Available online at www.sciencedirect.com
ScienceDirect
The Journal of Systems and Software 81 (2008) 1218–1226
The Journal of Systems and Software
www.elsevier.com/locate/jss

Improved certificate-based encryption in the standard model

David Galindo [a,*], Paz Morillo [b], Carla Ràfols [b]

[a] Computer Science Department, University of Malaga, 29071, Malaga, Spain
[b] Universitat Politècnica de Catalunya, ClJordi Girona, 1-3 08034 Barcelona, Spain

Received 11 October 2006; received in revised form 9 August 2007; accepted 9 September 2007
Available online 15 September 2007

Abstract

Certificate-based encryption has been recently proposed as a means to simplify the certificate management inherent to traditional public key encryption. In this paper, we present an efficient certificate-based encryption scheme which is fully secure in the standard model. Our construction is more efficient (in terms of computational cost and ciphertext size) than any of the previous constructions known without random oracles.

Keywords: Identity-based encryption; Certificate-based encryption; Standard model

1. Introduction

In traditional public key cryptography (PKC) a certificate binding a public key and its owner's identity is used in order to prevent man-in-the-middle attacks. The management of these certificates during a key's lifetime is a complex issue, and it is often mentioned as one of the main drawbacks against a widespread use of PKC. In Shamir (1985), the concept of identity-based cryptography (IBC) was proposed, which attempted to remove as much as possible the need for certificates. Roughly, the idea is that the identity of the user Bob acts as his public key, and therefore a link between Bob and his public key is no longer required. Now, Bob must identify himself to a trusted authority prior to decryption, which will send him his private key. There are some drawbacks in identity-based cryptography, the most important being the fact that it is inherently key escrowed, since the trusted authority computes the private keys of the users. A second drawback is that the secret keys must be sent to the users via a secret channel, which makes the problem of key distribution non-trivial. Finally, user revocation can be partially solved by adding expiry dates to the identities of users.

These disadvantages motivated the introduction of a new asymmetric encryption paradigm called certificate-based encryption (CBE) (Gentry, 2003) aimed at bridging the gap between traditional public key encryption and IBE. An especially challenging problem in certificate management in PKC is the revocation of certificates. In many situations, certificates need to be revoked, e.g. in case the user's secret key gets compromised. In the case of encryption, this means that Alice should know before encrypting to Bob whether Bob's public key has been revoked. Solving this problem requires a heavy infrastructure. CBE mitigates this problem by making certificate revocation implicit, in the sense that certificates have an expiry date, at the end of which a new certificate must be obtained from the trusted authority to be able to decrypt. Bob needs not only his private key SK_B to decrypt, but also this up-to-date certificate meaning that PK_B is still valid. Revocation is achieved by stopping the issuance of certificates for the revoked public key, which means one gets rid of third party (i.e. Alice) certificate status queries. CBE was proposed as an intermediate paradigm between identity-based encryption (IBE) and public key encryption (PKE), in the sense that it is not key escrowed and still simplifies

* Corresponding author. Tel.: +34 952134186.
E-mail addresses: dgalindo@lcc.uma.es (D. Galindo), paz@ma4.upc.edu (P. Morillo), crafols@ma4.upc.edu (C. Ràfols).

0164-1212/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2007.09.009

certificate management. An additional attractive property of CBE is that this up-to-date certificate can be sent over an insecure channel, in contrast to IBE, and therefore distributing keys is not an issue anymore. To summarize, the main advantages of CBE with respect to other asymmetric encryption paradigms are the removal of third party certificate status queries, simpler key distribution and absence of key escrow, while the disadvantage (with respect to IBE) is that public keys are not identity-based.

1.1. Previous work

Generic constructions of adaptive chosen-ciphertext secure (CCA-secure) CBE schemes were proposed in Al-Riyami and Paterson (2005),Yum and Lee (2004) but were later found to be flawed or to have unproven security claims (Galindo et al., 2006; Kang and Park, 2005). In the original work (Gentry, 2003), a CBE scheme building up from the IBE scheme (Boneh and Franklin, 2001) and using the random oracle heuristic (Bellare and Rogaway, 1993; Canetti et al., 2004) was presented.

In Dodis and Katz (2005), the problem of designing *multiple encryption* schemes with chosen-ciphertext security was addressed, i.e. the encryption of data using multiple, independent encryption schemes and resistant to chosen-ciphertext attacks. Since multiple encryption schemes can be used to enforce threshold access to data, they can be used to build CBE schemes. The intuition is very simple: a double encryption scheme requires two secret keys for decrypting; one secret key is only known to the trusted authority, while the other secret key is only known to the user. Thus, an uncertified user lacks the secret key owned by the trusted authority so he cannot decrypt; and the trusted authority does not have access to the user's secret key, so it cannot decrypt on behalf of the user.

The generic CCA-secure CBE construction proposed by Dodis and Katz in Dodis and Katz (2005) uses a one-time signature (OTS), and CCA-secure identity-based encryption and public key encryption schemes. The trusted authority is in possession of the master secret key of the IBE scheme, while the user is in possession of the decryption key of the PKE scheme. To encrypt a message M to the user with identity $\mathtt{id}$ and for time period i, a pair of verification/signing keys (vk, sk) for the OTS scheme is generated. Next, the message M is split in two shares M_1, M_2 such that $M = M_1 \oplus M_2$. Roughly speaking, the first message share is encrypted using the IBE scheme with respect to identity $\mathtt{id}\|i$ and 'label' vk, thus obtaining a ciphertext C_1; and the second message share is encrypted using the PKE scheme with 'label' vk, thus obtaining a ciphertext C_2. Finally, a signature $\sigma = \mathrm{Sign}_{sk}(C_1, C_2)$ is computed and the ciphertext is set to be

$$C = (vk, C_1, C_2, \sigma) \tag{1}$$

Decryption of a ciphertext of this form is done in the obvious way, as long as the user is in possession of the certificate for identity $\mathtt{id}\|i$, which in this case is just the IBE's secret key with respect to identity $\mathtt{id}\|i$. This construction is in the standard model provided that the underlying schemes are in the standard model.

1.2. Our results

Our goal is to design a CBE scheme without random oracles more efficient than the schemes resulting from the generic construction of Dodis–Katz (DK), which is the only other construction in the standard model. The idea is to find suitable chosen-plaintext secure (CPA-secure) IBE and PKE schemes with a similar structure and to exploit these similarities to design a more efficient combination, since CPA security is obtained at a lower cost than CCA security. We successfully apply this idea to the IBE and PKE schemes obtained from Waters (2005) and Boneh and Boyen (2004) schemes. Compared to the DK ciphertext as given in Eq. (1), our CBE scheme can be seen as the result of removing the component C_2 by 'embedding' it into C_1. Thus, our ciphertext is shortened to

$$C' = (vk, C_1, \sigma) \tag{2}$$

if compared to Eq. (1) when the DK construction is optimistically instantiated with the CCA-secure IBE schemes from (Boyen et al., 2005). This results in a new CBE scheme with reduced computational cost and ciphertext size. Our CBE scheme is proven secure under the standard decisional assumption in bilinear groups. A detailed numerical comparison is given in Section 4.3.

1.3. Extensions

- Better efficiency: It is possible to replace the one-time signature in our construction by (essentially) a message authentication code, as shown in Boneh and Katz (2005). This improved transformation results in shorter ciphertexts and more efficient encryption/decryption. This improvement is also possible for the DK construction.
- Hierarchical CBE: Although our scheme uses a single trusted authority, it is straightforward to adapt it to a hierarchy of authorities by replacing the IBE scheme in our construction with the hierarchical identity-based encryption scheme deriving from (Boneh and Boyen, 2004; Waters, 2005).
- Threshold CBE: The chosen-ciphertext secure schemes obtained by applying the transformation (Canetti et al., 2004) to IBE schemes built on bilinear pairings enjoy several public verifiability properties. This feature has been recently exploited in Boneh et al. (2006) to build threshold chosen-ciphertext secure PKE schemes in the standard model. It is possible to apply the same techniques to our CBE scheme in order to obtain a CBE scheme with threshold certificate generation. The idea of a threshold CBE scheme is that the secret key of the trusted authority is not stored in a single location,