Computer Standards & Interfaces 44 (2016) 117–121

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

Fully secure fuzzy identity-based encryption for secure IoT communications

Yijun Mao [a], Jin Li [b], Min-Rong Chen [c,d,*], Jianan Liu [e], Congge Xie [e], Yiju Zhan [f]

[a] School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, China
[b] School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China
[c] School of Computer, South China Normal University, Guangzhou 510631, China
[d] College of Information Engineering, Shenzhen University, Shenzhen 518060, China
[e] Department of Computer Science, Jinan University, Guangzhou 510632, China
[f] School of Engineering, Sun Yat-Sen University, Guangzhou 510275, China

ARTICLE INFO

Article history:
Received 12 February 2015
Received in revised form 1 June 2015
Accepted 25 June 2015
Available online 30 July 2015

Keywords:
Fuzzy identity-based encryption
Tight reduction
Standard model
Secure communications
Internet of things

ABSTRACT

How to securely transmit data is an important problem in Internet of Things (IoT). Fuzzy identity-based encryption (FIBE) is a good candidate for resolving this problem. However, existing FIBE schemes suffer from the following disadvantages: rely on random oracle models, merely secure in selective-ID model, long public parameters, and loose security reduction. In this paper, we propose a new FIBE scheme. Our scheme is secure in the full model without random oracles, and at the same time has a tight security reduction and short public parameters. This means that our scheme is quite suitable for secure transmitting data in IOT.

1. Introduction

In the past few years, Internet of Things (IoT) [1] has been widely used in our daily life. IoT can be viewed as a physical and logical extension of the current internet, populated by billions of intelligent networked devices or "things" [2]. Since the devices in IoT are physically vulnerable and are often left unattended, IoT applications are usually vulnerable to security attacks. Thus the security problems gain more and more attention in IoT. In particular, how to securely transmit data in IoT systems is an important problem. Encryption is a potential technique which can be used for secure communications in IoT. It is worth noting that, traditional encryption technique cannot be trivially used in IoT systems, since the devices in IoT are usually source-constrained, and hence the encryption scheme should be quite efficient. In addition, errors would usually occur during the data transmission, and hence the encryption scheme should provide the feasibility of correcting the errors, i.e., error-tolerance.

Identity Based Encryption (IBE), introduced by Shamir [3] in Crypto 1984, is a public key encryption mechanism where an arbitrary string (such as a user's phone number, email address, identity number, etc.) can serve as the public key. The ability to use identities as public keys can naturally eliminate the need for certificates as used in the traditional pubic key infrastructure (PKI), and hence IBE is more desirable than traditional public key encryption in PKI. IBE has attracted great interests in the past few years, and many IBE schemes and the variants have been proposed in the past years [4–12]. However, IBE cannot provide the property of error-tolerance. To address this problem, in Eurocrypt'05, Sahai and Waters [13] introduced a new notion named fuzzy identity-based encryption (FIBE). In a FIBE scheme, a user with a private key for an identity *ID* is able to decrypt a ciphertext encrypted with an identity *ID* ' if and only if *ID* and *ID* ' are within a certain distance of each other as judged by some metrics. This means that FIBE is error-tolerant.

In Eurocrypt'05, Sahai and Waters [13] presented two constructions of FIBE systems. The first construction (SW-I for short) only allows for limited attributes, and the second one (SW-II) is a large universe construction that uses all elements in $\mathbb{Z}_p^*$ as attributes. Both schemes are only secure in a weak security model named selective-ID model, in which the adversary must commit the target identity (which the adversary wants to attack) ahead of the system setup. Besides, the public parameters in both constructions are somewhat long, that is, the public parameters size in SW-I grows linearly with the number of possible attributes in the universe, and in SW-II it grows linearly in a parameter which is fixed as the maximum size identity one can encrypt to.

* Corresponding author at: College of Information Engineering Shenzhen University, Shenzhen 518060, China.
E-mail address: mrongchen@126.com (M.-R. Chen).

http://dx.doi.org/10.1016/j.csi.2015.06.007
0920-5489/

As mentioned above, Sahai-Waters FIBE systems are only secure in the selective-ID model. As shown in [13], suppose that all identities are composed of n attributes and $\mathcal{U}$ is the universe of attributes, then to achieve the full security, these schemes will introduce a security degradation of $(|\mathcal{U}|)$. We stress that, a loose security reduction implies a lower security or the requirement of larger keys and ciphertext sizes to obtain the same security level, and thus make the system inefficient. Hence a stronger requirement for our FIBE system proposed in this paper is to be secure in the full model (i.e., the adversary can commit the target identity at any time), and yet the security reduction is tight.

Baek et al. [14] presented another FIBE scheme with short public parameters in the random oracle model.[1] However, a proof in the random oracle model can only serve as a heuristic argument and does not imply the security in the real world [16–19]. Thus FIBE schemes secure in the standard model (i.e., without random oracles) are more desirable.

Ren et al. [20] proposed a new FIBE scheme, and claimed that their scheme is secure in the full model without random oracles. Unfortunately, Wang et al. [21] and Tian et al. [22] independently present attacks against Ren et al's FIBE scheme, and indicated that Ren et al.'s scheme is insecure in the full model. Other works have been devoted to FIBE. Pirretti et al. [15] examined methods for applying the Sahai-Waters FIBE systems into practice and presented an implementation of these constructions. Chase [23] gave a multi-authority construction of FIBE which allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. They also showed how to apply their techniques to achieve a multi-authority version of the large universe KP-ABE.

1.1. Our contributions

In this paper, we propose a new FIBE scheme. Unlike previous selective-ID secure FIBE schemes, our proposed scheme is secure in the full model without random oracles. In addition, our scheme has the advantage of tight security reduction. Thus in contrast to previous FIBE schemes with loose security reduction, our scheme needs not to enlarge the keys size and ciphertext sizes to obtain the same security level. Our scheme also enjoys the advantage of constant size of public parameters. All of these indicate that our FIBE scheme is more efficient that previous schemes, and hence is more suitable for secure IoT communications.

1.2. Organization

The rest of this paper is organized as follows. Section 2 gives an introduction to bilinear pairings and some complexity assumptions. In Section 3, we review the definition and security notion for FIBE. We present our FIBE scheme in Section 4. The security proof for our scheme and a comparison between our FIBE scheme and some other FIBE schemes are also given in this section. Finally, Section 5 concludes this paper.

2. Preliminaries

2.1. Notations

Throughout this paper, let $\mathbb{Z}_p$ denote the set $\{0, 1, 2, \cdots, p-1\}$, and $\mathbb{Z}_p^*$ denote $\mathbb{Z}_p \backslash \{0\}$. For a finite set S, we let $|S|$ denote the cardinality of S, and $x \xleftarrow{\$} S$ means choosing an element x from the set S with a uniform distribution.

[1] In a previous work [15], Pirretti et al. also observed that Sahai-Waters construction can be implemented more efficiently if the random oracle is employed.

2.2. Bilinear pairings

Let $\mathbb{G}$ be a cyclic multiplicative group of prime order p, and $\mathbb{G}_T$ be a cyclic multiplicative group of the same order p. A bilinear pairing is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ with the following properties:

- Bilinearity: $\forall g_1, g_2 \in \mathbb{G}, \forall a, b \in \mathbb{Z}_p^*$, we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$;
- Non-degeneracy: there exist $g_1, g_2 \in \mathbb{G}$ such that $e(g_1, g_2) \neq 1$;
- Computability: there exists an efficient algorithm to compute $e(g_1, g_2)$ for $\forall g_1, g_2 \in \mathbb{G}$.

As shown in [24], bilinear parings can be obtained from the Weil pairing or Tate pairing over supersingular elliptic curves or Abelian varieties.

2.3. Complexity assumptions

The security of our constructions is based on a variant of the q-bilinear Diffie–Hellman exponent (BDHE) assumption. We here first recall the q-BDHE assumption, which has been used to construct an efficient HIBE scheme in [4] and a broadcast encryption scheme in [25]. The q-BDHE assumption is stated as follows: given a vector of $2q+1$ elements

$$\left(g', g, g^{\alpha}, g^{(\alpha^2)}, \cdots, g^{(\alpha^q)}, g^{(\alpha^{q+2})}, \cdots, g^{(\alpha^{2q})}\right) \in \mathbb{G}^{2q+1}$$

as input, output $e(g, g')^{(\alpha^{q+1})}$. Since the input vector is missing the term $g^{(\alpha^{q+1})}$, the bilinear map does not seem to help compute $e(g, g')^{(\alpha^{q+1})}$.

For convenience, hereafter, we use g_i and g_i' to denote $g^{(\alpha^i)}$ and $g'^{(\alpha^i)}$ respectively. Gentry [6] defined an almost identical assumption named q augmented bilinear Diffie–Hellman exponent (q-ABDHE) assumption: given a vector of $2q+2$ elements

$$\left(g', g'_{q+2}, g, g_1, g_2, \cdots, g_q, g_{q+2}, \cdots, g_{2q}\right) \in \mathbb{G}^{2q+2}$$

as input, output $e(g_{q+1}, g')$. Introducing the additional term g'_{q+2} still does not appear to help compute $e(g_{q+1}, g')$, since the term $g^{(\alpha^{q+1})}$ is missed in the input vector.

We here further modify the q-ABDHE assumption by introducing another additional term g_{2q+1}. That is, given a vector of $2q+3$ elements

$$\left(g', g'_{q+2}, g, g_1, g_2, \cdots, g_q, g_{q+2}, \cdots, g_{2q}, g_{2q+1}\right) \in \mathbb{G}^{2q+3}$$

as input, output $e(g_{q+1}, g')$. Again, introducing the additional term g_{2q+1} still does not appear to help compute $e(g_{q+1}, g')$, since the input vector is missing the term $g'^{(\alpha^{q})}$. We refer to this modified assumption as q modified bilinear Diffie–Hellman exponent (q-MBDHE) assumption. Our proposed systems are based on the decisional q-MBDHE assumption. Formally,

Definition 1. The decisional q-MBDHE problem in groups $(\mathbb{G}, \mathbb{G}_T)$ is, given a vector

$$\left(g', g'_{q+2}, g, g_1, g_2, \cdots, g_q, g_{q+2}, \cdots, g_{2q}, g_{2q+1}\right) \in \mathbb{G}^{2q+3}$$

for unknown $\alpha \xleftarrow{\$} \mathbb{Z}_p^*$ and the random element $Z \xleftarrow{\$} \mathbb{G}_T$, to decide whether $Z = e(g_{q+1}, g')$. For a probabilistic polynomial-time adversary $\mathcal{B}$, we define his advantage against the decisional q-MBDHE problem in groups $(\mathbb{G}, \mathbb{G}_T)$ as

$$Adv_{\mathcal{B},(\mathbb{G},\mathbb{G}_T)}^{q-MBDHE} \triangleq \left| Pr\left[\mathcal{B}\left(g', g'_{q+2}, g, g_1, g_2, \cdots, g_q, g_{q+2}, \cdots, g_{2q}, g_{2q+1}, e\left(g_{q+1}, g'\right)\right) = 1\right] - Pr\left[\mathcal{B}\left(g', g'_{q+2}, g, g_1, g_2, \cdots, g_q, g_{q+2}, \cdots, g_{2q}, g_{2q+1}, Z\right) = 1\right] \right|,$$