xrightarrow{\text{PID}_{\text{U2}}}$

if $\text{Verify}(\text{ID}_{\text{RP2}}, \text{PID}_{\text{RP2}}, n_2)$

then $b \leftarrow_{\text{R}} \{0, 1\}; r \leftarrow \text{Random}(n);$

$u \leftarrow \{z, r\}; \text{PID}_{\text{U2}} \leftarrow F_{\text{PIDu}}(u_b, \text{ID}_{\text{RP1}})$

$\xleftarrow{\text{PID}_{\text{RP3}}}$

$\xrightarrow{\text{PID}_{\text{U3}}}$

if $\text{Verify}(\text{ID}_{\text{RP2}}, \text{PID}_{\text{RP3}}, n_3)$

then $\text{PID}_{\text{U3}} \leftarrow F_{\text{PIDu}}(u_{(1-b)}, \text{ID}_{\text{RP1}})$

$\xleftarrow{b'}$

$b' \leftarrow A_2(\text{ID}_{\text{RP1}}, \text{ID}_{\text{RP2}}, n_1, n_2, n_3, \text{PID}_{\text{U1}}, \text{PID}_{\text{U2}}, \text{PID}_{\text{U3}})$