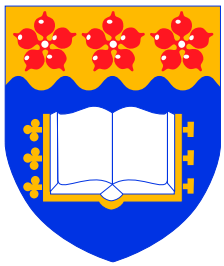
2009

Contributions to secure and privacy-preserving use of electronic credentials

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



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

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 Thorncharoensri), *Xinyi* (Xinyi Huang), and *Wei* (Wei Wu).

I spent almost three months in the *i*CORE 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 arised 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, *ASI-ACCS '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
$\mathbb{P}\mathrm{oly}\,(k)$	the set of all algorithms polynomial time in k
St_{X}	internal state information of algorithm X
$\|$	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
$x \xleftarrow{N} a$	value a mod N is assigned to variable x
$x \xleftarrow{\$} X$	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
$A \multimap(X)\mapsto B \mid C$	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 y
$\mathsf{Tr}\,[\mathsf{X}\,(x) \leftrightarrow \mathsf{Y}(y)]\,(a)$	transcript of a protocol run with public input a between X with private input x and Y with private input y
$\mathsf{ZK\text{-}PoK}\{x : a = g^x\}$	zero knowledge proof of knowledge of x such that $a = g^x$, where a and g are public inputs to the protocol
$\mathsf{X}\,(a)$ [desc.] Return x	algorithm X with input a and description [desc.] is run and x is returned as output

Contents

List of Tables

List of Figures