Cryptology ePrint Archive: Report 2011/182

Designated Confirmer Signatures With Unified Verification

Guilin Wang, Fubiao Xia, and Yunlei Zhao

Abstract: After the introduction of designated confirmer signatures (DCS) by Chaum in 1994, considerable researches have been done to build generic schemes from standard digital signatures and construct efficient concrete solutions. In DCS schemes, a signature cannot be verified without the help of either the signer or a semi-trusted third party, called the designated confirmer. If necessary, the confirmer can further convert a DCS into an ordinary signature that is publicly verifiable. However, there is one limit in most existing schemes: the signer is not given the ability to disavow invalid DCS signatures. Motivated by this observation, in this paper we first propose a new variant of DCS model, called designated confirmer signatures with unified verification}, in which both the signer and the designated confirmer can run the same protocols to confirm a valid DCS or disavow an invalid signature. Then, we present the first DCS scheme with unified verification and prove its security in the random oracle (RO) model and under a new computational assumption, called Decisional Co-efficient Linear (D-co-L) assumption, whose intractability in pairing settings is shown to be equivalent to the well-known Decisional Bilinear Diffie-Hellman (DBDH) assumption. The proposed scheme is constructed by encrypting Boneh, Lynn and Shacham's pairing based short signatures with signed ElGamal encryption. The resulting solution is efficient in both aspects of computation and communication. In addition, we point out that the proposed concept can be generalized by allowing the signer to run different protocols for confirming and disavowing signatures.

Category / Keywords: public-key cryptography /

Date: received 7 Apr 2011

Contact author: guilin at uow edu au

Available formats: PDF | BibTeX Citation

Version: 20110408:134352 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]