Cryptology ePrint Archive: Report 2011/150

A Novel k-out-of-n Oblivious Transfer Protocol from Bilinear Pairing

*Jue-Sam Chou*1, Cheng-Lun Wu 2, Yalin Chen 3*

Abstract: As traditional oblivious transfer protocols are treated as cryptographic primitives in most cases, they are usually executed without the consideration of possible attacks, e.g., impersonation, replaying, and man-in-the-middle attacks. Therefore, when these protocols are applied in certain applications, such as mental poker game playing and fairly contracts signing, some extra mechanisms must be combined to ensure its security. However, after the combination, we found that almost all of the resulting schemes are not efficient enough in communicational cost, which is a significant concern for all commercial transactions. Inspired by this observation, we propose a novel secure oblivious transfer protocol based on bilinear pairing which not only can provide mutual authentication to resist malicious attacks but also is efficient in communicational cost.

Category / Keywords: cryptographic protocols / oblivious transfer, mutual authentication, ID-based cryptosystem, impersonation, bilinear pairing

Date: received 25 Mar 2011

Contact author: jschou at mail nhu edu tw