Cryptology ePrint Archive: Report 2011/498

An Efficient Secure Anonymous Proxy Signature Scheme

**Jue-Sam Chou 1, Shih-Che Hung 2, Yalin Chen*

Abstract: Proxy signature schemes can be used in many business applications such as when the original signer is not present to sign important documents. Any proxy signature scheme has to meet the identifiability, undeniability, verifiability and unforgeability security requirements. In some conditions, it may be necessary to protect the proxy signer's privacy from outsiders or third parties. Recently, several studies about proxy signature schemes have been conducted but only Yu et al.' anonymous proxy signature scheme proposed in 2009 attempting to protect the proxy signer's privacy from outsiders. They claimed their scheme can make the proxy signer anonymous. However, based on our research, we determined that this was not the case and the proxy signer's privacy was not anonymous. Hence, in this paper, we propose a new anonymous proxy signature scheme that truly makes the proxy signer anonymous while making it more secure and efficient when compared with Yu et al.'s scheme in 2009. Our proxy signature scheme consists of two constructions. First, we mainly use random numbers and bilinear pairings to attain the anonymous property in our proxy. Secondly, we increase the security, integrity, and efficiency of our proxy through modifications.

Category / Keywords: public-key cryptography /

Date: received 14 Sep 2011

Contact author: jschou at mail nhu edu tw