ARTICLE IN PRESS

Information Sciences xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Information Sciences

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

Signatures in hierarchical certificateless cryptography: Efficient constructions and provable security ☆

Lei Zhang [a,*], Qianhong Wu [b], Josep Domingo-Ferrer [c], Bo Qin [d], Peng Zeng [a]

[a] Shanghai Key Laboratory of Trustworthy Computing, Software Engineering Institute, East China Normal University, Shanghai, China
[b] School of Electronic and Information Engineering, Beihang University, China
[c] UNESCO Chair in Data Privacy, Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Catalonia, Spain
[d] School of Information, Renmin University of China, Beijing, China

ARTICLE INFO

Article history:
Received 12 September 2012
Received in revised form 20 September 2013
Accepted 10 February 2014
Available online xxxx

Keywords:
Hierarchical cryptography
Certificateless cryptography
Hierarchical certificateless signature

ABSTRACT

Many efforts have been devoted in recent years to constructing secure schemes in certificateless cryptography. The aim is to eliminate the key escrow problem of identity-based cryptography. However, most of the work takes place in traditional certificateless cryptography, which suffers from the single-point problem. Hierarchical cryptography exploits a practical security model to mirror the organizational hierarchy in the real world and hence can eliminate the single-point problem. To incorporate the advantages of both types of cryptosystems, in this paper we instantiate hierarchical certificateless cryptography by formalizing the notion of hierarchical certificateless signatures. A concrete hierarchical certificateless signature scheme is also proposed. The security of our scheme is proven under the computational Diffie-Hellman assumption. As to efficiency, our scheme has constant complexity, regardless of the depth of the hierarchy. Therefore, our proposal is secure and scalable.

1. Introduction

Digital signatures are one of the most important primitives in public key cryptography. The public key of a signer can be leveraged by anyone to verify whether a signature attributed to this signer is valid or not. A problem for public key cryptography is that a user must be bound with her public key. The usual approach to solving this problem is to use a public key infrastructure (PKI), in which a trusted certificate authority authenticates the users' public keys. However, in practice, the management of public key certificates is extremely demanding in terms of computing time and storage space.

Identity-based cryptography (IBC) [24] was introduced to reduce the certificate management overhead in traditional PKI based cryptosystems. In IBC systems, the public key of a user is just her identity, e.g., an e-mail address, IP address, etc. Therefore, there is no need to maintain a complicated system to manage the addition, update or withdrawal of public key certificates. Hence, IBC systems are very efficient for some applications. Despite its advantages, the basic IBC system suffers from two limitations in practice. The first one is the single-point problem. In a basic IBC system, a single trusted third party (TTP) called Private Key Generator (PKG) is employed to generate a private key for each user by taking as input PKG's master

☆ Parts of this paper appeared in [28].

* Corresponding author. Tel.: +86 2162235306.
E-mail addresses: leizhang@sei.ecnu.edu.cn (L. Zhang), qhwu@xidian.edu.cn (Q. Wu), josep.domingo@urv.cat (J. Domingo-Ferrer), bo.qin@ruc.edu.cn (B. Qin), pzeng@sei.ecnu.edu.cn (P. Zeng).

http://dx.doi.org/10.1016/j.ins.2014.02.085
0020-0255/

secret key and the user's identity. Although having a single PKG would completely eliminate on-line lookup, it is undesirable for a large open network because the PKG may become a bottleneck. The PKG needs not only to generate private keys for a large number of users, but also to verify the identities of the users. The second limitation is the so-called key escrow problem. Since the PKG is used to generate the full private keys of the users in the system, the PKG knows each user's private key and a malicious PKG can forge signatures on behalf of any user without being detected. The above two limitations make IBC systems not scalable and not applicable to large open networks in which it is impractical to realize a third party fully trusted by all the distributed users.

Hierarchical identity-based cryptography (HIBC) [15] efficiently overcomes the single-point problem in IBC schemes. In HIBC, a *root* PKG is used to distribute the workload by delegating private key generation and identity authentication to *lower-level* PKGs. In this setting, multiple levels of PKGs and users as leaf nodes form a tree-like structure. HIBC was first instantiated by Horwitz and Lynn [15] with a hierarchical identity-based encryption (HIBE) scheme. Subsequent to the work in [15], Gentry and Silverberg [12] proposed a scalable HIBE scheme with full collusion resistance and chosen-ciphertext security. A hierarchical identity-based signature (HIBS) scheme was proposed in [12] as well. The concepts of HIBE and HIBS have been further investigated and more works can be found in [5,7,9,20,23]. HIBC efficiently overcomes the single-point bottleneck of IBC systems. However, it does not address the key escrow problem of such systems.

Certificateless cryptography (CLC) was introduced by Al-Riyami and Paterson to mitigate the key escrow problem. CLC also employs a third party called Key Generation Center (KGC) to help a user generate her private key. However, unlike the PKG in IBC, the KGC in CLC only extracts a partial private key for each user by taking as input a user's identity and the master key of the KGC. The full private key of a user is computed from the partial private key combined with some secret information chosen by the user herself. The corresponding public key is computed from the system's public parameters and the secret information of the user, and is finally published by the user herself. A number of contributions [1,2,10,16–19,21,26,27,30,31,29] have been devoted to the construction of secure schemes in CLC. In [1], Al-Riyami and Paterson proposed a certificateless encryption (CLE) scheme with chosen ciphertext security. A certificateless signature (CLS) scheme was also presented in [1] but no formal proof of security was provided. Subsequently, the security model of CLS schemes was formalized in [18] and the security of the Al-Riyami-Paterson CLS scheme was analyzed in this model. The security model of CLS schemes was further developed in [27] and later in [16,17]. Among them, Huang et al. [17] revisited the security models of CLS schemes.

From the above discussions, one may find that neither CLC nor HIBC address the single-point and the secret key escrow problems in IBC systems *simultaneously*. To fill this gap, hierarchical certificateless cryptography (HCLC) is introduced in [1]. In an HCLC system, a *root* KGC distributes the workload by delegating partial private key generation and identity authentication to *lower-level* KGCs. Multiple levels of KGCs and users as leaf nodes form a tree-like structure. This hierarchical design matches the structure of social organizations in the real world very well. HCLC was first instantiated in [1] with a hierarchical certificateless encryption scheme. However, no security formalization has been provided for that scheme so far. This paper concentrates on hierarchical certificateless signatures (HCLSs), which inherit the advantages of hierarchical identity-based signatures without suffering from the key escrow problem.

1.1. Our contributions

In the preliminary version [28] of this paper, we presented the first formalization of HCLSs as a new HCLC primitive. We explicitly defined the behaviors of adversaries against HCLSs with the help of a number of oracles. Two types of adversaries, i.e., Type I adversary and Type II adversary (see Section 2.2), were distinguished to simulate the collusive users and the malicious KGCs, respectively. Then we defined security as existential unforgeability against adaptive chosen-message attacks. We believe this strong security notion is suitable for most applications. We proposed a scalable HCLS scheme in which, to verify the validity of a signature from a signer, a verifier only needs to obtain the public parameters of the signer's *root* KGC, the user's identifying information (a user is uniquely identified by the path from the root to the user as a leaf node in the hierarchical tree) and the corresponding public key list. The verifier does not need an *on-line* lookup of the identities and public keys of the *lower-level* KGCs. The signing cost and the signature size are both constant, independent of the depth of the hierarchy. As for security, under the computational Diffie-Hellman (CDH) assumption, we showed that our scheme is provably secure against Type II adversaries under existential forgery attacks in the random oracle model [3].

In [28], we proposed a concrete HCLS scheme and gave a preliminary analysis of it. In this version, we provide a detailed analysis of the scheme. Firstly, we further study the behaviors of the adversaries against HCLSs. We show that the Types I and II adversaries in our security definition have similar abilities as the super Types I and II adversaries in [17] (see Section 2.2), who are the strongest adversaries against CLS so far. We also prove that our scheme is secure against enhanced Type I adversaries under existential forgery attacks. Secondly, we show how to detect a dishonest behavior of a malicious KGC in our scheme. Thirdly, we address the key revocation problem in HCLC. Fourthly, we discuss the computational cost of the proposed scheme. Finally, we distinguish our work from possible alternatives, namely a generic construction and a construction with short signatures.

The rest of this paper is organized as follows. In Section 2, we formalize the definition of HCLS schemes by defining the adversarial behaviors and the security notion of existential unforgeability. Our HCLS scheme is proposed in Section 3 and a detailed security analysis is given in Section 4. Section 5 distinguishes our work from other related HCLS constructions. We conclude our paper in Section 6.

Please cite this article in press as: L. Zhang et al., Signatures in hierarchical certificateless cryptography: Efficient constructions and provable security, Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.02.085