Cryptology ePrint Archive: Report 2011/460

Computationally Sound Symbolic Security Reduction Analysis of Group Key Exchange Protocol using Bilinear Pairings

Zijian Zhang and Liehuang Zhu and Lejian Liao

Abstract: Canetti and Herzog have proposed a universally composable symbolic analysis (UCSA) of mutual authentication and key exchange protocols within universally composable security framework. It is fully automated and computationally sound symbolic analysis. Furthermore, Canetti and Gajek have analyzed Diffie-Hellman based key exchange protocols as an extension of their work. It deals with forward secrecy in case of fully adaptive party corruptions. However, their work only addresses two-party protocols that use public key encryptions, digital signatures and Diffie-Hellman exchange. We make the following contributions. First, we extend UCSA approach to analyze group key exchange protocols that use bilinear pairings exchange and digital signatures to resist insider attack under fully adaptive party corruptions with respect to forward secrecy. Specifically, we propose an formal algebra, and property of bilinear pairings in the execution of group key exchange protocol among arbitrary number of participants. This provides computationally sound and fully automated analysis. Second, we reduce the security of multiple group key exchange sessions among arbitrary number of participants to the security of a single group key exchange session among three participants. This improves the efficiency of security analysis.

Category / Keywords: Universally Composable Symbolic Analysis, Computational Soundness, Bilinear Pairings, Group Key Exchange Protocol, Forward Secrecy.

Date: received 22 Aug 2011, last revised 10 Oct 2011

Contact author: zhangzijian at bit edu cn