Abstract

We present an ID-based escrow-able authenticated group key agreement (AGKA) protocol which is provably secure in random oracle model. Additionally, the proposed protocol neither involve NAXOS trick nor uses gap assumption. And the security is proven in stronger eCK model. To our best knowledge, the proposed protocol will be first provable Secure and escrow-able ID based authenticated group key agreement protocol without NAXOS trick in eCK model.

References


22. Ustaoglu B. Comparing session state reveal and ephemeral key reveal for Diffie-


Index Terms

Computer Science  Security

Keywords

Group key agreement, identity based, escrow-able, NAXOS trick