

University of Wollongong - Research Online

Thesis Collection

Title: Contributions to privacy preserving with ring signatures

Author: YiQun Chen

Year: 2006

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

2006

Contributions to privacy preserving with ring signatures

YiQun Chen
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

Chen, YiQun, Contributions to privacy preserving with ring signatures, MCompSc thesis, School of Information Technology & Computer Science, University of Wollongong, 2006. <http://ro.uow.edu.au/theses/591>

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.



Contributions to Privacy Preserving with Ring Signatures

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

Master of Computer Science by Research

from

UNIVERSITY OF WOLLONGONG

by

YiQun Chen

School of Information Technology and Computer Science
August 2006

© Copyright 2006

by

YiQun Chen

All Rights Reserved

Dedicated to
My Dad & Mum

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.

YiQun Chen
August 23, 2006

Abstract

A ring signature is a cryptographic primitive that enables a signer to produce a signature without revealing his or her identity. In this thesis, we propose two ring signature schemes for privacy-preserving applications over the Internet.

First we design a protocol that enables a ring signer to receive an acknowledgement from the verifier. We propose two constructions. With the basic construction, the verifier can send a message back to the original signer while keeping the latter's identity hidden. Additionally, the verifier is assured that the signer is indeed the user in a group. We then extend our basic construction to a multi-party scenario. In the second construction, the verifier can discern a certain number of signers involved in the specific signature while their identities remain anonymous. We also investigate the possible applications of our schemes, such as in E-Commerce and Pay-TV.

Then, we introduce the concept of *identity-based anonymous designated ring signatures*, which has not been studied before. This concept extends the existing notion of ring signatures in two ways: firstly, it allows a member of the ring to sign a message directed to a designated verifier. Secondly, we enable the concept of anonymous designated verifier. We show that it has useful applications in Peer-to-Peer networks and provide a construction based on bilinear pairings. Furthermore, we formulate a security model and prove the security of our proposed construction against a chosen message attack. We extend the scheme to construct a convertible version of the previous scheme, which enables a designated verifier to prove its participation in a particular session in case of dispute.

Acknowledgements

I would like to thank Associate Professor Yi Mu and Associate Professor Willy Susilo, my supervisors, for their patient guidance and constant support during my study. Many thanks for choosing me as their student. I admire their wealth of knowledge in security and cryptography, and appreciate them taking me into the area of cryptography. I am also grateful to Dr. Kathleen Weekley for her kind help in the English expression of this thesis. Finally, I would like to thank my family and friends for their enduring love and support.

Publications

YiQun Chen, Willy Susilo and Yi Mu. “Identity-based Anonymous Designated Ring Signatures”, Computer and Network Security Symposium, IWCMC, 2006.

Contents

Abstract	vi
Acknowledgements	vii
Publications	viii
1 Introduction	1
1.1 Challenges	2
1.2 Existing Solutions	3
1.3 Aims and Objectives	4
1.4 Contributions	5
1.5 Structure of Thesis	5
1.6 Notation and Abbreviations	6
2 Background	8
2.1 Mathematical Background	8
2.1.1 Number Theory	8
2.1.2 Group Theory	9
2.2 Public Key Infrastructure	9
2.3 Identity-Based Cryptosystems	10
2.4 Digital Signature Schemes	11
2.4.1 Basics of Digital Signature Schemes	11
2.4.2 Group Signatures	13
2.4.3 Ring Signature	14
2.4.4 Designated Verifier Signature	16

2.5	Encryption Schemes	18
2.5.1	Basics of Encryption Scheme	18
2.5.2	Broadcast Encryption	19
2.6	Commitment Schemes	21
2.7	Zero Knowledge Proofs	22
2.7.1	Proof of Knowledge	22
2.8	Signature of Knowledge	23
2.9	Security Requirements for Digital Signatures	24
2.10	Security Proofs	25
2.11	Cryptographic Tools	26
2.11.1	Hash Functions	26
2.11.2	Bilinear Pairing	26
2.11.3	Time Stamp	27
2.11.4	Intractable Problems	28
2.11.5	Random Oracle Model	29
2.12	Summary	30
3	User Privacy Protection with Ring Signatures	31
3.1	Introduction	31
3.1.1	Motivation	31
3.1.2	Contributions of This Chapter	32
3.2	Definition of Our Scheme	32
3.2.1	System Model	32
3.2.2	Definition of Our Ring Signature Scheme	33
3.2.3	Definition of the Broadcast Encryption Scheme	33
3.2.4	Cryptographic Requirement	34
3.3	Our Scheme	36
3.3.1	Preclusion and Assumption	37
3.3.2	Basic Construction	37
3.3.3	Multi-User Construction	39
3.4	Security Analysis	40

3.5	Efficiency	44
3.6	Applications	44
3.6.1	E-Commerce	44
3.6.2	Pay-TV	47
3.7	Summary	48
4	Identity-Based Anonymous Designated Ring Signature	49
4.1	Introduction	49
4.1.1	Motivation	49
4.1.2	Contributions of This Chapter	50
4.2	Our Construction	50
4.2.1	System Model	50
4.2.2	Cryptographic Requirements	51
4.3	Implementation of Our Scheme	53
4.4	Security Analysis	55
4.5	Convertible Identity-Based Anonymous Designated Ring Signature . . .	58
4.5.1	System Model	59
4.5.2	Cryptographic Requirements	59
4.5.3	A Convertible ID-ADRS scheme based on pairings	60
4.5.4	Security Analysis	61
4.6	Summary	63
5	Conclusion	64
	Bibliography	66

List of Tables

List of Figures

4.1	ID-ADRS Sign and Verify	53
-----	-----------------------------------	----