Computers and Mathematics with Applications 61 (2011) 2518–2527

Contents lists available at ScienceDirect

Computers and Mathematics with Applications

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

An efficient dynamic authenticated key exchange protocol with selectable identities

Hua Guo [a,b,*], Zhoujun Li [c], Yi Mu [d], Fan Zhang [b], Chuankun Wu [e], Jikai Teng [e]

[a] State Key Laboratory of Software Development Environment, Beihang University, Beijing, PR China
[b] School of Computer Science & Engineering, Beihang University, Beijing, PR China
[c] Beijing Key Laboratory of Network Technology, BeiHang University, Beijing, PR China
[d] School of Computer Science Software Engineering, University of Wollongong, NSW, Australia
[e] State Key Lab of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, PR China

ARTICLE INFO

Article history:
Received 21 June 2010
Received in revised form 28 February 2011
Accepted 28 February 2011

Keywords:
Identity-based key exchange
Computer security
Cryptography

ABSTRACT

In the traditional identity-based cryptography, when a user holds multiple identities as its public keys, it has to manage an equal number of private keys. The recent advances of identity-based cryptography allow a single private key to map multiple public keys (identities) that are selectable by the user. This approach simplifies the private key management. Unfortunately, the existing schemes have a heavy computation overhead, since the private key generator has to authenticate all identities in order to generate a resultant private key. In particular, it has been considered as a drawback that the data size for a user is proportional to the number of associated identities. Moreover, these schemes do not allow dynamic changes of user identities. When a user upgrades its identities, the private key generator (PKG) has to authenticate the identities and generate a new private key. To overcome these problems, in this paper we present an efficient dynamic identity-based key exchange protocol with selectable identities, and prove its security under the bilinear Diffie–Hellman assumption in the random oracle model.

1. Introduction

The concept of identity-based cryptography was introduced by Shamir in 1984 [1]. The idea is to allow a user identity to serve as a public key. The corresponding private key is created by binding the identity string with a master secret of a trusted authority called the private key generator (PKG). Due to its advantage in key management in comparison to the traditional PKI-based cryptography, identity-based cryptography has received a lot of attention. The introduction of pairings to cryptography [2,3] opened up an entirely new field for identity-based cryptography. Many novel identity-based key agreement protocols from pairings have been introduced and proved in different security models (e.g., [4–9]).

In an identity-based system, a private key is created by binding an identity string and the master key of PKG. An obvious key management issue arises, when a user holds multiple identities, as multiple identities lead to multiple private keys. Moreover, using multiple private keys and public keys in key agreement could result in high computational complexity.

To simplify private key management for a user with multiple identities, we seek a solution where multiple identities are associated with a single private key. Recently, Guo et al. [10,11] introduced an encryption scheme that captures the features of multiple identities. However the security proof in [10] is pointed out to be incorrect [12]. Furthermore, [12] presented a

* Corresponding author.
E-mail address: hguo.xyz@163.com (H. Guo).

0898-1221/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2011.02.041

new authenticated key agreement protocol with selectable identities. To prove the security of their scheme in the random oracle model, they also introduced a new assumption called the k-multiple bilinear collision attack assumption (k-MBCAA1).

Unfortunately, the Guo et al. scheme [12] is inefficient in terms of the computation cost. Suppose that user A has m identities and B has n identities and that A chooses k identities as B's public key. During a key agreement process, A has to generate n data items for exchange and carry out $(k+1)n$ scalar multiplications and kn addition operations in ellipse curves. Furthermore, in their scheme, the PKG has to authenticate all identities and generate a resultant private key for a user. This would be a burden to the PKG for a large group of users. We also notice that their scheme is not dynamic. When a new identity is added or an old identity is canceled, the corresponding private key will become invalid and a new private key needs to be issued by the PKG. This implies that the PKG has to re-authenticate the identities that it has authenticated before, as these data are not recorded. In a dynamic environment where users change some of their identities from time to time, their scheme is not practical because PKG needs to be "online", which is not desirable for the PKG.

We observed that identities for a user can be classed as permanent and temporary in the real world. For example, the birthday and the identity card number are permanent identities, while the mobile phone number and the student card number might be temporary identities. When user A wants to establish a session key with user B, he could just select a permanent identity and several temporary identities, instead of all identities, from B's identity set as B's public key. For example, when A wants to purchase something from an online shop, she only needs to choose B's (as a seller) identity card number, and mobile phone number as B's public keys. The staff from the Traffic Management Bureau could choose just B's identity card number, driver's license number, email address and other related identities as B's public key.

In this paper, we present an efficient dynamic identity-based key agreement protocol with selectable identities. The key idea is that we use a private key corresponding to a permanent identity as the user's private key. Using this private key, a user with multiple identities can establish a shared session key with another user. As a result, our scheme has the following features:

- The PKG avoids authenticating all of the identities when generating a private key for a user. It only needs to authenticate one identity and generate a private key for the user corresponding to this identity at the beginning of the setup stage. After that, PKG can be "offline" as in other identity-based schemes.
- Our scheme achieves the dynamic property. A user can add, delete, or update temporary identities at will, which will not affect its private key.
- Our scheme is efficient in terms of the computation cost. In our scheme, A only needs to generate k messages ($k \leq n$, where by n we denote the number of identities that a user holds), and needs to do k scalar multiplications and k addition operations. The computation cost is only related to k, which is generally small in the real world.
- The security of our scheme can be reduced to the bilinear Diffie–Hellman assumption, which is a standard assumption and is weaker than the "k-multiple bilinear collision attack assumption (k-MBCAA1)" used in the proof of the scheme in [12].

The rest of this paper is organized as follows. In Section 2, we describe the preliminaries including bilinear pairing, security assumption and the security model. In Section 3, we present a multi-identity key agreement protocol. In Section 4, we prove the security of the multi-identity key agreement protocol. In Section 5, we conclude the paper.

2. Preliminaries

In this section, we introduce the background knowledge that will be used for our scheme. We give the basic definition and properties of bilinear pairings, the computational problems and the security model.

2.1. The bilinear map and security assumption

We first revisit the basic definition of bilinear map and the bilinear Diffie–Hellman problem. The details can be found in [3].

The bilinear map $\hat{e}$ is defined over two groups of the same prime order q denoted by $\mathbb{G}$ and $\mathbb{G}_T$ in which the computational Diffie–Hellman problem is hard. More formally, we have the following definition:

Definition 1 (*Bilinear Map*)**.** Let $\mathbb{G}$ be an additive group of prime order q and $\mathbb{G}_T$ a multiplicative group of the same order. Let P denote a generator of $\mathbb{G}$. An admissible pairing is a bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ which has the following properties:

- Bilinear: given $Q, R \in \mathbb{G}$ and $a, b \in \mathbb{Z}_q^*$, we have $\hat{e}(aQ, bR) = \hat{e}(Q, R)^{ab}$.
- Non-degenerate: $\hat{e}(P, P) \neq 1_{\mathbb{G}_T}$.
- Computable: $\hat{e}$ is efficiently computable.

Typically, the map $\hat{e}$ can be derived from either the Weil pairing or Tate pairing on an elliptic curve over a finite field. More details on how these groups, pairings and other parameters should be selected in practice for efficiency and security can be found in [3,13,14].