International Journal of Innovative Computing, Information and Control
Volume **7**, Number **9**, September **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 5557–5569

A PROVABLY SECURE CERTIFICATELESS PROXY SIGNATURE SCHEME

Yu-Chi Chen[1], Chao-Liang Liu[2], Gwoboa Horng[1] and Kuo-Chang Chen[1]

[1]Department of Computer Science and Engineering
National Chung Hsing University
No. 250, Kuo Kuang Rd., Taichung 40227, Taiwan
{ s9756034; gbhorng; s9756013 }@cs.nchu.edu.tw

[2]Department of Information Science and Applications
Asia University
No. 500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
jliu@asia.edu.tw

Received July 2010; revised November 2010

Abstract. *Proxy signature, a variant of digital signature, is in the limelight in recent years for secure communication. For instance, when a manager is occupied with business matters, or travelling on business, he has to delegate an agent to deal with his day-to-day office concerns. Therefore, a proxy signature scheme is necessary in this scenario. Although identity-based proxy signature schemes have been proposed in many studies, certificateless public key cryptography (CL-PKC), first proposed by Al-Riyami and Paterson, has been widely used to avoid the key escrow problem in identity-based public key cryptography. In this paper, we combine the concepts of certificateless cryptography and proxy signature to propose a certificateless proxy signature scheme from bilinear pairings, and we also present its security model. This scheme is provably secure and existentially unforgeable under the chosen message attack in the random oracle model.*

Keywords: Proxy signature, Certificateless cryptography, Certificate signature, Pairing

1. **Introduction.** Digital signature is able to provide authenticity, integrity and non-repudiation on a message. A conventional digital signature scheme is composed of a signer and a verifier, where a signer generates a signature with his private key and the verifier checks this signature with the signer's public key. In certain scenarios such that the signer is unavailable, a delegate agent is definitely needed to impersonate the proxy signer with the ability to sign messages. In these cases, a proxy signature scheme which consists of original signer, proxy signer and verifier is completely suitable, which means the proxy signer can sign a message and that the verifier must verify the signature with both the original singer and the proxy signer's. We also can refer to many studies related to signature schemes [1, 2, 3].

Certificates of public keys, identifications, and other information are all under the management of the certificate authority (CA) in traditional public key cryptography, but it wastes communication cost to obtain certificates. Compared with the traditional public key infrastructure (PKI), identity-based public key cryptography (ID-PKC) [4, 5, 6] and certificateless cryptography (CL-PKC) [7] do not rely on the extra trusted party to manage certificates. Unfortunately, key escrow is a problem suffered by ID-PKC since the private key generator (PKG) can generate any user's full private key. Differing from ID-PKC, the key generation center (KGC) in CL-PKC cannot derive any user's full private key, but only the user's **partial-private-key**. Most CL-PKC schemes [8, 9, 10, 11, 12] are proposed based on Al-Riyami and Paterson's CL-PKC scheme [7].