Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER Applied Mathematics and Computation 168 (2005) 447–464

APPLIED MATHEMATICS AND COMPUTATION

www.elsevier.com/locate/amc

Several security schemes constructed using ECC-based self-certified public key cryptosystems

Woei-Jiunn Tsaur

Department of Information Management, Da-Yeh University, 112 Shan-Jiau Road,
DaTsuen Changhua 51505, Taiwan, ROC

Abstract

In this paper, we develop an efficient ECC-based self-certified public key cryptosystem (ECCSCPKC) quite suitable for efficiently securing electronic transactions. The proposed ECCSCPKC is constructed based on the elliptic curve cryptosystems (ECC) and the ID-based self-certified public key cryptosystems. The approaches proposed in this paper possess the following advantages:

(1) When verifying the validity of public key, it does not need to spend extra much time to verify the signature in the digital certificate used in the certificate-based public key cryptosystem.
(2) Both distributing a session key and verifying the validity of public key can be concurrently achieved in a logically single step.
(3) Verifying both a signature and the validity of public key can be concurrently accomplished in a logically single step.
(4) Both decrypting a cipher correctly and verifying the validity of public key can be concurrently finished in a logically single step.

E-mail address: wjtsaur@yahoo.com.tw

0096-3003/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.amc.2004.09.010

(5) Since the proposed methods are combined with the ID-based and ECC public key cryptosystems, they can reduce the computation cost greatly.

In summary, based on the above characteristics, the proposed ECCSCPKC and its related security schemes can gain much efficiency in saving both the communicational cost and the computational effort, because they can simplify public key distribution. Also, since the proposed ECCSCPKC does not need to manage the key directory, the cost of system maintenance can be greatly reduced.

Keywords: Elliptic curve cryptosystems; Self-certified public key cryptosystems; ID-based public key cryptosystems; Certificate-based public key cryptosystems; Information security

1. Introduction

Public key cryptosystems are primary basics for the realization of contemporary encryption or digital signature schemes, where one secret key is used as the decryption key or signature generation key and the corresponding public key is used as the cipher text generation key or signature verification key. It is pointed out that most of the public key cryptosystems are vulnerable to the so-called active attacks, such as the attempts to substitute or modify a genuine public key by a fake one during key distribution [9]. The solution to this problem is obviously for an authority to provide authenticated public keys. The most widely adopted approach for public key verification is named as the certificate-based public key cryptosystems [14,23]. The certificate-based approach requires an extra public key certificate issued by the certification authority (CA) after user registration. In the certificate-based approach, anyone that wants to use a public key for certain subsequent cryptographic application (e.g., key exchange or signature verification) should independently perform public key verification and subsequent cryptographic application through two separate steps. Another approach to create authenticated public keys is known as the ID-based public key cryptosystems proposed by Shamir [31]. The ID-based approach employs the user's identity as his/her public key, and hence needs no extra public key certificate and no verification of signatures, which can reduce the amount of storage, communication and computation. In the ID-based approach, it usually requires an interactive identification protocol for authenticating the user's identity (i.e., the public key) before executing certain cryptographic application. Although the ID-based approach effectively solves the problem of public key verification for practical usage, its security disadvantage is that CA knows all users' secret keys after user registration. Therefore, CA may have the opportunity to masquerade as any legitimate user by generating a valid public-key/secret-key pair for the user without being detected.