Stand Space Theory and its Application on SET Protocol

Xu Feng[1, 2], Li Dake[2], Huang Hao[1]
[1]Department of Computer Science, Nanjing University, Nanjing, Jiang Su 210093, China
[2]College of Computer & Information Engineering, Hohai University, Nanjing, Jiang Su 210098, China
E-mail: njxufeng@163.com **Tel:** 13951835506

ABSTRACT

This paper detailed introduces Strand space theory - an advanced method of protocol analysis. Then, uses it to analyze Secure Electronic Transaction (SET) protocol and prove its secrecy property.

Keywords: Strand space; Secure Electronic Transaction protocol; protocol proof; formal method; secrecy property (For the completeness of this paper, we introduce the theory of strand space firstly. So from section 1 to section 4 is based on [1])