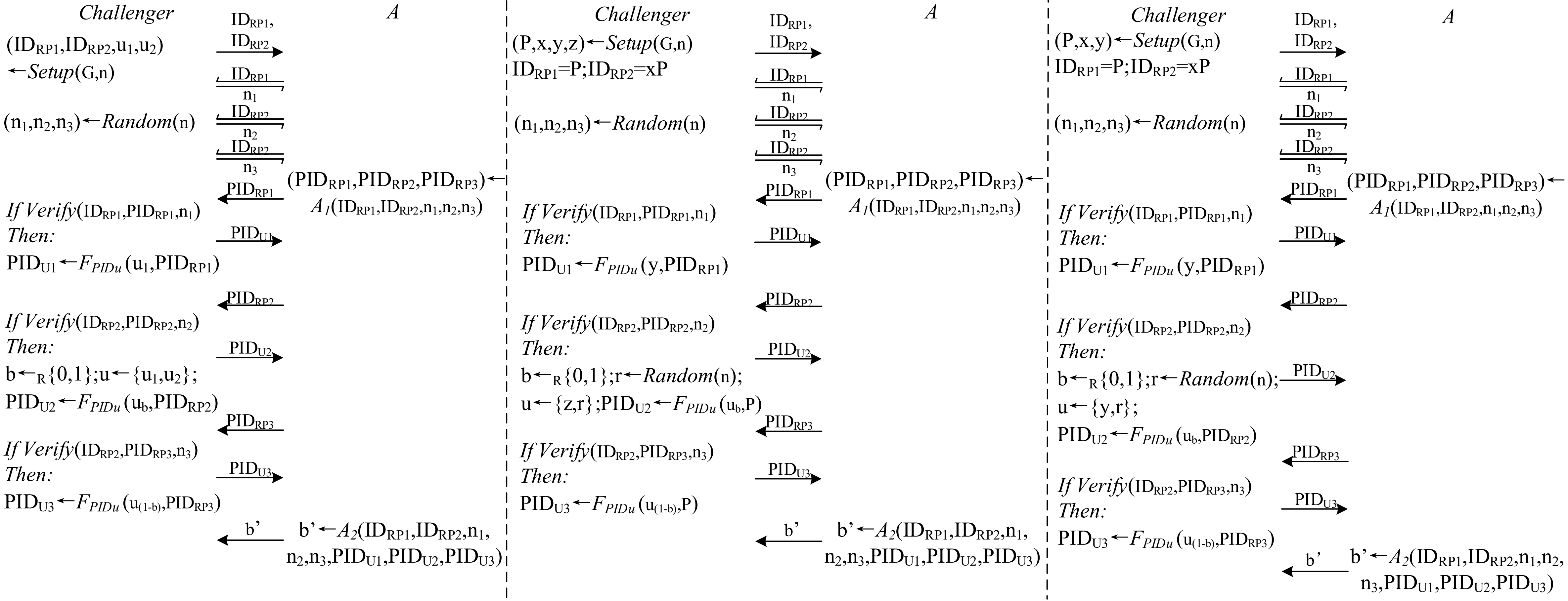
Challenger
A
$(ID_{RP1}, ID_{RP2}, u_1, u_2) \leftarrow Setup(G,n)$
ID_{RP1}, ID_{RP2}
ID_{RP1}
n_1
$(n_1,n_2,n_3) \leftarrow Random(n)$
ID_{RP2}
n_2
ID_{RP2}
n_3
$(PID_{RP1},PID_{RP2},PID_{RP3}) \leftarrow A_1(ID_{RP1},ID_{RP2},n_1,n_2,n_3)$
PID_{RP1}
If $Verify(ID_{RP1},PID_{RP1},n_1)$ Then:
$PID_{U1} \leftarrow F_{PIDu}(u_1,PID_{RP1})$
PID_{U1}
PID_{RP2}
If $Verify(ID_{RP2},PID_{RP2},n_2)$ Then:
$b \leftarrow_R \{0,1\}; u \leftarrow \{u_1,u_2\};$
$PID_{U2} \leftarrow F_{PIDu}(u_b,PID_{RP2})$
PID_{U2}
PID_{RP3}
If $Verify(ID_{RP2},PID_{RP3},n_3)$ Then:
$PID_{U3} \leftarrow F_{PIDu}(u_{(1-b)},PID_{RP3})$
PID_{U3}
b'
$b' \leftarrow A_2(ID_{RP1},ID_{RP2},n_1,n_2,n_3,PID_{U1},PID_{U2},PID_{U3})$
Game 0
Challenger
A
$(P,x,y,z) \leftarrow Setup(G,n)$
$ID_{RP1}=P; ID_{RP2}=xP$
ID_{RP1}, ID_{RP2}
ID_{RP1}
n_1
$(n_1,n_2,n_3) \leftarrow Random(n)$
ID_{RP2}
n_2
ID_{RP2}
n_3
$(PID_{RP1},PID_{RP2},PID_{RP3}) \leftarrow A_1(ID_{RP1},ID_{RP2},n_1,n_2,n_3)$
PID_{RP1}
If $Verify(ID_{RP1},PID_{RP1},n_1)$ Then:
$PID_{U1} \leftarrow F_{PIDu}(y,PID_{RP1})$
PID_{U1}
PID_{RP2}
If $Verify(ID_{RP2},PID_{RP2},n_2)$ Then:
$b \leftarrow_R \{0,1\}; r \leftarrow Random(n);$
$u \leftarrow \{z,r\}; PID_{U2} \leftarrow F_{PIDu}(u_b,P)$
PID_{U2}
PID_{RP3}
If $Verify(ID_{RP2},PID_{RP3},n_3)$ Then:
$PID_{U3} \leftarrow F_{PIDu}(u_{(1-b)},P)$
PID_{U3}
b'
$b' \leftarrow A_2(ID_{RP1},ID_{RP2},n_1,n_2,n_3,PID_{U1},PID_{U2},PID_{U3})$
Game 1
Challenger
A
$(P,x,y) \leftarrow Setup(G,n)$
$ID_{RP1}=P; ID_{RP2}=xP$
ID_{RP1}, ID_{RP2}
ID_{RP1}
n_1
$(n_1,n_2,n_3) \leftarrow Random(n)$
ID_{RP2}
n_2
ID_{RP2}
n_3
$(PID_{RP1},PID_{RP2},PID_{RP3}) \leftarrow A_1(ID_{RP1},ID_{RP2},n_1,n_2,n_3)$
PID_{RP1}
If $Verify(ID_{RP1},PID_{RP1},n_1)$ Then:
$PID_{U1} \leftarrow F_{PIDu}(y,PID_{RP1})$
PID_{U1}
PID_{RP2}
If $Verify(ID_{RP2},PID_{RP2},n_2)$ Then:
$b \leftarrow_R \{0,1\}; r \leftarrow Random(n);$
$u \leftarrow \{y,r\};$
$PID_{U2} \leftarrow F_{PIDu}(u_b,PID_{RP2})$
PID_{U2}
PID_{RP3}
If $Verify(ID_{RP2},PID_{RP3},n_3)$ Then:
$PID_{U3} \leftarrow F_{PIDu}(u_{(1-b)},PID_{RP3})$
PID_{U3}
b'
$b' \leftarrow A_2(ID_{RP1},ID_{RP2},n_1,n_2,n_3,PID_{U1},PID_{U2},PID_{U3})$
Game 2
Game 0 Game 1 Game 2