24.A Provably Secure General Construction For Key Exchange Protocols Using Smart Card And Password

Abstract:

Quite recently, two smart-card-based passwords authenticated key exchange protocols were proposed by Lee et al. and Hwang et al. respectively. However, neither of them achieves two-factor authentication fully since they would become completely insecure once one factor is broken. To overcome these congenital defects, this study proposes such a secure authenticated key exchange protocol that achieves fully two-factor authentication and provides forward security of session keys. And yet our scheme is simple and reasonably efficient. Furthermore, we can provide the rigorous proof of the security for it.