Democratic Group Signatures

Mark Manulis
Horst-Görtz Institute for IT-Security
Ruhr-University of Bochum, Germany
mark.manulis@rub.de

For many mutli-party applications *group signatures* are important cryptographic primitives that can be used for the purpose of anonymity and privacy. Group signatures can be used by employees of a company to sign documents on behalf of the company, or in electronic voting and bidding scenarios. In classical group signatures members of a group are able to sign messages anonymously on behalf of the group. However, there exists a designated authority, called *group manager*, that initializes the scheme, adds new group members, and is able to open group signatures, i.e., identify the signer. Some group signature schemes distinguish between two management authorities: a membership manager that sets up the scheme and controls admission to the group, and a revocation manager that opens the signatures. Obviously, in classical group signatures the group manager is given enormous power compared to other group members and is required to be trusted to act as predestinated. On the other hand there exist multi-party applications where such centralized control (trust) is undesirable, e.g., distributed or federated systems. For this kind of applications it is desirable to have a group signature scheme which provides similar properties but is independent of any centralized control.

In this talk we summarize research results concerning this issue. In particular we have proposed a novel group-oriented signature scheme called *democratic group signatures* [Ma06] which can be seen as a variant of classical group signatures with group manager's rights equally distributed between all members of the group. In democratic group signatures each group member can sign on behalf of the group and is also able to identify the signer of a given group signature. The signer's anonymity is provided only against non-members who are only able to verify group signatures. The group membership is controlled jointly by all group members. We also consider dynamic groups where group membership may vary other time. Obviously, for security reasons in this case relevant group secrets have to be changed. In a subsequent work [MaSaSc06] we have described *linkable democratic group signatures* where anonymity requirement has been relaxed to allow linkability of issued group signatures. Linkability is useful in some application scenarios which subsume communication of group members and non-members. By allowing linkability we were also able to obtain more efficient constructions.

References

[Ma06] Mark Manulis. *Democratic Group Signatures - On an Example of Joint Ventures - Fast Abstract.* In Proceedings of ACM Symposium on Information, Computer and Communications Security (ASIACCS'06), pp. 365, ACM Press, 2006. Full version at: http://eprint.iacr.org/2005/446.

[MaSaSc06] Mark Manulis and Ahmad-Reza Sadeghi and Jörg Schwenk. *Linkable Democratic Group Signatures.* In Proceedings of the 2nd Information Security Practice and Experience Conference (ISPEC 2006), LNCS 3903, pp. 187–201, Springer, 2006.