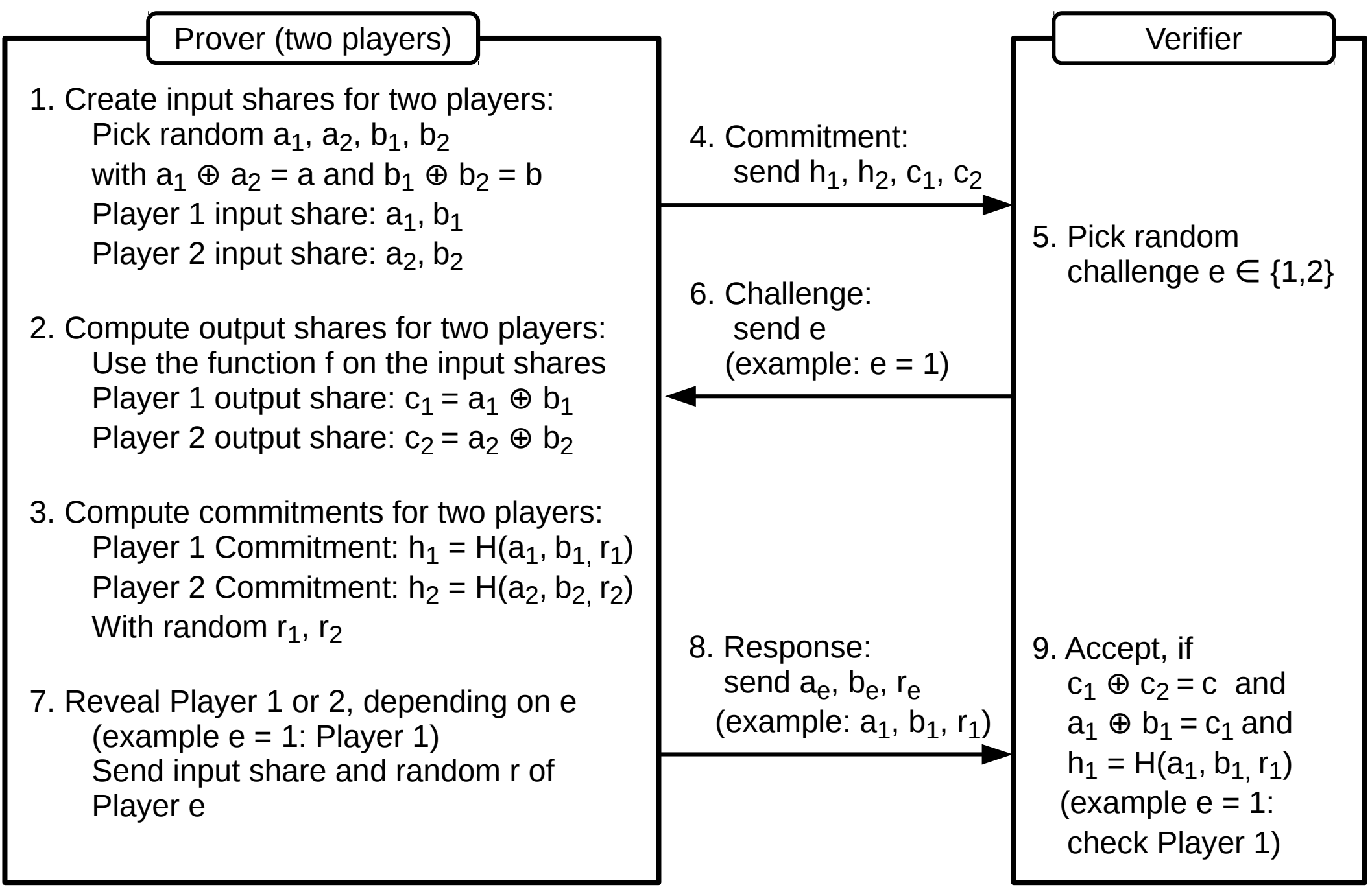
Prover (two players)
Verifier
1. Create input shares for two players:
Pick random a_1, a_2, b_1, b_2
with $a_1 \oplus a_2 = a$ and $b_1 \oplus b_2 = b$
Player 1 input share: a_1, b_1
Player 2 input share: a_2, b_2
2. Compute output shares for two players:
Use the function f on the input shares
Player 1 output share: $c_1 = a_1 \oplus b_1$
Player 2 output share: $c_2 = a_2 \oplus b_2$
3. Compute commitments for two players:
Player 1 Commitment: $h_1 = H(a_1, b_1, r_1)$
Player 2 Commitment: $h_2 = H(a_2, b_2, r_2)$
With random r_1, r_2
7. Reveal Player 1 or 2, depending on e
(example e = 1: Player 1)
Send input share and random r of
Player e
4. Commitment:
send h_1, h_2, c_1, c_2
5. Pick random
challenge e ∈ {1,2}
6. Challenge:
send e
(example: e = 1)
8. Response:
send a_e, b_e, r_e
(example: a_1, b_1, r_1)
9. Accept, if
$c_1 \oplus c_2 = c$ and
$a_1 \oplus b_1 = c_1$ and
$h_1 = H(a_1, b_1, r_1)$
(example e = 1:
check Player 1)