APPENDIX F
EXAMPLE OF ATTACK-TRACES FOUND WITH PHOEBE

We now details on some attacks, as found by Phoebe.

Example 10 (Anonymity for PrivAuth⋆.) Phoebe shows the following run breaking anonymity of C in *PrivAuth* *.

```
[1.(a,C,1,{kb})?: (b,n1,a){⟨pubk(b),n1⟩}_a
,2.(a,C,1,{kb})!: (n2){⟨a,n1,n2⟩}_b ]
```

The run starts with a receive by agent ag = (a,C,1,[Kb]), and the intruder sent a “hello” message pretending to be b. Upon receiving the “ack” back and without decrypting its second part, the intruder deduces that the responder is a, as participants other than a would not reply to its “hello”. Also, the intruder deduces that “pubk(b) ” is in a’s whitelist.

Example 11 (Strong Sessions-Unlinkability for the Basic Hash Protocol.) Phoebe shows the following run violating the strong sessions-unlinkability of the Basic-Hash, with maxSessions = 3 and tagNames = [Tag 1, Tag 2], i.e., with more sessions than tag names. The intruder implicitly knows that there are not enough tag names to have distinct tags for three sessions.

```
[1.(t1,T,1,{})!: (n1)⟨n1,hash(⟨n1,k1⟩)⟩
,1.(t1,T,2,{})!: (n2)⟨n2,hash(⟨n2,k1⟩)⟩
,1.(t1,T,3,{})!: (n3)⟨n3,hash(⟨n3,k1⟩)⟩ ]
```

Example 12 (Sessions-Unlinkability by Key for the Tag Reader Protocol TR.) Phoebe shows the following run violating our Property 6, i.e., “weak unlinkability by key” for TR.

```
Just [1.(t1,T,1,{})!: (n1){|n1|}_k1
,1.(t2,T,2,{})!: (n2){|n2|}_k1
,1.(r1,R,1,{k1,k2})?: (){|n1|}_k1
,2.(r1,R,1,{k1,k2})!: (n3){|n3|}_k1
,2.(t1,T,1,{})?: (){|n2|}_k1
,2.(t2,T,2,{})?: (){|n1|}_k1
,3.(t1,T,1,{})!: (){|⟨n2,n1⟩|}_k1
,3.(t2,T,2,{})!: (){|⟨n1,n2⟩|}_k1 ]
```

By replaying the message of $t1$ for $t2$, the intruder deduces that they have the same shared-key with the reader.