

$sk(I), pk(I), pk(R), pk(E)$

$I(\text{honest})$

nonce ni

$sk(R), pk(R), pk(I), pk(E)$

$R(\text{honest})$

$sk(E), pk(R), pk(I), pk(E)$

$E(\text{dishonest})$

$\left\{ \left\langle I, \{ni\}_{pk(R)} \right\rangle \right\}_{pk(R)}$

$\left\{ \left\langle E, \left\{ \left\langle I, \{ni\}_{pk(R)} \right\rangle \right\}_{pk(R)} \right\rangle \right\}_{pk(R)}$

$\left\{ \left\langle R, \left\{ \left\langle I, \{ni\}_{pk(R)} \right\rangle \right\}_{pk(E)} \right\rangle \right\}_{pk(E)}$

$\left\{ \left\langle E, \{ni\}_{pk(R)} \right\rangle \right\}_{pk(R)}$

$\left\{ \left\langle R, \{ni\}_{pk(E)} \right\rangle \right\}_{pk(E)}$

$\left\{ \left\langle R, \{ni\}_{pk(I)} \right\rangle \right\}_{pk(I)}$

ni is secret

