Li, Mengjun; Li, Zhoujun; Chen, Huowang
SPVT: an efficient verification tool for security protocols. (Chinese. English summary)

Summary: This paper describes the security protocol verifier SPVT developed by Objective-Caml. In SPVT (security protocol verifying tool), the specification language is a \(\pi\)-like calculus extended with three appendixes. The simplified Needham-Schroeder public-key authentication protocol is used to exemplify the automatic verification process of security protocols with SPVT, and the results show the validity of the verifier.

MSC:
68P25 Data encryption (aspects in computer science)
68M12 Network protocols
68M10 Network design and communication in computer systems

Software:
OCaml; SPVT-II

Full Text: DOI