IEICE Transactions on Communications
E86-B(5): 1679-1681

Cryptanalysis and Restriction of an Automatic Signature Scheme in Distributed Systems

Tseng, Yuh-Min

Abstract

Lin and Jan recently proposed a new automatic signature scheme using a compiler in distributed systems. The proposed scheme adopts a digital signature scheme to detect the change of computer programs, thus it allows computer programs prevent from the infection of computer viruses. However, this article will present a forgery signature attack on their scheme. Moreover, the author also points out one restriction in their scheme. It is impractical for most application programs.

Key words：Cryptography; Cryptanalysis; Signature; Computer viruses