

A trace has been found.

Honest Process

Attacker

!

{2}new computerId
{3}new sk
{4}new sk_auth_kem
{5}new ltdh

$(\sim M, (\sim M_1, \sim M_2, \sim M_3)) = (\text{id}(\text{pk}(\text{sk}), \text{ltdh}, \text{kempk}(\text{sk\_auth\_kem})), (\text{pk}(\text{sk}), \text{ltdh}, \text{kempk}(\text{sk\_auth\_kem})))$

{8}event eShareLT(ltdh)
{9}event eHonest(pk(sk))
{10}event eHonest(kempk(sk_auth_kem))
{11}new sk_3
{12}new sk_auth_kem_3
{13}new ltdh_3
{14}new computerId_3

$(\sim M_4, (\sim M_5, \sim M_6, \sim M_7)) = (\text{id}(\text{pk}(\text{sk}_3), \text{ltdh}_3, \text{kempk}(\text{sk\_auth\_kem}_3)), (\text{pk}(\text{sk}_3), \text{ltdh}_3, \text{kempk}(\text{sk\_auth\_kem}_3)))$

{17}event eShareLT(ltdh_3)
{18}event eHonest(pk(sk_3))
{19}event eHonest(kempk(sk_auth_kem_3))

!

!

!

!

!

Beginning of process I

$(a_1, (a_2, (a_3, a_4)))$

{292}event eMethodOk(a_1)
{293}new X_3
{294}new random_authR_3
{295}new EAD
{296}event eShare(X_3)

{300}if (choice[id(pk(sk),ltdh,kempk(sk\_auth\_kem)),  
id(pk(sk\_3),ltdh\_3,kempk(sk\_auth\_kem\_3))] ≠  
id(pk(sk\_3),ltdh\_3,kempk(sk\_auth\_kem\_3)))  
This process performs a test that may succeed on  
one side and not on the other.