Theoretical Computer Science 412 (2011) 5446–5457

Contents lists available at ScienceDirect

Theoretical Computer Science

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

Certificateless cryptography with KGC trust level 3

Guomin Yang *, Chik How Tan

Temasek Laboratories, National University of Singapore, Singapore

ARTICLE INFO

Article history:
Received 25 January 2011
Received in revised form 9 May 2011
Accepted 9 June 2011
Communicated by X. Deng

Keywords:
Certificateless cryptography
Public key encryption
Digital signature
Trust hierarchy

ABSTRACT

A normal certificateless cryptosystem can only achieve KGC trust level 2 according to the trust hierarchy defined by Girault. Although in the seminal paper introducing certificateless cryptography, Al-Riyami and Paterson introduced a binding technique to lift the KGC trust level of their certificateless schemes to level 3, many subsequent work on certificateless cryptography just focused on the constructions of normal certificateless schemes, and a formal study on the general applicability of the binding technique to these existing schemes is still missing. In this paper, to address the KGC trust level issue, we introduce the notion of Key Dependent Certificateless Cryptography (KD-CLC). Compared with conventional certificateless cryptography, KD-CLC can achieve stronger security, and more importantly, KGC trust level 3. We then study generic techniques for transforming conventional CLC to KD-CLC. We start with the binding technique by Al-Riyami and Paterson, and show that there are some technical difficulties in proving that the binding technique is generally applicable. However, we show that a slightly modified version of the binding technique indeed can be proved to work under the random oracle assumption. Finally, we show how to perform the transformation using a standard cryptographic primitive instead of a random oracle.

1. Introduction

Certificateless Cryptography (CLC), introduced by Al-Riyami and Paterson [1], aims to avoid the drawbacks of both traditional public key cryptography which requires a public key infrastructure (PKI), and identity-based cryptography [17] which has the inherent key escrow problem. In a normal certificateless cryptosystem, a user secret key *usk* is derived from two partial secrets: one is an identity-based secret key (also known as partial secret key) *psk* generated by a Key Generation Center (KGC) based on the user's identity *ID*, and the other is a user self-generated secret key *sk* which corresponds to an uncertified public key *pk*. In many existing certificateless cryptosystems (e.g. [4,10,11,5,12]), the user secret key is simply set as $usk = (psk, sk)$.

Since there is no authentication information (such as an X.509 certificate in a PKI) for the user public key *pk*, an adversary can replace the public key either in the transmission or in a public directory with another public key. If a key replacement attack happens, then the security of a certificateless cryptosystem would just rely on its identity-based component. On the other hand, if the partial secret key *psk* of a user is leaked, then an adversary can always launch the key replacement attack to break a conventional type certificateless cryptosystem. Because of this reason, in most of the existing certificateless cryptosystems, the KGC can only be trusted by all the users. Recall the trust hierarchy by Girault [8] for public key cryptography.

Level 1. The "trusted" authority (e.g. the CA in a PKI, the KGC in an identity-based or certificateless cryptosystem) knows the secret key of any user.

* Corresponding author. Tel.: +65 65161147.
E-mail addresses: tslyg@nus.edu.sg (G. Yang), tsltch@nus.edu.sg (C.H. Tan).

0304-3975/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2011.06.015

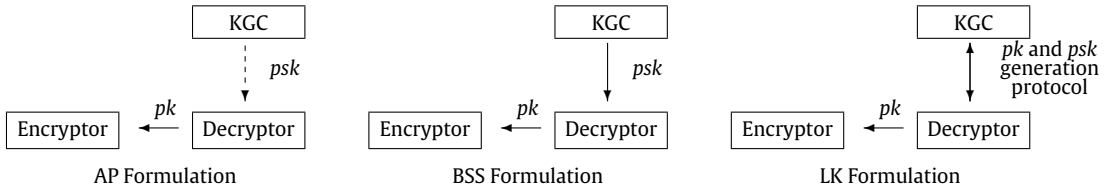

Fig. 1. The existing CLE architectures.

Level 2. The authority cannot compute users' secret keys. However, it can still impersonate a user by generating false guarantees (e.g. false certificates in a PKI, false public keys in a certificateless cryptosystem).

Level 3. The authority cannot compute users' secret keys, and it can be proven that it generates false guarantees of users if it does so.

We can see that identity-based cryptosystems [17] fall into Level 1, conventional certificateless cryptosystems fall into level 2, and a traditional PKI can achieve level 3.

In order to achieve the same trust level as that of a traditional PKI, Al-Riyami and Paterson proposed in their seminal paper [1] a simple binding technique for their certificateless cryptosystems without formal security proofs. However, most of the subsequent research work on certificateless cryptography ignored this important issue and just focused on designing certificateless schemes with KGC trust level 2, and it is unknown if there exist general and provably secure techniques to lift the KGC trust level of these existing schemes to level 3 — the same level as is enjoyed in a traditional PKI.

Our work. In this paper, to address the KGC trust level issue, we formalize the notion of *Key Dependent Certificateless Cryptography (KD-CLC)*. In a key dependent certificateless cryptosystem, the user partial secret key is generated in the following way: a user with identity ID first generates a public/private key pair (pk, sk), and sends pk to the KGC, who then generates the partial secret key psk based on both pk and ID. The advantage of this approach is that even if psk is exposed, an outside adversary cannot break the system by launching a key replacement attack. The reason is that for a replaced pk', the adversary needs to know the (new) partial secret key psk' corresponding to ID and pk', which can only be generated by the KGC. Now, the same statement as in [1] can be made here:

> "A KGC who replaces an entity's public key will be implicated in the event of a dispute: the existence of two working public keys for an identity can only result from the existence of two partial secret keys binding that identity to two different public keys; only the KGC could have created these two partial secret keys."

Then we propose a formal security model for key dependent certificateless cryptography, and study the problem of transforming conventional type certificateless cryptosystems into their key dependent counterparts. A good starting point is to consider the binding technique by Al-Riyami and Paterson. The idea is very simple: after a user with identity ID has created a public key pk, it simply uses $ID\|pk$ ($\|$ denotes string concatenation) as the "identity" for partial secret key generation. Although the idea looks reasonable, we show that some difficulties arise when one wants to formally prove this technique works. On the other hand, we show that a slightly modified binding can be proved to work: instead of using $ID\|pk$, we use $H(ID\|pk)$ where H is a cryptographic hash function. We prove that in the random oracle model, this simple (but useful) binding technique can transform any conventional certificateless encryption or signature scheme (with KGC trust level 2) into a key dependent scheme (with trust level 3). Finally, we show how to perform the transformation using another standard cryptographic primitive – a Trapdoor Hash Function, instead of a random oracle.

Paper organization. In the next section, we review some related work on certificateless cryptography. In Section 3, we formally define key dependent certificateless encryption (KD-CLE) and two generic constructions (with and without random oracle, respectively) of KD-CLE schemes from conventional CLE schemes. Then in Section 4, we show that our generic transformations can also be applied to construct key dependent certificateless signature schemes. The paper is concluded in Section 5.

2. Related work

Certificateless cryptography, introduced by Al-Riyami and Paterson [1] with the purpose of avoiding the drawbacks of both traditional public key cryptography and identity-based cryptography [17], has drawn a lot of attentions in recent years. A detailed survey on certificateless encryption schemes can be found in [5].

According to the categorization by Dent [6], we can separate existing certificateless cryptosystems into three categories: AP Formulation [1], BSS Formulation [3], and LK Formulation [14], which are demonstrated in Fig. 1. The dotted arrow denotes the fact that the public key can be published before the partial secret key psk is obtained. Most of the existing certificateless cryptosystems (e.g. [15,7,10,11,5,4,12]) follow the AP formulation.

In [16], Liu et al. introduced the notion of self-generated-certificate public key cryptography which can prevent the Denial-of-Decryption attacks. They also proposed a generic construction of self-generated-certificate encryption scheme based on a certificateless encryption scheme and a certificateless signature scheme. It is observed by Dent [6] that the minimum requirement for a certificateless encryption scheme to achieve Denial-of-Decryption security is that it is expressed