Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

On the security of two identity-based conditional proxy re-encryption schemes

Kai He [a,c], Jian Weng [a,*], Robert H. Deng [b], Joseph K. Liu [c]

[a] Department of Computer Science, Jinan University, Guangzhou 510632, China
[b] School of Information Systems, Singapore Management University, Singapore 178902, Singapore
[c] Faculty of Information Technology, Monash University, Australia

ARTICLE INFO

Article history:
Received 6 November 2015
Received in revised form 10 June 2016
Accepted 29 August 2016
Available online xxxx
Communicated by X. Deng

Keywords:
Conditional proxy re-encryption
Identity-based
Single hop
Multi-hop
Chosen-ciphertext security

ABSTRACT

Proxy re-encryption allows a semi-trusted proxy with a re-encryption key to convert a delegator's ciphertext into a delegatee's ciphertext, and the semi-trusted proxy cannot learn anything about the underlying plaintext. If a proxy re-encryption scheme is indistinguishable against chosen-ciphertext attacks, its initialized ciphertext should be non-malleable. Otherwise, there might exist an adversary who can break the chosen-ciphertext security of the scheme. Recently, Liang et al. proposed two proxy re-encryption schemes. They claimed that their schemes were chosen-ciphertext secure in the standard model. However, we find that the original ciphertext in their schemes are malleable. Thus, we present some concrete attacks and indicate their schemes fail to achieve chosen-ciphertext security in the standard model.

© 2016 Published by Elsevier B.V.

1. Introduction

The notion of proxy re-encryption (PRE) was initially introduced by Blaze et al. [1]. In a PRE system, Alice can transform the ciphertext which is encrypted under her public key to another ciphertext which is encrypted under Bob's public key, so that Alice can securely share her information to Bob. According to the direction of transformation, PRE can be categorized into an undirectional PRE and a bidirectional PRE. In the unidirectional PRE, the ciphertext can be transformed from Alice to Bob. But in the bidirectional PRE, the ciphertext can be transformed not only from Alice to Bob, but it also can be transformed from Bob to Alice. According to another function, PRE can be categorized into a single-hop PRE and a multi-hop PRE. In the single-hop PRE, the ciphertext can only be transformed one time. But in the multi-hop PRE, the transformed ciphertext can continuously be transformed to the another user. PRE is a very useful primitive, it has many applications, such as encrypted e-mail forwarding, key distribution, access control and distributed file systems [2–10].

Chosen-ciphertext security is one of the most important goals to construct a PRE scheme. In 1998, Blaze et al. [1] proposed a bidirectional PRE scheme with chosen-plaintext security. In 2007, Canetti and Hohenberger [11] defined a chosen-ciphertext security model for the PRE scheme and proposed two bidirectional multi-hop PRE schemes with chosen-ciphertext security. One is proved in the random oracle model. The other one is proved in the standard model. After that, many bidirectional secure PRE schemes (e.g. [12,13]) have been proposed. Any unidirectional PRE scheme can be easily transformed to a bidirectional one by running the former in both directions, while whether the reverse holds is unknown. In 2005, Ateniese et al. [8,9] first presented two practical unidirectional PRE schemes from bilinear map and both of the

* Corresponding author.
E-mail address: cryptjweng@gmail.com (J. Weng).

http://dx.doi.org/10.1016/j.tcs.2016.08.023
0304-3975/© 2016 Published by Elsevier B.V.

two schemes are chosen-plaintext secure. In 2008, Libert and Vergnaud [14] proposed the first unidirectional PRE scheme against replayable chosen-ciphertext attacks in the standard model. Since then, many unidirectional PRE schemes with chosen-ciphertext security have been proposed (e.g., [15–18]) and all these schemes are single-hop PRE schemes.

If a PRE scheme is in the identity-based setting [19], each user's public key is the user's identity, (e.g. email address). In 2007, Green and Ateniese [20] proposed the first unidirectional identity-based proxy re-encryption (IBPRE) scheme, which is chosen-ciphertext secure in the random oracle model. Then, many IBPRE schemes have been proposed, such as [21,10, 22–29].

In order to facilitate fine-grained access control in the PRE or IBPRE system, the type-based PRE scheme [30] and the conditional PRE scheme [31] were proposed. In both cases, the proxy can re-encrypt the ciphertext if and only if the condition in the ciphertext is the same as in the re-encryption key. In 2009, Weng et al. [32] proposed a new conditional PRE scheme with chosen-ciphertext security and re-formed the definition and security notion for a conditional PRE scheme. Additionally, they pointed out the secure risk in the scheme [31].

Recently, Liang et al. proposed two identity-based conditional PRE schemes. One is a unidirectional single-hop conditional PRE (UniSH-IBCPRE) scheme [33], the other one is a bidirectional multi-hop conditional PRE (BiMH-IBCPRE) scheme [34]. They claimed that their schemes can achieve chosen-ciphertext security in the standard model. However, we find the original ciphertext in their schemes cannot ensure the non-malleability. There may exist an adversary who can break the security of their schemes. For example, given a challenge ciphertext $CT^*_{ID^*_i} = \mathrm{Enc}(ID^*_i, m_\beta) = (\cdots, C^*, \cdots)$ under the target identity ID^*_i, where the ciphertext component C^* is not verified. First, the adversary modifies C^* to C', so it obtains another ciphertext $CT'_{ID^*_i} = (\cdots, C', \cdots)$. Then, it issues a re-encryption query on $CT'_{ID^*_i}$ to achieve another ciphertext CT'_{ID_j} under a corrupted user ID_j. Note that it is legal for the adversary to issue the re-encryption query. Since $(ID^*_i, CT'_{ID^*_i})$ is not a derivative of $(ID^*_i, CT^*_{ID^*_i})$. Next, the adversity uses the corrupted user ID_j's private key sk_{ID_j} to derive the underlying plaintext from the ciphertext CT'_{ID_j}.

Based on the above analysis, in this paper, we present an outside adversary to break the chosen-ciphertext security of Liang et al.'s schemes [33,34] and an inside adversity to break the chosen-ciphertext security of [33]. The outside adversary does not collude with the semi-trusted proxy. The inside adversity is a semi-trusted proxy, who can collude with a delegatee. Thus, we indicate that their schemes fail to achieve chosen-ciphertext security.

1.1. Organization

The rest of the paper is organized as follows. In Section 2, we review the bilinear map and the decisional bilinear Diffie–Hellman assumption. In section 3, we first review the definition, the security model and the construction of Liang et al.'s UniSH-IBCPRE scheme [33], and then we present the security analysis for the UniSH-IBCPRE scheme. In section 4, we first review the definition, the security model and the construction of Liang et al.'s BiMH-IBCPRE scheme [34], and then we present the security analysis for the BiMH-IBCPRE scheme. Finally, we draw conclusions in Section 5.

2. Preliminaries

2.1. Bilinear map

$\mathcal{G}$ and $\mathcal{G}_T$ are cyclic multiplicative groups of order p, g is a generator of $\mathcal{G}$. A bilinear map is a map $e : \mathcal{G} \times \mathcal{G} \to \mathcal{G}_T$ with the following properties:

- **Bilinearity:** $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for all $g_1, g_2 \in \mathcal{G}$ and $a, b \in \mathcal{Z}_p^*$.
- **Non-degeneracy:** There exists $g_1, g_2 \in \mathcal{G}$ such that $e(g_1, g_2) \neq 1_{\mathcal{G}}$.
- **Computability:** There exists an efficient algorithm to compute $e(g_1, g_2)$ for $g_1, g_2 \in \mathcal{G}$.

2.2. Decisional Bilinear Diffie–Hellman (DBDH) assumption

The DBDH problem in a bilinear group $(p, \mathcal{G}, \mathcal{G}_T, e)$ is defined as follows: Given a tuple (g, g^a, g^b, g^c, T) as input, output 1 if $T = e(g, g)^{abc}$ and 0 otherwise. The advantage of an algorithm $\mathcal{A}$ in solving the DBDH problem is defined as $Adv^{\mathrm{DBDH}}_{\mathcal{A}} = |\Pr[\mathcal{A}(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - \Pr[\mathcal{A}(g, g^a, g^b, g^c, T) = 1]|$, where $g \in \mathcal{G}, a, b, c \leftarrow \mathcal{Z}_p^*$, T is chosen randomly from $\mathcal{G}_{\mathcal{T}}$. We say that the DBDH assumption holds in the bilinear group $(p, \mathcal{G}, \mathcal{G}_{\mathcal{T}}, e)$ if all probabilistic polynomial-time (PPT) algorithms have negligible advantage in solving the DBDH problem.

3. Cryptanalysis of Liang et al.'s UniSH-IBCPRE scheme

In this section, first, we shall review the definition, the security model and the construction of Liang et al.'s UniSH-IBCPRE scheme [33]. Then, we give the security analysis for their construction.

Please cite this article in press as: K. He et al., On the security of two identity-based conditional proxy re-encryption schemes, Theoret. Comput. Sci. (2016), http://dx.doi.org/10.1016/j.tcs.2016.08.023

Download English Version:

https://daneshyari.com/en/article/4952334

Download Persian Version:

https://daneshyari.com/article/4952334

Daneshyari.com