Information Processing Letters 115 (2015) 462–467

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Identity-based proxy re-signatures from lattices

Miaomiao Tian

School of Computer Science and Technology, University of Science and Technology of China, Hefei, 230026, China

ARTICLE INFO

Article history:
Received 26 March 2014
Received in revised form 17 October 2014
Accepted 2 December 2014
Available online 9 December 2014
Communicated by Jinhui Xu

Keywords:
Cryptography
Proxy re-signature
Lattice

ABSTRACT

Proxy re-signature is an important cryptographic primitive in which a semi-trusted proxy is able to transform a delegatee's signature on some message into a delegator's signature on the same message, while the proxy itself cannot generate any signatures for either the delegatee or the delegator. The existing proxy re-signature schemes in the literature all rely on the hardness assumptions that can be easily solved by quantum algorithms. In this paper we present an identity-based proxy re-signature scheme from lattice assumptions. The scheme supports multi-use bidirectional conversion, and is provably secure in the random oracle model under conventional small integer solution assumption that is as hard as approximating several standard lattice problems. As the underlying lattice problems are intractable even for quantum computers, our scheme would work well in the quantum age.

1. Introduction

In many scenarios, it would be very convenient if we could transform a signature signed by Alice on some message into a signature on the same message signed by Bob. For instance, when we want to verify a signature signed by Alice but we don't know Alice's public key or it has expired, then we have to convert the signature into a signature signed by Bob, a person whose public key is available. To achieve this conversion, we could use proxy re-signature scheme by which a semi-trusted proxy with a re-signature key is able to turn a delegatee's signature into a delegator's one on the same message, but the proxy itself cannot create any signatures for either the delegatee or the delegator.

The concept of proxy re-signature was first introduced by Blaze, Bleumer and Strauss [5] at EUROCRYPT 1998. At CCS 2005, Ateniese and Hohenberger [3] revisited the concept and provided formal definitions as well as two specific schemes based on bilinear groups. One of the schemes is bidirectional and the other is unidirectional. Roughly speaking, bidirectional proxy re-signature scheme allows a semi-trusted proxy translating Alice's signatures to Bob's and vice-versa, while the proxy in an unidirectional proxy re-signature scheme can only convert a signature from Alice into one from Bob. After Ateniese and Hohenberger's work, several proxy re-signature schemes promptly emerged, e.g., [12,6,8]. Particularly, Shao et al. [12] in 2007 implanted proxy re-signature into identity-based cryptography [11] and proposed an identity-based bidirectional proxy re-signature scheme in bilinear groups from Waters's work [16]. Compared with traditional proxy re-signatures, identity-based proxy re-signatures need to deal with more challenges, nevertheless they are also more popular in real-world applications because they could eliminate the onerous certificate management procedure in traditional proxy re-signatures by setting users' identities as their public keys (for this to be possible, a trusted private key generator should be involved in to generate users' secret keys). We note, unfortunately, that all the existing proxy re-signature schemes including Shao et al.'s identity-based one suffer from a potential security problem. Namely, they are all built on the discrete logarithm related hardness assumptions, and hence will be insecure once quantum computer becomes a reality, by the result of [13].

E-mail address: miaotian@mail.ustc.edu.cn.

http://dx.doi.org/10.1016/j.ipl.2014.12.002
0020-0190/© 2014 Elsevier B.V. All rights reserved.

1.1. Our contribution

In this paper we present the first identity-based bidirectional proxy re-signature scheme from lattices. This scheme is proven to be secure in the random oracle model under the conventional small integer solution (SIS) assumption. By the result of [10], we can see that the scheme is secure in the random oracle model under the worst-case hardness of approximating some standard lattice problems. Since those lattice problems are intractable even for quantum algorithms, our scheme would remain secure in the quantum world. Moreover, our scheme also allows multi-use, that is, a signature translated from Alice to Bob could be further translated from Bob to Carol.

1.2. Related work

The first proxy re-signature scheme designed by Blaze, Bleumer and Strauss [5] is a multi-use bidirectional scheme. Later, Ateniese and Hohenberger [3] gave a new multi-use bidirectional proxy re-signature scheme and proved its security in the random oracle model. Shao et al. [12] removed the random oracle in the multi-use bidirectional scheme of Ateniese and Hohenberger via Waters's technique [16]. Additionally, Shao et al. in the same paper also provided an identity-based version of their multi-use bidirectional proxy re-signature scheme.

1.3. Paper organization

The remainder of this paper is organized as follows. Section 2 will give the definition and security model of identity-based (bidirectional) proxy re-signature schemes. Section 3 provides some preliminaries to be used in this work. Section 4 presents our identity-based proxy re-signature scheme from lattices and also demonstrates its security. Finally, Section 5 concludes this paper.

2. Identity-based proxy re-signature scheme

2.1. Syntax

Definition 1. An identity-based (bidirectional) proxy re-signature scheme is a tuple of probabilistic polynomial time (PPT) algorithms (Setup, Extract, ReKey, Sign, ReSign, Verify), where:

- Setup. Given a security parameter n, this algorithm outputs the public parameters PP and a master secret key MSK of the private key generator (PKG).
- Extract. Given the public parameters PP, the PKG's master secret key MSK and an identity ID, this algorithm outputs a secret key sk_{ID} corresponding to the identity ID.
- ReKey. Given the public parameters PP as well as two secret keys sk_{ID_A} and sk_{ID_B} corresponding to the identities ID_A and ID_B respectively, this algorithm outputs a re-signature key $rk_{A\leftrightarrow B}$.
- Sign. Given the public parameters PP, a secret key sk_{ID} corresponding to identity ID and a message μ, this algorithm outputs a signature sig on message μ under identity ID.
- ReSign. Given the public parameters PP, a re-signature key $rk_{A\leftrightarrow B}$ and a signature sig on message μ under identity ID_A, this algorithm outputs a signature sig$'$ on the same message μ under identity ID_B.
- Verify. Given the public parameters PP, a message μ, an identity ID and a signature sig, this algorithm outputs 1 if the signature sig is valid. Otherwise, it outputs 0.

Let (PP, MSK) be the output of $\mathsf{Setup}(n)$. For correctness, we require that for any message μ as well as any identities ID_A and ID_B, if $\mathsf{sig} = \mathsf{Sign}(PP, sk_{ID}, \mu)$ and $\mathsf{sig}' = \mathsf{ReSign}(PP, rk_{A\leftrightarrow B}, \mathsf{sig}, \mu, ID_A)$, then the conditions $\mathsf{Verify}(PP, \mu, ID_A, \mathsf{sig}) = 1$ and $\mathsf{Verify}(PP, \mu, ID_B, \mathsf{sig}') = 1$ must both hold with overwhelming probability, where $sk_{ID} = \mathsf{Extract}(PP, MSK, ID)$ for any identity ID and $rk_{A\leftrightarrow B} = \mathsf{ReKey}(PP, sk_{ID_A}, sk_{ID_B})$.

2.2. Security model

The security model of identity-based bidirectional proxy re-signatures we consider in this work is the existential unforgeability under adaptive chosen message and identity attacks. The model is described via the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Setup. The challenger $\mathcal{C}$ runs the algorithm $\mathsf{Setup}(n)$ to generate public parameters PP, and then sends PP to the adversary $\mathcal{A}$.

Queries. The adversary $\mathcal{A}$ can issue the following types of queries adaptively.

- Extract-query. To get the secret key of the user with identity ID, the adversary $\mathcal{A}$ issues such a query on the identity ID. In response, the challenger $\mathcal{C}$ runs the algorithm $\mathsf{Extract}(PP, MSK, ID)$ and returns a secret key sk_{ID}.
- ReKey-query. On input two secret keys sk_{ID_A} and sk_{ID_B} corresponding to the identities ID_A and ID_B, the challenger $\mathcal{C}$ runs the algorithm $\mathsf{ReKey}(PP, sk_{ID_A}, sk_{ID_B})$ and returns a re-signature key $rk_{A\leftrightarrow B}$.
- Sign-query. When the adversary $\mathcal{A}$ issues such a query on identity ID and message μ, the challenger $\mathcal{C}$ returns a signature sig as a response.

Forgery. The adversary $\mathcal{A}$ outputs a signature sig* on message μ^* under identity ID^*. $\mathcal{A}$ wins the game if: (i) $\mathsf{Verify}(PP, \mu^*, ID^*, \mathsf{sig}^*) = 1$, (ii) $(\cdot, \mu^*)$ has never been submitted to Sign-query, and (iii) all identities related to ID^* have never been submitted to Extract-query (here we say an identity ID is related to ID^* if $ID = ID^*$ or there is a path between ID and ID^* such that all edges in the path have been submitted to ReKey-query).

We define the advantage $\mathsf{Adv}_{\mathcal{A}}(n)$ of the adversary $\mathcal{A}$ in the above game to be the probability that $\mathcal{A}$ wins the game, taken over the coin tosses made by $\mathcal{A}$ and the challenger $\mathcal{C}$.

Definition 2. An identity-based bidirectional proxy re-signature scheme is said to be existential unforgeable against adaptive chosen message and identity attacks if for any polynomial time adversary $\mathcal{A}$ the advantage $\mathsf{Adv}_{\mathcal{A}}(n)$ in the above game is negligible.