

2009

Contributions to secure and privacy-preserving use of electronic credentials

Siamak F. Shahandashti
University of Wollongong, siamak@uow.edu.au

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

Shahandashti, Siamak F., Contributions to secure and privacy-preserving use of electronic credentials, Doctor of Philosophy thesis, School of Computer Science and Software Engineering - Faculty of Informatics, University of Wollongong, 2009. <https://ro.uow.edu.au/theses/3036>

NOTE

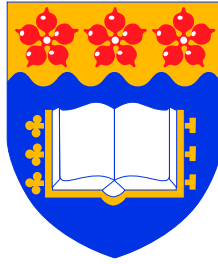
This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

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 Secure and Privacy-Preserving Use of Electronic Credentials

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

Doctor of Philosophy

from

UNIVERSITY OF WOLLONGONG

by

Siamak Fayyaz Shahandashti

School of Computer Science and Software Engineering
Faculty of Informatics
October 2009

© Copyright 2009

by

Siamak Fayyaz Shahandashti

All Rights Reserved

Dedicated to

my wife: Sara

my mum: Behdokht

and my dad: Ali

Certification

I, Siamak Fayyaz Shahandashti, declare that this thesis, submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the School of Computer Science and Software Engineering, Faculty of Informatics, University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. The document has not been submitted for qualifications at any other academic institution.

Siamak Fayyaz Shahandashti
October 5, 2009

Abstract

In this thesis, we make contributions to secure and privacy preserving use of electronic credentials in three different levels.

First, we address the case in credential systems where a credential owner wants to show her credential to a verifier without taking the risk that the ability to prove ownership of her credential is transferred to the verifier. We define *credential ownership proof* protocols for credentials signed by standard signature schemes. We also propose proper security definitions for the protocol, aiming to protect the security of both the credential issuer and the credential owner against concurrent attacks. We give two generic constructions of credential ownership proofs based on identity-based encryption and identity-based identification schemes. Furthermore, we show that signatures with credential ownership proofs are equivalent to identity-based identification schemes, in the sense that any secure construction of each implies a secure construction of the other. Moreover, we show that the GQ identification protocol yields an efficient credential ownership proof for credentials signed by the RSA signature scheme and prove the protocol concurrently-secure.

Then, we give a generic construction for universal (mutli) designated-verifier signature schemes from a large class of signature schemes, referred to as Class \mathbb{C} . The resulting schemes are efficient and have two important properties. Firstly, they are provably DV-unforgeable, non-transferable and also non-delegatable. Secondly, the signer and the designated verifier can independently choose their cryptographic settings. We also propose a generic construction for (hierarchical) identity-based signature schemes from any signature scheme in \mathbb{C} and prove that the construction is secure against adaptive chosen message and identity attacks. We discuss possible extensions of our constructions to identity-based ring signatures and identity-based designated-verifier signatures from any signature in \mathbb{C} . Furthermore, we show that it is possible to combine the above constructions to obtain signatures with combined functionalities.

Finally, inspired by the recent developments in attribute-based encryption, we propose *threshold attribute-based signatures* (t-ABS). In a t-ABS, signers are associated with a set of attributes and verification of a signed document against a verification attribute set succeeds if the signer has a threshold number of (at least t) attributes in common with the verification attribute set. A t-ABS scheme enables a signature holder to prove possession of signatures by revealing only the relevant (to the verification attribute set) attributes of the signer, hence providing *signer-attribute privacy* for the signature holder. We define t-ABS schemes, formalize their security and propose two t-ABS schemes: a basic scheme secure against selective forgery and a second one secure against existential forgery, both provable in the standard model, assuming hardness of the computational Diffie-Hellman problem. We

show that our basic t-ABS scheme can be augmented with two extra protocols that are used for efficiently issuing and verifying t-ABS signatures on committed values. We call the augmented scheme a threshold attribute based c-signature scheme (t-ABCS). We show how a t-ABCS scheme can be used to realize a secure *threshold attribute-based anonymous credential system* (t-ABACS) providing signer-attribute privacy. We propose a security model for t-ABACS and give a concrete scheme using t-ABCS scheme. Using the simulation paradigm, we prove that the credential system is secure if the t-ABCS scheme is secure.

Acknowledgments

I would like to start by thanking my supervisor *Rei* (Professor Reihaneh Safavi-Naini). Her vast knowledge of the area and her macroscopic intuition of the bits and pieces in the field assisted me to obtain a better understanding of cryptographic research. Although only few can come close to her twelve-hour-per-day average working time! She has also been of great support in my non-academic life.

From the beginning of my candidature in the now School of Computer Science and Software Engineering (SCSSE), then School of IT and CS (SITACS) at University of Wollongong, I have been based in 3.234 with lab-mates that I have the honour to call ‘friends’ now. I would like to credit these guys since without them it would have been a much harder job to live in a whole new country and do a PhD. I would like to specially thank *Angela* (Angela Piper), *Noi* (Rungrat Wiangsripanawan), and *Reza* (Mohammad Reza Reyhanitabar) for the uncountable little and big things they have done for me. I also extend my acknowledgment to my friends *Allen* (Man Ho Au), *Jeff* (Dr. Jeffrey Horton), *John* (Tsz Hon Yuen), *Martin* (Jan Martin Surminen), *Michael* (Wenming Lu), *Pairat* (Pairat Thorcharoensri), *Xinyi* (Xinyi Huang), and *Wei* (Wei Wu).

I spent almost three months in the *iCORE* Information Security Lab of the University of Calgary as a visitor and I would like to thank the lab for hosting me. During this period I made new friends, *Jason* (Dr. M. Jason Hinek) and *Michal* (Dr. Michal Sramka), and here I would like to thank them for being there for me. I also like to thank Dr. Shaoquan Jiang for the fruitful discussions we had.

I would like to thank *James* (James Atkinson), head of Campus East, a place that I called home for almost 3 years. James trusted me with a residential advisor position for 2 years which was both a unique life learning experience and a considerable financial assistance.

I thank Professor Willy Susilo for helping me out here and there. I appreciate Professor Philip Ogunbona, my co-supervisor, and Dr. Jonsang Baek’s guidance of my thesis. I also thank Professor Jennifer Seberry, Associate Professor Yi Mu, and Professor Farzad Safaei for their kindness towards me. I would like to mention Dr. Shuhong Wang for the usefull discussions we had.

I extend my gratitude to the anonymous reviewers of ASIACCS ’07, PKC ’08, AfricaCrypt ’09, and the IET Journal of Information Security for their comments on my papers, and similarly to Professor Colin Boyd of the Information Security Institute of the Queensland University of Technology and Associate Professor Michael Jacobson of the Institute for Security, Privacy and Information Assurance of the University of Calgary, my thesis examiners, for their extremely comprehensive and useful comments on my thesis.

Last, but certainly not least, I am most grateful of the love of my life, my lovely wife, *Sara*, for accompanying me in diving to a wholly unknown new life in Australia and supporting me through the period. I also thank my mum and dad, *Behdokht* and *Ali*, for their total support and love during the almost three decades of my life. I am grateful of my brothers, *Siavash* and *Kiavash*, for not saying no to any of the little annoying favours I asked them during these years. I thank my parents-in-law, *Maryam* and *Hassan*, and my brother-in-law, *Ata*, for their love and support.

Publications

The following publications have arisen from the research carried out during the PhD candidature and hence the material in this thesis is largely based on them.

- [SSB07] Siamak F Shahandashti, Reihaneh Safavi-Naini, and Joonsang Baek. Concurrently-Secure Credential Ownership Proofs. In Feng Bao and Steven Miller, editors, *ASIACCS '07*, pages 161–172. ACM, 2007.
- [SS08] Siamak F Shahandashti and Reihaneh Safavi-Naini. Construction of Universal Designated-Verifier Signatures and Identity-Based Signatures from Standard Signatures. In Ronald Cramer, editor, *Public Key Cryptography (PKC '08)*, volume 4939 of *Lecture Notes in Computer Science*, pages 121–140. Springer, 2008.
- [SS09b] Siamak F Shahandashti and Reihaneh Safavi-Naini. Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems. In Bart Preneel, editor, *AfricaCrypt '09*, volume 5580 of *Lecture Notes in Computer Science*, pages 198–216. Springer, 2009.
- [SS09a] Siamak F Shahandashti and Reihaneh Safavi-Naini. Generic Constructions for Universal Designated-Verifier Signatures and Identity-Based Signatures from Standard Signatures. *IET Information Security*, (to appear), 2009.

Free personal versions of the above publications are available via the World-Wide Web as follows:

- [SSB06] Siamak F Shahandashti, Reihaneh Safavi-Naini, and Joonsang Baek. Concurrently-Secure Credential Ownership Proofs. Available through corresponding author's home page: <http://sites.google.com/site/siamax/>. Full version of [SSB07].
- [SS07] Siamak F Shahandashti and Reihaneh Safavi-Naini. Construction of Universal Designated-Verifier Signatures and Identity-Based Signatures from Standard Signatures. Cryptology ePrint Archive, Report 2007/462, 2007. <http://eprint.iacr.org/2007/462>. Full version of [SS08].
- [SS09c] Siamak F Shahandashti and Reihaneh Safavi-Naini. Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems. Cryptology ePrint Archive, Report 2009/126, 2009. <http://eprint.iacr.org/2009/126>. Full version of [SS09b].

Notation

Xyz	algorithm Xyz
XYZ	security notion XYZ
\mathcal{X}_{yz}	oracle \mathcal{X}_{yz}
Xyz	string Xyz
ε	the empty string
$\mathbb{P}\text{oly}(k)$	the set of all algorithms polynomial time in k
St_{X}	internal state information of algorithm X
\parallel	concatenation
\setminus	set subtraction
$ x $	bit length of the quantity x
$ S $	cardinality of the set S
$\varphi(\cdot)$	Euler's totient function
$x \leftarrow a$	value a is assigned to variable x
$x \stackrel{N}{\leftarrow} a$	value $a \bmod N$ is assigned to variable x
$x \stackrel{\$}{\leftarrow} X$	a member is chosen randomly from set X and assigned to variable x
$x \leftarrow \mathsf{X}(a; r : \mathcal{O})$	algorithm X with access to oracle \mathcal{O} , input a , and random tape r is run and the output is assigned to variable x
$A \dashv(X) \rightarrow B \mid C$	A sends X to B if condition C holds
$(s, t) \leftarrow [\mathsf{X}(x) \leftrightarrow \mathsf{Y}(y)](a)$	interactive protocol between X with private input x and Y with private input y is run with public input a , X outputs s and Y outputs t
$\text{Tr}[\mathsf{X}(x) \leftrightarrow \mathsf{Y}(y)](a)$	transcript of a protocol run with public input a between X with private input x and Y with private input y
$\text{ZK-PoK}\{x : a = g^x\}$	zero knowledge proof of knowledge of x such that $a = g^x$, where a and g are public inputs to the protocol
$\mathsf{X}(a)$	algorithm X with input a and description [desc.] is run and x is
[desc.]	returned as output
Return x	

Contents

Abstract	V
Acknowledgments	VII
Publications	IX
Notation	X
1 Introduction	1
1.1 Credential Ownership Proofs	4
1.2 Universal Designated Verifier Signatures	6
1.2.1 Further Identity-Based Constructions	8
1.3 Attribute-Based Signatures	9
1.4 Attribute-Based Anonymous Credential Systems	11
2 Preliminaries	14
2.1 Public Key Cryptography and Provable Security	14
2.2 Computational Assumptions	16
2.3 Interactive Proof Systems	18
2.4 Identification and Signature Schemes	21
2.5 Identity-Based Cryptography	25
3 Concurrently-Secure Credential Ownership Proofs	29
3.1 Introduction	29
3.1.1 Related Work	30
3.1.2 Our Contributions	31
3.2 Defining Credential Ownership Proofs	32
3.2.1 Defining Credential Ownership Proof Security	33
3.2.2 Security Treatment of Baek et al.	36
3.3 Generic Construction from IBE	37
3.3.1 IBE and Its Security	38
3.3.2 Naor Transform	39
3.3.3 IBE-Based COP	40
3.4 Equivalence with IBI	42
3.5 Efficient COP from GQ	43

3.5.1	The GQ Identification Scheme	44
3.5.2	RSA-FDH Credential Ownership Proof	45
3.5.3	Efficiency of the Scheme	48
3.6	Concluding Remarks	49
4	Generic Construction of Universal Designated-Verifier Signatures and Identity-Based Signatures	51
4.1	Introduction	51
4.1.1	Our Contributions	52
4.1.2	Related Work	55
4.2	Preliminaries	56
4.2.1	Proofs of Knowledge	56
4.2.2	The Fiat-Shamir Transform	57
4.2.3	On Public-Private Key Pairs	59
4.2.4	The Forking and Reset Lemmas	60
4.3	Defining the Class \mathbb{C} of Signatures	62
4.3.1	On Simulatability of Signature Schemes	64
4.3.2	Examples of Signatures in Class \mathbb{C}	65
4.4	Universal Designated Verifier Signatures	66
4.4.1	Definition and Security	66
4.4.2	Generic Construction of UDVS And Its Security	72
4.4.3	Comparison	81
4.5	Identity-based Signatures	83
4.5.1	Generic Construction of IBS and Its Security	83
4.5.2	Comparison	87
4.6	Combined Constructions	89
4.7	Concluding Remarks	90
5	Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems	92
5.1	Introduction	92
5.1.1	Our Contributions	94
5.1.2	Related Work	95
5.2	Notation and Preliminaries	96
5.3	Threshold Attribute-Based Signatures	97
5.3.1	Definition	97
5.3.2	Additional Protocols	99
5.3.3	Constructions	101
5.4	Threshold Attribute-Based C-Signatures	106
5.4.1	Definition	107
5.4.2	Construction	108
5.5	Threshold Attribute-Based Anonymous Credential Systems	114
5.5.1	Security Framework	114

5.5.2	Ideal Model for t-ABACS	116
5.5.3	A Concrete t-ABACS System	118
5.6	Concluding Remarks	123
6	Conclusions and Open Problems	125
	Bibliography	130
	Index	141

List of Tables

3.1	Comparison of security notions for IBE with the new notion highlighted	38
3.2	Equivalence between S+COPs and IBIs	43
3.3	Comparison of RSA-COP Costs with other ZK Solutions	49
4.1	Examples of Σ protocols for proof of knowledge	57
4.2	Examples of signatures in \mathbb{C}	66
4.3	Examples of signatures in \mathbb{C} (Cont'd)	67
4.4	Comparison of previous UDVS schemes with our GUDVS counterparts	82
4.5	Comparison of previous UMDVS schemes with their GUMDVS counterparts	84
4.6	Four new IBS schemes based on discrete logarithms, RSA, and pairings	89
4.7	Comparison of previous IBUDVS schemes with counterparts in our construction	90
6.1	Credential ownership proofs in comparison with other credential system solutions . . .	126
6.2	A summary of constructions in Chapter 4	127
6.3	Summary of how our UDVS constructions compare with previous schemes	128

List of Figures

2.1	The RSA experiment	16
2.2	One more RSA inversion experiment	17
2.3	The discrete logarithm and CDH experiments	18
2.4	A three-move public-coin protocol in the canonical form	19
2.5	Identification scheme IMP-ATK-security experiments ($\text{ATK} \in \{\text{PA}, \text{AA}, \text{CA}\}$)	23
2.6	Signature scheme EUF-CMA-security experiment	24
2.7	The Fiat-Shamir transform	24
2.8	Identity-based identification scheme ID-IMP-ATK-security exp's ($\text{ATK} \in \{\text{PA}, \text{AA}, \text{CA}\}$)	26
2.9	Identity-based signature scheme ID-EUF-CMA-security experiment	27
3.1	Credential ownership proof COP-IMP-ATK-security experiments	35
3.2	Universal designated-verifier signature proof IM-TYPE- i security experiments	36
3.3	Hypothetical IM-TYPE-3 security experiments	37
3.4	Identity-based encryption scheme OWE-ID-CCA-security experiments	39
3.5	The Naor transform of an identity-based encryption scheme	40
3.6	The identity-based encryption scheme based credential ownership proof	40
3.7	The GQ identification scheme	44
3.8	The RSA-FDH signature scheme	45
4.1	Schemes constructed generically in this chapter based on signature S in \mathbb{C}	55
4.2	A canonical Σ protocol for proof of disjunctive knowledge	58
4.3	The non-interactive proof from applying Fiat-Shamir to the protocol in Figure 2.4	58
4.4	The signature scheme from applying Fiat-Shamir to the protocol in Figure 2.4	59
4.5	RSA, GQ and DL family key generation algorithms	60
4.6	The bifurcation in the h_i inputs of the forked algorithm	61
4.7	Reset Lemma experiments	62
4.8	Mechanism of security proofs for non-FL-Based and FL-Based signatures	65
4.9	Universal designated-verifier signature DV-EUF-CMA-security experiment	69
4.10	Universal designated-verifier signature PR-security experiments	70
4.11	Our generic construction of universal designated-verifier signatures	73
4.12	Mechanism of GUDVS DV-EUF-CMA-security proof	76
4.13	Our generic construction of identity-based signatures	85
5.1	The real model vs. the ideal model	115

5.2	Simulation of the ideal model in Figure 5.1	120
-----	---	-----