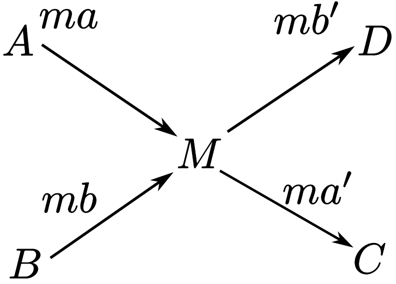
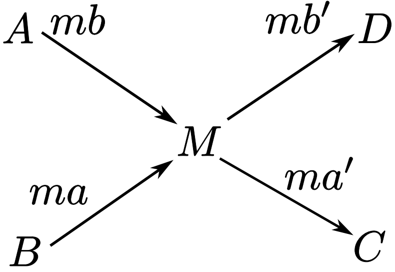


(1)



(2)

$$ma = \{\!\!\{\mathsf{Nonce}\,na, \mathsf{Agent}\,C, \{\!\!\{\mathsf{Nonce}\,na'\}\!\!\}_{\mathsf{pubK}\ C}\}\!\!\}_{\mathsf{pubK}\ M}, \; ma' = \{\!\!\{\mathsf{Nonce}\,na'\}\!\!\}_{\mathsf{pubK}\ C}$$

$$mb = \{\!\!\{\mathsf{Nonce}\,nb, \mathsf{Agent}\,D, \{\!\!\{\mathsf{Nonce}\,nb'\}\!\!\}_{\mathsf{pubK}\ D}\}\!\!\}_{\mathsf{pubK}\ M}, \; mb' = \{\!\!\{\mathsf{Nonce}\,nb'\}\!\!\}_{\mathsf{pubK}\ D}$$