Practical (fully) distributed signatures provably secure in the standard model.

Summary: A distributed signature scheme allows participants in a qualified set to jointly generate a signature which cannot be forged even when any unqualified set of participants collude together. In this paper, we propose an efficient scheme that supports any monotone access structures and show its unforgeability and robustness under the computational Diffie-Hellman (CDH) assumption in the standard model. For 192-bit security, its secret key shares and signature fragments are as short as 511 bits and 1022 bits, which are shorter than existing schemes assuming random oracle. We then propose two extensions. The first one allows new participants to dynamically join the system without any help from the dealer. The second one supports a type of multipartite access structures, where the participant set is divided into multiple disjoint groups, and each group is bounded so that a distributed signature cannot be generated unless a pre-defined number of participants from multiple groups work together. Finally, we present a fully distributed signature scheme such that the centralized trusted dealer can be removed from the system, and the secret keys (shares) can be jointly computed by the involved participants.

Keywords: distributed signature; threshold signature; secret sharing; verifiable secret sharing; monotone span program; multipartite access structure; standard model

doi:10.1016/j.tcs.2015.06.029