**SPASS Protocol Analyzer**

**Neumann-Stubblebine Protocol – 25/04/2014

Prof. Bosco

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**begin\_problem(SPASS\_Completion\_With\_Query).**

**list\_of\_descriptions.**

 **name({\*Neumann-Stubblebine\*}).**

 **author({\*Christoph Weidenbach\*}).**

 **status(unsatisfiable).**

 **description({\* Fact2: see the paper Christoph Weidenbach, 1999,**

 **"Towards an Automatic Analysis of Security Protocols in First-Order Logic",**

 **16th International Conference on Automated Deduction, CADE-16, LNAI 1632 \*}).**

**end\_of\_list.**

**list\_of\_symbols.**

 **functions[(tb, 1), (nb, 1), (na, 0), (at, 0), (bt, 0), (t, 0), (b, 0), (a, 0), (kt, 1), (encr, 2), (sent, 3), (key, 2), (quadr, 4), (triple, 3), (pair, 2)].**

 **predicates[(P, 1), (Bf, 1), (Tk, 1), (Sb, 1), (Bk, 1), (Sa, 1), (Ak, 1), (M, 1)].**

**end\_of\_list.**

**list\_of\_formulae(axioms).**

**formula(or(Bk(key(kt(na),a))),34).**

 **formula(or(M(sent(a,b,pair(encr(triple(a,kt(na),tb(na)),bt),encr(nb(na),kt(na)))))),31).**

 **formula(or(Ak(key(kt(na),b))),32).**

 **formula(or(M(sent(t,a,triple(encr(quadr(b,na,kt(na),tb(na)),at),encr(triple(a,kt(na),tb(na)),bt),nb(na))))),28).**

 **formula(or(M(sent(b,t,triple(b,nb(na),encr(triple(a,na,tb(na)),bt))))),19).**

 **formula(or(Sb(pair(a,na))),17).**

 **formula(or(M(sent(a,b,pair(a,na)))),10).**

 **formula(or(Tk(key(bt,b))),5).**

 **formula(or(Tk(key(at,a))),6).**

 **formula(or(Bk(key(bt,t))),7).**

 **formula(or(Sa(pair(b,na))),8).**

 **formula(or(Ak(key(at,t))),9).**

 **formula(or(P(t)),1).**

 **formula(or(Bf(na)),2).**

 **formula(or(P(b)),3).**

 **formula(or(P(a)),4).**

**end\_of\_list.**

**list\_of\_formulae(conjectures).**

 **formula(exists([x],and(Ak(key(x,b)),Bk(key(x,a))))).**

**end\_of\_list.**

**end\_problem.**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Your WebSPASS form submission is now being processed ...**

--------------------------SPASS-START-----------------------------

Input Problem:

1[0:Inp] || -> P(a)\*.

2[0:Inp] || -> P(b)\*.

3[0:Inp] || -> Bf(na)\*.

4[0:Inp] || -> P(t)\*.

5[0:Inp] || -> Ak(key(at,t))\*.

6[0:Inp] || -> Sa(pair(b,na))\*.

7[0:Inp] || -> Bk(key(bt,t))\*.

8[0:Inp] || -> Tk(key(at,a))\*.

9[0:Inp] || -> Tk(key(bt,b))\*.

10[0:Inp] || -> Sb(pair(a,na))\*.

11[0:Inp] || -> Ak(key(kt(na),b))\*.

12[0:Inp] || -> Bk(key(kt(na),a))\*.

13[0:Inp] || -> M(sent(a,b,pair(a,na)))\*.

14[0:Inp] || Bk(key(U,a))\* Ak(key(U,b)) -> .

15[0:Inp] || -> M(sent(b,t,triple(b,nb(na),encr(triple(a,na,tb(na)),bt))))\*.

16[0:Inp] || -> M(sent(a,b,pair(encr(triple(a,kt(na),tb(na)),bt),encr(nb(na),kt(na)))))\*.

17[0:Inp] || -> M(sent(t,a,triple(encr(quadr(b,na,kt(na),tb(na)),at),encr(triple(a,kt(na),tb(na)),bt),nb(na))))\*.

 This is a monadic Horn problem without equality.

 The following monadic predicates have finite extensions: M, Sb, Tk, Bk, Sa, Ak, Bf, P.

 Axiom clauses: 16 Conjecture clauses: 1

 Inferences: IORe=1

 Reductions: RFMRR=1 RBMRR=1 RObv=1 RUnC=1 RTaut=1 RFSub=1 RBSub=1 RCon=1

 Extras : Input Saturation, Dynamic Selection, No Splitting, Full Reduction, Ratio: 5, FuncWeight: 1, VarWeight: 1

 Precedence: tb > nb > kt > encr > key > pair > sent > triple > quadr > div > id > P > Bf > Tk > Sb > Bk > Sa > Ak > M > na > at > bt > t > b > a

 Ordering : KBO

Processed Problem:

Worked Off Clauses:

Usable Clauses:

3[0:Inp] || -> Bf(na)\*.

4[0:Inp] || -> P(t)\*.

2[0:Inp] || -> P(b)\*.

1[0:Inp] || -> P(a)\*.

10[0:Inp] || -> Sb(pair(a,na))\*.

6[0:Inp] || -> Sa(pair(b,na))\*.

9[0:Inp] || -> Tk(key(bt,b))\*.

8[0:Inp] || -> Tk(key(at,a))\*.

5[0:Inp] || -> Ak(key(at,t))\*.

7[0:Inp] || -> Bk(key(bt,t))\*.

11[0:Inp] || -> Ak(key(kt(na),b))\*.

12[0:Inp] || -> Bk(key(kt(na),a))\*.

19[0:Res:11.0,14.1] || Bk(key(kt(na),a))\* -> .

13[0:Inp] || -> M(sent(a,b,pair(a,na)))\*.

14[0:Inp] || Ak(key(U,b)) Bk(key(U,a))\* -> .

15[0:Inp] || -> M(sent(b,t,triple(b,nb(na),encr(triple(a,na,tb(na)),bt))))\*.

16[0:Inp] || -> M(sent(a,b,pair(encr(triple(a,kt(na),tb(na)),bt),encr(nb(na),kt(na)))))\*.

17[0:Inp] || -> M(sent(t,a,triple(encr(quadr(b,na,kt(na),tb(na)),at),encr(triple(a,kt(na),tb(na)),bt),nb(na))))\*.

SPASS V 3.0

SPASS beiseite: Proof found.

Problem: /tmp/webspass-webform\_2014-04-25\_18:31:24\_28006l.txt

SPASS derived 2 clauses, backtracked 0 clauses and kept 18 clauses.

SPASS allocated 511 KBytes.

SPASS spent 0:00:00.01 on the problem.

 0:00:00.00 for the input.

 0:00:00.00 for the FLOTTER CNF translation.

 0:00:00.00 for inferences.

 0:00:00.00 for the backtracking.

 0:00:00.00 for the reduction.

--------------------------SPASS-STOP------------------------------

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***