Computer Standards & Interfaces 34 (2012) 380–389

Contents lists available at SciVerse ScienceDirect

Computer Standards & Interfaces

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

Hierarchical conditional proxy re-encryption

Liming Fang [a], Willy Susilo [b,*], Chunpeng Ge [a], Jiandong Wang [a]

[a] *College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China*

[b] *Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Australia*

ARTICLE INFO

Article history:
Received 2 September 2010
Received in revised form 21 October 2011
Accepted 2 January 2012
Available online 11 January 2012

Keywords:
Proxy re-encryption
Hierarchical conditional proxy re-encryption
Chosen-ciphertext security

ABSTRACT

In this paper, we introduce a new primitive called hierarchical conditional proxy re-encryption (HC-PRE) that enhances the concept of C-PRE by allowing more general re-encryption key delegation patterns. Hierarchical conditional proxy re-encryption (HC-PRE) scheme is the hierarchical extension of conditional proxy re-encryption (C-PRE) where the condition is a vector of keywords. We present an efficient construction of hierarchical key derivation C-PRE scheme where the ciphertext length is independent from the depth of the hierarchy. We further extend our work by presenting a more generalized key delegation, by allowing the use of a wildcard in the keyword vector.

1. Introduction

The notion of proxy re-encryption (PRE) scheme was put forth by Blaze, Bleumer, and Strauss [4]. The goal of such a system is to securely enable a proxy to re-encrypt a ciphertext under a delegator's public-key and designate it to a delegatee without relying on any trusted parties. The notion of PRE has been found very useful in many applications, such as in law enforcements, cryptographic operations in storage-limited devices and email forwarding. For example, users can assign their email server as the proxy such that it can re-encrypt the emails to allow different users to open it without the need to know the contents of the email.

A proxy in traditional PRE system is too powerful as it has the ability to encrypt *all* of the user's (such as Alice) emails to another user (such as Bob). In a corporate email forwarding scenario, instead of converting *all* ciphertexts (which are the encrypted emails), Alice may only want the proxy to convert the ciphertexts with a certain keyword. In particular, for example when Alice is away on holiday, she only wants Bob to read emails with the keyword “business” that will require her urgent attention, instead of reading all of her emails. To fill this gap, Weng et al. [22] presented the notion of conditional proxy re-encryption (C-PRE), whereby only ciphertexts satisfying a certain keyword condition set by Alice can be transformed by the proxy.

Although C-PRE is useful in many applications, we found that sometimes we need more than its basic features (to be discussed further later). Furthermore, there remain some important issues to consider as follows.

- (*Re-delegation.*) Suppose a proxy Charlie has the re-encryption key under the keyword “Subject: finance”. It means that Charlie can re-encrypt any encrypted emails that Alice receives which has the keyword “Subject: finance”. Suppose, Charlie is away in July and he would like to re-delegate the re-encryption rights under the keyword vector “Date: July” and “Subject: finance” to another proxy, David, then Charlie will be required to derive a re-encryption key with a keyword vector $W' =$ (“*Date*: *July*”, “*Subject* : *finance*”) from the re-encryption key with the keyword vector $W =$ (“*Subject*: *finace*”) that he acquired originally from Alice. Hence, the re-delegation will require a C-PRE scheme that supports *re-delegation* from a keyword vector W to W', where $W \subseteq W'$.
- (*Conjunctive Delegation.*) Traditional C-PRE schemes only allow the proxy to re-encrypt the ciphertext that match a certain keyword, but do not allow for boolean combinations of several keywords. For example, we define an email to have the following keyword fields: “From”, “Date”, “Importance”, and “Subject”. Suppose Alice will be away, then she wants a proxy to re-encrypt any important emails. Rather than re-encrypting all emails, Alice might only want those emails that are marked “From: Bob” with “Date: July”, “Importance: High” and pertain to “Subject: finance”. It is unfortunate that the traditional C-PRE cannot be used to solve this case. In this scenario, the ability to re-encrypt on the conjunction of the keywords, “Bob”, “July”, “High” and “finance” is required. Furthremore, Weng et al. [22] also left an open problem on how to construct CCA-secure C-PRE schemes supporting “OR”

[*] Corresponding author.
E-mail addresses: fangliming@nuaa.edu.cn (L. Fang), wsusilo@uow.edu.au (W. Susilo).

0920-5489/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2012.01.002

and "AND" gates over conditions. A possible approach is to define a meta-keyword for every possible conjunction of keywords. Like regular keywords, these meta-keywords can be associated with ciphertext. For example, an email that contains the keywords "Bob", "July", "High " and "finance" may be augmented with the meta-keyword "Bob:July:High:finance". The obvious drawback of this approach is that an email that contains m keywords requires an additional 2^m meta-keywords to allow all possible conjunctive re-encryption keys.

1.1. Our contributions

In this paper, we introduce a new primitive called hierarchical conditional proxy re-encryption (HC-PRE) that enhances the concept of C-PRE by allowing more general re-encryption key delegation patterns. HC-PRE scheme is the hierarchical extension of C-PRE where the condition is vectors of keywords. The re-encryption keys for a proxy with keyword vector length k can derive re-encryption keys for their children, i.e. with length $k+1$. We formalize the HC-PRE security model by incorporating the advantages in the previous C-PRE schemes. We also define the first level and second level ciphertext security for HC-PRE.

One may think that HC-PRE can be trivially obtained from a CCA secure C-PRE scheme. However, unfortunately this is not trivial to do so due to the collusion problem. To illustrate this, we will demonstrate that Weng et al.'s C-PRE scheme (which is CCA secure) cannot be converted trivially to HC-PRE. This is because the keyword $(H_2(pk_i,w))^{-sk_i}$ in the re-encryption key $(H_2(pk_i,w)pk_j^s)^{-sk_i}$ in Weng et al.'s scheme is not equipped with any random value, and hence collusion attack can be mounted when HC-PRE scheme is constructed this way. Furthermore, adding a random value to the existing scheme is not a trivial task either.

Subsequently, we present an efficient construction of hierarchical conditional proxy re-encryption (HC-PRE) scheme. Our efficient construction has several advantages over previous such systems, including:

- (*Re-delegation.*) The re-encryption keys for the proxy with keyword vector length k can derive re-encryption keys for their children, which are of length $k+1$.
- (*Constant Size Ciphertext.*) Two level ciphertexts produced by our scheme are independent of the keyword vector length. In our first HC-PRE scheme, the second level ciphertext contains only five elements. The first level ciphertext contains only three elements and decryption requires only one bilinear map computation.
- (*Chosen-Ciphertext Security.*) Our scheme achieves chosen-ciphertext security on the first and second level ciphertext security.

Finally, we also extend our hierarchical conditional proxy re-encryption scheme to achieve a more generalized key delegation by allowing more general re-encryption key delegation patterns. That means a re-encryption key is derived for a vector of a keyword vector, where entries can be left blank using a wildcard. This re-encryption key can then be used to derive re-encryption keys for *any* pattern that replaces wildcards with concrete keyword strings.

1.2. Related work

The concept of PRE was proposed by Blaze et al. [4]. PRE can be categorized into bidirectional PRE and unidirectional PRE. In a bidirectional PRE, the proxy can transform from a delegator to a delegatee and vice versa. In contrast, the proxy in unidirectional PRE cannot transform ciphertexts in the opposite direction. PRE also can be categorized into single-hop and multi-hop. Single-hop means that a re-encrypted ciphertext cannot be further re-encrypted. In contrast, multi-hop means that a ciphertext can be re-encrypted several times. In 2005, Ateniese et al. [1] demonstrated how to construct unidirectional schemes using bilinear maps and simultaneously prevent proxies from colluding with delegatees in order to expose the delegator's secret key. Since then, there are many PRE schemes were presented using pairing [8,15,9,17,24]. Since in a PKI-based setting, it is needed to distribute public key certificates, the work [15,9] extended the above notion to identity-based proxy re-encryption (IB-PRE). Since pairing computations are very costly, the subsequent work [12,19,11,16] studied the construction of PRE schemes without bilinear pairings, which is particularly useful in the resource limited environment.

Weng et al. [22] introduced the notion of conditional proxy re-encryption (or C-PRE), whereby only ciphertexts satisfying one condition set by Alice can be transformed by the proxy and then decrypted by Bob. They also proposed a CCA secure C-PRE scheme in the random oracle model. Unfortunately, Weng et al. [23] showed that Weng et al.'s C-PRE scheme [22] fails to achieve the CCA-security, and subsequently they proposed a more efficient CCA secure C-PRE scheme, and proved its chosen ciphertext security under the decisional bilinear Difie-Hellman (DBDH) assumption in the random oracle model. Similarly, in the full version of paper in PKC 08, Libert and Vergnaud [17] introduced a PRE scheme to provide warrant-based and keyword-based delegations. Tang et al. [20] also introduced type-based proxy re-encryption. Recently, Chu et al. introduced a conditional proxy broadcast re-encryption [10], in which the proxy can delegate decryption rights to a set of users at a time. Since the conditions in the previous C-PRE are not anonymous, based on PRE and PEKS (public key encryption with keyword search [3,7,18,25]), Fang et al. [14] presented a replayable CCA secure anonymous conditional proxy re-encryption scheme without requiring random oracle. Vivek et al. [21] proposed an efficient C-PRE scheme which uses substantially less number of bilinear pairings compared to Weng et al.'s scheme [23]. Nevertheless, the security notions in [21] only considered the second level ciphertext security, and hence, it does not address the first level ciphertext (original ciphertext) security, and therefore, it is deemed to be incomplete. Furthermore, in Vivek et al.'s definition, the proxy requires two key pairs (i.e., the partial re-encryption key and the condition key) to perform the transformation, and the drawback is that the condition key ck_{i^*,w^*} is same for different delegatees when the delegator is the same. Thus, the adversary can combine the condition key ck_{i^*,w^*} and the re-encryption key $rk_{i^*,j}$ with pk_j to attack the C-PRE scheme, and that is the reason why they prohibit this query. Hence, we consider that this approach is rather unnatural in practice.

1.3. Paper organization

The rest of this paper is organized as follows. In Section **2**, we will provide the definitions and complexity assumption that will be used throughout this paper, together with the security model of hierarchical C-PRE schemes. In Section **3**, we present our hierarchical C-PRE in the random oracle model. In Section **4**, we extend our HC-PRE scheme to achieve a more generalized key delegation. In Section **5**, we provide some applications for HC-PRE schemes. Finally, Section **6** concludes the paper.

2. Definitions

In this section, we first review the complexity assumptions required in our schemes, and then provide the definition and security of a hierarchical conditional proxy re-encryption scheme.

2.1. Negligible function

A function $\epsilon(n)$: $N \mapsto R$ is negligible in n if $1/\epsilon(n)$ is a non-polynomially-bounded quantity in n.