

Challenger

A

$(ID_{RP1}, ID_{RP2}, u_1, u_2) \leftarrow Setup(G, n)$

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

$(n_1, n_2, n_3) \leftarrow Random(n)$

$\xrightarrow{\overline{ID_{RP1}}}$

n_1

$\xrightarrow{\overline{ID_{RP2}}}$

n_2

$\xrightarrow{\overline{ID_{RP2}}}$

n_3

if $Verify(ID_{RP1}, PID_{RP1}, n_1)$
then $PID_{U1} \leftarrow F_{PIDu}(u_1, PID_{RP1})$

$\xleftarrow{PID_{RP1}}$

$\xrightarrow{PID_{U1}}$

$\xleftarrow{PID_{RP2}}$

if $Verify(ID_{RP2}, PID_{RP2}, n_2)$
then $b \leftarrow_R \{0, 1\}; u \leftarrow \{u_1, u_2\};$
 $PID_{U2} \leftarrow F_{PIDu}(u_b, PID_{RP2})$

$\xrightarrow{PID_{U2}}$

$\xleftarrow{PID_{RP3}}$

if $Verify(ID_{RP2}, PID_{RP3}, n_3)$
then $PID_{U3} \leftarrow F_{PIDu}(u_{(1-b)}, PID_{RP3})$

$\xrightarrow{PID_{U3}}$

$\xleftarrow{b'}$

$(PID_{RP1}, PID_{RP2}, PID_{RP3}) \leftarrow$
 $A_1(ID_{RP1}, ID_{RP2}, n_1, n_2, n_3)$

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