Collusion-Resistant Unidirectional Proxy Re-Encryption Scheme from Lattices

Kee Sung Kim and Ik Rae Jeong

Abstract: **Most of the previous proxy re-encryption schemes rely on the average-case hardness problems such as the integer factorization problems and the discrete logarithm problems. Therefore, they cannot guarantee its security under quantum analysis, since there exist quantum algorithms efficiently solving the factorization and logarithm problems. In the paper, we propose the first proxy re-encryption scheme based on the hard worst-case lattice problems. Our scheme has many useful properties as follows: Unidirectional, collusion-resistant, noninteractive, proxy invisible, key optimal, and nontransitive. We also provided the formal security proof of the proposed scheme in the random oracle model.**

Index Terms: **Collusion-resistance, proxy re-encryption, unidirectional lattice.**

I. INTRODUCTION

IN 1998, [1] introduced a cryptographic primitive called *proxy re-encryption*, in which a semi-trusted proxy converts a ciphertext for user A into a ciphertext for user B. In the other words, if the proxy has a re-encryption key from user A to user B, the proxy can convert a ciphertext under the public key of user A into a ciphertext under the public key of user B. However, the proxy cannot learn anything about the plaintext from the ciphertexts. According to the direction of transformation, a proxy re-encryption scheme can be classified into two types [1], *bidirectional* and *unidirectional*. The former means that a proxy who has a bidirectional re-encryption key $rk_{A\leftrightarrow B}$ can transform a ciphertext under the public key of user $A(B)$ into a ciphertext under the public key of user $B(A)$. The latter means that a proxy given a unidirectional re-encryption key $rk_{A\rightarrow B}$ can convert only a ciphertext under the public key of user A into a ciphertext under the public key of user B. In practice, the unidirectional schemes have attracted more attention. Due to its transformation property, the proxy re-encryption scheme has found numerous practical applications, particularly in key distribution, distributed file system, secure e-mail list, access control, and digital right management (DRM).

Since the introduction of the proxy re-encryption scheme by [1], many papers have been proposed with different security properties such as CPA-secure [1], [2] and CCA-secure [3]–[6] and particularly, schemes in [2], [4]–[6] have proven their security in the standard model. In the proxy re-encryption schemes, another important security notion is *collusion-resistance*. Even if user B colludes with a proxy who knows a re-encryption key $rk_{A\rightarrow B}$, they cannot recover the secret key of user A. There are a few schemes which satisfy the collusion-resistance security [2], [5].

Most of the previous proxy re-encryption schemes rely on the average-case hardness problems such as the integer factorization problems and the discrete logarithm problems. Quantum algorithms solving the integer factorization problems and the discrete logarithm problems was proposed in [7]. That is, the previous re-encryption schemes are not secure against quantum analysis.

Lattice-based cryptosystems are rapidly emerging in recent years by the following reasons. First, the lattice-based cryptosystems are based on the *worst-case* hard problems, i.e., if an adversary can break the cryptosystems, then he can also solve any instance of the lattice problems. Second, the lattice-based cryptosystems are believed to be secure against quantum analysis whereas the factorization-based and discrete logarithm-based cryptosystems are insecure against quantum analysis. Finally, the lattice-based cryptosystems require less computational overhead than the factorization-based and discrete logarithm-based cryptosystems. There are some cryptosystems based on the lattice hard problems, including encryption schemes [8], [9], ID-based encryption schemes [10]–[13] and signature schemes [10], [14]. However, there is no lattice-based proxy re-encryption scheme yet.

In the paper, we propose a collusion-resistance unidirectional proxy re-encryption scheme based on the worst-case lattice problems. Our scheme also satisfies the following additional properties described in [2].

- *Noninteractive*: To generate unidirectional re-encryption key $rk_{A\rightarrow B}$, user A does not need the trusted third party or interaction with user B.
- *Proxy invisibility*: User B should not know whether a proxy exists. This means that B will not be able to distinguish an encryption computed under his public key from a re-encryption of a ciphertext intended for another party.
- *Nontransitive*: A proxy who knows re-encryption keys $rk_{A\rightarrow B}$ and $rk_{B\rightarrow C}$ should not be able to construct a re-encryption key $rk_{A\rightarrow C}$.
- *Key optimal*: The size of secret keys of user A and user B is independent of the number of re-encryption keys generated.

II. PRELIMINARIES

A. Notation

If D is a distribution, $s \leftarrow D$ means that s was sampled from distribution D. Matrices are denoted by capital letters, e.g. A. The ith column vector of a matrix A is denoted by a_i. We define

Manuscript received July 10, 2012; approved for publication by Daojing He, Division I Editor, August 3, 2015.

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2013R1A2A2A01068200).

The authors are with the Graduate School of Information Security, CIST, Korea University, Korea, email: {gisung2137, irjeong}@korea.ac.kr.

Digital object identifier 10.1109/JCN.2016.000003