2006

# Contributions to privacy preserving with ring signatures

YiQun Chen
*University of Wollongong*


# 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

*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

# List of Tables

# List of Figures