One-Move Nominative Signature: 
The Ambiguity Property and 
Efficient Constructions in the Standard Model

Submitted to
Department of Computer Science
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy

by

Liu Yan Wang Dennis

June 2014
Abstract

Digital Signature is one of the essential tools to ensure authentication, non-repudiation and integrity of electronic information nowadays. Analogous to hand-written signature, digital signatures provide a clue of the origin of a piece of electronic message, \( m \), or a commitment of \( m \) by the signer. Additionally, digital signatures provide a clue of integrity of \( m \) since \( m \) is signed. Digital signature is self-authenticating in a sense that given a message \( m \) and the corresponding signature \( \sigma \), anyone can verify the validity of \((m, \sigma)\). However, this simple signature-generation-and-verification model of digital signatures is not desirable in some actual scenarios. For example, the signer may not want the signature to be publicly verifiable if the signature is commercially or personally sensitive. To illustrate it by a scenario, suppose a software supplier wants to release a software package and allows only its paying customers to verify if the software is genuine and unmodified. Self-authenticating signature is not able to fulfill the requirement because anyone having a copy of the software is able to perform the verification on the signed software. Therefore, there is a variant of digital signatures called Undeniable Signatures (US). By using US, the validity or invalidity of an undeniable signature on the software can be ascertained by conducting a protocol with the signer, assuming the signer participates. Nonetheless, there are some even more sophisticated scenarios that
US still cannot be applicable. For example, in user certification systems, which concern about showing the validity of users’ birth certificates, driving licences and academic transcripts, an authority $A$ is responsible to issue a certificate to a user $B$. Due to privacy reason, $B$ may want to control the audiences of the certificate. In other words, only $B$ is able to prove the validity of the certificate to any verifiers $C$. Even $A$ is not able to do so. Therefore, another digital signature variant, called Nominative Signatures, has been invented to solve this problem.

A Nominative Signature (NS) is a non-self-authenticating signature which is jointly generated by a signer (or a nominator) and a user (or a nominee), but once generated, its validity can only be determined by the user. No one else including the signer can tell the signature’s validity without the aid of the user. In other words, the user has to participate in a protocol with the verifier to prove the validity of the signature. The main differences of NS from US are that, (1) two parties, namely the signer and the user, must cooperate to generate the signature; and (2) only the user is able to prove the validity of the signatures to the verifier. One possible application of NS is the certification of patients’ medical records by a hospital authority. The hospital authority is acting as the signer and the patient is acting as the user. The hospital authority and the patient jointly create a nominative signature on some medical record. The role of NS in this scenario is to produce a mutual agreement on the validity of the medical records – without the hospital’s authority, the professional validity of the medical records cannot be ensured, while without the patient’s agreement, the hospital cannot forge any medical record of the patient. Due to the privacy of the patient, the patient does not want anybody
to disseminate his/her medical records. That means, only the patient have full control on who can verify the validity of his/her medical records.

Since its introduction in 1996, nominative signatures has drawn cryptographic researchers’ attention and in this thesis, we investigate the details of NS in terms of its security model and scheme constructions. Here are the contributions of this thesis:

- One-move NS is an efficient type of NS that requires the signer to send only one message to the user during the signature generation stage. Currently, there exists only a one-move NS scheme which is proven secure in the standard model (proposed by Schuldt et al. in 2011), and is convertible, that is, the user can transform a nominative signature to a publicly verifiable one without the help of the signer. However, in such scheme, the number of elements in the keys of both signer and user grows linearly with the value of the security parameter. Therefore, we propose a new one-move NS scheme which is convertible, can be proven secure in the standard model, and also has a constant number of elements in the keys of both signer and user. We apply the Boneh-Boyen short standard signature in a novel way to build this nominative signature scheme. The security of our scheme relies on the standard q-SDH and XDH assumptions. Also, our scheme has a 45% increase in efficiency during signature generation, in terms of number of modular exponentiation calculations, when compared with the existing one-move NS scheme.

- Current available NS schemes are based on concrete instantiations of cryptographic schemes (e.g., digital signature and encryption schemes) and there exists no generic construction of secure NS schemes. Inspired
by our concrete construction proposed in this thesis, we will present a
generic construction by utilizing secure standard signature schemes and
secure encryption schemes, and give an instantiation of the generic con-
struction, which provides a supporting evidence that the existence of
secure standard signature schemes and secure encryption schemes im-
plies the existence of nominative signature schemes. The efficiency of
our instantiation of the generic construction is comparable to our first
proposed efficient NS scheme. While the efficiency remains the same
in terms of the signer’s key size and number of modular exponentiation
calculations for the signer during signature generation, the instantiation
requires only four more elements in total from $\mathbb{Z}_p$ for both the signature
$\sigma$ and the key of the user, and four more times of modular exponentiation
calculation for the user during signature generation.

– We study the existing security models of nominative signature and show
that though the existing models have captured the essential security re-
quirements of nominative signature in a strong sense, especially on the
unforgeability against malicious signers/users and invisibility, they are
yet to capture a requirement regarding the privacy of the signer and the
user, and this requirement has been one of the original ones since the
notion of nominative signature was first introduced. In particular, we
show that it is possible to build a highly efficient nominative signature
scheme which can be proven secure in the existing security models, while
in practice it is obvious to find out from the component(s) of a nomi-
native signature on whether a particular signer or user has involved in
the signature generation, which may not be desirable in some actual ap-
plications. We therefore propose an enhanced security property, named “Ambiguity”, and also propose a new one-move nominative scheme for fulfilling this new security requirement without random oracles.
# Contents

Abstract i

Acknowledgements vi

1 Introduction 1

1.1 Digital Signature Variants 2

1.1.1 Undeniable Signatures 2

1.1.2 Designated Confirming Signatures 5

1.1.3 Designated Verifier Signatures 8

1.1.4 Universal Designated Verifier Signature 11

1.1.5 Nominative Signatures 12

1.1.6 Comparisons 17

1.2 Publications and Origins of Contributions 19

1.3 Chapter Summary 19

2 Preliminaries 20

2.1 Notations 20

2.2 Digital Signatures 21

2.2.1 Definitions 23

2.2.2 Security 23

2.2.3 Boneh-Boyen Standard Signature Scheme 24

2.3 Convertible Undeniable Signatures 25

2.3.1 Definitions 26

2.3.2 Security 28
### CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.3 Huang-Wong Convertible Undeniable Signature Scheme</td>
<td>30</td>
</tr>
<tr>
<td>2.4 Public-Key Encryption Scheme</td>
<td>33</td>
</tr>
<tr>
<td>2.4.1 Definitions</td>
<td>34</td>
</tr>
<tr>
<td>2.4.2 Security</td>
<td>35</td>
</tr>
<tr>
<td>2.4.3 ElGamal Encryption Scheme</td>
<td>36</td>
</tr>
<tr>
<td>2.5 Zero-Knowledge Interactive Proofs</td>
<td>37</td>
</tr>
<tr>
<td>2.6 Collision Resistant Hash Functions</td>
<td>38</td>
</tr>
<tr>
<td>2.6.1 Programmable Hash Function</td>
<td>40</td>
</tr>
<tr>
<td>2.7 Standard Model vs Random Oracle Model</td>
<td>41</td>
</tr>
<tr>
<td>2.8 Number-Theoretic Assumptions</td>
<td>44</td>
</tr>
<tr>
<td>2.8.1 (\phi)-Strong Diffie-Hellman Assumption [12, 13]</td>
<td>44</td>
</tr>
<tr>
<td>2.8.2 (\phi)-Hidden Strong Diffie-Hellman Assumption [20]</td>
<td>44</td>
</tr>
<tr>
<td>2.8.3 (\phi)-Decisional Hidden Strong Diffie-Hellman Assumption</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>2.8.5 Decision Linear Problem Assumption [13]</td>
<td>46</td>
</tr>
<tr>
<td>2.8.6 Weak Computational Diffie-Hellman I Assumption [54]</td>
<td>46</td>
</tr>
<tr>
<td>2.8.7 Weak Computational Diffie-Hellman II Assumption [54]</td>
<td>47</td>
</tr>
<tr>
<td>2.8.8 Weak Decisional Diffie-Hellman Assumption [54]</td>
<td>47</td>
</tr>
<tr>
<td>2.8.9 3-Decisional Diffie-Hellman Assumption [119]</td>
<td>47</td>
</tr>
<tr>
<td>2.9 Chapter Summary</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Nominative Signatures</td>
<td>49</td>
</tr>
<tr>
<td>3.1 Definitions</td>
<td>49</td>
</tr>
<tr>
<td>3.2 Security Model</td>
<td>52</td>
</tr>
<tr>
<td>3.2.1 Unforgeability Against Malicious Users</td>
<td>54</td>
</tr>
<tr>
<td>3.2.2 Unforgeability Against Malicious Signers</td>
<td>56</td>
</tr>
<tr>
<td>3.2.3 Invisibility</td>
<td>57</td>
</tr>
<tr>
<td>3.2.4 Non-transferability</td>
<td>59</td>
</tr>
<tr>
<td>3.2.5 User-only Conversion</td>
<td>60</td>
</tr>
</tbody>
</table>
CONTENTS

3.3 Chapter Summary ........................................... 62

4 A New Efficient Construction of One-Move Nominative Signature 63
  4.1 Construction (Scheme I) ................................. 64
  4.2 Security Analysis .......................................... 69
  4.3 Chapter Summary .......................................... 75

5 A Generic Construction of One-Move Nominative Signature 76
  5.1 Generic Construction ....................................... 77
  5.2 Security Analysis .......................................... 79
  5.3 Instantiation (Scheme II) ................................. 83
  5.4 Chapter Summary .......................................... 86

6 Ambiguous One-Move Nominative Signature 87
  6.1 An Efficient NS Construction (Scheme III) .............. 88
    6.1.1 Security Analysis ...................................... 91
  6.2 Security Model: Ambiguity ................................ 96
  6.3 A New NS Construction Supporting Ambiguity (Scheme IV) . 102
    6.3.1 Security Analysis ...................................... 105
    6.3.2 An Alternative NS scheme (Scheme V) ................ 110
  6.4 Chapter Summary .......................................... 111

7 Security and Efficiency Analysis 112
  7.1 Security and Efficiency Analysis ......................... 112
  7.2 Chapter Summary .......................................... 116

8 Conclusion and Future Work 117

List of Publications 121

Bibliography 122