

University of Wollongong - Research Online

Thesis Collection

Title: A study on undeniable signatures and their variants

Author: Xinyi Huang

Year: 2009

Repository DOI:

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: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. 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.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

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

2009

A study on undeniable signatures and their variants

Xinyi Huang
University of Wollongong

Follow this and additional works at: <https://ro.uow.edu.au/theses>

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: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. 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.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Recommended Citation

Huang, Xinyi, A study on undeniable signatures and their variants, PhD thesis, School of Computer Science and Software Engineering, University of Wollongong, 2009. <http://ro.uow.edu.au/theses/788>

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 Wiangsripanawan, 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.

1. Xinyi Huang, Willy Susilo, Yi Mu and Wei Wu. *Secure Universal Designated Verifier Signature without Random Oracles*. International Journal of Information Security 7(3), pages 171-183. Springer, 2008.
2. Xinyi Huang, Willy Susilo, Yi Mu and Futai Zhang. *Short Designated Verifier Signature Scheme and Its Identity-based Variant*. International Journal of Network Security 6(1), pages 82-93. 2008.
3. Wei Wu, Yi Mu, Willy Susilo and Xinyi Huang. *Provably Secure Identity-Based Undeniable Signatures with Selective and Universal Convertibility*. In Dingyi Pei, Moti Yung, Dongdai Lin and Chuankun Wu, editors, Information Security and Cryptology, Third SKLOIS Conference, Inscrypt 2007, Lecture Notes in Computer Science 4990, pages 25-39. Springer, 2008.
4. Xinyi Huang, Willy Susilo, Yi Mu and Wei Wu. *Delegating Authentication Power in Mobile Networks*. Book Chapter in S. Gritzalis, T. Karygiannis and C. Skianis, editors, Security and Privacy in Wireless and Mobile Computing. Troubador Publishing, 2009.
5. Xinyi Huang, Yi Mu, Willy Susilo and Wei Wu. *Provably Secure Pairing-Based Convertible Undeniable Signature with Short Signature Length*. In Tsuyoshi Takagi, Tatsuaki Okamoto, Eiji Okamoto and Takeshi Okamoto, editors, Pairing-Based Cryptography-Pairing 2007, First International Conference, Lecture Notes in Computer Science 4575, pages 367-391. Springer, 2007.
6. Xinyi Huang, Yi Mu, Willy Susilo and Wei Wu. *A Generic Construction for*

- Universally-Convertible Undeniable Signatures*. In Feng Bao, San Ling, Tatsuaki Okamoto, Huaxiong Wang and Chaoping Xing, editors, Cryptology and Network Security, 6th International Conference, CANS 2007, Lecture Notes in Computer Science 4856, pages 15-33. Springer, 2007.
7. Dennis Y. W. Liu, Duncan S. Wong, Xinyi Huang, Guilin Wang, Qiong Huang, Yi Mu and Willy Susilo. *Formal Definition and Construction of Nominative Signature*. In Sihan Qing, Hideki Imai and Guilin Wang, editors, Information and Communications Security, 9th International Conference, ICICS 2007, Lecture Notes in Computer Science 4861, pages 57-68. Springer, 2007.
 8. Wei Wu, Yi Mu, Willy Susilo and Xinyi Huang. *Convertible Undeniable Proxy Signatures: Security Models and Efficient Construction*. In Sehun Kim, Moti Yung and Hyung-Woo Lee, editors, Information Security Applications, 8th International Workshop, WISA 2007, Lecture Notes in Computer Science 4867, pages 16-29. Springer, 2008.
 9. Xinyi Huang, Willy Susilo, Yi Mu and Wei Wu. *Universal Designated Verifier Signature Without Delegatability*. In Peng Ning, Sihan Qing and Ninghui Li, editors, Information and Communications Security, 8th International Conference, ICICS 2006, Lecture Notes in Computer Science 4307, pages 479-498. Springer, 2006.
 10. Xinyi Huang, Willy Susilo, Yi Mu and Futai Zhang. *Short (Identity-Based) Strong Designated Verifier Signature Schemes*. In Kefei Chen, Robert H. Deng, Xuejia Lai, Jianying Zhou, editors, Information Security Practice and Experience, Second International Conference, ISPEC 2006, Lecture Notes in Computer Science 3903, pages 214-225. Springer, 2006.
 11. Xinyi Huang, Willy Susilo, Yi Mu and Futai Zhang. *Certificateless Designated Verifier Signature Schemes*. In 20th International Conference on Advanced Information Networking and Applications, AINA 2006, pages 15-19. IEEE Computer Society, 2006.
 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,

Third International Conference, UIC 2006, Lecture Notes in Computer Science 4159, pages 874-882. Springer, 2006.

Other Publications.

1. Raylin Tso, Xun Yi and Xinyi Huang. *Efficient and Short Certificateless Signature*. In Matthew K. Franklin, Lucas Chi Kwong Hui and Duncan S. Wong, editors, Cryptology and Network Security, 7th International Conference CANS 2008, Lecture Notes in Computer Science 5339, pages 64-79. Springer, 2008.
2. Wei Wu, Yi Mu, Willy Susilo and Xinyi Huang. *Server-Aided Verification Signatures: Definitions and New Constructions*. In Joonsang Baek, Feng Bao, Kefei Chen and Xuejia Lai, editors, Provable Security, Second International Conference, ProvSec 2008, Lecture Notes in Computer Science 5324, pages 141-155. Springer, 2008.
3. Wei Wu, Yi Mu, Willy Susilo and Xinyi Huang. *Certificate-Based Signatures: New Definitions and A Generic Construction from Certificateless Signatures*. In Information Security Applications, 9th International Workshop, WISA 2008, Lecture Notes in Computer Science 5379, pages 99-114, Springer, 2009.
4. Jiguo Li, Xinyi Huang, Yi Mu, Willy Susilo and Qianhong Wu. *Constructions of Certificate-Based Signature Secure against Key Replacement Attacks*. Journal of Computer Security. (Accepted, 2008)
5. Lei Zhang, Futai Zhang and Xinyi Huang. *A Secure and Efficient Certificateless Signature Scheme Using Bilinear Pairing*. Chinese Journal of Electronics, 18(1), pages 145-148. 2009.
6. Jiguo Li, Xinyi Huang, Yi Mu and Wei Wu. *Cryptanalysis and Improvement of An Efficient Certificateless Signature Scheme*. Journal of Communications and Networks 10(1), pages 10-17. 2008.
7. Yong Yu, Chunxiang Xu, Xinyi Huang and Yi Mu. *An Efficient Anonymous Proxy Signature Scheme with Provable Security*. Computer Standards & Interfaces, 31(2), pages 348-353. 2009.

8. Xu'an Wang, Xinyi Huang, and Xiaoyuan Yang. *Further Observations on Certificateless Public Key Encryption*. In Information Security and Cryptology, 4th SKLOIS Conference, Inscrypt 2008. Lecture Notes in Computer Science 5487, pages 217-239, Springer, 2009.
9. Dongdong Sun, Xinyi Huang, Yi Mu and Willy Susilo. *Identity-Based On-line/Off-line Signcryption*. In 2008 IFIP International Conference on Network and Parallel Computing, pages 34-41. IEEE Computer Society, 2008.
10. Xinyi Huang, Yi Mu, Willy Susilo, Duncan S. Wong and Wei Wu. *Certificateless Signature Revisited*. In Josef Pieprzyk, Hossein Ghodosi and Ed Dawson, editors, Information Security and Privacy, 12th Australasian Conference, ACISP 2007, Lecture Notes in Computer Science 4586, pages 308-322. Springer, 2007.
11. Yong Yu, Bo Yang, Xinyi Huang and Mingwu Zhang. *Efficient Identity-Based Signcryption Scheme for Multiple Receivers*. In Bin Xiao, Laurence Tianruo Yang, Jianhua Ma, Christian Müller-Schloer, and Yu Hua, editors, Autonomic and Trusted Computing, 4th International Conference, ATC 2007, Lecture Notes in Computer Science 4610, pages 13-21. Springer, 2007.
12. Wei Wu, Yi Mu, Willy Susilo, Jennifer Seberry and Xinyi Huang. *Identity-Based Proxy Signature from Pairings*. In Bin Xiao, Laurence Tianruo Yang, Jianhua Ma, Christian Müller-Schloer, and Yu Hua, editors, Autonomic and Trusted Computing, 4th International Conference, ATC 2007, Lecture Notes in Computer Science 4610, pages 22-31. Springer, 2007.
13. Jiguo Li, Xinyi Huang, Yi Mu, Willy Susilo and Qianhong Wu. *Certificate-Based Signature: Security Model and Efficient Construction*. In Javier Lopez, Pierangela Samarati and Josep L. Ferrer, editors, Public Key Infrastructure, 4th European PKI Workshop: Theory and Practice, EuroPKI 2007, Lecture Notes in Computer Science 4582, pages 110-125. Springer, 2007.
14. Shidi Xu, Yi Mu, Willy Susilo, Xinyi Huang, Xiaofeng Chen, and Fangguo Zhang. *Efficient Authentication Schemes for AODV and DSR*. Book Chapter in Security in Distributed and Networking Systems, pages 367-390. World Scientific Publishing, 2007.

15. Xinyi Huang, Willy Susilo, Yi Mu and Futai Zhang. *Breaking and Repairing Trapdoor-Free Group Signature Schemes from Asiacrypt'2004*. Journal of Computer Science and Technology 22(1), pages 71-74. Springer, 2007.
16. Xinyi Huang, Willy Susilo, Yi Mu and Wei Wu. *Proxy Signature Without Random Oracles*. In Jiannong Cao, Ivan Stojmenovic, Xiaohua Jia and Sajal K. Das, editors, Mobile Ad-hoc and Sensor Networks, Second International Conference, MSN 2006, Lecture Notes in Computer Science 4325, pages 473-484. Springer, 2006.

Contents

Abstract	v
Acknowledgement	vii
Publications	viii
1 Introduction	1
1.1 Background	2
1.1.1 Undeniable Signatures with Selective and Universal Convert- ibility	2
1.1.2 Strong Designated Verifier Signatures	3
1.1.3 Universal Designated Verifier Signatures	5
1.2 Aims and Objectives	6
1.3 Structure of This Thesis and Contributions	7
1.4 Complexity Problems on \mathbb{Z}_p	8
1.5 Bilinear Maps and Related Complexity Problems	9
2 Convertible Undeniable Signatures with Short Signature Length	12
2.1 Introduction	12
2.2 Definitions of Convertible Undeniable Signatures	16
2.2.1 Difference from Previous Definitions	18
2.2.2 (Strong) Unforgeability of Convertible Undeniable Signatures .	19
2.2.3 (Strong) Invisibility of Convertible Undeniable Signatures . . .	20
2.2.4 (Strong) Anonymity of Convertible Undeniable Signatures . . .	22
2.2.5 Relationship Between Anonymity and Invisibility in Convert- ible Undeniable Signatures	24
2.2.6 Security of S-Convert	25

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

4.4.1	Unforgeability of Identity-based Strong Designated Verifier Signatures	86
4.4.2	Privacy of Signer’s Identity in Identity-based Strong Designated Verifier Signatures	87
4.4.3	The Proposed Short Identity-based Strong Designated Verifier Signature Scheme	88
4.4.4	Security Analysis: Unforgeability	89
4.4.5	Security Analysis: Privacy of Signer’s Identity	93
4.5	Efficiency Comparison	99
4.6	Conclusion	100
5	New Constructions of Universal Designated Verifier Signatures	101
5.1	Introduction	101
5.2	Definitions of Universal Designated Verifier Signatures	103
5.2.1	Unforgeability of Universal Designated Verifier Signatures	105
5.3	Analysis of A UDVS Scheme without Random Oracles in [ZFI05]	107
5.3.1	Review of Zhang <i>et al.</i> ’s [ZFI05] UDVS Scheme	107
5.3.2	Analysis of Non-Transferability	108
5.4	A New Construction of UDVS without Random Oracles	109
5.4.1	The Proposed Scheme	110
5.4.2	Security Analysis: Unforgeability	111
5.4.3	Security Analysis: Non-Transferability	117
5.4.4	Comparison with Other Schemes	118
5.5	Delegatability of (Universal) Designated Verifier Signatures	119
5.5.1	Vergnaud’s UDVS-BB [Ver06]	120
5.5.2	Vergnaud’s UDVS-BLS [Ver06]	121
5.5.3	Definition of Non-Delegatability	123
5.6	Universal Designated Verifier Signatures without Delegatability	124
5.6.1	Security Analysis: Non-Transferability	126
5.6.2	Security Analysis: Non-Delegatability	126
5.6.3	Security Analysis: Unforgeability	127
5.7	Conclusion	131
6	Conclusions	132
6.1	Undeniable Signatures with Selective and Universal Convertibility	132

6.2	Strong Designated Verifier Signatures	133
6.3	Universal Designated Verifier Signatures	134
	Bibliography	136

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