Theoretical Computer Science 539 (2014) 87–105

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts

Kaitai Liang [a,*], Cheng-Kang Chu [b], Xiao Tan [a], Duncan S. Wong [a,*], Chunming Tang [c], Jianying Zhou [b]

[a] Department of Computer Science, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong Special Administrative Region
[b] Infocomm Security Department, Institute for Infocomm Research, 1 Fusionopolis Way, Singapore 138632, Singapore
[c] School of Mathematics and Information Science, Guangzhou University, 230 Wai Huan Xi Road, Guangzhou 510006, China

ARTICLE INFO

Article history:
Received 13 March 2013
Received in revised form 15 February 2014
Accepted 22 April 2014
Communicated by X. Deng

Keywords:
Conditional proxy re-encryption
Identity-based proxy re-encryption
Bilinear map
Chosen-ciphertext security
Constant size ciphertext

ABSTRACT

Proxy Re-Encryption (PRE) allows one user to delegate the decryption rights of his/her ciphertexts to another user. Since the introduction of Multi-Hop Identity-Based PRE (MH-IBPRE) by Green and Ateniese, the ciphertext size and the decryption complexity *grow linearly* in the number of re-encryption "hops". In this paper, for the first time, we propose an MH-IBPRE that maintains the (constant) ciphertext size and computational complexity regardless of the number of re-encryption hops. Moreover, our scheme is bidirectional and also supports conditional re-encryption. The scheme is proven secure against selective identity and chosen-ciphertext attacks and collusion resistant in the standard model. As of independent interest, we also show that the conditional re-encryption can also be extended to a set of conditions.

1. Introduction

Public Key Encryption (PKE) is a useful cryptographic primitive, whereby it allows a user to encrypt data under the public key of a receiver such that only the legitimate receiver with the corresponding private key can access the data. In social networks, a data is often shared among different users. A user, say Alice, can share a data, e.g., a picture or video with her friend, say Bob, without loss of confidentiality by using the traditional PKE. Sometimes, Bob might choose to further share the same data with another user, say Carol. In the context of PKE, Bob should first decrypt the ciphertext of the data sent by Alice, and next re-encrypt the data to Carol so as to finish data sharing. This, nevertheless, does not scale well when Bob is off-line or unavailable. An alternative way is that Bob delegates a proxy to encrypt the data to Carol when he is absent. However, this kind of delegation relies on either the accessibility of the data or knowledge of Bob's private key in the view of proxy.

To increase the flexibility of data sharing in the context of PKE, Blaze, Bleumer and Strauss [3] defined the notion of Proxy Re-Encryption (PRE), in which a *semi-trusted proxy* is allowed to transform a ciphertext intended for Alice into another ciphertext of the same plaintext intended for Bob using a given re-encryption key without accessing the underlying plaintext. If the re-encryption key allows the proxy to transform ciphertexts intended for Alice (i.e. *delegator*) to ciphertexts intended for Bob (i.e. *delegatee*) and vice versa, the scheme is *bidirectional*. Whereas, if the re-encryption key only supports

* Corresponding author. Tel.: +852 3442 8020/3442 9719; fax: +852 3442 0503.
E-mail addresses: kliang4-c@my.cityu.edu.hk (K. Liang), chengkangchu@gmail.com (C.-K. Chu), xiaotan4@gapps.cityu.edu.hk (X. Tan), duncan@cityu.edu.hk (D.S. Wong), ctang@gzhu.edu.cn (C. Tang), jyzhou@i2r.a-star.edu.sg (J. Zhou).

http://dx.doi.org/10.1016/j.tcs.2014.04.027
0304-3975/

the transformation from Alice to Bob (resp. from Bob to Alice), the scheme is *unidirectional*. PRE further comes to two flavors: one is *single-hop* PRE, and the other is *multiple-hop* PRE. If a ciphertext can be re-encrypted from Alice to Bob and cannot be further converted, the scheme is single hop. In multi-hop setting, a ciphertext can be re-encrypted from Alice to Bob and to Carol, and so on. The latter might be more desirable than the former in practice as it provides the flexibility of re-delegation, that is, the delegatee can re-delegate the ciphertexts to another users. PRE is applicable to many network applications, such as secure distributed files systems [1] and cloud storage systems (such as SugarSync[1] and Box[2]).

To implement PRE in the identity-based cryptographic setting with multi-hop property, Green and Ateniese [14] defined the notion of multi-hop identity-based proxy re-encryption (MH-IBPRE), and proposed a concrete scheme satisfying the new notion. The scheme allows a proxy to re-encrypt ciphertexts under an identity, e.g., ID_{Alice}, to another identity, e.g., ID_{Bob}, such that Bob can also decrypt, while the proxy can further re-encrypt the ciphertexts intended for a new identity, say ID_{Carol}, and so on. Since the introduction by Green and Ateniese [14], there are a few MH-IBPRE schemes that have been proposed in the literature.

Motivation. MH-IBPRE explores the applications of PRE in practice. In recent years, many Internet users and companies choose to store their data in cloud storage systems due to its considerable storage space. We here use cloud storage systems as an example to illustrate the application for MH-IBPRE so as to motivate our work. Suppose a group A of N employees will share some of their data mutually to fulfill a business project cooperatively. By employing MH-IBPRE, the data sharing can be fulfilled efficiently as follows. Without loss of confidentiality, each employee (e.g., $A.1$) might first encrypt his/her data (e.g., $m_{A.1}$) under the identity (e.g., $ID_{A.1}$) before uploading to the cloud. To share $m_{A.1}$ with another employee, say $A.2$, $A.1$ may generate a re-encryption key $rk_{A.1\rightarrow A.2}$ (from $A.1$ to $A.2$) for the cloud server (acting as a proxy) such that the server can further re-encrypt the ciphertexts of $A.1$ to $A.2$ (e.g., $Enc(ID_{A.1}, m_{A.1}) \rightarrow Enc(ID_{A.2}, m_{A.1})$). When $m_{A.1}$ is further shared with others (e.g., $A.3$), $A.2$ will upload a new re-encryption key $rk_{A.2\rightarrow A.3}$ to the cloud. The cloud then performs the corresponding conversion for $A.3$.

Although MH-IBPRE is proposed to employ the delegation of decryption rights in the context of IBE without losing confidentiality, it yields a price that both the size of ciphertext and decryption complexity grow linearly in the number of re-encryption hops. For example, if an original ciphertext $Enc(ID_{A.1}, m_{A.1})$ is chosen to be delegated via the direction $A.1 \rightarrow A.2 \rightarrow A.3 \rightarrow A.4$, then the size of the re-encrypted ciphertext (as well as decryption complexity) for $A.4$ will be triple larger than that of the original ciphertext. This is undesirable in practice because of the incurred linear communication bandwidth, storage cost and computation complexity.

Like traditional PRE, MH-IBPRE also incurs a potential risk for access control as the re-encryption power of a proxy cannot be controlled precisely. Generally speaking, given a re-encryption key $rk_{A.1\rightarrow A.2}$ the proxy is allowed to re-encrypt *all* $A.1$'s ciphertexts stored in the cloud to $A.2$ without any discrimination. This might contradict $A.1$'s will because $A.1$ might only prefer to share some data tagged with a specified condition, e.g., "public", other than the data labeled with "private" with $A.2$. Furthermore the sharing data might be described by a set of conditions other than a single one. For instance, $A.1$ shares the data, which is uploaded to the cloud in "July" containing keywords "meeting, project", with $A.2$. Here the condition set associated with the sharing data is seen as $W = \{July, meeting, project\}$.

As some data is allowed to be shared mutually among different employees, it indicates that the re-encryption for the ciphertext of the data should be considered in a bidirectional way (e.g., $A.1 \leftrightarrow A.2$). It will bring convenience for the data sharing if a pair of delegator and delegatee uses a bidirectional re-encryption key instead of two separated unidirectional ones. For example, given a re-encryption key $rk_{A.1,A.2}$ the proxy can fulfill not only the re-encryption from $A.1$ to $A.2$, but also the other way round. Here the number of re-encryption keys delivered in the communication channel could be reduced. If there are N employees in the group, only $N-1$ (i.e. $O(N)$) other than $N \times (N-1)$ (i.e. $O(N^2)$) re-encryption keys are required to be constructed and stored in the cloud. Nevertheless, none of existing MH-IBPRE supports the bidirectional property to date.

Open problems. The existing MH-IBPRE schemes leave us two interesting open problems: one is the fine-grained control of re-encryption, and the other is the construction of MH-IBPRE with constant complexity in terms of computation and communication. To tackle the problems, a novel MH-IBPRE system is desirable. The new scheme should not only support the bidirectional property, but also enjoy constant-size ciphertexts and decryption complexity no matter how many re-encryption hops have been traversed. Furthermore, it should allow the re-encryption power of the proxy to be limited to some pieces of conditions on the re-encryption key specified by the delegator (i.e. supporting *conditional re-encryption*).

1.1. Our contributions

- This paper formalizes the definition and security notion for bidirectional multi-hop identity-based conditional proxy re-encryption (BiMH-IBCPRE).
  1. In the definition, a condition is required as an auxiliary input to the re-encryption key generation, encryption, re-encryption and decryption algorithms.

[1] https://www.sugarsync.com/.
[2] https://www.box.com/.