Strongly Unforgeable Proxy Re-Signature Schemes in the Standard model

S. Sree Vivek, S. Sharmila Deva Selvi, Guhan Balasubramanian, C. Pandu Rangan

TCS Lab, IIT-Madras, India

Abstract. Proxy re-signatures are generally used for the delegation of signatures to a semi-trusted proxy which transforms the signatures between the users of the system. Its a handy primitive for network security and automated delegations in hierarchical organizations. Though proxy re-signature schemes that are secure in the standard model are available, none of them have addressed the security notion of strong existential unforgeability, where the adversary will not be able to forge even on messages for which signatures are already available.
In this paper, we define the security model for strong unforgeability of proxy re-signature schemes. We propose two concrete strong unforgeable proxy re-signature schemes, where we induce the strong unforgeability in the scheme by embedding the transformation techniques carefully in the sign and resign algorithms. The second scheme proposed also possesses a tight security reduction thereby strengthening our security argument. The security of both the schemes is related to the hardness of solving Computational Diffie-Hellman (CDH) problem.

Keywords Provable Security, Proxy Re-Signature, Strong Unforgeability, Standard Model.

1 Introduction

Proxy Re-Cryptography originally introduced by Blaze et. al. [3], has been an emerging field of interest in the research community. This has mainly been motivated by its applications and challenges faced in the construction of such schemes. Proxy Re-Signature and Proxy Re-Encryption schemes are the essential primitives in this field. Proxy Re-Encryption allows a semi-trusted proxy to convert a cipher text of a message such that it can be decrypted by another receiver instead of the intended receiver defined in the original encryption process. Many such schemes have been designed and are being used for various applications like distributed storage, distributed rights management and cloud infrastructure.

Proxy Re-Signature scheme involves a semi-trusted proxy between two parties A and B, where the proxy has the capability and information (Re-Signature Key) to convert the signature of a message from one user A, to the signature of the other user B on the same message signed by A [A-Delegatee, B-Delegator]. This kind of signature comes handy in situations where in B (the delegator) is not available to sign on a given message(m). Then using a signature of (the delegatee) A on the message(m), the semi-trusted proxy can generate a signature on behalf of B on the same message(m) with the help of a rekey(Re-Signature Key), without involving delegator B in the signing process. The properties of a proxy re-signature scheme are discussed in detail in appendix A.

Applications Proxy re-signature schemes have various applications. A few of them are listed below [2]:

1. In any huge organization, there may be frequent changes of competent authorities who authenticate documents on behalf of the organization. Here, it is appropriate to convert the individual signatures to that of the organizations' signature using a proxy re-signature.
2. In the case of an e-passport, the various check points can be associated with a semi trusted proxy, which converts the signature of the traveler to the signature of the corresponding check point indicating that the traveler has been verified at that point.
3. Certifying keys in public key infrastructure is an expensive process. Hence in public domain networks, in order to accept temporary users in the domain, rather than certifying and revoking each user it is easier to have a proxy associated for the corresponding domain and convert the signatures on messages signed by temporary users into the signature of the user who's key is already certified in the domain.

Proxy Re-Signatures are generally proved for an unforgeability notion where an adversary will be able to forge a signature/re-signature on a new message rather than on a message that has already been signed/resigned. It is also required that the signatures/re-signatures must be independent entities which cannot be modified into a publically verifiable form other than the proxy within the system. But there might be applications with stricter security, which require the system to protect the existing message-signature pairs from being forged. The security notion for such a requirement is called strong unforgeability, which we discuss in detail later.

Motivation: The property of strong unforgeability can also be adapted by applications shown above for a more stringent security. Consider sensitive applications where the signatures play a crucial role, there can be passive adversaries polling the communication channel. Hence they can store every message and its corresponding signature or re-signature. Then at a later time, they can modify these signatures due to their weak unforgeability property and present a new signature or re-signature for the same message at will.

An interesting example would be **Electronic money systems** can also be aided by proxy re-signatures. When the central issuing authority wants to transfer money to customers through various vendors, the original signature of the e-money is translated to the corresponding vendors' using a semi-trusted proxy. Every e-money has a unique signature and recorded in a central database (analogous to the number in currency notes). The signatures on the existing e-money cannot be forged, irrespective of whether the signature belongs to the issuing-authority/vendor. Otherwise, it might lead to counterfeit e-money. The strong unforgeable proxy re-signature scheme ensures that the existing signatures are unforgeable even after the signature translation process between the issuing authority and vendors. A Bi-Directional proxy re-signature scheme(discussed in Appendix-A) would be ideal for this situation since the e-money must flow in both directions.

We can adopt the same ideology for digital media rental services where the owner of the copyright(sign) would give the content to the retailers(resigned) from whom the customers can rent the media. The copyright materials embedded with the signature of the owner or the re-signature of the retailer must be unforgeable by an external adversary which otherwise might lead to piracy. Hence the strongly unforgeable proxy re-signature can come in handy for such a situation where the pirated copies cannot possess a valid publically verifiable signature apart from its original copy. It can be used in conjunction with proxy re-encrpytion in the digital rights management for authentication purposes.

Further we would like to emphasize that it is not trivial to attain strong unforgeability in proxy re-signatures as it is different from that for the notion in signatures. The attacker must not be able to modify the signatures/re-signatures to another entity which can be publicly verified.

Related Work

Table 1. Proxy Re-Signature Schemes in the Standard Model with desired properties

Properties	S_{mb}[11]	Libert [7]	Chow [5]	Ours
Uni-Directional	No	Yes	Yes	No
Multi-Use	Yes	Yes	No	Yes
Private Proxy	Yes	Yes	Yes	Yes
Non-Interactive	No	No	No	No
Non-Transitive	No	Yes	Yes	No
Transparent	Yes	No	No	No
Temporary	No	No	Yes	No
Strongly Unforgeable	No	No	No	Yes

Proxy Re-Signatures originally introduced by Blaze et. al. [3], is an interesting class of signature schemes. It was later formalized by Ateniese et. al. [2] who also defined a suitable security model for proving its security and supplementing it with two concrete schemes (one bi-directional and the other uni-directional) both secure in the random oracle model. Shao et. al. [11] proposed the first proxy re-signature scheme, which was bi-directional and secure in the standard model, with a new perspective on the security (Static

Corruption similar to that in proxy re-encryption schemes). Chow et. al [5] showed an insecurity in Shao's scheme and gave a new proxy re-signature scheme, which was secure in the standard model but at the cost of transparency. Libert et. al. [7] came up with a multi-use, uni-directional (Open problem left in [2]) and non-transparent proxy re-signature scheme that is secure in the standard model. Recently, Shao et. al. came up with a novel approach [12] for the first ID based multi-use proxy re-signatures. It is to be noted from Table 1.1 that none of the existing proxy re-signature schemes secure in the standard model satisfy the stronger notion of existential unforgeability [1], where an adversary will not be able to forge a previously signed or re-signed message. In this paper we address this issue by defining a security model for such a security notion and propose two concrete schemes for the same.

1.1 Our Contribution

In this paper, we first define a security notion for strongly unforgeable proxy re-signature schemes based on the static corruption security model defined by Shao et. al. [11]. Then, based on a Waters scheme [14] we propose two strongly unforgeable proxy re-signature schemes secure in the standard model. After reviewing the existing transformation techniques for converting existentially unforgeable signatures to strongly unforgeable ones, we choose the transformation technique proposed by Boneh et. al.'s [4] strong unforgeability transformation and Susilo et. al.'s generic transformation [6] which uses chameleon hash function. The schemes are constructed using bilinear maps and their security is based on the Computational Diffie-Hellman (CDH) assumption. We also suggest some efficiency improvements for the schemes and highlight the tight reduction obtained from the second scheme [6].

1.2 Paper Organization

The paper is organized as follows. In Section 2 we give the various definitions which are involved in constructing and proving the security of the scheme. In Section 3 and 4 we propose two concrete strongly unforgeable proxy re-signatures and also provide suggestions for efficiency improvement. Conclusion is offered in Section 5. The Appendix A defines the properties of proxy re-signature schemes, the Appendix B reviews the available strong unforgeability transformations techniques in the standard model.

2 Definitions

2.1 Proxy Re-Signature

The proxy re-signature is a collection of probabilistic polynomial time algorithms (KeyGen, ReKey, Sign, Verify, Re-Sign):
{ KeyGen, Sign } : These algorithms are taken from the underlying signature scheme, and hence retain all its functionality and properties. We are using the same key construct (pk-public key, sk-secret key) for the rest of the scheme.
ReKey : On input of the secret keys (sk_A, sk_B) , the re-key generation algorithm generates a re-key which is to be stored in the proxy. The re-signature key may be calculated through an interactive protocol, where the secret keys of A and B are used to compute the re-key. At the end of the protocol, the proxy will obtain the re-key $(rk_{A\to B})$ without gaining any information regarding the corresponding secret keys of A and B. This re-key $(rk_{A\to B})$ is used by the proxy to transform the signatures of user A to that of user B.
ReSign : Takes as input $(rk_{A\to B}, pk_A, m, \sigma_A)$ and it first verifies whether the given signature is that of user A by performing $Verify(pk_A, m, \sigma_A)$. If the Verify returns false, then the algorithm aborts and reports of an invalid signature. Otherwise, the transformation of the signature takes place using the re-key and the transformed signature $\sigma_B = ReSign(ReKey(sk_A, sk_B), pk_A, m, \sigma_A)$ is returned.
Verify : The signature σ_B on message m, when generated directly by user B, will be verified by the Verify algorithm of the underlying signature scheme. However, if σ_B is generated by the proxy, we may use a different algorithm.
Correctness : All the untransformed and transformed signatures will satisfy the Verify algorithm.
Verify1(m, σ_A, pk_A) = True

Verify2(m, ReSign(ReKey(sk_A, sk_B), pk_A, m, σ_A), pk_B) = True

Note: We are using two verification algorithms Verify1 and Verify2 in order to verify the signature and re-signature respectively. Depending on the transparency property of the scheme, if the output of the sign and re-sign algorithm are computationally indistinguishable, the Verify1 and Verify2 are one and the same. On the other hand, in the case of non-transparency where the signature and the re-signature are distinguishable, the Verify1 and Verify2 are different algorithms. For multi-use, non-transparent schemes, the Verify2 will be varying for each level of signature translation. Hence Verify algorithm varies depending on the nature of the signature.

Security Model for Proxy Re-Signature Scheme
We present a security model for the proxy re-signature scheme, which ensures the strong unforgeability property. The security of the scheme defined here is inspired by Shao et al.'s security model [11] for existential unforgeability under static corruption. *We introduce some extra features to the model to capture the strong unforgeability property.*
The security model is defined as the game between the forger F (the adversary trying to attack the system) and the challenger $\mathbb{C}$. The security is based on the ideology of static corruption where, a forger who is trying to attack the signature scheme determines the corrupted parties of the system prior to the start of game (between F and $\mathbb{C}$). It does not allow adaptive corruption of users of the system in between the security game. Hence our security model will deal with corrupted and uncorrupted parties accordingly. The security game is defined in the following phases:

Training Phase: The challenger simulates the following oracles, which the forger is allowed to query during this phase.

1. $O_{UKeyGen}$ Key Generation for Uncorrupted user : This oracle generates the key pair using the KeyGen and returns the public keys of uncorrupted users in the system.
2. $O_{CKeyGen}$ Key Generation for Corrupted user : This oracle generates the key pair using KeyGen and returns the public key and secret key of the corresponding corrupted user.
3. O_{ReKey} Re-Signature Key Generation : This oracle when given the public key of users A and B, generates a re-key $rk_{A\to B}$ only when both user A and B are either corrupted or uncorrupted. When one of them is corrupted and the other one is not, $\perp$ is returned.
4. O_{Sign} Signature : Given the input public key for user A which was generated by the one of the KeyGen oracles and a message m, the signature $\sigma_A(m)$ for the corresponding public key on the message is returned. The signature on the message is returned regardless of user A being a corrupted or uncorrupted user.
5. O_{ReSign} Re-Signature : Given the input $(pk_B, pk_A, m, \sigma_A)$, this oracle will return the corresponding transformed signature σ_B regardless of A or B being a corrupted or uncorrupted user. Notice that the rekey is not generated by $\mathbb{C}$, when one of the users (A or B) is corrupted. Still, this oracle must be able to return the re-signature.

This ensures that the forger gets all his training by querying the oracles (polynomial number of queries with respect to the security parameter) available to any user in the system. It is inherent that the forger controls the corrupted users. After the training phase, the strong unforgeability is captured in the following phase which exposes the true potential of the forger.

Forgery Phase : The forger after the training phase will return the forgery (m^*, pk^*, σ^*). The forgery is said to be a valid one if the following conditions are satisfied,

1. Verify algorithm must satisfy for (m^*, pk^*, σ^*) where σ^* can either be a transformed or untransformed signature.
2. pk^* used for forgery must be uncorrupted and whose keys are generated by the uncorrupted key generation oracle.
3. σ^* is not the output during the training phase with (m^*, pk^*) as input to the sign oracle.
4. σ^* is not the output of the ReSign oracle with input as (pk^*, pk, m^*, σ) during the training phase, for any pk and σ.

Note: When we consider the strong unforgeability for proxy re-signatures, we must take into account the fact that any re-signature must always be generated using the resignature-key. This restricts the forger from generating re-signatures from signatures of the same user without any information with respect to the user's secret key or re-signature information.

2.2 Bilinear Pairing

Let $\mathbb{G}$ be an additive cyclic group generated by P, with prime order p, and $\mathbb{G}_1$ be a multiplicative cyclic group of the same order p. A bilinear pairing is a map $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ with the following properties.

- **Bilinearity.** For all $P, Q, R \in \mathbb{G}$,
  - $\hat{e}(P + Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$
  - $\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R)$
  - $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$
- **Non-Degeneracy.** There exist $P, Q \in \mathbb{G}$ such that $\hat{e}(P, Q) \neq I_{\mathbb{G}_1}$, where $I_{\mathbb{G}_1}$ is the identity in $\mathbb{G}_1$.
- **Computability.** There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}$.

2.3 Computational Diffie-Hellman Assumption

Computational Diffie-Hellman Problem: Let G be a group of prime order p and g be the generator of $\mathbb{G}$. The CDH problem can be defined as follows: An algorithm A is said to have an advantage ϵ in solving the CDH problem if

$$Pr[A(g, g^a, g^b) = g^{ab}] \geq \epsilon$$

where the probability is calculated over the random choices of a,b$\in \mathbb{Z}_p^*$, g $\in \mathbb{G}^*$ and the random bits used by algorithm A.

3 Scheme-1

In this section, we will present our first strongly unforgeable proxy re-signature scheme, which can be proved secure in the standard model. We name the scheme PRS_{SUF} , which is bidirectional, and single-use in nature. The construction of the scheme uses bilinear maps. The scheme uses the Boneh et. al.'s transformation technique and carefully adding extra randomness and certain parameters so that the proxy re-signature can remain strongly unforgeable from all aspects. The use of two key pairs for every user is justified by proving that the re-signature cannot be produced unless it is processed by the re-signature algorithm.
The input message to be signed can be of any size. This message will then be modified to a n-bit format before computing the signature or re-signature.
KeyGen(1^k): On the input of security parameter k, this algorithm performs the following computations to generate the keys of a user. Let $\mathbb{G}, \mathbb{G}_1$ be groups of prime order p. Let $\hat{e}$ be an admissible bilinear map where $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$.

We consider a collision resistant hash function which is defined as $H_1 : \{0,1\}^* \Rightarrow \{0,1\}^n$. Since the scheme is in the standard model, the hash functions can be instantiated with standard hash functions which can be implemented in the real world. Here the length(n) of the message digest (Output of the H_1) depends on the security parameter.

Let g a generator for group $\mathbb{G}$ and random elements $< g_2, h, u_0, u_1...u_n, v_0, v_1..v_n > \in G^{2n+4}$.
The system(trusted party) then fixes this as a common reference string for all users, with which they can generate their respective public and secret key components. Consider a user A, who chooses $a_1, a_2 \in_R \mathbb{Z}_p$ and sets $g_1 = g^{a_1}$ and $g_{11} = g^{a_2}$ as his public keys. The secret key components computed for the user is $g_2^{a_1}$ and $g_2^{a_2}$.
Sign(m, sk): On the input of the message m to be signed and secret key of the signer, the signature algorithm performs the following computations

- Let $r, s \in_R \mathbb{Z}_p$
- Compute $\sigma_2 = g^r \in \mathbb{G}$

– Set $\sigma_3 = s \in \mathbb{Z}_p$
  $t_1 = H_1(m||\sigma_2) \in \{0,1\}^n$
– Set $m^{(1)} = H_1(g^{t_1}h^s) \in \{0,1\}^n$.
  The computation of $m^{(1)}$ is in accordance to the strong unforgeability transformation.

  Define $m_u^{(1)} = u_0 \prod_{i=1}^{n} u_i^{m_i^{(1)}}$
  where $m^{(1)} = (m_1^{(1)}, m_2^{(1)}, m_3^{(1)} \ldots m_n^{(1)})$ denotes the n-bit representation of $\mathrm{m}^{(1)}$.
– Compute $\sigma_1 = sk_1.\left(m_u^{(1)}\right)^r \in \mathbb{G}$
  Thus, the signature $\sigma =< \sigma_1, \sigma_2, \sigma_3 >$ on the message m by the signer A with the secret key g_2^a is given by

$$(\sigma_1, \sigma_2, \sigma_3) = \left(g_2^{a_1}.\left(m_u^{(1)}\right)^r, g^r, s\right)$$

ReKey$(g_2^{a_1}, g_2^{b_1}, g_2^{b_2})$: In order to delegate the signing right from either A to B (or B to A as our scheme is bidirectional) the proxy will run an interactive protocol with A and B. The final re-signature key obtained by the proxy will be of the form

$$rk_{A\to B} = g_2^{b_1+b_2-a} \in \mathbb{G}$$

The Interactive protocol for using the secret keys of the users in a secure manner to calculate the final re-signature key is defined as follows:

1. The proxy initially chooses a random $\mathrm{R} \in \mathbb{Z}_p$, compute g_2^R and send it to user A.
2. Then A uses its secret key parameter a, computes and sends $g_2^R.g_2^{-a_1} = g_2^{R-a_1}$ to user B. B is chosen by A, as he is the user to whom A wishes to convert his signatures.
3. B uses his secret parameter b, computes and sends $(g_2^{R-a_1}).g_2^{b_1+b_2} = g_2^{R+b_1+b_2-a_1}$ to the proxy.
4. The proxy now computes $(g_2^{R+b_1+b_2-a}).g_2^{-R} = g_2^{b_1+b_2-a}$ as the re-signature key.

Remark: The rekey algorithm is performed during the system setup through a secure channel or in private. We claim that the above interactive protocol between the parties involved in delegations is unavoidable because it involves the use of their secret information. Since it performs a secure computation, a non-interactive zero knowledge will not serve the purpose in this scenario. This has been the approach used in all the proxy re-signatures with private proxy defined until now.

ReSign(pk_B, pk_A, m, σ): Proxy on receiving a signature $\sigma = < \sigma_1, \sigma_2, \sigma_3 >$ on the message m by user A associated with public key pk_A, re-signature key $rk_{A\leftarrow B}$ as input, performs the following to generate a signature on m for user B.

– First check whether the $Verify1(pk_A, m, \sigma)$ satisfies, if not abort reporting an invalid signature. Otherwise perform the following steps to generate the re-signature.
– Assign $\hat{\sigma_2} = \sigma_2 = g^r \in \mathbb{G}$
– Let $r_1 \in_R \mathbb{Z}_p$ and compute g^{r_1} and assign $\hat{\sigma_3} = g^{r_1} \in \mathbb{G}$
– Assign $\hat{\sigma}_4 = \sigma_3 = s \in \mathbb{Z}_p$
  $t_2 = H_1(m||g^{r_1}||g^r) \in \{0,1\}^n$
– Set $m^{(2)} = H_1(g^{t_2}h^{\sigma_3}) \in \{0,1\}^n$.
  The computation of $m^{(2)}$ is in accordance to the strong unforgeability transformation.

  Define $m_v^{(2)} = v_0 \prod_{i=1}^{n} v_i^{m_i^{(2)}}$
  where $m^{(2)} = (m_1^{(2)}, m_2^{(2)}, m_3^{(2)} \ldots m_n^{(2)})$ denotes the n-bit representation of $\mathrm{m}^{(2)}$.
– Compute $\hat{\sigma_1} = \sigma_1.rk_{A\to B}.\left(m_v^{(2)}\right)^{r_1} \in \mathbb{G}$

$$= g_2^{a_1}.\left(m_u^{(1)}\right)^r.g_2^{(b_1+b_2-a)}.\left(m_v^{(2)}\right)^{r_1}$$
$$= g_2^{b_1+b_2}.\left(m_u^{(1)}\right)^r.\left(m_v^{(2)}\right)^{r_1}$$

The Re-signature $\hat{\sigma} =< \hat{\sigma_1}, \hat{\sigma_2}, \hat{\sigma_3}, \hat{\sigma_4} >$ is given by,

$$(\hat{\sigma_1}, \hat{\sigma_2}, \hat{\sigma_3}, \hat{\sigma_4}) = \left(g_2^{b_1+b_2}.\left(m_u^{(1)}\right)^r.\left(m_v^{(2)}\right)^{r_1}, g^r, g^{r_1}, s\right)$$

Verify1(m, σ, pk): For verifying the signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ on the message m by the user corresponding to public key pk, any verifier can perform the following validity check. Initially compute,

- $\hat{t_1} = H_1(m, \sigma_2) \in \{0,1\}^n$
- $m^{(1)} = H_1(g^{\hat{t_1}} h^{\sigma_3}) \in \{0,1\}^n$
- Verify whether the following equation satisfies

$$\hat{e}\left(\sigma_1, g\right) \stackrel{?}{=} \hat{e}(m_u^{(1)}, \sigma_2)\hat{e}(g_2, g_1)$$

if the above test holds, output *Valid* otherwise output *Invalid*.

Correctness for verification of signature (Verify1):

$$\hat{e}(\sigma_1, g) \stackrel{?}{=} \hat{e}(m_u^{(1)}, \sigma_2)\hat{e}(g_2, g_1)$$

Right Hand Side:

$$\begin{aligned} &= \hat{e}(m_u^{(1)}, g^r)\hat{e}(g_2, g^{a_1}) \\ &= \hat{e}((m_u^{(1)})^r, g)\hat{e}(g_2^{a_1}, g) \end{aligned}$$

By Bilinearity property of the map e:

$$\begin{aligned} &= \hat{e}(g_2^{a_1}(m_u^{(1)})^r, g) \\ &= \hat{e}(\sigma_1, g) = LeftHandSide. \end{aligned}$$

Verify2$(m, \hat{\sigma}, pk)$: For verifying the re-signature $\hat{\sigma} = (\hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3, \hat{\sigma}_4)$ on the message m by the user corresponding to public key pk, any verifier can perform the following validity check on the transformed signature as follows,

- Compute $\hat{t_1} = H_1(m, \hat{\sigma}_2) \in \{0,1\}^n$
- $m^{(1)} = H_1(g^{\hat{t_1}} h^{\hat{\sigma}_4}) \in \{0,1\}^n$
- $\hat{t_2} = H_1(m, \sigma_2, \sigma_3) \in \{0,1\}^n$
- $m^{(2)} = H_1(g^{\hat{t_2}} h^{\hat{\sigma}_4}) \in \{0,1\}^n$
- $m_u^{(1)} = u_0 \prod_{i=1}^{n} u_i^{m_i^{(1)}}$
- $m_v^{(2)} = v_0 \prod_{i=1}^{n} v_i^{m_i^{(2)}}$
- Verify whether the following equation satisfies

$$\hat{e}(\hat{\sigma_1}, g) \stackrel{?}{=} \hat{e}(m_u^{(1)}, \hat{\sigma_2}).\hat{e}(m_v^{(2)}, \hat{\sigma_3}).\hat{e}(g_2, g_1).\hat{e}(g_2, g_{11})$$

if the above test holds, output *Valid* otherwise output *Invalid*.

Correctness for verification of re-signature (Verify2):

$$\hat{e}(\hat{\sigma_1}, g) \stackrel{?}{=} \hat{e}(m_u^{(1)}, \hat{\sigma_2}).\hat{e}(m_v^{(2)}, \hat{\sigma_3}).\hat{e}(g_2, g_1).\hat{e}(g_2, g_{11})$$

Right Hand Side:

$$= \hat{e}(m_u^{(1)}, g^r)\hat{e}(m_v^{(2)}, g^{r_1})\hat{e}(g_2, g^{b_1})\hat{e}(g_2, g^{b_2})$$
$$= \hat{e}((m_u^{(1)})^r, g)\hat{e}((m_v^{(2)})^{r_1}, g).\hat{e}(g_2^{b_1+b_2}, g)$$

By Bilinearity property of the map e:

$$= \hat{e}(g_2^{b_1+b_2}(m_u^{(1)})^r(m_v^{(2)})^{r_1}, g)$$
$$= \hat{e}(\hat{\sigma_1}, g) = LeftHandSide.$$

Note: The insecurities for construction with existing approaches using this transporation is elucidated in appendix C.

Proof of Security

We prove the security of the scheme PRS_{SUF} using the following theorem. In this theorem, we prove that breaking the scheme is hard as solving the CDH problem.

Theorem 1. *If there is an adversary, which can break the strongly unforgeable scheme PRS_{SUF} in polynomial time, by having q_s and q_{rs} queries to the sign and resign oracles and advantage (ϵ) with n as the size of the message, then the CDH problem can be broken with advantage $\epsilon'' \geq \epsilon/144q_s(q_s + q_{rs})(n+1)^2$*

1. The security proof of the PRS_{SUF} can be divided into two parts. The first one is where we prove the security of the underlying signature scheme by simulating a weaker form of the signature with the sign and resign oracles. Thus we prove the scheme to be secure for any message that was not queried during the training phase.
2. Once we have proved the existential forgery for the signature and re-signature scheme, we may apply transformation (modifying the message by binding it with a randomness, without affecting the internal structure of the signature or re-signature) and then derive the security for strong unforgeability. Since this transformation [4] uses the assumption of universal one way hash functions, the resulting strongly unforgeable scheme is also secure.

As mentioned in the model, the security is proved as game between the challenger $\mathbb{C}$ and forger F. F is trained with the working of the system through the following simulation by $\mathbb{C}$. We are simulating the training phase for the weaker form of the re-signature(without transformation) where $m^{(1)}$ or $m^{(2)}$=m and prove for its existential unforgeability prior to applying the strong unforgeability transformation.

$\mathbb{C}$ is given the input of the hard problem, g^a, g^b and is required to find the solution g^{ab} from the forgery performed by the forger. Hence $\mathbb{C}$ embeds the hard problem instances while simulating the system to the adversary, which is described as follows.

Training Phase

Setup: Consider public key $g_1 = g^a$, $g_2 = g^b$ and therefore the solution to the hard problem is finding the secret key $g_2^{a_1} = g^{ab}$. The second secret key component $g_2^{a_2}$ does not involve in the hard problem solving and hence is generated in a similar fashion as in the KeyGen algorithm for each user.

Let the number of bits of the message be n. Let $l_n = 2(q_s + q_{rs})$ where q_s, q_{rs} are the number of queries to the sign/resign oracle, where $l_n(n+1) < p$ and let k_n be defined by $0 \leq k_n \leq n$. Let $x_0, x_1, ..., x_n \in \mathbb{Z}_{l_n}$ and similarly $y_0, y_1, ..., y_n \in \mathbb{Z}_p$.

$\mathrm{F(m)} = x_0 + \sum_{i \in U} x_i - l_n k_n$; $\mathrm{J(m)} = y_0 + \sum_{i \in U} y_i$

where U is set of all i from 1 to n, where $m_i = 1$. Let the parameters be

$u_0 = g_2^{x_0 - l_n k_n}.g^{y_0}$, $u_i = g_2^{x_i}.g^{y_i}$

Therefore, the hash function for Sign Oracle:

$m_u = u_0 \prod_{i=1}^{n} u_i^{m_i} = g_2^{F(m)} g^{J(m)}$

$l_m = 2q_{rs}$ where q_{rs} are the number of queries to the resign oracle, where $l_m(n+1) < p$ and let k_m be defined by $0 \leq k_m \leq n$. Let $z_0, z_1, ..., z_n \in \mathbb{Z}_{l_n}$ and similarly $w_0, w_1, ..., w_n \in \mathbb{Z}_p$.

$\mathrm{K(m)} = z_0 + \sum_{i \in U`} z_i - l_m k_m$; $\mathrm{L(m)} = w_0 + \sum_{i \in U`} w_i$
where $U`$ is set of all i from 1 to n, where $m_i = 1$. Let the parameters be
$u_0 = g_2^{z_0 - l_m k_m} . g^{w_0}$, $u_i = g_2^{z_i} . g^{w_i}$
Therefore, the hash function for Resign Oracle:
$m_v = v_0 \prod_{i=1}^{n} v_i^{m_i} = g_2^{K(m)} g^{L(m)}$

Hence, it is evident from the above-mentioned steps that for any given message(m) $\mathbb{C}$ can calculate the respective hash function for the corresponding oracle.

- $O_{UKeyGen}$: When F queries for the key generation of user A, $\mathbb{C}$ does the following
  1. Selects an element $x_i, \hat{x}_i \in_R \mathbb{Z}_p$. Here $\hat{x}_i$ denotes the second secret key component.
  2. Computes public key $pk_A = (g^a g^{x_i}, g^{\hat{x}_i}) = (g^{a+x_i}, g^{\hat{x}_i})$ and sends pk_A to F. Note that the primary secret key sk_A of user A, is $(a + x_i)$ implicitly and $\mathbb{C}$ does not know primary sk_A which is used for signing.
- $O_{CKeyGen}$: When a query is made by F, $\mathbb{C}$ responds with $sk_i = (x_i, \hat{x}_i)$ and $pk_i = (g^{x_i}, g^{\hat{x}_i})$ of a corrupted user where $x_i, \hat{x}_i \in_R \mathbb{Z}_p$.
- O_{ReKey}: On input with two public keys pk_i and pk_j $\mathbb{C}$ does the following, If both the users pk_i and pk_j (rekey between user i & j) are uncorrupted then $\mathbb{C}$ computes the rekey $g_2^{\hat{x_j} + \overline{x_j} - \overline{x_i}}$ where $\overline{x_j}$ and $\overline{x_i}$ are primary secret key components corresponding to pk_i and pk_j. The oracle returns $\perp$ and aborts if either one of the user corresponding to pk_i or pk_j is a corrupted user. The rekey $rk_{i \to j}$ is valid since by definition difference of the primary secret key component of the uncorrupted users $x_j - x_i$ when substituted with its values generated by $O_{UKeyGen}$ will be of the form $(a + \overline{x_j}) - (a + \overline{x_i})$ which is $\overline{x_j} - \overline{x_i}$. The second secret key component $\hat{x_j}$ will not be an issue, since it is a known value to $\mathbb{C}$.
- O_{Sign}: When F queries the sign oracle for message m to be signed by the primary secret key of the uncorrupted user corresponding to public key $pk_i = g^{a+x_i}$. If F(m) $\neq$ 0 (F(m) was defined using the Setup), then return the following signature

$$\begin{aligned}
\sigma_1 &= g_1^{-J(m)/F(m)} (g_2^{F(m)} g^{J(m)})^r . g_2^{x_i} \\
&= g_2^{a+x_i} (g_2^{F(m)} g^{J(m)})^{-a/F(m)} (g^{J(m)} g_2^{F(m)})^r \\
&= g_2^{a+x_i} (g_2^{F(m)} g^{J(m)})^{r - a/F(m)} \\
&= g_2^{x_i} g^{ab} (g_2^{F(m)} g^{J(m)})^{r - a/F(m)} \\
\sigma_2 &= g_1^{-1/F(m)} g^r
\end{aligned}$$

$\sigma = (\sigma_1, \sigma_2)$

$$= \left(g_2^{x_i} g_1^{-J(m)/F(m)} \left(g_2^{F(m)} g^{J(m)} g_2^{x_i} \right)^r , g_1^{-1/F(m)} g^r \right)$$

Otherwise if F(m)=0 mod p, $\mathbb{C}$ aborts.

Correctness of Sign oracle for uncorrupted signature: This cooked up signature will satisfy the verification algorithm as follows:

$$\hat{e}(\sigma_1, g) \stackrel{?}{=} \hat{e}(u_0 \prod_{i=1}^{n} u_i^{m_i}, \sigma_2) \hat{e}(g_2, g_1)$$

where $\sigma_1 = g_2^{a+x_i} (g_2^{F(m)} g^{J(m)})^{r - a/F(m)}$

Right Hand Side:

$$\begin{aligned}
&= \hat{e}(u_0 \prod_{i=1}^{n} u_i^{m_i}, \sigma_2) \hat{e}(g_2, g_1) \\
&= \hat{e}(g_2^{F(m)} g^{J(m)}, g^{r - a/F(m)}) \hat{e}(g_2, g^{a+x_i}) \\
&= \hat{e}(g_2^{F(m)} g^{J(m)})^{r - a/F(m)}, g) \hat{e}(g_2^{a+x_i}, g)
\end{aligned}$$

By Bilinearity property of the map e:

$$= \hat{e}(g_2^{a+x_i}(g_2^{F(m)}g^{J(m)})^{r-a/F(m)}, g)$$
$$= \hat{e}(\sigma_1, g) = LeftHandSide.$$

Note: The fact that should be remembered while simulating the re-sign oracle is that for every uncorrupted user, the randomness in the signature is of the form $\hat{r}$=r-a/F(m) and for every corrupted user it is $\hat{r}$=r where $r \in_R \mathbb{Z}_p$

– O_{ReSign}: On input the signature σ on message m of the user corresponding to public key pk_i and the public key pk_j of the user to whom the signature is being transformed to, there are 3 possibilities for the input of this re-sign oracle. They are
  1. Converting signature of an uncorrupted user to the signature of another uncorrupted user
  2. Converting signature of a uncorrupted user to that of an corrupted user
  3. Converting signature of an corrupted user to that of a uncorrupted user

$\mathbb{C}$ checks if Verify(m, σ, pk_i) is valid. If false $\mathbb{C}$ aborts, otherwise $\mathbb{C}$ does the following:
Consider $r_1 \in_R \mathbb{Z}_p$ to be the new randomness parameter used by the ReSign algorithm.
Case 1: If pk_i and pk_j are uncorrupted users, then $\mathbb{C}$ will call the $O_{ReKey}(pk_i, pk_j)$ to obtain $rk_{i\to j}$ and run the ReSign algorithm with new randomness $r_1 \in \mathbb{Z}_p$ and returns the re-signature to forger F.
Case 2: If pk_i corresponds to an uncorrupted user and pk_j to a corrupted user $\mathbb{C}$ is required to remove the hard problem instance g^{ab} while converting it to the corrupted user's signature. Hence the resulting ReSign must contain a g^{-ab} implicitly in order to cancel out the effect and thereby making it the signature of an corrupted user(whose primary secret key is $g_2^{x_j}$).
The input to the ReSign oracle for this case is as follows: $\sigma =< \sigma_1, \sigma_2 >$

$$\sigma_1 = g_1^{-J(m)/F(m)}(g_2^{F(m)}g^{J(m)})^r$$
$$= g_2^{x_i}g^{ab}(g_2^{F(m)}g^{J(m)})^{r-a/F(m)}$$
$$\sigma_2 = g_1^{-1/F(m)}g^r$$

the original randomness $\hat{r}$ = r - a/F(m).
The resignature for the corrupted user is calculated in the following manner:
Consider $r_1 \in \mathbb{Z}_p$

$$\hat{\sigma_1} = \sigma_1 g_2^{x_j+\hat{x}_j} g_1^{L(m)/K(m)}(g_2^{K(m)}g^{L(m)})^{r_1}$$
$$= g_2^{x_j+\hat{x}_j} g_1^{-J(m)/F(m)} g_1^{L(m)/K(m)}(g_2^{F(m)}g^{J(m)})^r$$
$$(g_2^{K(m)}g^{L(m)})^{r_1}$$
$$= g_2^{x_j+\hat{x}_j} g^{ab} g^{-ab}(g_2^{F(m)}g^{J(m)})^{r-a/F(m)}$$
$$(g_2^{K(m)}g^{L(m)})^{r_1+a/K(m)}$$
$$= g_2^{x_j+\hat{x}_j}(g_2^{F(m)}g^{J(m)})^{r-a/F(m)}(g_2^{K(m)}g^{L(m)})^{r_1+a/K(m)}$$

Hence the new randomness $\hat{r_1}$ = r + a/K(m).

$$\hat{\sigma_2} = \sigma_2 = g_1^{-1/F(m)}g^r = g^{r-a/F(m)}$$
$$\hat{\sigma_3} = g_1^{1/K(m)}g^{r_1} = g^{r_1+a/K(m)}$$

$\mathbb{C}$ outputs $\hat{\sigma} = (\hat{\sigma_1}, \hat{\sigma_2}, \hat{\sigma_3})$ to the forger.

$$= (g_2^{x_j+\hat{x}_j}\left(g_2^{F(m)}g^{J(m)}\right)^{r-a/F(m)}$$
$$\left(g_2^{K(m)}g^{L(m)}\right)^{r_1+a/K(m)}, g^{r-a/F(m)}, g^{r_1+a/K(m)})$$

To be noted that the above computation is possible only if F(m) and K(m) $\neq 0$ mod p. Otherwise, resign oracle returns $\perp$ and the game aborts.

Correctness of ReSign oracle for case 2: We show the correctness of the simulated $\hat{\sigma}$ as follows

$$\hat{e}(\hat{\sigma}_1, g) \stackrel{?}{=} \hat{e}(u_0 \prod_{i=1}^{n} u_i^{m_i^{(1)}}, \hat{\sigma}_2).$$
$$e(v_0 \prod_{i=1}^{n} v_i^{m_i^{(2)}}, \hat{\sigma}_3).\hat{e}(g_2, g_1).\hat{e}(g_2, g_{11})$$

Right Hand Side:

$$= \hat{e}(u_0 \prod_{i=1}^{n} u_i^{m_i^{(1)}}, \hat{\sigma}_2).$$
$$\hat{e}(v_0 \prod_{i=1}^{n} v_i^{m_i^{(2)}}, \hat{\sigma}_3).\hat{e}(g_2, g_1).\hat{e}(g_2, g_{11})$$
$$= \hat{e}(g_2^{F(m)} g^{J(m)}, g^{\hat{r}}) \hat{e}(g_2^{K(m)} g^{L(m)}, g^{\hat{r_1}}) \hat{e}(g_2, g^{x_j + \hat{x}_j})$$
$$= \hat{e}((g_2^{F(m)} g^{J(m)})^{\hat{r}}, g) \hat{e}((g_2^{K(m)} g^{L(m)})^{\hat{r_1}}, g) \hat{e}(g_2^{x_j + \hat{x}_j}, g)$$

By Bilinearity property of the map e:

$$= \hat{e}(g_2^{x_j + \hat{x}_j} (g_2^{F(m)} g^{J(m)})^{\hat{r}} (g_2^{K(m)} g^{L(m)})^{\hat{r_1}}, g)$$
$$= \hat{e}(\hat{\sigma}_1, g) = LeftHandSide.$$

Case 3: If pk_i corresponds to an corrupted user and pk_j to an uncorrupted user, then the $\mathbb{C}$ is required to induce the hard problem instance while converting it to the uncorrupted user's signature. Hence the resulting ReSign must contain a g^{ab} implicitly in order to induce the effect of the hard problem and thereby making it the signature of an uncorrupted user(whose primary secret key is $g_2^{x_j + a}$).
The input to the ReSign oracle for this case is as follows:

$$\sigma = \left(g_2^{x_i} . (u_0 \prod_{i=1}^{n} u_i^{m_i})^r, g^r \right)$$
$$= \left(g_2^{x_i} (g_2^{F(m)} g^{J(m)}), g^r \right)$$

where the original randomness $\hat{r}$=r.
The resignature for the uncorrupted user is calculated in the following manner:
Consider $r_1 \in \mathbb{Z}_p$

$$\hat{\sigma}_1 = \sigma_1 g_2^{-x_i} g_1^{-L(m)/K(m)} (g_2^{K(m)} g^{L(m)})^{r_1} . g_2^{x_j + \hat{x}_j}$$
$$= g_2^{x_i} g_2^{-x_i} g_1^{-L(m)/K(m)} (g_2^{F(m)} g^{J(m)})^r$$
$$(g_2^{K(m)} g^{L(m)})^{r_1} .. g_2^{x_j + \hat{x}_j}$$
$$= g^{ab} (g_2^{F(m)} g^{J(m)})^r (g_2^{K(m)} g^{L(m)})^{r_1 - a/K(m)}$$
$$= g_2^{x_j + \hat{x}_j} g^{ab} (g_2^{F(m)} g^{J(m)})^r (g_2^{K(m)} g^{L(m)})^{r_1 - a/K(m)}$$

Hence the new randomness $\hat{r_1}$ = r - a/K(m).

$$\hat{\sigma}_2 = \sigma_2 = g^r$$
$$\hat{\sigma}_3 = g_1^{-1/K(m)} g^{r_1} = g^{r_1 - a/K(m)}$$

$\mathbb{C}$ outputs $\hat{\sigma} = (\hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3)$

$$= (g_2^{x_j+\hat{x}_j} g^{ab} \left(g_2^{F(m)} g^{J(m)}\right)^r$$
$$\left(g_2^{K(m)} g^{L(m)}\right)^{r_1 - a/K(m)}, g^r, g^{r_1 - a/K(m)})$$

to the forger. To be noted that the above computation can be performed only if K(m) $\neq$ 0 mod p. Otherwise, resign oracle returns $\perp$ and the game aborts.

Correctness of ReSign oracle for case 3: We show the correctness of the simulated $\hat{\sigma}$ as follows:

$$\hat{e}(\hat{\sigma}_1, g) \stackrel{?}{=} \hat{e}(u_0 \prod_{i=1}^{n} u_i^{m_i^{(1)}}, \hat{\sigma}_2) \hat{e}(v_0 \prod_{i=1}^{n} v_i^{m_i^{(2)}}, \hat{\sigma}_3) \hat{e}(g_2, g_1) \hat{e}(g_2, g_{11})$$

Right Hand Side:

$$= \hat{e}(u_0 \prod_{i=1}^{n} u_i^{m_i^{(1)}}, \hat{\sigma}_2)$$
$$\hat{e}(v_0 \prod_{i=1}^{n} v_i^{m_i^{(2)}}, \hat{\sigma}_3) \hat{e}(g_2, g_1) \hat{e}(g_2, g_{11})$$
$$= \hat{e}((g_2^{F(m)} g^{J(m)}), g^{\hat{r}}) \hat{e}((g_2^{K(m)} g^{L(m)}), g^{\hat{r_1}})$$
$$\hat{e}(g_2, g^{a+x_j}) \hat{e}(g_2, g^{\hat{x}_j})$$
$$= \hat{e}((g_2^{F(m)} g^{J(m)})^{\hat{r}}, g) \hat{e}((g_2^{K(m)} g^{L(m)})^{\hat{r_1}}, g)$$
$$\hat{e}(g_2^{a+x_j+\hat{x}_j}, g)$$

By Bilinearity property of the map $\hat{e}$:

$$= \hat{e}(g_2^{a+x_j+\hat{x}_j} (g_2^{F(m)} g^{J(m)})^{\hat{r}} ((g_2^{K(m)} g^{L(m)})^{\hat{r_1}}, g)$$
$$= \hat{e}(\hat{\sigma}_1, g) = LeftHandSide.$$

After the training phase, the forger F submits a **Forgery** : (m^*, pk^*, σ^*) for a message m^* corresponding to uncorrupted user's public key pk^*. If F is able to come up with a forgery for the uncorrupted user either on the signature or re-signature, then the Challenger $\mathbb{C}$ using the output of F, can find the solution for the CDH hard problem. Since the public key pk^* corresponds to an uncorrupted user, the forgery will always contain an instance of the hard problem solution in the signature.
The existential forgery on chosen message m^* is considered a valid forgery if it satisfies the following requirements:

1. None of the messages m_i among the q_s sign queries during the training phase has $F(m_i) \equiv 0 \ mod \ p$.
2. It is required that m^* is not among the Sign and ReSign queries in the training phase.
3. For a forgery of a re-signature, The condition $F(m^*) \equiv 0 \ mod \ p$ and $K(m^*) \equiv 0 \ mod \ p$ must satisfy in order for the $\mathbb{C}$ to compute the hard problem.

Signature of uncorrupted user (pk^*) is of the following form with the constraint that $F(m^*) \equiv 0 \ mod \ p$

$$(\sigma_1, \sigma_2) = \left(g_2^{x_i} g^{ab} \left(g_2^{F(m^*)} g^{J(m^*)}\right)^{r^*}, g^{r^*}\right)$$

Hence the solution to the CDH problem with respect to a *new* message m^*:

$$\begin{aligned}\sigma_1 &= g_2^{x_i} g^{ab} \left(g_2^{F(m^*)} g^{J(m^*)}\right)^{r^*} \\ &= g^{ab+bx_i+J(m^*)r^*} \\ &= \frac{g^{ab+bx_i+J(m^*)r^*}}{(g^{bx_i}.g^{r^*})^{J(m^*)}} \\ &= g^{ab}\end{aligned}$$

The forgery of the re-signature can be used to solve the CDH problem in a similar manner. Since the hard problem is induced accordingly depending on the nature of conversion between the uncorrupted and corrupted users.

The Re-Signature of uncorrupted user (pk^*) is of the following form with the constraint $F(m^*) \equiv 0 \ mod \ p$ and $K(m^*) \equiv 0 \ mod \ p$, $(\sigma_1, \sigma_2, \sigma_3)$
$= (g_2^{x_j+\hat{x}_j} g^{ab} \left(g_2^{F(m^*)} g^{J(m^*)}\right)^{r^*} \left(g_2^{K(m^*)} g^{L(m^*)}\right)^{r_1^*},$
$g^{r^*}, g^{r_1^*})$

Hence the solution to the CDH problem with respect to a *new* message m^*:

$$\begin{aligned}\sigma_1 &= g_2^{x_j+\hat{x}_j} g^{ab} \left(g_2^{F(m^*)} g^{J(m^*)}\right)^{r^*} \left(g_2^{K(m^*)} g^{L(m^*)}\right)^{r_1^*} \\ &= g^{ab+bx_j+b\hat{x}_j+J(m^*)r^*+L(m^*)r_1^*} \\ &= \frac{g^{ab+bx_j+b\hat{x}_j+J(m^*)r^*+L(m^*)r_1^*}}{(g^{bx_j+b\hat{x}_j} g^{r^*})^{J(m^*)} (g^{r_1^*})^{L(m^*)}} \\ &= g^{ab}\end{aligned}$$

Hence the probability is calculated in accordance to the game not aborting in any query of the training phase and obeys the conditions stated in the forgery phase.

In the training phase, there are few instances in the simulation of the underlying signature when the game aborts. And the forgery is only calculated if the stated conditions are met. Hence, the event of abort:
(F($m_i \equiv 0$ mod p) $\bigvee$ (F($m_i \equiv 0$ mod p $\bigwedge$
K($m_i \equiv 0$ mod p) $\bigwedge$ (F(m^*) $\not\equiv 0$ mod p
$\bigwedge$ K(m^*) $\not\equiv 0$ mod p)
Hence the probability,

$$\Pr[\neg abort] \leq \Pr[F(m^*) \not\equiv 0 mod p \bigwedge K(m^*) \not\equiv 0 mod p] + \sum_{1}^{q_s+q_{rs}} \Pr[F(m^*) = 0 \bigwedge F(m_i) = 0] +$$
$$\sum_{1}^{q_{rs}} \Pr[K(m^*) = 0 \bigwedge K(m_i) = 0]$$

Calculating the probability of the forger winning the game, in a similar fashion to that of [8] we obtain,

$$\epsilon' \geq \epsilon/16 q_{rs}(q_s + q_{rs})(n+1)^2$$

where q_s and q_{rs} is the total number of queries to the Sign and ReSign oracle. n is the number of bits of the message.

In the notion of strong unforgeability, the forgery can be made on any message including those which have already been signed. We first simulated the weaker form of the underlying signature(without the transformation) which was proven existentially unforgeable, i.e. only a forgery on a message which has not been signed before is considered valid. Then the existential forgery of the signature is used to solve the CDH problem

with a non-negligible probability. As stated earlier, the existential unforgeability result of the underlying signature scheme is transformed to a strongly unforgeable one using the stated transformation technique.

Now after applying the transformation [4] to both the signature and re-signature algorithms, where the message binds with the randomness and becomes a modified message input to the underlying existentially unforgeable re-signature scheme. As a result the re-signature becomes strongly unforgeable one and the security for the strong unforgeability is based on the security of the underlying existentially unforgeable signature scheme. (Proof can be referred from Theorem 1 of [4].)

To note that the randomness of the originial signature is bound with the message in the resign algorithm. This will retain the integrity of the resignature and prevent it from being split up as independent components. This plays an important role to prevent the forgery on resignatures.

After the application of the strong unforgeability transformation [4] to the signature and re-signature algorithms in PRS_{SUF} to get a strongly unforgeable one, the advantage of breaking the underlying existentially unforgeable re-signature scheme reduces to $1/3^{rd}$ since it is one of the three types of forgers according to Theorem 1 in [4]. Since we are applying to both the sign and re-sign algorithms, the advantage reduces to $1/9^{th}$. Hence the probability of solving the Computational Diffie-Hellman problem after applying the transformation is

$$\epsilon\text{“} \geq \epsilon/144 q_{rs}(q_s + q_{rs})(n+1)^2$$

4 Scheme-2

Recently Susilo et al. [6], proposed a new kind of strong unforgeability transformation which makes use of chameleon hash functions (Hash functions with a public-secret key pair and where a valid collision can be found using the private hash key). We can make use of this transformation as an alternative to the one suggested by [4]. The computation cost for this transformation is approximately the same compared to the one proposed by [4] as they have similar parameters and constructs. The transformation also provides another useful advantage - Tight Reduction. That is the probability of the forger breaking the scheme, is almost at the same level of the challenger solving the underlying hard problem(CDH Problem). The tight security reduction gives rise to practical strongly unforgeable proxy re-signature schemes. We name this alternate scheme $PRS2_{SUF}$

Tight Reduction: In a security proof, the success of the adversary ϵ is taken as an advantage to solve the underlying mathematical hard problem successfully with probability $\epsilon`$. This relation between $\epsilon$ and $\epsilon`$ is termed as security reduction. Without loss of generality, the relationship can be given by $\epsilon` = \frac{\epsilon}{\lambda}$ for some parameter $\lambda(\geq 1)$. We can say that the security of the scheme is tightly reduced to the mathematical hard problem if λ is close to one. This gives a strengthened security argument on how secure the scheme is designed.

In this proposed scheme, the tight reduction is obtained due to the fact that the probability of success is not related to the number of signing and resigning queries during the training phase. In the original Waters' [14] based construct, the probability of success is inversely proportional to the number of queries in the training phase. Hence with an increased number of queries to the singing and resining oracle will reduce the probability of success of solving the mathematical hard problem. This can be avoided using the technique suggested by Susilo et. al. [6] where there is no abort case in the training phase thereby making the probability independent of the number of queries and depend only on the forgery phase.

Chameleon Hash Function: Originally coined and introduced by Krawczyk, was extensively used to implement blind signatures. It is associated with a public hash key and private hash key. One can compute the hash value using the public hash key. It is possible to find valid hash collisions only using the private hash key but cannot calculate the collision with only the chameleon hash and its public hash key. Let H_{ch} be a chameleon hash function with (m, s) as the input where m is the message and s is the randomness. It is easy to find a new pair $(\hat{m}, \hat{s})$ such that $H_{ch}(m, s) = H_{ch}(\hat{m}, \hat{s})$ with the knowledge of the private hash key. The construction for the chameleon hash function used is not an idealized one and hence it can use existing standard discrete log based constructions of chameleon hash functions [10].

Scheme Definitions:

KeyGen(1^k): Same as that in Scheme-1 where there are two pairs of secret,public key - $(g_2^{a_1}, g_1 = g^{a_1})$,

$(g_2^{a_2}, g_{11} = g^{a_2})$ where $a_1, a_2 \in_R \mathbb{Z}_p$. Define a standard hash function $H_2 : \{0,1\}^* \to \mathbb{Z}_p$. The Chameleon Hash used in this scheme [10] is defined as follows: Using the generator g $\in \mathbb{G}$, set the element $g_3 = g^\beta$ where $\beta \in \mathbb{Z}_p$.
The private hash key is β and public hash key is (g_3, g).

$$\text{The chameleon hash } H_{ch}(m,s) = (g_3^m g^s).$$

Given a new $\hat{m} \neq m$, it is easy to find a hash collision using the private hash key β by calculating $\hat{s} = (m - \hat{m})\beta + s$. It can observed that
$H_{ch}(\hat{m}, \hat{s}) = g_3^{\hat{m}} g^{\hat{s}} = g_3^m g^s = H_{ch}(m,s)$.

g_3 is added to the common reference string for all users and β can be stored secretly for every user and is mainly used in the sign and re-sign algorithms. To note that the β used by each user(including proxy) is different.

Hence the common reference string, $< g, g_2, u_0, u_1 ... u_n, v_0, v_1 ... v_n, > \in \mathbb{G}$.
Sign(m, sk): On the input of the message to be signed and secret key of the user signing the message m, the signer to return the signature, performs the following computations:

Consider the primary secret of the signer (user A) to be $g_2^{a_1}$.

- Pick a random $\gamma, r \in \mathbb{Z}_p$ and compute g^γ.
- Consider $m_1 = H_1(g^\gamma) \in \{0,1\}^n$ as the message and perform the Waters' Signature on it as follows:
- Define $m_u^{(1)} = u_0 \prod_{i=1}^{n} u_i^{m_{1_i}}$.
  where $m^{(1)} = (m_1^{(1)}, m_2^{(1)}, m_3^{(1)} \ ... \ m_n^{(1)})$ denotes the n-bit representation of $\mathrm{m}^{(1)}$.
- Compute $\sigma_1 = g_2^{a_1}.(m_u^{(1)})^r \in \mathbb{G}$.
- Compute $\sigma_2 = g^r \in \mathbb{G}$.
  Unforgeability transformation
- Compute $m^{`} = H_2(m, \sigma_2) \in \mathbb{Z}_p$.
- Compute $s_1 = \gamma - m^{`}\beta$.
- Assign $\sigma_3 = s_1 \in \mathbb{Z}_p$
  The signature $\sigma =< \sigma_1, \sigma_2, \sigma_3 >$

$$(\sigma_1, \sigma_2, \sigma_3) = \left(g_2^{a_1}.(m_u^{(1)})^r, g^r, s_1\right)$$

ReKey(g_2^a, g_2^b): In order to delegate the signing right from either A to B (or B to A as our scheme is bidirectional) the proxy will run an interactive protocol with A and B. The final re-signature key obtained by the proxy will be of the form

$$rk_{A \to B} = g_2^{b_1 + b_2 - a} \in \mathbb{G}$$

The Interactive protocol used to obtain the $rk_{A \to B}$ is the same as that defined in Section 3.
ReSign(pk_B, pk_A, m, σ): Proxy on receiving a signature $\sigma =< \sigma_1, \sigma_2, \sigma_3 >$ on the message m by user A associated with public key pk_A, re-signature key $rk_{A \leftarrow B}$ as input, performs the following to generate a signature on m for user B.

- First check whether the $Verify1(pk_A, m, \sigma)$ satisfies, if not abort reporting an invalid signature. Otherwise perform the following steps to generate the re-signature.
- Assign $\hat{\sigma}_2 = \sigma_2 = g^r \in \mathbb{G}$
- Let $\gamma_1, r_1 \in_R \mathbb{Z}_p$, compute and assign $\hat{\sigma}_3 = g^{r_1} \in \mathbb{G}$
- Consider $m_2 = H_1(g^{\gamma_1}) \in \{0,1\}^n$ as the message and perform the Waters' Signature on it as follows:
- Define $m_v^{(1)} = v_0 \prod_{i=1}^{n} v_i^{m_{2_i}}$.
  where $m^{(1)} = (m_1^{(1)}, m_2^{(1)}, m_3^{(1)} \ ... \ m_n^{(1)})$ denotes the n-bit representation of $\mathrm{m}^{(1)}$.
  Unforgeability transformation
- Compute $m^{``} = H_2(m, \hat{\sigma}_3) \in \mathbb{Z}_p$.
- Compute $s_2 = \gamma_1 - m^{``}\beta^{`}$.
- Assign $\hat{\sigma}_5 = s_2 \in \mathbb{Z}_p$

– Assign $\hat{\sigma}_4 = \sigma_3 = s_1 \in \mathbb{Z}_p$

Define $m_v^{(2)} = v_0 \prod_{i=1}^{n} v_i^{m_{2_i}}$

– Compute $\hat{\sigma}_1 = \sigma_1.rk_{A\to B}.(m_v^{(2)})^{r_1} \in \mathbb{G}$

$$= g_2^{a_1}.(m_u^{(1)})^r.g_2^{b_1+b_2-a}.(m_v^{(2)})^{r_1}$$
$$= g_2^{b_1+b_2}\left((m_u^{(1)})^r\right)^r\left((m_v^{(2)})^{r_1}\right)^{r_1}$$

The Re-signature $\hat{\sigma} = (\hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3, \hat{\sigma}_4, \hat{\sigma}_5)$

$$= \left(g_2^{b_1+b_2}\left((m_u^{(1)})^r\right)^r\left((m_v^{(2)})^{r_1}\right)^{r_1}, g^r, g^{r_1}, s_1, s_2\right)$$

for one transformation of the signature is returned.

Verify1(m, σ, pk): For verifying the signature $\sigma =< \sigma_1, \sigma_2, \sigma_3 >$ on the message m by the user corresponding to public key g^{a_1}, any verifier can perform the following validity check.

– Compute $t = H_2(\sigma_2, m)$

– $m^{(1)} = H_1(g_3^t g^{\sigma_3}) \in \{0,1\}^n$

– $m_u^{(1)} = u_0 \prod_{i=1}^{n} u_i^{m_i^{(1)}}$.

– Verify whether the following equation satisfies

$$\hat{e}(\sigma_1, g) \stackrel{?}{=} \hat{e}(m_u^{(1)}, \sigma_2)\hat{e}(g_2, g_1)$$

if the above test holds, output *Valid* otherwise output *Invalid*.

Verify2$(m, \hat{\sigma}, pk)$: For verifying the re-signature $\hat{\sigma} =< \sigma_1, \sigma_2, \sigma_3, \sigma_4 >$ on the message m by the user corresponding to public key pk, any verifier can perform the following validity check on the transformed signature as follows.

– Compute $t = H_2(m, \hat{\sigma}_2) \in \{0,1\}^n$

– $m^{(1)} = H_1(g_3^t g^{\hat{\sigma}_4}) \in \{0,1\}^n$

– $t_1 = H_2(m, \hat{\sigma}_3) \in \{0,1\}^n$

– $m^{(2)} = H_1(g_3^{t_1} g^{\hat{\sigma}_5}) \in \{0,1\}^n$

– $m_u^{(1)} = u_0 \prod_{i=1}^{n} u_i^{m_i^{(1)}}$

– $m_v^{(2)} = v_0 \prod_{i=1}^{n} v_i^{m_i^{(2)}}$

– Verify whether the following equation satisfies

$$\hat{e}(\hat{\sigma}_1, g) \stackrel{?}{=} \hat{e}(m_u^{(1)}, \hat{\sigma}_2).\hat{e}(m_v^{(2)}, \hat{\sigma}_3).\hat{e}(g_2, g_1)\hat{e}(g_2, g_{11})$$

if the above test holds, output *Valid* otherwise output *Invalid*.

The Correctness of the Verify algorithm is similar to that given in PRS_{SUF}.

Proof of Security

Theorem 2. *If there is an adversary, which can break the strongly unforgeable scheme $PRS2_{SUF}$ in polynomial time, by having q_s and q_{rs} queries to the sign and resign oracles and advantage (ϵ) with n as the size of the message, then the CDH problem can be broken with advantage $\epsilon^{\text{“}} \geq \epsilon/(2n+1)^2$.*

In this theorem we give an overview of the proof of security for the strongly unforgeable scheme defined above. The proof of this theorem can be easily deduced as a combination of the proof structure given in Theorem.1 along with the proof of tight reduction that is defined in [6].

Suppose there exists a $(t, q_s, q_{rs}, \epsilon)$ adversary that can break our strongly unforeable proxy re-signature scheme, then there is a challenger who can solve the computational Diffie-Hellman problem, i.e. when given a random tuple (g, g^a, g^b) then its output is g^{ab}. The initial training phase of the adversary is as follows:
Note: This scheme is proved secure against static corruption, where the corrupted entities are set prior to the beginning of the game.

Setup: To setup the common reference string used by the users, The $\mathbb{C}$ chooses n-length vectors (x_i) and (z_i) randomly from [1,2] and (w_i) and (z_i) randomly from $\mathbb{Z}_p$. $y_0, w_0 and \beta$ are also randomly taken from Z_p.

Then it chooses four integers $k_0, k_1, k_2, k_3 \in [0, 2n]$. After stating the secure collision resistant hash function H_1, $\mathbb{C}$ defines the reference string as, $g_1 = g^a, g_2 = g^b, g_3 = g^\beta$, and $g_{11} = g^{\hat{a}}$ where $\hat{a} \in_R \mathbb{Z}_p$ and known by the challenger.
$u_{00} = g_2^{-k_0} g^{y_0}, u_{01} = g_2^{-k_1} g^{y_0}$,
$u_i = g_2^{x_i} g^{y_i}, v_{00} = g_2^{-k_2} g^{w_0}$,
$v_{01} = g_2^{-k_3} g^{w_0}, v_i = g_2^{z_i} g^{w_i}$.

In order to choose the u_0 and v_0, the following operations are performed, $\mathbb{C}$ randomly chooses $d_1, ...d_{2q_s}$ and $e_1, e_2, ...e_{2q_{rs}} \in \mathbb{Z}_p$ and computes $M_i^{(1)} = H_1(d_i)$ and $M_i^{(2)} = H_1(e_i) \in \{0,1\}^n$ for every $i = 1, 2...q_s/q_{rs}$ where n is defined in the same way as in the scheme. Let,

$$F_0(M_i^{(1)}) = \sum_{i \in \mathbb{M}} x_i - k_0 \ , \ F_1(M_i^{(1)}) = \sum_{i \in \mathbb{M}} x_i - k_1.$$
$$K_0(M_i^{(2)}) = \sum_{i \in \mathbb{M}} z_i - k_2 \ , \ K_1(M_i^{(2)}) = \sum_{i \in \mathbb{M}} x_i - k_3.$$

If there are more than q_s number of d_i such that $F_j(M_i) = 0$ then there must more than q_s queries satisfying $F_{1-j}(M_i) \neq 0$. If j=1, then $F_0(M_i) \neq 0$ for particular $d_1, ...dq_s$ values which are stored by $\mathbb{C}$, then u_0 is assigned with u_{00}. Then the equation becomes,

$$u_0 \prod_{i \in M} u_i = g_2^{F_0(M)} g^{J(M)}$$

The same process can be followed for the resigning phase and we obtain the equation

$$v_0 \prod_{i \in M} v_i = g_2^{K_0(M)} g^{L(M)}$$

and these are taken into account for the signing/resigning phase.

Training Phase

The KeyGen and Rekey oracles for corrupted and uncorrupted users are taken in the same fashion as mentioned in Theorem-1. We assume $\hat{a}$ as the secondary secret component for both corrupted and uncorrupted users without loss of generality.

$\mathbb{O}_{UncorruptedSign}(m_i, pk_A) : \mathbb{C}$ chooses a d_i from the list which was stored in the setup phase and a random $r \in \mathbb{Z}_p$, for a given m_i and computes the signature $(\sigma_1, \sigma_2, \sigma_3)$ as follows:

$$= (g_1^{-J(M)/F_0(M)} \left(g_2^{F_0(M)} g^{J(M)} \right)^r ,$$
$$g^r . g_1^{-1/F_0(M)}, d_i - m_i \beta)$$

Hence there would be no abort scenario during the signing phase. This would aid in ignoring the corrupted users' re-signature queries.

$\mathbb{O}_{UnCorruptedReSign}(m_i, \sigma_i, pk_A, pk_B) : \mathbb{C}$ chooses a e_i from the list which was stored in the setup phase and a random $r_1 \in \mathbb{Z}_p$, for the given σ_i

First, the signature is verified using the Verify1 algorithm. If it does not satisfy, $\mathbb{C}$ returns $\perp$.

If the re-signature query is that from a corrupted to an uncorrupted user where $F_j(M)$ does not satisfy the protocol defined in the setup phase, then we can induce the hard problem using the following construct $(\hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3, \hat{\sigma}_4.\hat{\sigma}_5)$

$$
\begin{aligned}
=&(g_2^{\hat{a}} g_1^{-L(M)/K_0(M)} \left(g_2^{F_0(M)} g^{J(M)}\right)^{r} \left(g_2^{K_0(M)} g^{L(M)}\right)^{r_1} \\
&, g^{r}, g^{r_1}.g_1^{-1/K_0(M)}, d_i, e_i - m_i\beta^{`})
\end{aligned}
$$

where $\hat{a}$ is known by $\mathbb{C}$. Hence there is no abort scenario for the resigning queries. Thus we can conclude that the training phase can be run without an abort scenario and the end probability can be independent of the number of signing and resign queries made. This is the root cause for the tight reduction of the security proof.

Forgery: The adversary outputs a valid signature $(\sigma_1^*, \sigma_2^*, \sigma_3^*)$ or a valid re-signature $(\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*)$ for message m^*.

The forgery must always be done for an uncorrupted user, otherwise the hard problem cannot be solved and the game will abort.

Case 1: $m^* \neq m_i$ for i $\in \{m_1, ..., m_{q_s}/m_{q_{rs}}\}$ The forgery is on a new message. This is the same as that of existential forgeability.

With the security of the hash function we can conclude that

$$H_1(\sigma_{2_i}, m_i) \neq H_1(\sigma_2^*, m^*) \quad \forall i \in \{1...q_s\}.$$

With the security of the chameleon hash we can conclude that

$$g_3^{H_1(\sigma_{2_i}, m_i)} g^{\sigma_{3_i}} \neq g_3^{H_1(\sigma_2^*, m^*)} g^{\sigma_{3^*}}$$

The forgery must satisfy the fact that $F_0(M^*) = 0$, and is of the form:

$$(\sigma_1^*, \sigma_2^*, \sigma_3^*) = \left(g_2^a \left(u_0 \prod_{i \in M^*} u_i \right)^{r^*}, g^{r^*}, s \right)$$

$\mathbb{C}$ solves the hard problem by performing the following computations,

$$
\begin{aligned}
\frac{\sigma_1^*}{(\sigma_2^*)^{J(M^*)}} &= \frac{g_2^a \left(u_0 \prod_{i \in M^*} u_i \right)^{r^*}}{g^{J(M^*)r^*}} \\
&= \frac{g_2^a \left(g_2^{F_0(M^*)} g^{J(M^*)} \right)^{r^*}}{g^{J(M^*)r^*}} \\
&= g_2^a \\
&= g^{ab}
\end{aligned}
$$

When the forgery is for a re-signature, it must satisfy the fact that $F_0(M^*) = 0$ and $K_0(M^*) = 0$, and is of the form:

$$
\begin{aligned}
&(\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*.\sigma_5^*) \\
=&(g_2^{a+\hat{a}} \left(u_0 \prod_{i \in M^*} u_i \right)^{r^*} \left(v_0 \prod_{i \in M^*} v_i \right)^{r_1^*} \\
&, g^{r^*}, g^{r_1^*}, s^*, s_1^*)
\end{aligned}
$$

then the $\mathbb{C}$ solves the hard problem by performing the following computations,

$$\begin{aligned}
&\frac{\sigma_1^*}{(\sigma_2^*)^{J(M^*)}\,(\sigma_3^*)^{L(M^*)}\,g_2^{\hat{a}}} \\
&= \frac{g_2^{a+\hat{a}}\left(u_0\prod_{i\in M^*}u_i\right)^{r^*}\left(v_0\prod_{i\in M^*}v_i\right)^{r_1^*}}{g^{J(M^*)r^*}g^{L(M^*)r_1^*}g_2^{\hat{a}}} \\
&= \frac{g_2^{a}\left(g_2^{F_0(M^*)}g^{J(M^*)}\right)^{r^*}\left(g_2^{K_0(M^*)}g^{L(M^*)}\right)^{r_1^*}}{g^{J(M^*)r^*}g^{L(M^*)r_1^*}g_2^{\hat{a}}} \\
&= g_2^a \\
&= g^{ab}
\end{aligned}$$

Case 2: When $m^* = m_i$ it is evident that
$(\sigma_1^*, \sigma_2^*, \sigma_3^*) \neq (\sigma_{1_i}, \sigma_{2_i}, \sigma_{3_i})$ and $(\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*.\sigma_5^*) \neq (\sigma_{1_i}, \sigma_{2_i}, \sigma_{3_i}, \sigma_{4_i}, \sigma_{5_i})$, $\forall$ i = $\{m_1, ..., m_{q_s}/m_{q_{rs}}\}$.

In this type of forgery when $\sigma_2^* \neq \sigma_{2_i}$ or $\sigma_3^* \neq \sigma_{3_i}$ for the signature/re-signature, then the inequality will be similar to the above case.

When $\sigma_2^* = \sigma_{2_i}$ or $\sigma_3^* = \sigma_{3_i}$ for the signature/re-signature, we know $s^* \neq s_i$ or $s_1^* \neq s_{1_i}$. Hence we there will be an inequality of the chameleon hash and will lead to contradictory of the CDH assumption as seen before.

Thus the probability that the game will not abort is *Pr[Case 1 or 2].Pr[Not abort in Forgery Phase]*
$= \dfrac{1}{2(2n+1)(2n+1)}$

Here the (2n+1) is due to the fact that there will be only $k_i \in [0, 2n]$ for which $F_i = 0$ (for i=$\{0,1\}$) or $k_j \in [0, 2n]$ for which $K_j = 0$ (for j=$\{2,3\}$).

Thus the Computational Diffie-Hellman problem can be solved with a probability

$$\epsilon^{\text{“}} \geq \epsilon/2(2n+1)^2$$

4.1 Efficiency Improvements of Schemes

Due to the use of a signature construct similar to that of Waters' [14] , the number of public parameters used in the scheme is quite high. Especially, the two n-vector group elements consume a enormous amount of memory which is not healthy considering the limited storage capacity available. As Patterson [8] had pointed out, we can use the techniques suggested by Naccache and Chatterjee-Sarkar who claimed that the number of parameters can be reduced by making a small modification in the manner we consider the n-vector group elements based on the n-bits of the hash function output. Instead of considering the message digest (hash function output) as a string of bits, it is taken as concatenation of t-bit integers. Hence number of group elements $\hat{n} = \frac{n}{t}$.

Consider the message m to consist of n bits. It is being split into t-bit integers and computation is modified accordingly,

$$u_0\prod_{i=1}^{\hat{n}}u_i^{m_i} \text{ instead of } u_0\prod_{i=1}^{n}u_i^{m_i}$$

This reduction in number of parameters also increase the efficiency by reducing the computations [8] performed during signing and resigning. But at the same time, there is a reduce in the success probability for the $\mathbb{C}$ to solve the underlying hard problem by the order of the number of signing and resigning queries during the training phase during the security game. According to [8] we can deduce that the probability is reduced by a factor of approximately $\frac{2^{q_s}2^{q_{rs}}}{q_s q_{rs}}$. In order to compensate for the security loss, Chatterjee-Sarkar proposed an idea where the size of the group in which the CDH problem is hard. This will to an extent negate the effect of probability reduction due to q_s and q_{rs}.

5 Conclusion

We have presented in this paper, two strongly unforgeable proxy re-signature schemes, which can be proved secure in the standard model. We have made use of strong unforgeability transformation techniques to obtain the strongly unforgeable version of the signature scheme in order to make the resulting proxy re-signature scheme also as strongly unforgeable. However, there has been a trade off between efficiency and security, as we have by strengthening the security, reduced the efficiency due to the introduction of a large number of parameters. A few efficiency improvements have been suggested for the same. The second scheme proposed also possess a tight reduction to a weak assumption thereby strengthening our security argument. The future work for such strongly unforgeable, standard model (bi-directional/uni-directional) proxy re-signature schemes can be to propose and prove such schemes secure under the notion of adaptive corruption (for which the security model has been formalized [2] [5]) and also to increase its efficiency by reducing the number of parameters.

References

1. Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature and encryption. In *EUROCRYPT*, pages 83–107, 2002.
2. Giuseppe Ateniese and Susan Hohenberger. Proxy re-signatures: new definitions, algorithms, and applications. In *ACM Conference on Computer and Communications Security*, pages 310–319, 2005.
3. Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy cryptography. In *EUROCRYPT*, pages 127–144, 1998.
4. Dan Boneh, Emily Shen, and Brent Waters. Strongly unforgeable signatures based on computational diffie-hellman. In *Public Key Cryptography*, pages 229–240, 2006.
5. Sherman S. M. Chow and Raphael C.-W. Phan. Proxy re-signatures in the standard model. In *ISC*, pages 260–276, 2008.
6. Fuchun Guo, Yi Mu, and Willy Susilo. How to prove security of a signature with a tighter security reduction. In *ProvSec*, pages 90–103, 2009.
7. Benoît Libert and Damien Vergnaud. Multi-use unidirectional proxy re-signatures. In *ACM Conference on Computer and Communications Security*, pages 511–520, 2008.
8. Kenneth G. Paterson and Jacob C. N. Schuldt. Efficient identity-based signatures secure in the standard model. In *ACISP*, pages 207–222, 2006.
9. Jin Li Qiong Huang, Duncan S. Wong and Yi-Ming Zhao. Generic transformation from weakly to strongly unforgeable signatures. In *Journal of Computer Science and Technology*, volume 23, pages 240–252, 2007.
10. Adi Shamir and Yael Tauman. Improved online/offline signature schemes. In *CRYPTO*, pages 355–367, 2001.
11. Jun Shao, Zhenfu Cao, Licheng Wang, and Xiaohui Liang. Proxy re-signature schemes without random oracles. In *INDOCRYPT*, pages 197–209, 2007.
12. Jun Shao, Guiyi Wei, Yun Ling, and Mande Xie. Unidirectional identity-based proxy re-signature. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–5, june 2011.
13. Isamu Teranishi, Takuro Oyama, and Wakaha Ogata. General conversion for obtaining strongly existentially unforgeable signatures. In *INDOCRYPT*, pages 191–205, 2006.
14. Brent Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT*, pages 114–127, 2005.

A Properties of a Proxy Re-Signature scheme

There are various properties that define a proxy re-signature scheme depending on its construction. The Re-Signature scheme may require one or more of the following properties depending on the requirement of the application:

1. Bi-Directional & Uni-Directional: In a Bi-Directional scheme, the proxy using a re-key will be able to transform signatures from both A to B as well as from B to A. However, in a Uni-Directional scheme, the proxy will be able to perform the transformation only in one direction using a single re-key.
2. Multi-Use & Single-Use: In a multi-use scheme, the signature on a message can be transformed one or more times to another user's signature using the re-signature algorithm, while only one transformation with respect to the original signature is possible in a single-use scheme.

3. Private & Public Proxy: In private proxy schemes, the re-signature keys are kept secret by a trusted proxy and hence the proxy can control which signatures can be translated. In public proxy schemes, any user who is passively observing the proxy can recompute the re-signature keys.
4. Transparency: This is an important property, which conveys whether the signature and re-signature on the message are computationally indistinguishable. This property defines whether the existence of the intermediary proxy is publicly known.
5. Key-Optimal: The secret information stored by a user in the system is small and constant regardless of the number of signature delegations the user has given or accepted. On the other hand, the amount of secret information stored by the proxy should also be kept minimal.
6. Non-Interactive: The re-key is computed without the involvement of the delegatee(A), i.e. the public key of A is used instead of his secret key, in the computation of the re-signature key. Hence the involvement of A in the re-key computation process is not required in a non-interactive scheme.
7. Transitive: The ability of the proxy to re-delegate its signing rights using the transitive property of re-keys.
8. Temporary: This is more of a security related property, where the re-signing authority for a proxy is temporary with respect to two users.

B Strong Unforgeability Transformation Techniques

In this section we give an overview of the strong unforgeability property in signature schemes and provide our intuition regarding how we select and use the strong unforgeability transformation techniques for our constructions.

Generally signature schemes are proven for unforgeability under adaptive chosen message attack (The forger can adaptively choose a message for forgery). There are two kinds of security notions under this namely, strong and weak unforgeability. The most commonly used notion is the weak (existential) unforgeability, where the forgery is on a message that has never been queried for a signature, during the training phase.

This case is implicit for deterministic signature schemes where a message cannot have two different signatures with respect to an user. But, with the advent probabilistic signature schemes, the situation arises where a message can have one or more signatures with respect to a single user. Hence a stronger notion of security is required, where the forgery on a message which has already been signed (queried during the training phase) is also considered a valid attack on the system.
Let the forger have the following message signature pairs from the training phase:
(m_1, σ_1), (m_2, σ_2), ... , (m_q, σ_q). where q is the number of queries in the training phase.

- Weak forgeability: Here a forgery is on a message m^* where $m^* \notin \{m_1, m_2, ..., m_q\}$.

- Strong forgeability: Here, the forger may come up with a forgery (m^*, σ^*) where $(m^*, \sigma^*) \notin \{(m_i, \sigma_i) | 1 \leq i \leq q\}$. Note that, in the training phase, some of the queries may have m^* as the message.

Most of the signature schemes in the random oracle model are proved secure in the strongly unforgeable security notion. But there are very few Diffie-Hellman based schemes in the standard model, which possess this property. The forgery on signatures which do not satisfy the strong unforgeability is mainly through re-randomization. Chik-How TAN, analysed the Waters' signature scheme, and proved that the scheme is malleable and open to key substitution attack. The signature scheme is said to be malleable, when given a signature, message pair, it is easy to come up with another valid signature for the same message.

The motivation for designing schemes with this property is to convince the verifier that the signature has been generated by the signer himself, rather than an adversary modifying the randomness component. Even though this kind of attack does not modify the message, it creates a valid signature different from the one originally given by the signer. Strong unforgeability gives the verifier the assurance that the randomness present in the signature was by the original signer and not tampered by any one else.

One approach to introduce this strong unforgeability property is to use a transformation, which can convert the existing signature schemes to strongly unforgeable ones. There are various transformation techniques, which were proposed to convert the signatures with security of existential unforgeability to strongly

unforgeable ones. But there are very few transformation techniques available, which can return strongly unforgeable signature schemes, secure in the standard model. One of the most ideal technique (used in this paper) is the transformation proposed by Boneh, Shen and Waters'[4]. Their technique can be applied to a specific class of signatures called partition signatures. A signature is said to be partitioned if and only if

1. randomness and the message are independent.
2. given the message and randomness, the entire signature can be generated.

The *class of partitioned signatures* is mostly found in standard model discrete log based signature schemes [4] (namely Waters' Signature). Hence this technique is of prime importance to our paper due to its suitability since we are basing our scheme on the Waters' signature, which happens to be a partitioned signature.

Compared to the transformation technique used in this paper, the other transformation techniques, which are used to convert standard model signatures into strongly unforgeable ones [13], [9], are either based on stronger assumptions or are computationally inefficient as they include many extra parameters. There are many other conversion techniques which can be used, but they introduce a random oracle and are hence not suitable for the standard model. A generic transformation in the standard model was given by [**?**], but it leaves the underlying signature not flexible enough to be extended to a proxy re-signature.

Recently, Susilo et. al. [6] proposed a generic way of obtaining strongly unforgeable signatures using chameleon hash functions. This transformation can also be applied to the underlying Waters' signature [14] and a strongly unforgeable proxy re-signature can be derived. The message here is not signed directly, instead a random element is signed and is then bound with the message using an extra randomness. A concrete scheme based on this transformation is given in section 4.

It is evident that these techniques discussed above, cannot be applied direclty to existing standard model proxy re-signature schemes as they may not satisfy the strongly unforgeability notion in its true sense.

C Insecurities in other forms of constructions

Now if we take Shao's Proxy Re-signature scheme and apply the transformation in [4], the underlying signature may become strongly unforgeable, but the resulting re-signature conversion will not be possible because of the re-randomization that happens while converting the signature to the re-signature. This can be illustrated as follows:

Table 3.1 : Strong unforgeability transformation on Shao's Proxy Re-Signature [11]

Secret keys of A and B	g_2^a and g_2^b
Transformation [4]	$t = H_1(m, g^r)$, $\hat{m} = H_1(g^t h^s)$
Signature	$\sigma_1 = g_2^a.H_1(\hat{m})^r$, $\sigma_2 = g^r$,$\sigma_3 = s$
Rekey	rk = b/a
Re-Signature	$\hat{\sigma_1} = \sigma_1^{rk} = g_2^a.H_1(\hat{m})^{rb/a}$with the new randomness components to be $\hat{\sigma_2} = g^{rb/a}$.

Note that the resulting re-signature will not satisfy the verify algorithm. This is because of binding of message m with the original randomness r. Thus re-randomization of the entire signature results in an invalid re-signature as $\hat{m}$ cannot be modified.

Due to this drawback, the transformation can be applied to the proxy re-signature scheme separately in the signing and the resigning phase. Instead of re-randomizing the entire signature, we introduce a new randomness as an extra component along with retaining the original randomness of the signature thereby making the proxy re-signature scheme transparent. Otherwise the following insecurity arises,

Table 3.2: PRS_{SUF} Re-Signature without introducing the new randomness

Secret keys of A and B	g_2^a and g_2^b
Transformation [4]	$t = H_1(m, g^r)$, $\hat{m} = H_1(g^t h^s)$
Signature	$\sigma_1 = g_2^a.H_1(\hat{m})^r$, $\sigma_2 = g^r$, $\sigma_3 = s$
Re-Key	g_2^{b-a}
Re-Signature	$\hat{\sigma_1} = g_2^{b-a}.\sigma_1 = g_2^b.H_1(\hat{m})^r$, $\hat{\sigma_2} = \sigma_2 = g^r$, $\hat{\sigma_3} = \sigma_3 = s$
Insecurity (private proxy)	Forger passively obtains re-key using rk=$\hat{\sigma_1}/\sigma_1$=g_2^{b-a}

It is also evident from PRS_{SUF} that there is a dependency between both randomness components. This might protect the scheme from a strong unforgeability attack on the re-signature. Hence we bind the message and the old randomness with this new randomness using the same transformation in order to make sure that the resulting proxy re-signature scheme is also strongly unforgeable.

The problem of having just one secret key, public key pair will allow an adversary to generate re-signatures arbitrarily from signatures of the same user. Hence, in PRS_{SUF} using two key pairs the signature and re-signature differ by both a random component and a secret key component making it hard to forge a re-signature from a given signature.