1 Introduction

Key Protocol (NSPK, [18, 23]), as well as variants of the prot

2.2 Context-sensitive Properties

All used identifiers must be different from the IF keywords (step, section, intruder, equal, leq, not, state). The identifiers for types (

that the form of IF rules we have defined here is indeed compatible with our lazy intruder approach.

The rest of the semantics is straightforward: we have one or m

```
  SID: nat
  NA,NB,na,nb,ni: nonce

section inits:

  initial_state init1 :=
    iknows(i).
    % session 1 [A:a, B:b, KA:ka, KB:kb]
    state_Alice(0,a,b,ka,kb,ni,ni,1).
    state_Bob(0,b,a,kb,ka,ni,ni,2).
    iknows(a).iknows(b).iknows(ka).iknows(kb).
    % session 2 [A:a, B:i, KA:ka, KB:ki]
    state_Alice(0,a,b,ka,ki,ni,ni,3).
```

D2.3. The Intermediate Format

names of the involved agents, their public keys, their nonces, and a session identifier. This identifier is necessary to allow for several parallel sessions between the same agents, as it is similarly necessary in the c

```
state_Alice(0,A,B,KA,KS,ni,ni,Keyset,SID).
ceaistD435(N7(_)2.6009(A)2.6]7(_)2.60,7-7.3.603(.)2.604114Tm[(s)2.6009(t)2.
,ntlinD(taiD(B,KD),ceScKD2(<.6009(t)2.60a9(l).609(()m60s7(D)2.60a9(l)lTLT*[6
```

6 Conclusion

The IF is a low-level, simple but expressive language for specifying security protocols and their properties. IF specifications can be generated automatically by the HLPSL2IF translator from specifications written in the high-level