2007

Contributions to credential systems

Lan Zhou
University of Wollongong

Contributions to Credential Systems

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

Lan Zhou

School of Information Technology and Computer Science
May 2007

Dedicated to

my parents

Declaration

I, Lan Zhou, declare that this thesis, submitted in partial fulfilment of the requirements for the award of Master of Computer Science by research, in the School of Information Technology and Computer Science, University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. The document has not been submitted for qualification at any other academic institution.

Lan Zhou
May 22, 2007

Publication

Conference Papers

L. Zhou, W. Susilo, and Y. Mu. "Three-Round Secret Handshakes Based on Elgamal and DSA." In *Proceedings of The Second Information Security Practice and Experience Conference (ISPEC 2006)*, volume 3903 of *Lecture Notes In Computer Science*, pages 332–342. Springer-Verlag, 2006.

L. Zhou, W. Susilo, and Y. Mu. "Efficient ID-based Authenticated Group Key Agreement from Bilinear Pairings." In *Proceedings of The Second International Conference on Mobile Ad Hoc and Sensor Networks (MSN 2006)*, volume 4325 of *Lecture Notes In Computer Science*, pages 288–297. Springer-Verlag, 2006.

Abstract

Three separate credential systems, namely Secret Handshakes (SH), Oblivious Signature-Based Envelopes (OSBE) and Hidden Credentials, have been introduced in recent years. These credential systems are very useful in anonymous communication as they have an interesting common feature which is the ability to combine encryption with access control. This feature allows participants to protect their credentials from being disclosed while running the protocols, which makes these credential systems a natural fit for privacy-preserving and anonymity-oriented applications.

Since these systems have many similarities, interest has arisen in converting them from one to another. Consequently, a series of OSBE schemes based on ElGamal family signatures was proposed, along with a generic construction of SH from OSBE. According to this generic construction, any ElGamal family signature based OSBE scheme can be converted to SH within three communication moves, with the exception of the ElGamal and DSA signatures. To complement the previous result, we propose two three-move SH schemes based on ElGamal and DSA signatures, respectively.

Furthermore, we consider the question of extending the two-party SH to a multi-party setting. We observe that almost all of the SH schemes can be constructed from particular key agreement schemes. Hence we implement an efficient ID-based Authenticated Group Key Agreement (AGKA) scheme, from which we can construct a multi-party SH scheme. Very recently, a new multi-party SH scheme has been proposed based on an unauthenticated group key agreement scheme ahead of our implementation. However, we note that there exists a drawback in this scheme, which may cause the leakage of a valid member's group affiliation in a failed multi-party SH protocol. Therefore, we propose a Group Secret Handshake (GSH) scheme that resists against this attack, and prove that our scheme is secure.

Acknowledgements

I would like to thank my supervisors, Associate Professor Willy Susilo, Associate Professor Yi Mu, for their patient guidance and valuable suggestion during my study. I appreciate them for directing me into the area of cryptography.

I also feel very grateful for all the support I have received from all the staff in the School of Information Technology and Computer Science (SITACS), University of Wollongong.

Finally, I am extremely grateful to my parents for their strong and constantly support. Without their sacrifice, I would never have the opportunity to undertake this research work.

Contents

Publication v

Abstract vi

Acknowledgements vii

1 Introduction 1

1.1 Background . . . 1
1.2 Motivation . . . 3
1.3 Problems and Challenges . . . 5
1.4 Contributions of the Thesis . . . 6
1.5 Structure of the Thesis . . . 7
1.6 Glossary . . . 8

2 Cryptographic Background 10

2.1 Cryptographic Tools . . . 11
2.1.1 Cryptographic Hash Functions . . . 11
2.1.2 Random Oracle Model . . . 13
2.1.3 Elliptic Curves . . . 14
2.1.4 Bilinear Pairings . . . 16
2.2 Complexity Assumptions . . . 17
2.3 Digital Signatures . . . 19
2.3.1 Generic Schemes . . . 19
2.3.2 Attacks to Digital Signatures . . . 21
2.3.3 Example of Digital Signature Schemes . . . 22
2.4 Identity-Based Encryption . . . 24
2.5 Key Agreements . . . 26
2.5.1 Diffie-Hellman Key Exchange . . . 26

2.5.2 Group Key Agreements . . . 27
2.6 Credential Systems . . . 28
2.6.1 Oblivious Signature-Based Envelopes (OSBE) . . . 28
2.6.2 Secret Handshakes (SH) . . . 30
2.7 Reconciling Key Agreements, OSBE and Secret Handshakes . . . 32
2.7.1 Secret Handshakes from Key Agreements . . . 32
2.7.2 Secret Handshakes from OSBE . . . 33
2.8 Summary . . . 33

3 Existing Cryptographic Schemes 34
3.1 Oblivious Signature-Based Envelopes . . . 35
3.1.1 OSBE based on RSA signature . . . 35
3.1.2 OSBE based on Schnorr signature . . . 36
3.1.3 OSBE based on Nyberg/Rueppel signature . . . 36
3.1.4 OSBE based on ElGamal Family Signatures . . . 37
3.1.5 OSBE based on DSA Signature . . . 39
3.2 Two-Party Secret Handshakes . . . 40
3.2.1 SH based on Pairing-Based Key Agreements . . . 40
3.2.2 SH based on CA-Oblivious Encryption . . . 41
3.2.3 SH based on RSA signature . . . 42
3.3 Group Key Agreement Schemes . . . 45
3.4 Group Secret Handshakes . . . 48
3.5 Summary . . . 50

4 Secret Handshake Schemes based on ElGamal and DSA signatures 52
4.1 Security Arguments . . . 53
4.2 Constructions from previously proposed OSBE schemes . . . 54
4.3 Efficient Construction of ElGamal-based SH . . . 55
4.3.1 ElGamal-based Key Agreement Scheme . . . 55
4.3.2 ElGamal based Secret-handshake Scheme . . . 56
4.3.3 Security Proof . . . 58
4.4 Efficient Construction of DSA-based SH . . . 59
4.4.1 Security Proof . . . 61
4.5 Summary . . . 62

5 Group Key Agreement Schemes **63**
5.1 Security Arguments . . . 64
5.1.1 Security Model . . . 64
5.1.2 Security Notions . . . 65
5.2 One-Round Group Key Agreement Scheme . . . 66
5.2.1 The Scheme . . . 66
5.2.2 Security Proof . . . 67
5.3 Efficient Group Key Agreement Scheme . . . 70
5.3.1 The Scheme . . . 71
5.3.2 Security Proof . . . 72
5.4 Efficiency Comparison . . . 74
5.5 Summary . . . 75

6 Group Secret Handshakes **76**
6.1 Generic Scheme . . . 77
6.2 Security Arguments . . . 78
6.3 Concrete Construction from Bilinear Pairings . . . 80
6.3.1 The Scheme . . . 80
6.3.2 Security Proof . . . 83
6.4 Summary . . . 89

7 Conclusions and Future Work **90**

Bibliography **93**

List of Tables

1.1 Glossary 9

5.1 AGKA Scheme Efficiency Comparison 75

List of Figures

2.1 A Typical Hash Function 12
2.2 Elliptic Curve Addition 15
2.3 Creating a Digital Signature 20
2.4 Verifying a Digital Signature 20
2.5 Identity-Based Encryption 25
2.6 Diffie-Hellman Key Agreement 27
2.7 Oblivious Signature-Based Envelopes 29
2.8 Secret Handshake 31

5.1 One-Round ID-based Group Key Agreement 68
5.2 Two-Round ID-based Group Key Agreement 72