Theoretical Computer Science 542 (2014) 1–16

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

PRE: Stronger security notions and efficient construction with non-interactive opening ☆

Jiang Zhang [a,b], Zhenfeng Zhang [a,b,*], Yu Chen [c]

[a] Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
[b] State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
[c] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Article history:
Received 27 January 2013
Received in revised form 11 February 2014
Accepted 22 April 2014
Communicated by X. Deng

Keywords:
Public key encryption
Proxy re-encryption
Chosen key model
Knowledge of secret key model
Chosen-ciphertext security
DBDH

ABSTRACT

In a proxy re-encryption (PRE) scheme, a proxy is given a re-encryption key and has the ability to translate a ciphertext under one key into a ciphertext of the same message under a different key, without learning anything about the message encrypted under either key. This paper first shows that the chosen key (CK) model which allows the adversary to adaptively choose public keys for malicious users, is strictly stronger than the knowledge of secret key models (KOSK) that most of previous PREs rely on. Then, the paper presents an efficient CCA secure PRE scheme in the stronger CK model based on the decisional bilinear Diffie-Hellman (DBDH) assumption without the random oracle heuristic. The paper also considers a useful property in PRE applications, namely, "non-interactive opening" and an extended scheme is given to support the property. Compared with previous schemes, the PRE scheme in this paper has a good overall performance in terms of ciphertext length, computational cost, strong and realistic security model as well as a well-studied assumption.

1. Introduction

In 1998, Blaze, Bleumer, and Strauss [6] proposed the notion of "atomic proxy re-encryption", in which a semi-trusted proxy is given a re-encryption key that allows it to translate a ciphertext under one key into a ciphertext of the same message under a different key, without seeing the underlying plaintext. A proxy re-encryption (PRE) scheme is said to be *bidirectional* if a re-encryption key $rk_{1,2}$ allows the proxy to translate ciphertexts under the delegator's public key pk_1 to ciphertexts under the delegatee's public key pk_2 and *vice versa*, else it is *unidirectional* if a re-encryption key $rk_{1,2}$ only allows the proxy to translate ciphertexts under pk_1 to ciphertexts under pk_2. There is also another method to classify PRE schemes, namely, a scheme is *single-hop* [33] if the ciphertext can only be transformed once, otherwise it is *multi-hop* [9].

In the last decade, proxy re-encryption has attracted many researchers' attention [6,9,33,37] and has plenty of exciting applications in key management [6], email forwarding [29,26], law enforcement [23], publish/subscribe systems [28],

☆ The first and second authors are sponsored by the National Basic Research Program of China (No. 2013CB338003), the National Natural Science Foundation of China (Nos. 61170278, 91118006), and the 863 project (No. 2012AA01A403). The third author is sponsored by the National Natural Science Foundation of China under Grant No. 61303257.

* Corresponding author at: Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China.
E-mail addresses: jiangzhang09@gmail.com (J. Zhang), zfzhang@tca.iscas.ac.cn (Z. Zhang), cycosmic@gmail.com (Y. Chen).

http://dx.doi.org/10.1016/j.tcs.2014.04.028
0304-3975/

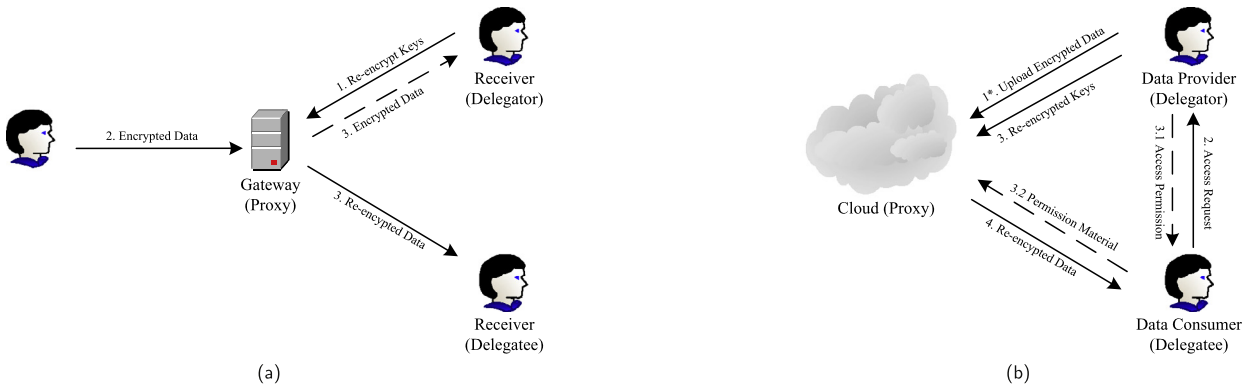

Fig. 1. Two classical usages of PREs in applications (1. The delegator itself may also be a delegatee, for example, in bidirectional schemes. 2. The re-encryption keys may be generated by running a multi-party protocol among the three users, not just simply by the delegator. 3. The dashed lines denote the possible steps. 4. The upload stage in Case (b) may continue through the life of the system).

multicast [40], secure file systems [2], telemedicine [25], digital right management [43] and so on. Abstractly, most of the applications use PREs in two classical ways as in Fig. 1. The first one purely uses PREs to delegate the decryption rights, namely, the delegator himself is a message receiver. For example, a manager wants to redirect his encrypted emails to his secretary. The second one employs PREs to provide access control, namely, the delegator creates the ciphertexts on his own and uses PREs to control which users (that he may not know when generating the ciphertexts) can access the underlying messages. For example, a data provider (continuously) uploads valuable information to a cloud server in encrypted form (since the cloud may not be worth trusting). Whenever a data consumer wants to read this information, he has to first acquire access permission from the data provider in order to obtain translated ciphertexts under his own key.

1.1. Related work

Mambo and Okamoto [35] proposed the idea of delegating decryption rights. Blaze et al. [6] later introduced the notion of "atomic proxy re-encryption", and gave a bidirectional scheme. Since then, many works of handling different practical problems appeared in the literature [24,23,46]. For example, in 2005, Ateniese et al. [2] considered PRE schemes with temporary delegation, where the delegator can periodically change delegation relationships without changing his public key. In such a system, a re-encryption key can only be used during a restricted time period. However, almost all the constructions above are only secure against *chosen-plaintext attacks (CPA)*, which may not meet the security requirement in real applications (e.g., encrypted email forwarding [9]).

But as Canetti and Hohenberger [9] commented, if we directly adapted the CCA security of normal PKEs to the PRE setting, it seems almost self-contradictory, since on the one hand, we require the ciphertext is non-malleable, on the other hand, we want the proxy to "translate" a ciphertext under one key to another key. Canetti and Hohenberger [9] circumvented this difficulty by introducing a notion related to the *replayable chosen-ciphertext attacks (RCCA)* [10] security,[1] that is, some legitimate modifications of a ciphertext are allowed (e.g., re-encryption). They also proposed a scheme that satisfied their security definition in the standard model, and left an open problem to construct an (R)CCA secure unidirectional PRE scheme (in the standard model). Later, Libert and Vergnaud [32] adapted their security definition to the single-hop unidirectional proxy re-encryption setting, and proposed the first RCCA secure single-hop unidirectional PRE scheme based on the 3-weak Decision Bilinear Diffie–Hellman Inversion (3-wDBDHI) assumption in the standard model. As in [9], they used the CHK technique [11] to achieve RCCA security, at the cost of increasing computational overhead and ciphertext length.

There are several unidirectional PRE schemes [2,42,13] in the random oracle model. In PKC 2009, Shao and Cao [42] constructed a unidirectional single-hop PRE scheme without pairings. Concretely, they constructed a scheme based on the DDH assumption over $\mathbb{Z}_{N^2}$ in the random oracle model. As the big size of the modulus N is needed (at least 1024 bits), Shao and Cao noticed that their scheme needs more time for computation and more storage for ciphertext than the scheme using pairings in the standard model [32].

In 2011, Libert and Vergnaud [33] noticed that most previous schemes are proven secure under the KOSK model (informally, all users including the adversaries have to reveal their private keys to a "key generation authority" whenever they create public keys for themselves), which might be worrisome in practice since current public key infrastructures (PKIs) do not suffice to meet such a strong requirement [33,5]. Thus, they considered the security in the CK model (also in the sense of RCCA) wherein the adversary itself can adaptively choose malicious users' public keys. Libert and Vergnaud [33] conjectured the KOSK model to be weaker than the CK model although they "did not find a strict separation in the context

[1] Informally, in the RCCA security game, the challenger rejects any decryption query that the underlying plaintext is either m_0 or m_1 in the second phase, where m_0, m_1 are the two equal length messages submitted by the adversary in the challenge phase.