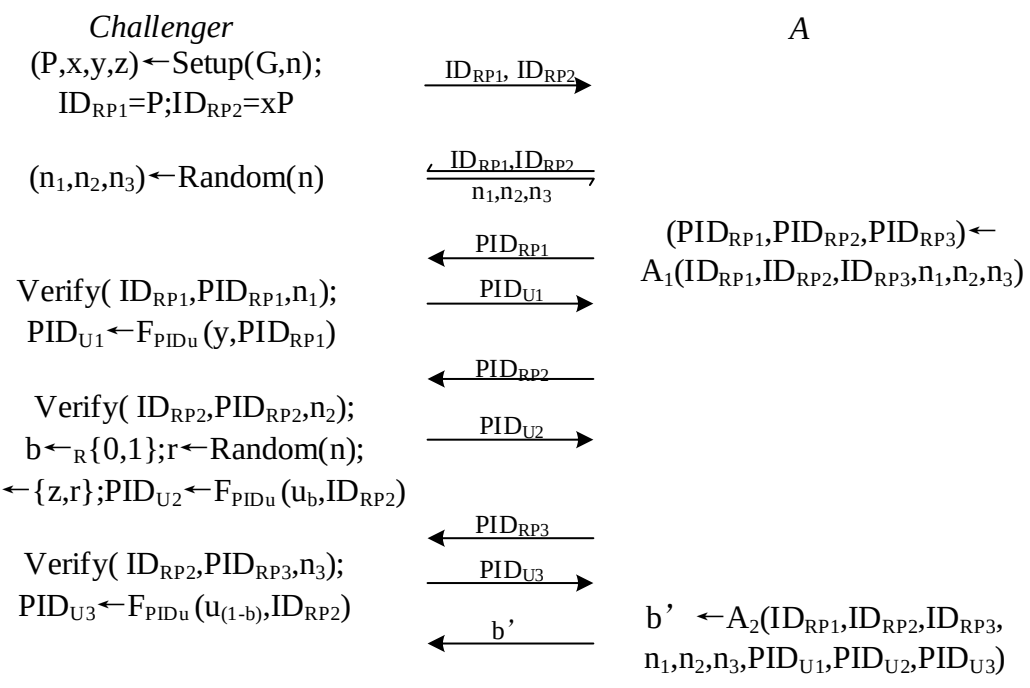
Challenger
A
(P,x,y,z)←Setup(G,n);
ID_RP1=P;ID_RP2=xP
ID_RP1, ID_RP2
(n1,n2,n3)←Random(n)
ID_RP1,ID_RP2
n1,n2,n3
PID_RP1
(PID_RP1,PID_RP2,PID_RP3)←
A1(ID_RP1,ID_RP2,ID_RP3,n1,n2,n3)
Verify(ID_RP1,PID_RP1,n1);
PID_U1←F_PIDu (y,PID_RP1)
PID_U1
PID_RP2
Verify(ID_RP2,PID_RP2,n2);
b←R{0,1};r←Random(n);
u←{z,r};PID_U2←F_PIDu (u_b,ID_RP2)
PID_U2
PID_RP3
Verify(ID_RP2,PID_RP3,n3);
PID_U3←F_PIDu (u_(1-b),ID_RP2)
PID_U3
b'
b' ←A2(ID_RP1,ID_RP2,ID_RP3,
n1,n2,n3,PID_U1,PID_U2,PID_U3)