Lowe's modified version of Yahalom

Author(s): Paulson 0, 2001
Last modified October 4, 2002

Summary: Lowe's modified version of the Yahalom protocol. Symmetric keys and trusted server.

Protocol specification (in common syntax)

```
A, B, S :        principal
Na, Nb :         number fresh
Kas, Kbs, Kab :  key

A knows :  A, B, S, Kas
B knows :  B, S, Kbs
S knows :  S, A, B, Kas, Kbs

1.    A  ->  B   :    A, Na
2.    B  ->  S   :    {A, Na, Nb}Kbs
3.    S  ->  A   :    {B, Kab, Na, Nb}Kas
4.    S  ->  B   :    {A, Kab}Kbs
5.    A  ->  B   :    {A, B, S, Nb}Kab
```

Remark

This version of the Yahalom protocol is presented in [Low98] to illustrate a verification technique by model checking.

Requirements

See Yahalom.

References

[Low98]

Claimed proofs

[Low98]

See also

Yahalom,
BAN simplified version of Yahalom,
Paulson's strengthened version of Yahalom.

Citations

[Low98] Gavin Lowe. Towards a completeness result for model checking of security protocols. Technical Report 1998/6, Dept. of Mathematics and Computer Science, University of Leicester, 1998.