

Challenger

A

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

$ID_{RP1} = P; ID_{RP2} = xP$

$\xrightarrow{ID_{RP1}, ID_{RP2}}$

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

$\xleftarrow{\frac{ID_{RP1}, ID_{RP2}}{n_1, n_2, n_3}}$

$\text{Verify}(ID_{RP1}, PID_{RP1}, n_1);$

$PID_{U1} \leftarrow F_{PIDu}(y, PID_{RP1})$

$\xleftarrow{PID_{RP1}}$

$\xrightarrow{PID_{U1}}$

$(PID_{RP1}, PID_{RP2}, PID_{RP3}) \leftarrow A_I(ID_{RP1}, ID_{RP2}, ID_{RP3}, n_1, n_2, n_3)$

$\text{Verify}(ID_{RP2}, PID_{RP2}, n_2);$

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

$u \leftarrow \{y, r\}; PID_{U2} \leftarrow F_{PIDu}(u_b, PID_{RP2})$

$\xleftarrow{PID_{RP2}}$

$\xrightarrow{PID_{U2}}$

$\text{Verify}(ID_{RP2}, PID_{RP3}, n_3);$

$PID_{U3} \leftarrow F_{PIDu}(u_{(1-b)}, PID_{RP3})$

$\xleftarrow{PID_{RP3}}$

$\xrightarrow{PID_{U3}}$

$\xleftarrow{b'}$

$b' \leftarrow A_2(ID_{RP1}, ID_{RP2}, ID_{RP3}, n_1, n_2, n_3, PID_{U1}, PID_{U2}, PID_{U3})$