Journal of Computer and System Sciences 81 (2015) 125–131

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

A strong provably secure IBE scheme without bilinear map ☆

Minghui Zheng [a,*], Yang Xiang [b], Huihua Zhou [a]

[a] *Department of Computer Science, Hubei Minzu University, Enshi, China*
[b] *School of Information Technology, Deakin University, Deakin, Australia*

ARTICLE INFO

Article history:
Received 31 January 2013
Accepted 13 December 2013
Available online 5 July 2014

Keywords:
Identity-based encryption
Bilinear map
Provable security
Combined public-key scheme

ABSTRACT

Identity-based encryption (IBE) allows one party to send ciphered messages to another using an arbitrary identity string as an encryption key. Since IBE does not require prior generation and distribution of keys, it greatly simplifies key management in public-key cryptography. According to the Menezes–Okamoto–Vanstone (MOV) reduction theory, the IBE scheme based on bilinear map loses the high efficiency of elliptic curve because of the requirement of large security parameters. Therefore, it is important to build a provably secure IBE scheme without bilinear map. To this end, this paper proposes an improved IBE scheme that is different from the previous schemes because this new scheme does not use symmetric encryption algorithm. Furthermore, it can be proven to be secure against adaptively chosen identity and chosen plaintext attacks in the standard model. Elaborated security and performance analysis demonstrate that this new scheme outperforms the previous ones in terms of the time complexity for encryption and decryption.

1. Introduction

To simplify the certificate management in traditional public key infrastructure (PKI), Shamir [1] pioneered a novel public-key encryption scheme, called identity-based encryption scheme that consists of four algorithms: *Setup*, *Extract*, *Encrypt*, *Decrypt*. The *Setup* algorithm generates the system parameters and private parameter. The *Extract* algorithm uses the private parameter to generate the private-key corresponding to a given identity. The *Encrypt* algorithm encrypts plaintext for a given identity. Finally, the *Decrypt* algorithm decrypts ciphertext using the private-key. This scheme can significantly reduce complexity, compared to the previous authentication schemes.

Years later, Boneh and Franklin [2] introduced the first identity-based encryption scheme using groups with efficiently computable bilinear maps. Although they used the random oracle (RO) heuristic to prove security under the bilinear Diffie–Hellman assumption [3], a significant open question was whether the RO model could be removed. Furthermore, by virtue of bilinear maps, Boneh and Boyen [4,5] proposed two IBE schemes, which are proven to be secure in the standard model. However, the IBE scheme in [4] is efficient under a weaker security definition, namely selective identity and chosen plaintext security (IND-sID-CPA security). The ciphertext of the IBE scheme from [5] is remarkably long, so it is also inefficient in practice. To overcome these disadvantages, Waters [6] used the bilinear maps to construct a new and efficient IBE scheme, which has a shorter ciphertext and is proved to be secure under the strongest security definition (in the standard model),

☆ Supported by the National Natural Science Foundation of China under Grant Nos. 61173175, 61262078, and by the Natural Science Foundation of Hubei Province under Grant No. 2012FFA006.

* Corresponding author at: 39 Xueyuan Road, Enshi, 445000, China.
E-mail address: mhzheng3@163.com (M. Zheng).

http://dx.doi.org/10.1016/j.jcss.2014.06.020
0022-0000/© 2014 Elsevier Inc. All rights reserved.

namely adaptively chosen identity and chosen plaintext security (IND-ID-CCA security) [7]. Following the work of Waters, Seo et al. [8,9] and Zhang et al. [10,11] proposed anonymous hierarchical IBE scheme with constant size ciphertext under the standard model.

Although all the aforementioned IBE schemes used the bilinear map, according to Menezes–Okamoto–Vanstone (MOV) reduction theory [2], the IBE scheme using the bilinear map often loses the high efficiency of elliptic curve. Specifically, these IBE schemes must rely on a supersingular elliptic curve. Therefore, it often requires a large security parameter (input size of the problem) and takes a huge cost to compute the bilinear map. Instead, the IBE scheme without bilinear map can rely on a non-supersingular elliptic curve. It often chooses the 160 bit security parameter. As a result, the IBE schemes without bilinear map have attracted much research attention all the time.

Based on the standard quadratic residuosity that modulo an RSA composite N in the RO model, Cocks [12] proposed an elegant IBE scheme without bilinear maps firstly. But this scheme is not efficient. For example, to encrypt a 128 bit plaintext using a 1024 bit modulus, it ends up with a ciphertext of the size 32,678 bytes. Following Cocks's scheme, Boneh et al. [13] constructed a space efficient IBE scheme in which the result of encrypting a 128 bit plaintext is a ciphertext of the size 145 bytes. Because the last two schemes have long ciphertext and high computation complexity (for each bit of plaintext, a computation of Jacobi symbol is needed), Xu et al. [14,15] proposed two new IBE schemes without bilinear map and having strong provable security. Although these schemes have high efficiency, short ciphertext , and tight reduction, they use symmetric encryption that needs more computing and inconvenient key management, and they do not have strong probable security.

Recently, several new IBE schemes have been proposed without bilinear map, such as the schemes based on the extended Chebyshev polynomial over finite fields [16], based on ideal lattice [17], and based on quadratic residuosity assumption [18,19]. But these schemes are all proven secure under the RO model. At the same time, several schemes that are proven secure under standard model have proposed, such as the schemes based on the quadratic residuosity assumption [13] and based on the tight security reduction [20].

This paper proposes an improved IBE scheme built upon the work of [14]. This new scheme has the strong provable security. Specifically, a secure hash function is used, and then the corresponding modification is given to complete the scheme. A detailed proof of security is given before the performance analysis of the new proposed scheme. The major contributions are summarized below:

(1) A one-way hash function is used in the *Extract* algorithm to replace the symmetric-encryption that needs more computing and inconvenient key management. As a result, the proposed new scheme is more efficient.
(2) Under the strong security definition of adaptively chosen identity and chosen plaintext security (IND-ID-CCA security), the proposed IBE scheme based on a weak hard problem contains the provable security. Therefore, the performance of security proof of the new IBE scheme is enhanced significantly.
(3) We analyze the tightness of the reduction and obtain an exact security bound that coincides with the one in the proof of security.

The remainder of this paper is organized as follows: Section 2 presents the definition of security. In Section 3, we propose an improved IBE scheme with strong provable security in details. In Section 4, we discuss provably security of the proposed scheme. The analysis of security reduction and efficiency are presented in Section 5. Finally, Section 6 concludes this paper.

2. Preliminaries

This section describes the underlying primitives used throughout this paper. The underlying primitives include the bilinear map, the computational Diffie–Hellman assumption, and the strongest security definition for IBE scheme currently.

2.1. Bilinear maps

Bilinear map was proposed by Boneh and Franklin [2] and was used to build some well-known and efficient IBE schemes.

Definition 1. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two groups of the large prime order q. The bilinear map is a map $\hat{e}:\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_2$ between these two groups, and the map must satisfy the following three properties:

(1) Bilinear: We say that a map $\hat{e}:\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_2$ is bilinear if $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$ for all $P,Q\in\mathbb{G}_1$ and $a,b\in\mathbb{Z}$.
(2) Non-degenerate: If P is a generator of $\mathbb{G}_1$ then $\hat{e}(P,P)$ is a generator of $\mathbb{G}_2$.
(3) Computable: There is an efficient algorithm to compute $\hat{e}(P,Q)$ for $\forall P,Q\in\mathbb{G}_1$.

2.2. CDH assumption

Definition 2. The N is the set of natural numbers and the R^+ is the set of positive real numbers. A function $\varepsilon:N\rightarrow R^+$ is said to be negligible if and only if for every polynomial $P(n)$ there exits an $n_0\in N$ such that for all $n>n_0$, $\varepsilon(n)\leq 1/P(n)$.