Information Sciences 180 (2010) 4042–4059

Contents lists available at ScienceDirect

Information Sciences

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

Multi-use and unidirectional identity-based proxy re-encryption schemes

Hongbing Wang [a], Zhenfu Cao [a,*], Licheng Wang [b]

[a] Department of Computer Science and Engineering, Shanghai Jiao Tong University, No. 800, Dongchuan Road, Shanghai 200240, PR China
[b] Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, PR China

ARTICLE INFO

Article history:
Received 16 October 2007
Received in revised form 7 May 2010
Accepted 18 June 2010

Keywords:
Random padding
Identity-based encryption
Proxy re-encryption
Bilinear pairing
Dynamic directed graph

ABSTRACT

In a proxy re-encryption scheme, a semi-trusted proxy is given special power that allows it to transform a ciphertext for Alice into a ciphertext for Bob without learning any information about the messages encrypted under either key. When a proxy re-encryption scheme is constructed in an identity-based setting, it means that a proxy converts a ciphertext encrypted under Alice's identity into a ciphertext under Bob's. Proxy re-encryption has become more and more popular these years due to the fact that it has many practical applications. In this paper, we present an IND-CCA2 secure identity-based proxy re-encryption scheme which has several useful properties, including, multi-use, unidirectionality, etc. Finding a unidirectional, multi-use, and CCA2-secure proxy re-encryption scheme is presented as an open problem by Green et al. Fortunately, our identity-based proxy re-encryption scheme is a solution to this problem. As a middleware for fulfilling our main goal, we also propose a new construction of identity-based encryption using random padding techniques. The security of our schemes is based on the standard decisional bilinear Diffie–Hellman assumption in the random oracle model.

1. Introduction

A basic goal of public-key encryption is to allow only the private key holder to decrypt the ciphertext which is encrypted under the corresponding public-key. Before the concept of the proxy re-encryption (PRE) was brought out, ciphertext conversion between different users was accomplished by means of decrypting the message, then-encrypting it with the new key, which implies access to the original plaintext and a reliable copy of the new encryption key [7]. In order to effectively remedy the drawback of the above approach, Mambo and Okamoto [26] introduced a methodology for delegating decryption rights. This can be considered as the primitive of proxy re-encryption.

But, the exact concept of proxy re-encryption was firstly introduced by Blaze et al. [7] at Eurocrypt'1998. In a PRE scheme, a proxy can convert a ciphertext computed under Alice's (delegator) public-key into a new ciphertext which could be decrypted by Bob (delegatee). When this concept extends to an identity-based proxy re-encryption (IB-PRE) setting, it means that a proxy can translate a ciphertext under Alice's identity into the one computed under Bob's identity. In a PRE, or an IB-PRE scheme, the proxy performs the transformation by using a re-encryption key which is, in general, generated by Alice. During the transformation, the proxy should not be able to learn the plaintext. Moreover, a PRE/IB-PRE scheme requires that no useful information on the secret keys of Alice and Bob can be deduced from the re-encryption keys. Both PRE and IB-PRE primitives could be used for different application scenarios, such as email forwarding, law enforcement, and performing cryptographic operations on storage-limited devices and secure network file storage [3,4,32,33].

* Corresponding author. Tel.: +86 21 34205345; fax: +86 21 34204728.
E-mail address: zfcao@cs.sjtu.edu.cn (Z. Cao).

0020-0255/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2010.06.029

The fundamental property of proxy re-encryption schemes is that the proxy is not fully trusted, i.e., it should not know the secret keys of Alice or Bob, and should not learn the plaintext during the conversion. For PRE schemes which are not against collusion attacks, we usually assume that at least one of the two principals (proxy and delegatee) is honest or that their collusion is preventable or detectable via some other means. A proxy re-encryption scheme requires the following data components [20]:

- *Public parameters.* All users in a proxy re-encryption deployment share a common set of public parameters. These parameters may be fixed (specified as a part of the scheme), or they may differ between deployments.
- *Public and secret key pairs.* Each user in a deployment generates a public/secret key pair. Just as in a public-key encryption scheme, the public-key is published (preferable in an authenticated form), while the secret key remains unknown to anybody but the user.
- *Delegation keys.* Each user may generate an arbitrary number of delegation (re-encryption) keys, e.g., $rk_{Alice\rightarrow Bob}$, $rk_{Alice\rightarrow Carol}, \ldots$, etc. To generate $rk_{Alice\ \rightarrow Bob}$, Alice combines her secret key with Bob's public-key. The resulting delegation key may then be transmitted (securely) to a re-encryption proxy.
- *Ciphertexts.* Ciphertexts are created when a user encrypts a message (plaintext) under some public-keys. In a proxy re-encryption scheme, the ciphertexts can generally be divided into the following three types:

1. *Non-re-encryptable ciphertexts* have a structure that cannot be re-encrypted by a proxy (proxies). The use of non-re-encryptable ciphertexts is appropriate for certain applications where a sender wishes to ensure that only the specified recipient has the ability to decrypt the ciphertexts.
2. *Re-encryptable ciphertexts* can be re-encrypted by a proxy (proxies). This is the standard form of ciphertexts in a proxy re-encryption scheme.
3. *Re-encrypted ciphertexts* are generated when a proxy re-encrypts a re-encryptable ciphertext. In some schemes, re-encrypted ciphertexts have the same form as non-re-encryptable ciphertexts. In this case, the delegatee Bob may not learn whether the ciphertext was originally encrypted to him, or to some other users.

Similar to most of the existing proxy re-encryption schemes, we do not consider the non-re-encryptable ciphertexts in our IB-PRE construction. For clarity, we adopt Green's notion of "encryption level" [21] as an implicit property of a re-encryptable ciphertext. A ciphertext generated directly using the encrypt algorithm is termed a "*first-level*" ciphertext. The application of the re-encryption algorithm to an *ith-level* ciphertext results in an $(i+1)$*th-level* ciphertext.

1.1. Related work

There are several papers worthy of being mentioned after the birth of the concept of proxy re-encryption [7], such as those have been proposed in the context of public-key encryption [2–4,11,15,23,25,29,30], and those in the identity-based settings [21]. Note that there are two similar but a little different concepts, proxy encryption and proxy re-encryption. In proxy encryption, Alice allows Bob to decrypt ciphertexts meant for her. While proxy re-encryption schemes are a (strict) subset of proxy encryption schemes [11], where a newly introduced, semi-trusted proxy can convert ciphertexts for Alice into ciphertexts for Bob. Thus Bob can decrypt it directly with his own private key. Proxy encryption schemes are currently realized under a broader class of complexity assumptions than proxy re-encryption. Some proxy cryptosystematic works include [12,22,34].

In 2006, Green and Atenises [21] firstly presented two identity-based proxy re-encryption schemes: one is IND-Pr-ID-CPA secure and the other is IND-Pr-ID-CCA secure. Both of them are proven secure in the random oracle model under the decisional bilinear Diffie–Hellman (DBDH) assumption. Their CCA-secure IB-PRE scheme is unidirectional and single-use. Concurrently and independently, Canetti and Hohenberger [11] proposed a CCA-secure public-key PRE scheme which is bidirectional and multi-use. Relative to IB-PREs, public-key PREs have made more progress, such works include [2–4,15,25,29], etc. Most recently, Ateniese et al. described a new attribution of PRE - key-privacy, they also proposed a CPA-secure unidirectional, single-use and key-private PRE scheme in [2]. Key-privacy is a very useful attribution of PRE. In [2], Ateniese et al. indicated that there are no PRE schemes satisfy the newly proposed attribution except theirs.

Comparisons between some PRE/IB-PRE schemes are shown in Table 1. These schemes are all implemented in bilinear groups.

1.2. Our contributions

Inspired by the famous IBE scheme BF01, which is named after its inventors Boneh and Franklin [10], we at first construct a new identity-based encryption scheme (IBE). In our scheme, we use random padding techniques to ensure the non-malleability of the ciphertexts instead of using a hash encapsulated on a bilinear pairing. Then, based on this newly derived IBE scheme, we design an identity-based proxy re-encryption scheme by adopting the method in [21]. Our IB-PRE is unidirectional, multi-use and IND-CCA2 secure under the DBDH assumption in the random oracle model. Our solution gives a confirmable answer to the open problem mentioned in [21], i.e., to find efficient constructions for multi-use CCA-secure IB-PRE schemes.