2010

Contributions to pairing-based cryptography

Tsz Hon Yuen
University of Wollongong

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

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 *concinnous 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

List of Tables

List of Figures

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
$S_1 \backslash S_2$	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
$\mathrm{ord}(\mathbb{G})$	order of a group $\mathbb{G}$
$\Pr[E]$	probability of event E occurring
$E_1 \vert E_2$	event E_1 occurring given event E_2
$\vert s \vert$	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.
$s_1 \vert\vert s_2$	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