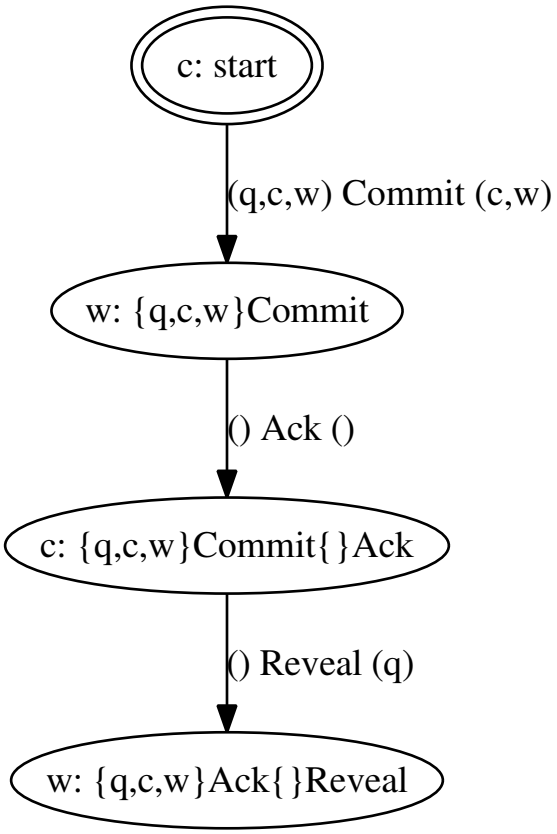
c: start
(q,c,w) Commit (c,w)
w: {q,c,w}Commit
() Ack ()
c: {q,c,w}Commit{ }Ack
() Reveal (q)
w: {q,c,w}Ack{ }Reveal