Proxy Re-signatures in the Standard Model

Sherman S.M. Chow\textsuperscript{1} and Raphael C.-W. Phan\textsuperscript{2,⋆}

\textsuperscript{1} Department of Computer Science  
Courant Institute of Mathematical Sciences  
New York University, NY 10012, USA  
schow@cs.nyu.edu  
\textsuperscript{2} Electronic & Electrical Engineering  
Loughborough University  
LE11 3TU, United Kingdom  
r.phan@lboro.ac.uk

Abstract. This paper studies proxy re-signature schemes. We first classify the expected security notions for proxy re-signature schemes with different properties. We then show how to attack on a recently proposed bidirectional scheme that is purported to be secure without random oracles, and discuss the flaw in their proof. Next, we show how to design a generic unidirectional proxy re-signature scheme using a new primitive called homomorphic compartment signature as the building block. We give a concrete instantiation which yields the first known unidirectional proxy re-signature scheme which is proven secure under standard assumption in the standard model. We also discuss how to incorporate the concept of forward-security into the proxy re-signature paradigm, such that the signing and the transformation are both time-limited.

Keywords: Proxy re-signature, compartment signature, standard model.

1 Introduction

Proxy re-cryptography is about delegating transformation rights of cryptographic objects to a semi-trusted proxy, such that a cryptographic task which can only be completed by a delegator now becomes a task that can only be completed by a delegatee. This idea was introduced by Blaze, Bleumer, and Strauss \cite{2}. For proxy re-signature, signatures signed by a delegator can be transformed into ones signed by a delegatee, without allowing the proxy to sign on any other messages.

1.1 Applications

Proxy re-signatures have many interesting applications \cite{1,2}. One of which is about public-key certificates management. Public-key certificates issued by certification authorities are often deployed in e-commerce infrastructure to allow...
validating online transactions. Proxy re-signatures ease the certificates deployment by transforming signatures of a certification authority’s new public keys into signatures that can be verified with public keys already certified in existing certificates. Generalizing, this leads to transparent cross-certification between different certification authorities, i.e. certificates from one authority can be converted into certificates from the others.

Proxy re-signatures aid in the usage of machine readable travel documents like e-passports. From one point to another the signature within the passport can be transformed, beginning with the issuer’s certification on the passport holder’s identity, through the different check points, each time requiring only one transformable signature to be kept within the passport. Generalizing, it can also trace the path taken by a travelling salesperson on business trips.

Yet another use of proxy re-signatures is in the generation of anonymous group signatures, for instance by transforming any signature by an employee to one verifiable under the corporate’s public key. This conceals the unique identity of the employee to prevent information leakage says on the company’s corporate structure or employment profile, while still allowing for internal auditing.

1.2 Our Contributions

1. We build on the security notions for proxy re-signatures of Ateniese and Hohenberger [1], and discuss what to expect for schemes with different properties including private proxy, non-interactivity, transparency, transitivity and bidirectional properties. While their definition is general enough, not much discussion is made on which notion should be considered for different combination of properties and why a certain property is ensured.

2. We show how to attack on a bidirectional proxy re-signature scheme recently proposed by Shao et al. [10], that came with a security proof without random oracles. We pinpoint the reason accounting for the insecurity and suggest how the attacks could be prevented.

3. We generalize the concept of hierarchical signatures to the notion of (homomorphic) compartment signatures. Using this new primitive as a building block, we show how to design a generic proxy re-signature scheme.

Table 1. Comparison of Properties with Existing Proxy Re-Signature Schemes

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Private proxy</td>
<td>✘</td>
<td>✖</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Unidirectional</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Non-interactive</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Multi-use</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Transparent</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Non-transitive</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Temporary</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Standard model proof</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>