Challenger	ID_{RP1} ,	A	Challenger	ID_{RP1} ,	A	 Challenger	ID_{RP1} ,	A
$(ID_{RP1},ID_{RP2},u_1,u_2)$	ID_{RP2}	 	$(P,x,y,z) \leftarrow Setup(G,n)$	ID_{RP2}		$(P,x,y) \leftarrow Setup(G,n)$	ID_{RP2}	•
$\leftarrow Setup(G,n)$	<u>ID_{RP1}</u>	į	$ID_{RP1}=P;ID_{RP2}=xP$, ID _{RP1}		$ ID_{RP1}=P;ID_{RP2}=xP$, ID _{RP1}	_
$(n_1,n_2,n_3) \leftarrow Random(n)$	$ \begin{array}{c} II_1\\ \underline{ID_{RP2}}\\ n_2\\ \underline{ID_{RP2}} \end{array} $		$(n_1,n_2,n_3) \leftarrow Random(n)$	n ₁ , ID _{RP2} , ID _{RP2}		$ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ $	$ \begin{array}{c} ID_{RP2} \\ \underline{ID_{RP2}} \\ ID_{RP2} \end{array} $	7
	n_3 PID_{RP1}	$(PID_{RP1},PID_{RP2},PID_{RP3}) \leftarrow$		n_3 PID_{RP1}	$(PID_{RP1},PID_{RP2},PID_{RP3}) \leftarrow$	 	n ₃ PID _{nn} ,	$(PID_{RP1},PID_{RP2},PID_{RP3}) \leftarrow$
<i>If</i> $Verify(ID_{RP1},PID_{RP1},n_1)$	₹ 1D _{RP1}	$A_I(ID_{RP1},ID_{RP2},n_1,n_2,n_3)$	If $Verify(ID_{RP1},PID_{RP1},n_1)$	₹ ID _{RP1}	$A_I(ID_{RP1},ID_{RP2},n_1,n_2,n_3)$	If $Verify(ID_{RP1},PID_{RP1},n_1)$	₹ ID _{RPI}	$A_{I}(ID_{RP1},ID_{RP2},n_{1},n_{2},n_{3})$
Then:	PID _{U1}		Then:	PID _{UI}		Then:	PID _{U1}	•
$PID_{U1} \leftarrow F_{PIDu}(u_1, PID_{RP1})$)	İ	$PID_{U1} \leftarrow F_{PIDu}(y,PID_{RP1})$			$ PID_{U1} \leftarrow F_{PIDu}(y, PID_{RP1}) $		
	PID _{RP2}			PID_{RP2}		! 	PID _{RP2}	_
$If Verify(ID_{RP2},PID_{RP2},n_2)$	•	į	$If Verify(ID_{RP2},PID_{RP2},n_2)$	•		$If Verify(ID_{RP2},PID_{RP2},n_2)$	•	
Then:	PID _{U2}	 	Then:	PID _{U2}		! Then:		
$b \leftarrow_R \{0,1\}; u \leftarrow \{u_1,u_2\};$		 	$b \leftarrow_R \{0,1\}; r \leftarrow Random(n);$	ŕ		$b \leftarrow_{\mathbb{R}} \{0,1\}; r \leftarrow Random(n)$); <u>PID_{U2}</u>	•
$PID_{U2} \leftarrow F_{PIDu}(u_b, PID_{RP2})$)	İ	$\mathbf{u} \leftarrow \{\mathbf{z},\mathbf{r}\}; PID_{\mathbf{U}2} \leftarrow F_{PIDu}(\mathbf{u}_{b},\mathbf{r})$	P)		¹ u←{y,r};		
XCXX . (()	PID _{RP3}	 		PID _{RP3}		$ PID_{U2} \leftarrow F_{PIDu}(u_b, PID_{RP2}) $		
If $Verify(ID_{RP2},PID_{RP3},n_3)$	PID _{U3}		If $Verify(ID_{RP2},PID_{RP3},n_3)$	PID _{U3}			$ Arr PID_{RP3}$	_
Then:		İ	Then:	111003		If $Verify(ID_{RP2},PID_{RP3},n_3)$	DID	
$PID_{U3} \leftarrow F_{PIDu}(u_{(1-b)}, PID_{RP3})$)		$PID_{U3} \leftarrow F_{PIDu}(u_{(1-b)},P)$		4	¹ Then:	PID _{U3}	•
	← b′	$b' \leftarrow A_2(ID_{RP1},ID_{RP2},n_1,$		← b'	$b' \leftarrow A_2(ID_{RP1},ID_{RP2},n_1,$	$PID_{U3} \leftarrow F_{PIDu}(u_{(1-b)}, PID_{RP3})$)	1.4 (77)
		$(n_2,n_3,PID_{U1},PID_{U2},PID_{U3})$			$n_2, n_3, PID_{U1}, PID_{U2}, PID_{U3})$	 	◆ b'	$b' \leftarrow A_2(\mathrm{ID}_{\mathrm{RP1}}, \mathrm{ID}_{\mathrm{RP2}}, n_1, n_2,$
		, 				 -		n_3 ,PID _{U1} ,PID _{U2} ,PID _{U3})
	Game 0			Game 1			Game 2	