Breaking Yum and Lee Generic Constructions of Certificate-Less and Certificate-Based Encryption Schemes

David Galindo[1], Paz Morillo[2], and Carla Ràfols[2]

[1] Institute for Computing and Information Sciences,
Radboud University Nijmegen, P.O. Box 9010,
6500 GL, Nijmegen, The Netherlands
d.galindo@cs.ru.nl
[2] Universitat Politècnica de Catalunya,
C/Jordi Girona, 1-3 08034 Barcelona
{paz, crafols}@ma4.upc.edu

Abstract. Identity-based public key cryptography is aimed at simplifying the management of certificates in traditional public key infrastructures by means of using the identity of a user as its public key. The user must identify itself to a trusted authority in order to obtain the secret key corresponding to its identity. The main drawback of this special form of public key cryptography is that it is key escrowed. Certificate-based and certificate-less cryptography have been recently proposed as intermediate paradigms between traditional and identity-based cryptography, seeking to simplify the management of certificates while avoiding the key escrow property of identity-based cryptography. In this work we cryptanalyse the certificate-based and certificate-less encryption schemes presented by Yum and Lee at EuroPKI 2004 and ICCSA 2004 conferences.

Keywords: public-key infrastructure, identity-based encryption, certificate-based and certificate-less encryption, cryptanalysis.

1 Introduction

In traditional public key cryptography (PKC) the authenticity of the public keys must be certified by a trusted third party, which is called Certification Authority (CA). The infrastructure required to support traditional PKC is the main difficulty in its deployment. Many of the problems of any public key infrastructure arise from the management of certificates, which includes storage, revocation and distribution.

In 1984, Shamir proposed the concept of identity-based PKC, which sought to reduce the requirements on the public key infrastructure by using a well-known aspect of the client's identity as its public key. With this approach, certification becomes implicit. For instance, in the case of identity-based encryption (IBE), the sender of a message does not need to check whether the receiver is certified or not. Instead, prior to decryption, the receiver must identify himself to a trusted

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 81–91, 2006.

authority who is in possession of a master key. If the identification is successful, the authority sends the user his private key. The first practical provably secure IBE scheme was proposed by Boneh and Franklin in 2001, using bilinear maps on elliptic curves and it was proven secure in the random oracle model [7]. The main drawback of IBE is that it is inherently key escrowed, which limits the applicability of IBE.

Motivated by the above problem, the concept of certificate-based PKC was introduced by Gentry in [11]. In this model, certificates are needed to generate the user's secret key, so certification becomes implicit. In addition there is no key escrow, since the user's secret key is generated by joining both the certificate and a private information only known to the user. In a certificate-based encryption (CBE) scheme, senders are not required to obtain fresh information of receivers' certificate status; the receiver will be able to decrypt only if its public key is certified.

Independently from the previous work, the concept of certificate-less PKC was introduced by Al Riyami and Paterson in [1]. In contrast to traditional public key cryptographic systems, CL-PKC does not require the use of certificates to guarantee the authenticity of public keys. It does rely on the use of a trusted authority who is in possession of a master key. On the other hand, CL-PKC does not suffer from key escrow, since the authority does not have access to the user's private key. Several cryptographic primitives for certificate-less PKC were proposed in [1], including a certificate-less public key encryption (CL-PKE) scheme.

In contrast to IBE, the confidentiality of CBE and CL-PKE schemes must be protected against dishonest users as well as against the trusted authorities. Security notions taking into account these new scenarios were proposed in the seminal works [11, 1].

Thus, certificate-less PKC and certificate-based PKC can be conceptually seen as intermediates between traditional PKC and identity-based PKC. This idea motivated the work by Yum and Lee [15, 16], in which they tried to show a formal equivalence among IBE, CBE and CL-PKE. In particular, their intention was to show that IBE implies both CBE and CL-PKE by giving a generic construction from IBE to those primitives. To do so, they defined a weaker security model for CL-PKE than the original model introduced in [1]. Their generic constructions have been cited as sound constructions in the works [2, 3, 9, 12, 13][1].

Our contribution. In this paper we show that a dishonest authority can break the security of the three generic constructions of CBE and CL-PKE schemes given in [15, 16]. These constructions are inherently flawed due to a naive use of double encryption as highlighted in [10]. We stress that our attacks are within the restricted security model proposed by Yum and Lee, that is, *our results contradict* three of their theorems.

Related work. In a recent work, Libert and Quisquater [13] show that the transformation from IBE to CL-PKE in [15] due to Yum and Lee is insecure in

[1] In the work [13] only the transformations in [16] are regarded as valid constructions in the restricted security model.