Slight Homomorphic signature for Access controlling in Cloud Computing

With the popularity of cloud computing, how to securely authenticate a user while not releasing user's sensitive information becomes a challenge. In this paper, we introduce a slight homomorphic signature, which is suitable to implement an access controlling service in cloud computing. In slight homomorphic signature, each user in cloud computing who have a set of identity attributes, firstly computes a full signature on all his identity attributes, and sends it to a semi-trusted access controlling server. The access controlling server verifies the full signature for all identity attributes. After then, if the user wants to require a cloud service, which may have a special requirement on one of the servers which does not know the secret key can compute a partial signature on this special identity attribute, and then sends it to the cloud server for authentication. In the paper, we give a formal secure definition of this slight homomorphic signature, and construct a scheme from Boheh-Boyen signature. We prove that our scheme is secure under q-SDH problem with a weak adversary.