Pseudonym Signatures: New paradigm for group communication security - Anonymity outside the group, not inside

Mark Manulis
HGI, Ruhr-University of Bochum, Germany
mark.manulis@nds.rub.de

Ahmad-Reza Sadeghi
HGI, Ruhr-University of Bochum, Germany
sadeghi@crypto.rub.de

Jörg Schwenk
HGI, Ruhr-University of Bochum, Germany
joerg.schwenk@nds.rub.de

Justification

We describe a new security paradigm called *pseudonym signatures* that can be used for privacy and authenticity in different group communication scenarios that assume the existence of the shared communication channel, i.e., a broadcast channel. We consider this as a new paradigm for group communication security: existing group-oriented digital signatures, like classical group signatures, ring signatures, traceable signatures, threshold signatures and multi-signatures, that have been proposed over past years do not fulfill all requirements that pseudonym signatures fulfill. As we point out in the paper, there exists a wide range of applications in business, research, education, military, transportation, multimedia, and sports areas where existing group-oriented schemes are not applicable because of the different trust relationship between participants or special privacy and authenticity requirements. Pseudonym signatures can be used in such scenarios because of equal rights for all group members and anonymity, which is provided only against non-members who receive signed messages of group members. None of the existing schemes can be used here instead of pseudonym signatures, unless its definition and security requirements (trust relationship and anonymity) are changed. For example, group signatures require that signer's anonymity should be preserved in communication with both, outsiders and insiders, and that no recognition of the signer must be possible.

The pseudonym signatures paradigm is independent of any criteria that specifies when one participant is allowed to become a group member or has to remain a non-member. Such criteria should be defined externally and serve as input. However, it provides equal rights for all group members concerning group decisions and computations on behalf of the group, like computation of any group secrets. More specific, there should be no central controller that is allowed to compute any secrets on behalf of the group. Presented paradigm of pseudonym signatures

- allows group members to send authentic messages such that other group members and non-members who verify the authenticity of the message are convinced that its author is a valid group member. Additionally, all other group members are able to identify this member as the author of the message, whereas non-members obtain a recognition parameter called a *pseudonym* of the author.
- provides to non-members recognition parameters of all group members, called *pseudonyms*, so that any non-member who verifies the authenticity of the message is able to figure out, which pseudonym belongs to its author.

Pseudonym signatures not only act as stand-alone applications but they can also be combined with other cryptographic primitives, like symmetric and asymmetric encryption, in order to fulfill a variety of requirements concerning privacy and authentication of different group communication scenarios. They

- allow group members to communicate securely over the broadcast channel using a secure symmetric encryption scheme. Any group member can send encrypted messages that are received by all participants, but can be decrypted only by valid group members.
- allow any non-member to send encrypted messages to the whole group over the broadcast channel using a secure asymmetric encryption scheme.
- allow any group member to set up an authentic and secure virtual point-to-point channel on top of the broadcast channel with any non-member using a secure asymmetric encryption scheme.

We remark that our construction of pseudonym signatures incorporates key management for symmetric and asymmetric encryption.

We believe that our contribution would arise an interesting discussion on the topic of authentication and privacy in group communication scenarios at the workshop, also for participants that are less familiar with it.

Attendance Statement

One author wishes to attend the workshop.