Proxy Re-signature Scheme That Translates One Type of Signature Scheme to Another Type of Signature Scheme

N.R. Sunitha[1] and B. Bharat Amberker[2]

[1] Dept. of Computer Science & Engg., Siddaganga Institute of Technology, Tumkur, Karnataka, India
[2] Dept. of Computer Science & Engg., National Institute of Technology, Warangal, Andhra Pradesh, India

Abstract. In 1998, Blaze, Bleumer, and Strauss (BBS) proposed proxy re-signatures, in which a semi-trusted proxy acts as a translator between Alice and Bob to translate a signature from Alice into a signature from Bob on the same message. The proxy, however, does not learn any signing key and cannot sign arbitrary messages on behalf of either Alice or Bob. In the 12^{th} ACM Conference on Computer and Communications Security (CCS 2005), Ateniese and Hohenberger formalised the definition of security for a proxy re-signature and presented two secure proxy re-signature schemes based on bilinear maps. They left open the problem of determining whether or not a proxy re-signature scheme can be built that translates one type of signature scheme to another i.e. a scheme that translates Alice's Schnorr signatures into Bob's RSA based ones.

In this paper we address this open problem. We construct proxy signature scheme that translates Alice's Schnorr/ElGamal signature to Bob's RSA signature. We construct this by generating suitable proxy re-sign keys by establishing communication among delegatee, proxy signer and the delegator. At no point of conversion the security of Schnorr, ElGamal and RSA signature schemes are compromised. The Signatures generated by regular signature generation algorithm and the proposed re-signature algorithm are indistinguishable.

Keywords: Signature translation, Proxy re-signature, Proxy Signature, Proxy revocation, Proxy key.

1 Introduction

In Eurocrypt 98, Blaze, Bleumer, and Strauss (BBS)[5] proposed proxy re-signatures, in which a semi-trusted proxy acts as a translator between Alice and Bob. To translate, the proxy converts a signature from Alice into a signature from Bob on the same message. The proxy, however, does not learn any signing key and cannot sign arbitrary messages on behalf of either Alice or Bob. Since the BBS proposal, the proxy re-signature primitive has been largely ignored, until Ateniese and Hohenberger [1] showed that it is a very useful tool

N. Meghanathan et al. (Eds.): CNSA 2010, CCIS 89, pp. 270–279, 2010.

for sharing web certificates, forming weak group signatures, and authenticating a network path.

The proxy signatures introduced by Mambo, Usuda and Okamoto [10,11] must not be confused with proxy re-signatures. A proxy signature [10,11,8,7] allows one user Alice, called the original signer, to delegate her signing capability to another user Bob, called the proxy signer. After that, the proxy signer Bob can sign messages on behalf of the original signer Alice. Upon receiving a proxy signature on some message, a verifier can validate its correctness by the given verification procedure. By this the verifier is convinced of the original signer's agreement on the signed message. In proxy re-signature, a proxy translates a perfectly-valid and publicly-verifiable signature, $\sigma_A(m)$, from Alice on a certain message, m , into a signature, $\sigma_B(m)$, from Bob on the same message m. Notice that, in proxy re-signature, the two signatures, one from Alice and the other from Bob as generated by the proxy, can coexist and both can be publicly verified as being two signatures from two distinct people on the same message. Moreover, the proxy can convert a single signature into multiple signatures of several and distinct signers, and vice-versa.

Ateniese and Hohenberger [1] re-opened the discussion of proxy re-signature by providing four separate results: (1) motivation for the need of improved schemes, by pointing out that the original BBS scheme [5], while satisfying their security notion, is unsuitable for most practical applications, including the ones proposed in the original paper, (2) formal definitions and a security model, (3) provably secure proxy re-signature constructions from bilinear maps, and (4) new applications. Nevertheless, they left open the following problem: Determining whether or not proxy re-signature scheme can be built that translate from one type of signature scheme to another i.e. like a scheme that translates Alice's Schnorr signatures into Bob's RSA based ones.

To address the open problem of Ateniese and Hohenberger, we present construction of schemes which converts Alice's Schnorr/ElGamal signature to Bob's RSA signature. We construct this by generating suitable proxy re-sign keys which are computed by establishing communication among delegatee, proxy signer and the delegator. At no point of conversion the security of Schnorr, ElGamal and RSA signature schemes are compromised. Signatures of Schnorr and ElGamal get converted to RSA signatures by providing only the signature and re-sign keys as input to Re-sign algorithm.

The organisation of our paper is as follows: In Section 2, we define the proxy re-signature. In Section 3, we explain two conversion schemes i.e Schnorr to RSA Conversion Scheme and ElGamal to RSA Conversion Scheme along with proxy revocation and properties of the scheme. In Section 4, we discuss the security of our scheme. In section 5, we discuss the application of conversion of signatures. Lastly in Section 6, we conclude.

2 Definition of Proxy Re-signature Scheme

We follow the definitions given in [1]. A proxy re-signature scheme is a tuple of polynomial time algorithms (KeyGen, ReKey, Sign, ReSign, Verify), where,