ance. In doing so, we see our contributions as follows.

$$S^{\square} = (S \setminus (\mathrm{state}(m_2\sigma) \,\square\, \overline{P_1}\sigma)) \,\square\, \mathrm{state}(m_3\sigma)$$
$$\square\, \mathrm{i\_knows}(m_4\sigma) \,\square\, P_2\sigma \} \,. \qquad (9)$$

Here and elsewhere, we simplify notatioT for singletoT

ents, i.e., overloading notation,⟦{c

This rule is the same as ours, except that the constraint
governing the derivavlesin293(ofpt)-3.6(t)8.3(h)7(e)0328.k(v)27.2yls

Intuitively, (10) requires that the intruder knowledge increase monotonically, and (11) requires that every vari-

intruder knowledge) is often neglected in other presentations of symbolic intruder approaches. One solution is to proceed on demand: a message in the intruder knowledge is analyzed iff the result of this analysis can be unified with a message the intruder has to generate. We adopt

would have 24 instances. However, under the demand-driven strategy of the lazy intruder, not all of these in-

Table 1. Performance of OFMC over the flawed protocols of the Clark/

49. Thayer Fábrega FJ, Herzog JC, Guttman JD (1999) Strand spaces: proving security protocols correct. J Comput Secur 7:191–230
50. Turuani M (2003) Sécurit´