Title: **Beyond Secret Handshakes: Affiliation-Hiding Authenticated Key Exchange**

Author: **Jarecki, S., Kim, J. and Tsudik, G.**

Published in: *Topics in Cryptology - CT-RSA 2008, Lecture Notes in Comput. Sci.*, **4964**, 352–369, (2008)

Review by: Mario Forcinito

When two parties want to recognize each other as belonging to a private group, they can perform a protocol called Affiliation-Hiding Authentication Protocol or Secret Handshake, that will prove to each party the other is a member of the group without revealing their identities or the identity of the private group. If one of them does not belong to the group the protocol shall fail.

Within the Public Key Infrastructure, the use of certificates issued by the private group makes easy to perform secret handshakes, each party has to prove the other that it has a valid certificate. Moreover this operation can be performed privately, that is, the identity of the group is not revealed to the party that does not belong to the group.

In this paper the authors strengthen the notion of Affiliation-Hiding Authentication Key Exchange (AH-AKE) by requiring that the security of the session is guaranteed even if one of the participants become corrupted. This notion is called Perfect Forward Secrecy (PFS).

In addition a property called Linkable Affiliation-Hiding (LAH) that defines the exact level of privacy protection is introduced.

The authors show a protocol that achieves both, PFS and LAH under the RSA assumption.

See also:

1. Castelluccia, C., Jarecki, S.and Tsudik, G., Secret Handshakes from CA-Oblivious Encryption
   `http://www.ics.uci.edu/~stasio/Papers/cjt04.pdf`

2. Jarecki, S., Kim, J. and Tsudik, G., Authentication for Paranoids: Multi-Party Secret Handshakes
http://www.ics.uci.edu/∼stasio/Papers/ACNS06.pdf

3. Abdalla, M. and Kim, J. - CRYP-401*Key Exchange - Presentation RSA 2008*,
https://365.rsaconference.com/servlet/JiveServlet/download/2028-1-1493/CRYP-401.pdf