Information Sciences 372 (2016) 745–757

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A provably secure certificate-based encryption scheme against malicious CA attacks in the standard model

Yang Lu*, Jiguo Li

College of Computer and Information, Hohai University, No. 8, Focheng Xi Road, Jiangning District, Nanjing, China

ARTICLE INFO

Article history:
Received 19 October 2015
Revised 2 April 2016
Accepted 26 August 2016
Available online 28 August 2016

Keywords:
Public key cryptography
Certificate-based encryption
Malicious ca attack
Chosen-ciphertext security
Standard model

ABSTRACT

Certificate-based encryption (CBE) is a new public-key cryptographic paradigm that represents an interesting balance between conventional public-key encryption and identity-based encryption. It not only simplifies the certificate revocation problem in conventional public-key encryption, but also solves the key escrow problem inherent in identity-based encryption. In CBE, a certificate authority (CA) is employed to initialize the system and issue certificates for users. Each user needs both a private key and an up-to-date certificate to decrypt ciphertexts. In the previous concrete constructions of CBE, the CA is assumed to be honest-but-curious, that is, the CA always starts launching attacks only after it has initialized the system honestly. However, it seems that such an assumption does not necessarily reflect reality when we consider a malicious CA that is trying every effort to break the system. To show that the malicious CA attack exists in CBE, we present two concrete attacks against a previous CBE scheme. In both attacks, a malicious CA can easily break any user's confidentiality by implanting a trapdoor in the public system parameters. To fight against malicious CA attacks, we propose a new CBE scheme. The proposed CBE scheme is proven to be chosen-ciphertext secure against malicious CA attacks in the standard model. Performance comparison shows that it is efficient and practical.

1. Introduction

In Eurocrypt 2003, Gentry [16] introduced the notion of certificate-based encryption (CBE). This new cryptographic paradigm combines identity-based encryption (IBE) and conventional public-key encryption (PKE) while overcoming some of their inherent drawbacks. As in conventional PKE, each user in CBE generates a public/private key pair independently and then sends his/her public key to a trusted certificate authority (CA) to request a certificate. The certificate in CBE acts not only as a public key certificate (as in conventional PKE) but also as a partial decryption key. This functionality provides an implicit certificate property so that each receiver needs both his/her private key and an up-to-date certificate to decrypt the received ciphertexts, while the senders need not be concerned about the receiver's certificate revocation problem. The property of implicit certificate eliminates the third-party queries for the certificate status and enables efficient certificate revocation. As introduced by Gentry in [16], CBE can be used to build efficient public key infrastructures requiring fewer infrastructures than the conventional ones. Furthermore, there are no key escrow problem (because the CA does not know any user's private key) and key distribution problem (because the certificates need not be kept secret and can be sent to the users via public communication channels) in CBE.

* Corresponding author.
E-mail addresses: luyangnsd@163.com (Y. Lu), ljg1688@163.com (J. Li).

http://dx.doi.org/10.1016/j.ins.2016.08.082
0020-0255/© 2016 Elsevier Inc. All rights reserved.

1.1. Related works

In recent years, CBE has aroused great interest in the research community and numerous schemes have been published in the literature.

In [16], Gentry brought forth the notion and the first concrete construction of CBE. Gentry's CBE scheme was constructed from the well-known IBE scheme proposed by Boneh and Franklin [6] and was proven secure in the random oracle model [4]. A subsequent paper by Yum and Lee [49] indicated that IBE implies both CBE and certificateless public-key encryption (CL-PKE) [1] by providing a generic construction from IBE to those primitives respectively. However, Galindo et al. [13] pointed out that Yum-Lee's constructions are not secure against the chosen ciphertext attacks because they are inherently flawed due to a naive use of double encryption without further security treatments. To solve this problem, Lu et al. [35] adopted the techniques of Fujisaki and Okamoto [11,12] and proposed two generic constructions of chosen-ciphertext secure CBE by combining IBE with conventional PKE. In [2], Al-Riyami and Paterson gave a detailed analysis for the notion of CBE and proposed a generic conversion from CL-PKE to CBE. They claimed that their generic conversion can be used to derive a chosen-ciphertext secure CBE scheme from any chosen-ciphertext secure CL-PKE scheme. However, Kang and Park [22] indicated that Al-Riyami and Paterson's generic conversion was incorrect due to a flaw in their security proof. Wu et al. [42] and Gao et al. [15] made a further observation on the relations between CL-PKE and CBE and proposed a new generic construction of CBE from CL-PKE respectively. Wu et al. [42] also derived a concrete CBE scheme from the CL-PKE scheme proposed by Dent et al. [9]. In [36], Morillo and Ràfols proposed the first CBE scheme without using the random oracles. Their scheme was constructed by combining Waters' IBE scheme [41] with Boneh and Boyen's IBE scheme [5]. So far, many researchers have attempted to build CBE schemes with better efficiency or stronger security [14,27,29,32,37,44,46,47]. Furthermore, some variants of CBE (e.g., separable CBE [21,50], multi-receiver CBE [10,38], certificate-based proxy encryption [40] and certificate-based proxy re-encryption [26,34,39]) have been proposed.

1.2. Motivation and contributions

A user in CBE can perform decryption operations successfully only when both his/her private key and an up-to-date certificate are known. In other words, if only knowing one of a user's private key and certificate, an adversary is unable to compromise this user. As introduced in [16,2], two different types of adversaries (*i.e.*, Type I adversary and Type II adversary) should be considered in the CBE security model:

- Type I adversary simulates an uncertified user who knows the target user's private key, but cannot access the target user's certificate and the CA's master secret key.
- Type II adversary simulates a CA who knows the master secret key and controls the generation of certificates, but cannot access the target user's private key.

We notice that all the previous concrete constructions of CBE implicitly assume that the Type II adversary simulates an honest-but-curious CA. In other words, all of them assume that the CA always generates the master secret key and the public system parameters honestly in complete accordance with the scheme specification, but once after setting up the system, it suddenly becomes curious and gets ready to eavesdrop on users. Thus, the Type II adversary is given the master secret key and the public system parameters at the very beginning of the adversarial game, instead of generating them by itself. It seems that such an assumption does not completely reflect reality. In the real world, a CA may be dishonest and malicious at the very beginning of the setup stage of the system and may not follow the scheme specification for setting up the system. This means that a CA may maliciously implant a trapdoor in the public system parameters and then attempt to attack user confidentiality. What's worse is that the occurrence of the malicious CA attack is difficult to be detected, because the CA need not actively forge the user's certificate or compromise the user's device for corrupting the private key.

Similar attack (known as malicious KGC attack) was introduced by Au et al. [3] to the security of certificateless public-key cryptography (CL-PKC). A number of certificateless schemes have been proposed to fight against malicious KGC attacks, e.g. [19,20,31,43,45,48,51]. However, as shown in [18], the malicious KGC security may be the strongest Type II security level for the certificateless schemes, only few certificateless schemes can be proven secure under the malicious KGC adversarial model. To the best of our knowledge, there exist only three CL-PKE schemes secure against malicious KGC attacks in the literature so far. The first one is due to Libert and Quisquater [28]. But the security proof is given by Au et al. in [3]. The second one is the generic CL-PKE scheme proposed by Huang and Wong [19], which can generally build CL-PKE schemes by combining IBE with conventional PKE. The third one is the recent CL-PKE scheme proposed by Yang et al. [45]. Despite the fact that the malicious KGC attack problem has attracted high attention in the certificateless setting, none of the precious concrete constructions of CBE has considered the malicious CA attack problem. We notice that Wu et al. [42] provided the definition of malicious CA security and claimed that their generic construction can be used to derive a CBE scheme secure against malicious CA attacks from any CL-PKE scheme with malicious KGC security. However, no formal security proof is given in [42]. So, it is fair to say that devising a provably secure CBE scheme against malicious CA attacks remains an unsolved problem until now. Since the CA in CBE is not fully trusted, it is necessary and important for us to develop CBE schemes that can withstand the malicious CA attacks, to reduce our trust in the CA.

In this paper, by giving two concrete attacks, we first show that the CBE scheme presented by Wu et al. [42] does not achieve chosen-ciphertext security against malicious CA attacks. Both attacks indicate that a malicious CA can implant a