

University of Wollongong - Research Online

Thesis Collection

Title: Contributions to pairing-based cryptography

Author: Tsz Hon Yuen

Year: 2010

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

2010

Contributions to pairing-based cryptography

Tsz Hon Yuen
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

Yuen, Tsz Hon, Contributions to pairing-based cryptography, Doctor of Philosophy thesis, School of Computer Science and Software Engineering - Faculty of Informatics, University of Wollongong, 2010.
<https://ro.uow.edu.au/theses/3185>

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

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 Pairing-based Cryptography

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

Doctor of Philosophy

from

UNIVERSITY OF WOLLONGONG

by

Tsz Hon Yuen

School of Computer Science and Software Engineering
November 2010

© Copyright 2010

by

Tsz Hon Yuen

All Rights Reserved

*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.

Tsz Hon Yuen
November 15, 2010

Abstract

Pairing-based cryptography is an active research area in cryptography in the last decade. Pairings are bilinear mappings defined over cyclic groups wherein the discrete logarithm problem is hard. The bilinear property of pairings enables researchers to solve open problems like the construction of practical identity-based encryption, or short signatures without random oracles. Pairings can also be used to construct new cryptographic primitives.

This thesis contributes to the pairing-based cryptography in three areas. Firstly, we show that pairings can be used to construct efficient and provably secure digital signature schemes. We give the first convertible undeniable signatures without random oracles, and the first concrete sanitisable signatures without random oracles. We also construct a new signature primitive called *concinuous signatures*, which is designed to facilitate fair exchange of digital signatures without any trusted third party.

Secondly, we analyse the identity-based cryptosystems which extensively use pairings. We mainly focus on the key escrow problem of identity-based cryptography. We propose the notion of *escrow-free identity-based signatures*. Furthermore, we discuss the impossibility of ideal escrow-free identity-based encryption. After that, we investigate the best defence against the key escrow problem of identity-based encryption. We categorise the existing solutions into *preventive measure* and *blaming mechanism*. In the category of preventive measure, we propose the notion of *fully anonymous identity-based encryption*. In the category of blaming mechanism, we also construct a new accountable-authority identity-based encryption.

Finally, we construct new cryptographic primitives and frameworks using pairings. We give new instantiations and applications of lossy trapdoor function. We give a new cryptographic primitive called *two-tier trapdoor functions*. From two-tier trapdoor functions, we construct a new encryption primitive called *two-tier encryption*. It is a generalisation of a number of encryption schemes, including identity-based encryption. We also propose a cryptographic treatment of publish/subscribe systems.

Acknowledgement

First of all, I would like to thank my supervisors Willy Susilo and Yi Mu. They are very supportive to both my research and give me valuable advices and innovative ideas to my works. I am also grateful for their assistant to help me adapting the life in the university.

I would like to express my gratitude to the researchers who collaborate with me during my Ph.D. study, including Man Ho Au, Qiong Huang, Joseph K. Liu, Duncan S. Wong and Guomin Yang.

Last but certainly not least, I would like to thank my family for their love and support throughout my study.

Publications

In this thesis, the following publications published in refereed conference are included:

- T. H. Yuen, W. Susilo, and Y. Mu. Cryptographic treatment of publish/subscribe systems. In S.-H. Heng, R.N. Wright, and B.-M. Goi, editors, *CANS 2010*, volume 6467 of LNCS, pages 201220. Springer, 2010.
- T. H. Yuen, W. Susilo, and Y. Mu. How to construct identity-based signatures without the key escrow problem. In F. Martinelli and B. Preneel, editors, *EuroPKI 2009*, volume 6391 of LNCS, pages 286301. Springer, 2010.
- T. H. Yuen, W. Susilo, J. K. Liu, and Y. Mu. Sanitizable signatures revisited. In M. K. Franklin, L. C. K. Hui, and D. S. Wong, editors, *CANS 2008*, volume 5339 of LNCS, pages 80-97. Springer, 2008.
- T. H. Yuen, M. H. Au, J. K. Liu, and W. Susilo. (Convertible) undeniable signatures without random oracles. In S. Qing, H. Imai, and G. Wang, editors, *ICICS 2007*, volume 4861 of LNCS, pages 83-97. Springer, 2007.

The following paper is published in journal:

- T. H. Yuen, W. Susilo, and Y. Mu. How to construct identity-based signatures without the key escrow problem: Formal definitions and constructions. *Int. J. Inf. Secur.*, 9(4):297-311, 2010.

The following papers are currently under review by the editors of journals:

- T. H. Yuen, W. Susilo, and Y. Mu. Lossy trapdoor functions: New instantiations and applications. Submitted to *Information and Computation*.
- T. H. Yuen, W. Susilo, and Y. Mu. Two-tier encryption and two-tier trapdoor functions. Submitted to *Theoretical Computer Science*.

- T. H. Yuen, W. Susilo, and Y. Mu. Cryptographic treatment of publish/subscribe systems. Submitted to *IEEE Transactions on Information Forensics and Security*.

The following manuscripts are currently under submission to conferences:

- T. H. Yuen, W. Susilo, Duncan S. Wong and Qiong Huang. Concinnous signatures: Fair exchange of digital signatures.
- T. H. Yuen, W. Susilo, and Y. Mu. Impossibility to ideal escrow-free identity-based encryption.
- T. H. Yuen, W. Susilo, and Y. Mu. On the anonymity of identity-based encryption.
- T. H. Yuen, W. Susilo, and Y. Mu. Black-box accountable authority IBE revisited.

Other publications published during my Ph.D. study which are not included in this thesis:

- T. H. Yuen, Q. Huang, Y. Mu, W. Susilo, D. S. Wong, and G. Yang. Efficient non-interactive range proof. In H.Q. Ngo, editor, *COCOON 2009*, volume 5609 of LNCS, pages 138-147. Springer, 2009.
- M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen. Certificate based (linkable) ring signature. In E. Dawson and D. S. Wong, editors, *ISPEC 2007*, volume 4464 of LNCS, pages 79-92. Springer, 2007.
- J. Li, T. H. Yuen, K. Kim. Practical threshold signatures without random oracles. In W. Susilo, J. K. Liu, and Y. Mu, editors, *ProvSec 2007*, volume 4784 of LNCS, pages 198-207. Springer, 2007.

Contents

Abstract	v
Acknowledgement	vi
Publications	vii
List of Notations	1
Abbreviations	2
1 Introduction	3
1.1 Motivations of the Thesis	5
1.2 Thesis Organisation	5
2 Definitions	7
2.1 Algebra and Number Theory	7
2.1.1 Groups	7
2.1.2 Elliptic Curves	8
2.1.3 Pairings	9
2.2 Complexity Theory	14
2.2.1 Order Notation	14
2.2.2 Algorithms and Protocols	15
2.2.3 Relations and Languages	16
2.2.4 Intractability	17
2.3 Information Theory	19
2.3.1 Entropy	19
2.3.2 Extracting Randomness	19

3	Backgrounds	21
3.1	Cryptographic Primitives	21
3.1.1	Trapdoor Functions	21
3.1.2	Hash Functions	23
3.1.3	Random Oracle Model	24
3.1.4	Pseudorandom Functions	25
3.2	Public Key Cryptography	26
3.2.1	Public Key Encryption	26
3.2.2	Digital Signatures	27
3.3	Identity-based Cryptography	31
3.3.1	Identity-based Signatures	32
3.3.2	Identity-based Encryption	32
3.4	Cryptographic Protocols	33
3.4.1	Oblivious Transfer	33
3.4.2	Secret Sharing	33
3.4.3	Fair Exchange	34
4	Digital Signatures	39
4.1	Undeniable Signatures without Random Oracles	40
4.1.1	Security Models of Undeniable Signatures	42
4.1.2	Convertible Undeniable Signature Scheme	45
4.2	Sanitisable Signatures without Random Oracles	55
4.2.1	Security Models of Sanitisable Signatures	58
4.2.2	Sanitisable Signature Scheme	63
4.3	Concinnous Signatures	70
4.3.1	Security Models of Concinnous Signatures	73
4.3.2	Concinnous Signature Scheme	79
4.3.3	Summary	87
5	Identity-based Cryptography	88
5.1	Key Escrow in Identity-based Cryptography	88
5.1.1	Preventive Measure and Blaming Mechanism	89
5.1.2	Non-identity-based Solutions	91
5.2	Escrow-free Identity-based Signatures	91
5.2.1	Security Model for Escrow-free Identity-based Signatures	93
5.2.2	Generic Construction	98

5.2.3	User Public Key Anonymity	101
5.2.4	Construction with User Public Key Anonymity	102
5.2.5	Comparison	111
5.3	Impossibility of Ideal Escrow-free IBE	112
5.3.1	Ideal Escrow-free IBE	113
5.3.2	Security Notions	113
5.3.3	Exceptional Cases	115
5.4	IBE with Anonymity against the PKG	115
5.4.1	Security Model for Fully Anonymous IBE	118
5.4.2	Our First Construction	122
5.4.3	Our Second Construction	136
5.4.4	Our Second Construction in Prime Order Groups	150
5.4.5	Comparison	161
5.5	Black-Box Accountable Authority IBE	165
5.5.1	Security Model for Black-Box Accountable Authority IBE . . .	166
5.5.2	Indistinguishability for Tracing Ciphertext	171
5.5.3	Another Black-box Accountable Authority IBE	173
5.5.4	Summary	180
6	New Cryptographic Primitives and Protocols	182
6.1	Lossy Trapdoor Functions	183
6.1.1	Lossy Trapdoor Functions from DDH-Easy Groups	184
6.1.2	More Applications using Lossy and ABO Trapdoor Functions .	192
6.2	Two-Tier Encryption and Two-Tier Trapdoor Functions	199
6.2.1	Two-Tier Trapdoor Functions	204
6.2.2	Realisation of Two-Tier TDF from DBDH	208
6.2.3	Two-Tier Encryption	213
6.2.4	Realisation of Two-Tier Encryption	217
6.3	A Formal Treatment of Publish/Subscribe Systems	228
6.3.1	Publish/Subscribe Systems and their Security Models	230
6.3.2	Our Construction	241
6.3.3	Related Works	254
7	Conclusion and Future Work	257
A	Remark	259

List of Tables

2.1	Comparison of representation sizes	13
2.2	Comparison of estimated calculation times on the same elliptic curves at the same security levels	13
3.1	Input and output values of fair exchange system	35
4.1	Comparison of undeniable signatures in the standard model	55
4.2	Comparison of sanitisable signature schemes	69
4.3	Comparison of the efficiency of three sanitisable signature schemes . . .	70
4.4	Flow diagram of concurrent signatures and concinnous signatures . . .	72
4.5	Concinnous signature protocol	74
5.1	Comparison of the public information known by the verifier and the level of trust to the PKG	92
5.2	Comparison of our IBS schemes against the existing schemes	112
5.3	Information that the adversary has in different security models of IBE .	118
5.4	Comparison of efficiency and the loss due to the number of signing oracle query q	135
5.5	Review of the security of some IBE schemes according to our security model	161
5.6	Comparison of the loss due to the number of key extraction oracle query q	164
5.7	Comparison of black-box A-IBE schemes	180
6.1	Summary of different constructions of lossy TDFs	184
6.2	Comparison of the work from Peikert and Waters and this section . . .	184
6.3	Black-box constructions between lossy TDFs, tag-based encryption and public key encryption	196
6.4	Primitives from two-tier encryption	202

6.5	Intractability assumptions required to satisfy requirements in different encryption schemes	205
6.6	Classification of two-tier encryption	218
6.7	Comparison of pub/sub schemes providing confidentiality	255

List of Figures

2.1	Elliptic curve operations over the real number field \mathbb{R}	9
4.1	How sanitisable signatures work in an firewall scenario	56
5.1	Classification of solutions to the key escrow problem	90
6.1	Comparison of the public key encryption and the two-tier encryption .	201
6.2	Publish/subscribe system	229
6.3	Brokers in publish/subscribe system	231

List of Notations

Below introduces the notations commonly used through out the rest of the thesis. Some notation will also be defined locally near its first use, while other notation will be used without further definition.

$S_1 \cup S_2$	union of sets S_1 and S_2
$S_1 \setminus S_2$	difference of sets S_1 and S_2
$S_1 \subseteq S_2$	S_1 is a subset of S_2
$x \in S, x \notin S$	element x (not in) set S
$x \in_R S$	sampling element x uniformly random in set S
$L_1 \prec L_2$	L_1 is polynomial-time many-one reducible to L_2
$\mathbb{N}, \mathbb{Z}, \mathbb{R}$	sets of natural numbers, integers, and real numbers
\mathbb{Z}^+	set of positive integers
\mathbb{Z}_n	integers modulo n
\mathbb{Z}_n^*	multiplicative group of integers modulo n
$a \pmod{b}$	modulo operation: remainder of a divided by b
\forall	for all
\exists	there exists
\vee, \wedge, \neg	boolean operators OR, AND, and NOT
$\text{ord}(\mathbb{G})$	order of a group \mathbb{G}
$\Pr[E]$	probability of event E occurring
$E_1 E_2$	event E_1 occurring given event E_2
$ s $	number of elements in s if s is a finite set, or the length of s if s is a string, or the bit-length/size of s if s is an integer.
1^k	the string of k ones.
$s_1 s_2$	string s_1 concatenate with string s_2 .
$\binom{n}{r}, C_r^n$	binomial coefficient.

Abbreviations

Below introduces the abbreviations commonly used through out the rest of the thesis. They will be defined locally near its first use.

ABO:	All-but-one
A-IBE:	Accountable Authority Identity-based Encryption
CBPS:	Content-based Publish/subscribe System
CCA:	Chosen Ciphertext Attack
CDH:	Computational Diffie-Hellman
CRS:	Common Reference String
DL:	Discrete Logarithm
DLIN:	Decision Linear
IBE:	Identity-based Encryption
IBS:	Identity-based Signatures
NIZK:	Non-interactive Zero Knowledge
PKG:	Private Key Generator
PoK:	Proof of Knowledge
Pub/sub	Publish/subscribe
ROM:	Random Oracle Model
SDH:	Strong Diffie-Hellman
SoK:	Signature of Knowledge
TDF:	Trapdoor Function