2009

Contribution to privacy-preserving cryptographic techniques

Man Ho Allen Au
University of Wollongong, aau@uow.edu.au

Contribution to Privacy-Preserving Cryptographic Techniques

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

Doctor of Philosophy

from

UNIVERSITY OF WOLLONGONG

by

Man Ho Allen Au

School of Computer Science and Software Engineering
May 2009

Dedicated to
My mother and my father

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.

Man Ho Allen Au
May 8, 2009

Abstract

Digital signatures are fundamental cryptographic primitives. They are useful as a stand-alone application and building blocks of complex cryptographic systems. Accumulators are another useful cryptographic primitive which provide a way to combine a set of values into one short value. They are useful in improving efficiency of cryptographic systems. In particular, these two primitives are key components in privacy-preserving cryptographic systems.

In this thesis, we study the use of digital signatures and accumulators in cryptographic applications. We design digital signature schemes and accumulators with different features that are suitable for a wide range of applications. We are interested in privacy-preserving cryptographic applications including anonymous electronic cash systems, anonymous authentication schemes and anonymous credential systems.

We construct three different digital signature schemes, each with distinctive features. We also propose two novel constructions of accumulators. Based on our signature schemes and accumulators, we design two compact electronic cash schemes and a divisible electronic cash scheme. All our schemes are truly anonymous, meaning that privacy of the users is well-protected. We also explore other applications of our newly proposed signatures and accumulators. Specifically, we give a construction of k-times anonymous authentication schemes and attribute-based anonymous credential systems.

During the course of the development of the thesis, we generalise existing techniques of zero-knowledge proof-of-knowledge protocol of double-discrete logarithms into zero-knowledge proof-of-knowledge protocol of representation of a committed value. Our protocol is compatible with existing zero-knowledge proof-of-knowledge protocols that demonstrate relationship amongst discrete logarithms. We believe that this protocol, together with the newly introduced primitives, are of independent interest.

Acknowledgement

My experience as a graduate student in the University of Wollongong has been wonderful. I am grateful to my principal supervisor Willy Susilo for this opportunity. Willy has been an excellent supervisor who has offered me directions yet enough freedom for me to explore different areas. I would like to express my gratitude to my co-supervisor Yi Mu for his guidance. Yi has always been nice to me. I still remember the day when he brings me to the supermarket when I first arrived.

My sincere thanks to Dr. Duncan Wong for all his support and advice. The days when I was a research assistant in City University of Hong Kong are so valuable. Duncan and his research group, including Dr. Xiaojian Tian, Tommy Yang, Dennis Liu, Bessie Hu, Jing Chen, etc, are amazing. Special thanks to Qiong Wong with his valuable comments to many of my works. All the discussions are very helpful in the development of this thesis.

I would also like to thank Dr. Lucas Hui and Dr. Siu-Ming Yiu of the Hong Kong University for all the guidance and support. Many thanks to Pierre for her help during my stay as a research assistant in the Hong Kong University. My stay there allows me to build up my foundations before I start my doctorate degree programme. My first research project on e-cash started there and I am thankful to have worked with Sherman Chow.

I am fortunate to be here with a team of interesting people. Discussions are always stimulating and rewarding. I still miss Dr. Qianhong Wu and Dr. Shuhong Wang. The following people must be mentioned. Tsz Hon Yuen, who happened to be my classmate from undergraduate in Hong Kong to graduate student here. Cedric, who brought me around and offered me to stay at his place when I was homeless. I have enjoyed discussions with Xinyi Huang, Wei Wu, Shidi Xu, Mohammad Reza Reyhanitabar, Pairat Thorncharoensri, Liang Lu, Yi Gao, Shams Ud Din Qazi, Siamak Fayyaz Shahandashti, etc. The list goes on and on.

I wish to take this opportunity to give my heartfelt thanks to Prof. Victor Wei,

my supervisor when I was doing a master degree at the Chinese University of Hong Kong. It is Prof. Wei who brings me into the field of cryptography. I would also like to thank my peers at that time, Joseph Liu and Patrick Tsang. They have taught me a lot. Collaborations with them have been rewarding.

This thesis benefited immeasurably from the comments of the panel of knowledgeable thesis examination committee. My heartfelt thanks to Professor Masahiro Mambo and Professor Colin Boyd.

I am fortunate to have knowledgeable, and meticulous panel for my doctoral defense seminar, namely: Prof. Colin Boyd, Prof. Colin Fidge, and Dr. Greg Maitland. This thesis benefited immeasurably from their scrutiny, their relentless precision, and their impeccable taste.

I would like to thank Cindy Chan and Cindy Li for their emotional support. I am grateful to my roommates and friends Chris, Patrick, Emily, Grace, Wendy, Fran, Johnny, Christy, etc. for being with me during my stay in Australia. Finally, special thanks to Jenny Cheung for proof-reading this thesis.

My love and gratitude to my parents Sandra, David and my brother Albert for everything, everything and everything.

Publications

The following papers have been published or presented, and contain materials based on the content of this thesis.

1. Man Ho Au, Patrick P. Tsang, Willy Susilo and Yi Mu. Dynamic Universal Accumulators for DDH Groups and Their Application to Attribute-Based Anonymous Credential Systems (Extended version available from http://uow.academia.edu/ManHoAu/Papers). In Marc Fischlin, editor, Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, Proceedings. Lecture Notes in Computer Science 5473, pages 295 - 308, Springer 2009.

2. Man Ho Au, Willy Susilo and Yi Mu. Practical Anonymous Divisible E-Cash from Bounded Accumulators (Extended version available from http://eprint.iacr.org/2007/459). In Gene Tsudik, editor, Financial Cryptography and Data Security, 12th International Conference, FC 2008, Revised Selected Papers. Lecture Notes in Computer Science 5143, pages 287 - 301, Springer 2008.

3. Man Ho Au, QianHong Wu, Willy Susilo and Yi Mu. Compact E-Cash from Bounded Accumulator. In Masayuki Abe, editor, Topics in Cryptology - CT-RSA 2007, The Cryptographers' Track at the RSA Conference 2007, Proceedings. Lecture Notes in Computer Science 4377, pages 178 - 195, Springer 2007.

4. Patrick P. Tsang, Man Ho Au, Apu Kapadia and Sean W. Smith. Blacklistable Anonymous Credentials: Blocking Misbehaving Users without TTPs (Extended version available as BLAC: Revoking Repeatedly Misbehaving Anonymous Users Without Relying on TTPs from http://www.cs.dartmouth.edu/reports/abstracts/TR2008-635). In Peng Ning,

Sabrina De Capitani di Vimercati, Paul F. Syverson, editors, Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, pages 72-81, ACM 2007.

5. Man Ho Au, Willy Susilo and Yi Mu. Practical Compact E-Cash. In Josef Pieprzyk, Hossein Ghodosi, Ed Dawson, editors, Information Security and Privacy, 12th Australasian Conference, ACISP 2007, Proceedings. Lecture Notes in Computer Science 4586, pages 431 - 445, Springer 2007.

6. Man Ho Au, Willy Susilo and Yi Mu. Constant-Size Dynamic k-TAA (Extended version available from http://eprint.iacr.org/2008/136). In Roberto De Prisco, Moti Yung, editors, Security and Cryptography for Networks, 5th International Conference, SCN 2006, Proceedings. Lecture Notes in Computer Science 4116, pages 111 - 125, Springer 2006.

7. Man Ho Au, Willy Susilo, Yi Mu and Sherman S.M. Chow. Constant-Size Dynamic k-Times Anonymous Authentication. In submission to International Journal of Information Security. Full version of 6.

8. Man Ho Au, Willy Susilo and Siu-Ming Yiu. Event-Oriented k-times Revocable-iff-Linked Group Signatures. In Lynn Margaret Batten, Reihaneh Safavi-Naini, editors, Information Security and Privacy, 11th Australasian Conference, ACISP 2006, Proceedings. Lecture Notes in Computer Science 4058, pages 223 - 234, Springer 2006.

9. Man Ho Au, Sherman S.M. Chow, Willy Susilo. Short E-Cash. In Subhamoy Maitra, C. E. Veni Madhavan, Ramarathnam Venkatesan, editors, Progress in Cryptology - INDOCRYPT 2005, 6th International Conference on Cryptology in India, Proceedings. Lecture Notes in Computer Science 3797, Springer 2005.

I am thankful to have opportunities to collaborate with others in other areas of computer and communications security. The contributions are listed below and they are beyond the scope of this thesis.

1. Patrick P. Tsang, Man Ho Au, Apu Kapadia and Sean W. Smith. PEREA: Towards Practical TTP-Free Revocation in Anonymous Authentication. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, Proceedings of the 2008 ACM Conference on Computer and Communication Security, CCS 2008, pages 333-344, ACM 2008.

2. Man Ho Au, Qiong Huang, Joseph K. Liu, Willy Susilo, Duncan S. Wong, and Guomin Yang. Traceable and Retrievable Identity-Based Encryption. In Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors, Applied Cryptography and Network Security, 6th International Conference, ACNS 2008, New York, NY, USA, June 3-6, 2008. Proceedings, volume 5037 of Lecture Notes in Computer Science, pages 94-110, 2008.

3. Man Ho Au, Yi Mu, Jing Chen, Duncan S. Wong, Joseph K. Liu, and Guomin Yang. Malicious KGC Attacks in Certificateless Cryptography. In ASIACCS 2007: Proceedings of the 2nd ACM symposium on Information, computer and communications security, pages 302-311, New York, NY, USA, 2007. ACM.

4. Joseph K. Liu, Man Ho Au, and Willy Susilo. Self-Generated-Certificate Public Key Cryptography and Certificateless Signature/Encryption Scheme in the Standard Model: Extended Abstract. In ASIACCS 2007: Proceedings of the 2nd ACM symposium on Information, computer and communications security, pages 273-283, New York, NY, USA, 2007. ACM.

5. Tsz Hon Yuen, Man Ho Au, Joseph K. Liu, and Willy Susilo. (Convertible) Undeniable Signatures without Random Oracles. In Sihan Qing, Hideki Imai, and Guilin Wang, editors, Information and Communications Security, 9th International Conference, ICICS 2007, Zhengzhou, China, December 12-15, 2007, Proceedings, volume 4861 of Lecture Notes in Computer Science, pages 83-97. Springer, 2007.

6. Man Ho Au, Joseph K. Liu, Willy Susilo, and Tsz Hon Yuen. Certificate Based (Linkable) Ring Signature. In Ed Dawson and Duncan S. Wong, editors, Information Security Practice and Experience, Third International Conference, ISPEC 2007, Hong Kong, China, May 7-9, 2007, Proceedings, volume 4464 of Lecture Notes in Computer Science, pages 79-92. Springer, 2007.

7. Man Ho Au, Sherman S. M. Chow, Willy Susilo, and Patrick P. Tsang. Short Linkable Ring Signatures Revisited. In Andrea S. Atzeni and Antonio Lioy, editors, Public Key Infrastructure, Third European PKI Workshop: Theory and Practice, EuroPKI 2006, Turin, Italy, June 19-20, 2006, Proceedings, volume 4043 of Lecture Notes in Computer Science, pages 101-115. Springer, 2006.

8. Man Ho Au, Joseph K. Liu, Willy Susilo, and Tsz Hon Yuen. Constant-Size Id-Based Linkable and Revocable-iff-Linked Ring Signature. In Rana Barua and Tanja Lange, editors, Progress in Cryptology - INDOCRYPT 2006, 7th International Conference on Cryptology in India, Kolkata, India, December 11-13, 2006, Proceedings, volume 4329 of Lecture Notes in Computer Science, pages 364-378. Springer, 2006.

9. Man Ho Au, Joseph K. Liu, Tsz Hon Yuen, and Duncan S. Wong. Id-Based Ring Signature Scheme Secure in the Standard Model. In Hiroshi Yoshiura, Kouichi Sakurai, Kai Rannenberg, Yuko Murayama, and Shin ichi Kawamura, editors, Advances in Information and Computer Security, First International Workshop on Security, IWSEC 2006, Kyoto, Japan, October 23-24, 2006, Proceedings, volume 4266 of Lecture Notes in Computer Science, pages 1-16. Springer, 2006.

Contents

Abstract **v**

Acknowledgement **vi**

Publications **viii**

1 Introduction **1**

2 Background **5**

2.1 Preliminaries 5

2.1.1 Miscellaneous Notations 5

2.1.2 Complexity Theory 6

2.1.3 Abstract Algebra 7

2.1.4 Bilinear Map 7

2.1.5 Number-Theoretic Problems 8

2.2 Cryptographic Tools 11

2.2.1 Commitment Schemes 12

2.2.2 Cryptographic Hash Functions 13

2.2.3 Digital Signatures 14

2.2.4 Encryption 15

2.3 Zero-Knowledge Proof-of-Knowledge 16

2.3.1 ZKPoK about Discrete Logarithms 18

2.3.2 ZKPoK about Double Discrete Logarithms 23

3 Signature Schemes with Efficient Protocols **25**

3.1 Syntax 27

3.2 BBS+ Signature 30

3.2.1 Relationship of BBS+ with the BBS Group Signature 30

3.2.2 Construction of BBS+ . . . 30
3.2.3 Security Analysis of BBS+ . . . 33
3.3 ESS+ Signature . . . 37
3.3.1 A Commitment Scheme . . . 37
3.3.2 Construction of ESS+ . . . 38
3.3.3 Security Analysis of ESS+ . . . 41
3.4 C-Signature . . . 43
3.4.1 Proof-of-Knowledge of Representation of a Committed Value . 45
3.4.2 Construction of a C-Signature . . . 48
3.4.3 Security Analysis of C-Signature . . . 51
3.5 Chapter Summary . . . 53

4 Accumulators 54
4.1 Syntax . . . 58
4.1.1 Dynamic Multiversal Accumulator . . . 58
4.1.2 Bounded Accumulator . . . 62
4.2 The Constructions . . . 63
4.2.1 (Bounded) Accumulator . . . 63
4.2.2 Universal Accumulator . . . 64
4.2.3 Multiversal Accumulator . . . 65
4.2.4 Dynamic Multiversal Accumulator . . . 66
4.3 Σ-Protocols for our DMA . . . 67
4.3.1 Knowledge of a Committed Value Inside an Accumulator . . . 67
4.3.2 Knowledge of a Committed Value Not Inside an Accumulator 68
4.4 Chapter Summary . . . 69

5 Application to Electronic Cash Systems 70
5.1 Background . . . 70
5.1.1 Electronic Payment Methods . . . 70
5.1.2 More on Electronic Cash . . . 72
5.1.3 Related Works . . . 75
5.1.4 Our Contributions . . . 76
5.2 Syntax . . . 76
5.2.1 Security Model . . . 78
5.3 Practical Compact E-Cash . . . 81

5.3.1 An Overview of CHL Compact E-Cash 82
5.3.2 Generic Construction of Practical Compact E-Cash 83
5.3.3 Security Analysis of Our Generic Construction 87
5.3.4 Actual Construction of Practical Compact E-Cash 90
5.3.5 Arbitrary Wallet Size for Compact E-Cash 94
5.4 Compact E-Cash from Bounded Accumulator 95
5.4.1 Short E-Cash 95
5.4.2 The Original Version and Its Flaw 97
5.4.3 The Revised Version 99
5.4.4 Security Analysis of Our Revised Version 102
5.5 Divisible E-Cash 106
5.5.1 On Practicality of the CG07 Scheme 106
5.5.2 Overview of Our Construction 107
5.5.3 High Level Description of our Construction 108
5.5.4 The Actual Construction 113
5.5.5 Security Analysis of Our Divisible E-Cash 117
5.5.6 Efficiency Analysis 120
5.6 Extension to Coin Tracing and Revocability 121
5.6.1 Tools - Verifiable Encryption 122
5.6.2 Revocability 122
5.6.3 Coin Tracing of Double-Spender 122
5.6.4 Universal Coin-Tracing 123
5.7 Chapter Summary 124

6 Other Privacy-Preserving Applications 125
6.1 Dynamic k Times Anonymous Authentication 125
6.1.1 Related Works 126
6.1.2 Syntax 127
6.1.3 The Scheme 128
6.2 Attribute-Based Anonymous Credential Systems 133
6.2.1 Overview of the Existing Constructions 133
6.2.2 A Generalisation to ACS 134
6.2.3 Syntax 136
6.2.4 Our Construction 137
6.2.5 Security Analysis 139

7 Concluding Remarks **146**

7.1 Summary of Our Contributions 146

7.1.1 New Construction of CL Signatures. 146

7.1.2 New Construction of Accumulators with Extra Features 146

7.1.3 New Construction of Electronic Cash with Desirable Properties 146

7.1.4 Other Applications of the New Primitives 147

7.2 Open Problems 147

Bibliography **148**

List of Tables

3.1 Summary of our Proposed CL-Signatures 53

4.1 Summary of Existing Accumulators 56

5.1 Time and Space Complexities of Our Scheme and CG07. 121
5.2 Summary of our Proposed Electronic Cash Systems 124

List of Figures

5.1 The life-cycle of an electronic coin 73
5.2 Construction of A Binary Tree (L=3) 109
5.3 Spending 4 coins 111
5.4 Algorithm ComputeAllNodeKeys 114
5.5 Deposit Protocol - Computation of All Serial Numbers Associated with a Particular Coin 116
5.6 RevokeDoubleSpender Algorithm - Computation of a Node Key from a Parent Serial Number 116