2009

A study on undeniable signatures and their variants

Xinyi Huang

University of Wollongong

Recommended Citation


Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au
NOTE

This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

UNIVERSITY OF WOLLONGONG

COPYRIGHT WARNING

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.
A Study on Undeniable Signatures and Their Variants

A thesis submitted in fulfillment of the requirements for the award of the degree

Doctor of Philosophy

from

UNIVERSITY OF WOLLONGONG

by

Xinyi Huang

School of Computer Science and Software Engineering
June 2009
© Copyright 2009

by

Xinyi Huang

All Rights Reserved
Dedicated to

My Family
Declaration

This is to certify that the work reported in this thesis was done by the author, unless specified otherwise, and that no part of it has been submitted in a thesis to any other university or similar institution.

Xinyi Huang
June 3, 2009
Abstract

In an ordinary digital signature scheme, the verification of a signature requires the associated message, the signer’s public key and other public information (e.g. public parameter). Anyone in the system can verify the validity of the digital signature. This property is useful, as it has many applications. However, it is undesirable for some situations where signer’s privacy is a concern, especially in personally and commercially sensitive applications. In this thesis, we investigate several special signature schemes that accommodate the signer privacy.

In undeniable signatures, the most distinctive feature is that the signer is able to choose who can be convinced about his/her undeniable signature, as the validity of an undeniable signature can only be verified in collaboration with the signer. The property selective convertibility enables the signer to convert one or more undeniable signatures into ordinary digital signatures at some time later, while one can make all his/her undeniable signatures publicly verifiable in an undeniable signature scheme with universal convertibility. Undeniable signatures with selective and universal convertibility have found many applications in practice such as keeping digital records of confidential political decisions. However, the most known constructions bear a long signature length and some schemes can only be proven secure under strong complexity assumptions. In this thesis, we describe a new undeniable signature scheme with selective and universal convertibility, of which the signature length is the shortest among all comparable ones and the security can be reduced to weaker complexity assumptions. This scheme is considered in the traditional public key infrastructure, where the authenticity of a user’s public key is ensured by certificates. We also provide the first selectively and universally convertible undeniable signature scheme where a user’s public key is his/her identity.

Designated verifier signatures bridge the gap between ordinary digital signatures and undeniable signatures, in the sense that they will limit who can be convinced by the signer’s signature without any collaboration with the signer. The designated
verifier can be chosen by the signer in the generation of designated verifier signatures. Although the verification of a designated verifier signature usually needs only public information, only the designated verifier can believe that the designated verifier signature has been generated by the signer. This is due to the fact that the designated verifier is able to generate designated verifier signatures which are indistinguishable from those produced by the signer. Strong designated verifier signatures provide a higher level of privacy, as anyone cannot even verify the validity of strong designated verifier signatures with public information. All known constructions of strong designated verifier signatures have a relatively long signature length and require costly operations, which affect the overall performance of the system. In this thesis, we present two new constructions of strong designated verifier signatures, in traditional public key infrastructure and in identity-based cryptography, respectively. Both schemes have high computational efficiency, short signature length and provable security in the random oracle model.

We finally consider universal designated verifier signatures, which can be viewed as an application of the general idea of designated verifier signatures. This notion was introduced to address the user privacy issue in certification systems, where a certificate holder (or more generally, a signature holder) wishes to generate a proof which can prove to a designated verifier his/her possession of the certificate, but does not want anyone else to be convinced. Universal designated verifier signatures achieve this by giving the designated verifier the full ability to generate that proof. The conviction thus is no longer transferable. In this thesis, we revise the notion of non-transferability in universal designated verifier signatures and give a new definition, which is meaningful both in theory and in practice. Our analysis, however, shows that not all existing schemes have that property. We describe a new universal designated verifier signature scheme, which can be proven secure without random oracles and has the property of non-transferability defined in this thesis. This thesis also investigates another property “delegatability”, which was previously believed as an inherent flaw in universal designated verifier signatures. We show that this problem can be overcome by proposing the first universal designated verifier signature scheme without delegatability.
Acknowledgement

I am most grateful to my supervisor Associate Professor Yi Mu, for his support and guidance of this thesis. He has been providing invaluable suggestions and encouragement from the beginning of my research career. This thesis would have been impossible without his support.

I would like to thank my co-supervisor, Associate Professor Willy Susilo, for his continuous guidance in the process of conducting this research. My thanks also go to Professor Futai Zhang for his advice and support since 2003. I have had helpful discussions and suggestions from many people, a non-exhaustive list of whom includes: Man Ho Au, Xiaofeng Chen, Hua Guo, Fuchun Guo, Shekh Faisal ABDUL LATIP, Jiguo Li, Ching Yu Ng, Angela Piper, Shams Ud Din Qazi, Mohammad Reza Reyhanitabar, Siamak Fayyaz Shahandashti, Pairat Thorncharoensri, Raylin Tso, Rungrat Wiangsripinanwan, Duncan S. Wong, Qianhong Wu, Shidi Xu, Yong Yu, Tsz Hon Yuen and Fangguo Zhang, as well as the anonymous referees who reviewed the papers included in this thesis. I would also like to thank all staff of Centre for Computer and Information Security Research and the School of Computer Science and Software Engineering.

I am also grateful to the International Postgraduate Research Scholarships and the University Postgraduate Awards, which were essential in helping me achieve my goals.

I would like to thank my wife Wei Wu, for her patience and love. Without her, this work would never be possible.
Publications

During my PhD studies, I wrote and published the following papers which are related to this thesis.


6. Xinyi Huang, Yi Mu, Willy Susilo and Wei Wu. *A Generic Construction for


12. Xinyi Huang, Willy Susilo, Yi Mu and Futai Zhang. *Restricted Universal Designated Verifier Signature*. In Jianhua Ma, Hai Jin, Laurence Tianruo Yang and Jeffrey J. P. Tsai, editors, Ubiquitous Intelligence and Computing,

Other Publications.


2.3 The Proposed Scheme ........................................... 27
  2.3.1 The Description of Our Scheme ............................. 27
  2.3.2 Security Analysis: Confirmation and Disavowal ............ 30
  2.3.3 Security Analysis: Unforgeability ......................... 32
  2.3.4 Security Analysis: Invisibility ............................ 34
  2.3.5 Security Analysis: S-Convert ............................... 39
  2.3.6 Comparison with Other Schemes ............................ 42
2.4 Conclusion ..................................................... 42

3 Selectively and Universally Convertible Identity-based Undeniable Signatures 43
  3.1 Introduction .................................................. 43
  3.2 Definitions of Identity-based Convertible Undeniable Signatures 45
    3.2.1 Unforgeability of Identity-based Convertible Undeniable Signatures ......................................... 47
    3.2.2 Invisibility of Identity-based Convertible Undeniable Signatures ........................................... 48
    3.2.3 Security of S-Convert ................................... 50
  3.3 The Proposed Scheme .......................................... 51
    3.3.1 The Description of Our Scheme ........................... 52
    3.3.2 Security Analysis: Confirmation and Disavowal .......... 55
    3.3.3 Security Analysis: Unforgeability ....................... 57
    3.3.4 Security Analysis: Invisibility ........................... 61
    3.3.5 Security Analysis: S-Convert ............................. 66
  3.4 Conclusion .................................................. 71

4 Short (Identity-based) Strong Designated Verifier Signatures 72
  4.1 Introduction .................................................. 72
  4.2 Definitions of Strong Designated Verifier Signatures .......... 74
    4.2.1 Unforgeability of Strong Designated Verifier Signatures ......................................................... 75
    4.2.2 Privacy of Signer’s Identity .............................. 76
  4.3 A Short Strong Designated Verifier Signature Scheme .......... 77
    4.3.1 The Description of Our Scheme ........................... 77
    4.3.2 Security Analysis: Unforgeability ....................... 78
    4.3.3 Security Analysis: Privacy of Signer’s Identity ........ 81
  4.4 Short Identity-based Strong Designated Verifier Signatures .... 85
List of Tables

2.1 Existing Undeniable Signature Schemes with Convertibility . . . . . . 15
2.2 Comparison with A Pairing-based Scheme [LV05b] . . . . . . . . . . . 42

4.1 Comparison with Two Efficient DVS Schemes [SKM03, LV04a] . . . . 100
4.2 Comparison with An ID-based DVS Scheme [SZM04] . . . . . . . . . 100

5.1 Comparison with A UDVS Scheme Without Random Oracles [Ver06] 119