


Advances in Cyber Security: Principles, Techniques, and Applications


Kuan-Ching Li · Xiaofeng Chen
Willy Susilo
Editors

Advances in Cyber Security: Principles, Techniques, and Applications


Editors

Kuan-Ching Li 

Department of Computer Science and
Information Engineering
Providence University
Taichung, Taiwan

Willy Susilo 

School of Computing and Information
Technology
University of Wollongong
Wollongong, NSW, Australia

Xiaofeng Chen 

School of Cyber Engineering
Xidian University
Xi'an, Shaanxi, China

ISBN 978-981-13-1482-7

ISBN 978-981-13-1483-4 (eBook)

<https://doi.org/10.1007/978-981-13-1483-4>

Library of Congress Control Number: 2018958348

© Springer Nature Singapore Pte Ltd. 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd. The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Foreword I

With the rapid development of cyber technology, more and more users and organizations are willing to use cyber technology for work and daily life. All agree that cyber technology has great potential to transform the way human beings work, live, and behave. However, cybersecurity events ranging from data leakage to all kinds of ransomware happen with frequency higher than past years. The wanton outbreak of ransomware WannaCry caused great harm to the network users. The “Snowden event” exemplified the world that cybersecurity has a direct consequence on the national security. Currently, cybersecurity has received widespread attention in academic, industrial community, and government. On the other hand, the development of cloud computing, IoT, and big data makes the distributed networked systems more sophisticated, powerful and easy to use. In the meantime, these new technologies bring new challenges to cybersecurity. Therefore, one should seek solutions to build secure network and systems which are also more effective, intelligent, adaptive, and high performance for real-world applications.

The current book, *Advances in Cyber Security: Principles, Techniques, and Applications*, covers the recent advances in cybersecurity, which is true value to the individual, organization, and human society to understand the fundamental and realistic issue about cybersecurity. The field include: lightweight solutions for public key encryption in resource-constrained environments, nonintrusive load monitoring algorithms to mine consumer privacy in smart grid, accountable anonymous credentials, CAPTCHA design and security issues, ring signature, authenticated data redaction with privacy-preserving and flexible redaction control, a methodology for retrofitting privacy and its application to e-shopping transactions, pseudonymous signature schemes.

In the field of fundamental study, this book has included a survey of stateful public key encryption schemes. The idea of the stateful public encryption is to reuse some random parameters in the encryption algorithm by maintaining a state to save the current random variable, which is used to generate the concerned random parameters. The heavy computations like exponentiation operations can be reduced. This book also discussed possible applications of stateful encryption schemes for building up lightweight asymmetric encryption primitives for the IoT (Internet of Things) environment. On the other hand, the widespread use of CAPTCHAs these

days has made them an integral part of the Internet for providing online services, which are intended for humans, with some level of protection against automated abuse. This book gives an overview of research examining a wide range of issues that have been conducted on different types of CAPTCHAs.

In the field of practical application, this book has included the nonintrusive load monitoring algorithms to mine consumer privacy in the smart grid. This book covers the background and advantages of NILM method and the classification of NILM method, depicts the general and specific process of NILM method, and discusses examples of supervised and unsupervised NILM, and finally, examples of applications of NILM method are presented. In the cyber world, anonymous authentication is an important tool for privacy protection. However, users may misbehave under the cover of anonymity. Thus, accountability is crucial in any practical privacy-preserving authentication. This book reviews the concept of anonymous credentials and discusses various accountability mechanisms, discussing as well how recent development of blockchain and quantum computers have influenced the recent research advances in this area. Moreover, the way how anonymous credentials are applied in real-world applications in cryptocurrencies is also discussed. The huge growth of e-shopping has brought convenience to customers and increased revenue to merchants and financial entities. Nowadays, e-shopping has evolved to possess many functions, features, and requirements. However, customer privacy has been mostly ignored. This book introduces a methodology for privacy augmentation design namely “utility, privacy, and then utility again” paradigm, which is suitable for real-world engineering processes that need to adhere to the aforementioned constraints.

In the field of signature, this book introduces the basics of ring signature, including the security model and a simple construction based on discrete logarithm setting, covering also a variant called linkable ring signature that provides linkability in addition to the property of a normal ring signature. This book introduces a commercial application of (linkable) ring signature in blockchain called Ring Confidential Transaction (RingCT), which is the privacy-preserving protocol used in Monero, one of the largest cryptocurrencies in the world. Traditional data signatures are designed to protect signed messages from any changes in data integrity and authenticity verification properties. However, appropriate alteration of the signed message should be allowed for the purposes of privacy protection in scenarios as medical data sharing, outsourced databases, etc. Redactable signatures, a branch of homomorphic signatures for editing, allow any party to delete some sub-message blocks from a signed message and generate a valid signature on the remaining message without any help of the original signer. This book introduces the state-of-the-art redactable signature schemes. In addition, it depicts three integrated solutions, which hopefully offer more insights into this crucial problem.

This book also introduces the pseudonymous signature schemes. The pseudonymous signature schemes aim to provide a strong cryptographic evidence of the integrity of the signed data and origin of the signature, but at the same time have to hide the identity of the signatory. There are two crucial properties that are specific for pseudonymous signatures: ability to recover the real identity of the

signatory in certain circumstances and resilience to Sybil attacks. Despite using a single private key, the signatory can create a (single) unlinkable pseudonym for each domain or sector of activity and generate signatures corresponding to this pseudonym.

Overall, this book represents a solid research contribution to state-of-the-art studies and practical achievements in algorithms, analytics, and applications over cybersecurity, and puts the basis for further efforts in this challenging scientific field that will even more play a leading role in next-generation research. The Editors are confident that this book will significantly contribute towards the challenging field of cybersecurity.

West Lafayette, USA
June 2018

Elisa Bertino
Purdue University

Foreword II

Due to the rapid development of cyber technology in recent years, the protection of computing systems in institutions, organizations, and devices has been magnified against threats and attacks, and strengthened early vulnerable ones. Cybersecurity and privacy events ranging from data leakage to network collapse occur with higher frequency than past years, and these have become the grand challenges in today's society. The ability to perceive, discover, and prevent malicious actions or events within the cyberspace has attracted considerable interest in both academic and industrial communities.

It is important to the individuals, organizations, and human society hinging on understanding and solving fundamental and realistic issues about security and privacy in the cyberspace. These include lightweight cryptographic solutions in resource-constrained environments, privacy protection methods in smart grid monitoring, anonymous credentials and confidential transaction in crypto currency, security in reverse Turing tests design, privacy-preserving data redaction and privacy retrofitting solutions, and pseudonymous signature schemes. The current book, *Advances in Cyber Security: Principles, Techniques, and Applications* comes at the right time with the right purpose, containing herein the description of the following research ideas:

Chapter “[Stateful Public-Key Encryption: A Security Solution for Resource-Constrained Environment](#)” provides an extensive survey of original stateful public key encryption schemes and their extensions. It discusses also the possible applications of stateful encryption schemes for building up lightweight asymmetric encryption primitives for Internet of Things (IoT) environments.

Chapter “[Non-intrusive Load Monitoring Algorithms for Privacy Mining in Smart Grid](#)” introduces the background and advantages of nonintrusive load monitoring (NILM) method, as well as the classification of NILM method. It also depicts the general and specific process of NILM method, and discusses the examples of supervised and unsupervised NILM, and finally, examples of applications of NILM method are presented.

Chapter “[Accountable Anonymous Credentials](#)” reviews the concept of anonymous credentials and discusses various accountability mechanisms, as well as how recent development of blockchain and quantum computers have influenced the recent research advances in this area. Moreover, the way how anonymous credentials are applied in real-world applications in crypto-currencies is also discussed.

Chapter “[CAPTCHA Design and Security Issues](#)” examines and discusses a wide range of issues that have been conducted on different types of CAPTCHAs.

Chapter “[Ring Signature](#)” depicts the basics of ring signature and presents a commercial application of (linkable) ring signature in blockchain, which is the privacy-preserving protocol used in Monero, one of the largest cryptocurrencies in the world.

Chapter “[Data Authentication with Privacy Protection](#)” provides a basic introduction to the state-of-the-art redactable signature schemes, and it mainly considers the redaction control problem of redactable signature schemes in different applications. Moreover, three integrated solutions are depicted, which hopefully offer more insights into this crucial problem.

Chapter “[A Methodology for Retrofitting Privacy and Its Application to e-Shopping Transactions](#)” puts forward a methodology for privacy augmentation design namely “utility, privacy, and then utility again” paradigm, specially suitable for real-world engineering processes that need to adhere to the aforementioned constraints, which gives an e-shopping system with enhanced privacy features, presents a set of “utility-privacy tradeoffs”, and showcases a practical approach implementing the notion of “privacy by design” while maintaining as much compatibility as possible with current infrastructures.

Chapter “[Pseudonymous Signature Schemes](#)” aims to provide a strong cryptographic evidence of integrity of the signed data and origin of the signature, despite having to hide the identity of the signatory.

The editors have assembled an impressive book consisting of eight chapters, written by well-established authors from countries across America, European, Australia, and Asia. Notwithstanding authors come from different disciplines and subfields, their journey are the same: to discover and analyze cybersecurity and to create value for their organizations and society. The chapters are well written and organized by various authors who are active researchers or practical experts in the area related to or in cybersecurity. Advances in cybersecurity will contribute tremendously to the security and privacy protection process and help generate many new research fields and disciplines such as those in multi-functionality, lightweight, and privacy-preserving cryptographic protocol designing. On the other hand, it will stimulate technology innovation and possibly inspire entrepreneurship. In addition, it will have a great impact on Internet, IoT, cloud computing, big data, data mining, and electronic currency.

I would like to thank and congratulate the editors of this book: Kuan-Ching Li, Xiaofeng Chen, and Willy Susilo, for their tireless energy and dedication in putting together this significant volume. In the cyber era, countries, enterprises, and institutions have launched their cybersecurity strategy, and this book aims exactly at essential cybersecurity issues such as multi-functionality, lightweight,

privacy-preserving technologies, and their applications. This book has great potential to provide fundamental security and privacy to individuals, long-lasting value to organizations, and security and sustainability to both academic and industrial communities.

Xi'an, China
June 2018

Jianfeng Ma
Xidian University

Preface

The rapid development of cyber technology has been accompanied with serious security challenges nowadays. Cybersecurity events ranging from data leakage to network collapse happen with frequency higher than past years, and the most famous one is “Snowden event”, that exemplified the world that cybersecurity has a direct consequence on the national security. Currently, cybersecurity has attracted considerable interest in both academic and industrial community, especially techniques of Cloud Computing, IoT, and Big Data that make the distributed networked systems more sophisticated, powerful, easy to use. Nevertheless, security problems may be an Achilles’ heel. Based on these circumstances, one should seek solutions to build secure network and systems which are also more effective, intelligent, adaptive, and high performance for real-world applications.

One of the most problematic elements of cybersecurity is the quickly and constantly evolving nature of security risks and activities. The traditional approach has been targeted to focus most resources on the most crucial system components and protect against the largest known threats, necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Nevertheless, such an approach is insufficient in the current environment.

Based on this methodological vision, this book is organized to provide the description of chapters as follows:

Chapter “[Stateful Public-Key Encryption: A Security Solution for Resource-Constrained Environment](#)”, Lightweight Solutions for Public Key Encryption in Resource-Constrained Environments: A Survey of Stateful Public Key Encryption Schemes, by Joonsang Baek, Willy Susilo, Khaled Salah, Jun Su Ha, Ernesto Damiani, and Ilsun You, considers that stateful public key encryption proposed by Bellare, Kohno, and Shoup (2006) significantly improves the efficiency of encryption portion of ElGamal-like public key encryption schemes. The idea of the stateful public key encryption is to reuse some random parameters in the encryption algorithm by maintaining a state to save the current random variable, which is used to generate the concerned random parameters. This turns out to be highly effective in reducing heavy computations like exponentiation operations in the encryption process. Since its invention, several variants and extensions have been proposed.

This chapter provides an extensive survey of original stateful public key encryption schemes and their extensions. Possible applications of stateful encryption schemes for building up lightweight asymmetric encryption primitives for the IoT (Internet of Things) environment are also discussed.

Chapter “[Non-intrusive Load Monitoring Algorithms for Privacy Mining in Smart Grid](#)”, by Zijian Zhang, Jialing He, Liehuang Zhu, and Kui Ren, moves the attention on nonintrusive load monitoring (NILM) method that is essentially artificial intelligence algorithms for energy conservation and privacy mining through decomposing aggregated meter readings of consumer energy consumption into the individual devices energy consumption. The authors introduce the background and advantages of NILM method and the classification of NILM method, depict the general and specific process of NILM method, and discuss examples of supervised and unsupervised NILM, and finally, examples of applications of NILM method are presented.

Chapter “[Accountable Anonymous Credentials](#)”, by Zuoxia Yu, Man Ho Au, and Rupeng Yang, focuses on the significance of anonymity, which refers to the absence of identifying information associated with an interaction. In the cyber world, anonymous authentication is an important tool for privacy protection. However, users may misbehave under the cover of anonymity. Thus, accountability is crucial in any practical privacy-preserving authentication. In this chapter, authors review the concept of anonymous credentials and discuss various accountability mechanisms, discussing as well how recent development of blockchain and quantum computers have influenced the recent research advances in this area. Moreover, the way how anonymous credentials are applied in real-world applications in cryptocurrencies is also discussed.

Chapter “[CAPTCHA Design and Security Issues](#)”, by Yang-Wai Chow, Willy Susilo, and Pairat Thorncharoensri, moves the attention to the concept of reverse Turing tests, commonly known as CAPTCHAs, for distinguishing between humans and computers has been around for many years. The widespread use of CAPTCHAs these days has made them an integral part of the Internet for providing online services, which are intended for humans, with some level of protection against automated abuse. Since their inception, much research has focused on investigating various issues surrounding the design and security of CAPTCHAs. A fundamental requirement of CAPTCHAs necessitates that they must be designed to be easy for humans but difficult for computers. However, it is well recognized that the tradeoff between usability and security is difficult to balance. In addition, numerous attacks have been developed to defeat CAPTCHAs. In response to this, many different CAPTCHA design variants have been proposed over the years. Despite the fact that CAPTCHAs have been around for more than two decades, the future of CAPTCHAs remains an open question. It is shown in this chapter an overview of research examining a wide range of issues that has been conducted on different types of CAPTCHAs.

Chapter “[Ring Signature](#)”, by Joseph K. Liu, discusses the basics of ring signature, including the security model and a simple construction based on discrete logarithm setting, covering also a variant called linkable ring signature that provides

linkability in addition to the property of a normal ring signature. In this chapter, he presents a commercial application of (linkable) ring signature in blockchain called Ring Confidential Transaction (RingCT), which is the privacy-preserving protocol used in Monero, one of the largest cryptocurrencies in the world.

Chapter “[Data Authentication with Privacy Protection](#)”, Authenticated Data Redaction with Privacy Preserving and Flexible Redaction Control, by Jianghua Liu, Yang Xiang, Wanlei Zhou, Xinyi Huang, and Jinhua Ma, puts emphasis on digital signatures, aimed at protecting a signed message from any alteration with the properties of data integrity and authenticity authentication. However, appropriate alteration of the signed message should be allowed for the purposes of privacy protection in scenarios as medical data sharing, outsourced databases, etc. Redactable signatures, a branch of homomorphic signatures for editing, allow any party to delete some sub-message blocks from a signed message and generate a valid signature on the remaining message without any help of the original signer. This chapter provides a basic introduction to the state-of-the-art redactable signature schemes, and authors mainly consider the redaction control problem of redactable signature schemes in different applications. In addition, it depicts three integrated solutions, which hopefully offer more insights into this crucial problem.

Chapter “[A Methodology for Retrofitting Privacy and Its Application to e-Shopping Transactions](#)”, by Jesus Diaz, Seung Geol Choi, David Arroyo, Angelos D. Keromytis, Francisco B. Rodriguez, and Moti Yung, addressed to the fact that huge growth of e-shopping has brought convenience to customers and increased revenue to merchants and financial entities. In addition, e-shopping has evolved to possess many functions, features, and requirements (e.g., regulatory ones). However, customer privacy has been mostly ignored, and while it is easy to add simple privacy to an existing system, this typically causes loss of functions. What is needed is enhanced privacy on one hand, while retaining the critical functions and features on the other hand. This is a dilemma which typifies the “privacy versus utility” paradigm, especially when it is applied to an established primitive with operational systems, where applying conventional privacy by design principles is not possible and completely altering information flows and system topologies is not an option. This dilemma is becoming more problematic with the advent of regulations such as the European GDPR, which requires companies to provide better privacy guarantees whenever and wherever personal information is involved. In this chapter, authors put forward a methodology for privacy augmentation design namely “utility, privacy, and then utility again” paradigm, specially suitable for real-world engineering processes that need to adhere to the aforementioned constraints, which gives an e-shopping system with enhanced privacy features, presents a set of “utility-privacy tradeoffs”, and showcases a practical approach implementing the notion of “privacy by design” while maintaining as much compatibility as possible with current infrastructures.

Chapter “[Pseudonymous Signature Schemes](#)”, by Przemysław Błażkiewicz, Lucjan Hanzlik, Kamil Kluczniak, Łukasz Krzywiecki, Mirosław Kutylowski, Marcin Słowik, and Marta Wszola, concerns cryptographic schemes enabling to sign digital data in a pseudonymized way. The schemes aim to provide a strong

cryptographic evidence of integrity of the signed data and origin of the signature, but at the same time have to hide the identity of the signatory. There are two crucial properties that are specific for pseudonymous signatures: ability to recover the real identity of the signatory in certain circumstances and resilience to Sybil attacks. Despite using a single private key, the signatory can create a (single) unlinkable pseudonym for each domain or sector of activity and generate signatures corresponding to this pseudonym.

Overall, this book represents a solid research contribution to state-of-the-art studies and practical achievements in algorithms, analytics, and applications over cybersecurity, and puts the basis for further efforts in this challenging scientific field that will even more play a leading role in next-generation research. The Editors are confident that this book will significantly contribute towards the challenging field of cybersecurity.

Taichung, Taiwan
Xi'an, China
Wollongong, Australia

Kuan-Ching Li
Xiaofeng Chen
Willy Susilo

Acknowledgements

First and foremost, we would like to thank and acknowledge the contributors to this book for their support, and the reviewers for their valuable and useful comments and suggestions that sought in improving the earlier outline and presentation of the book.

We extend our deepest thanks to editorial team from Springer Nature for their collaboration, guidance, and most importantly, patience in finalizing this book in highest standards. Additionally, we acknowledge the efforts of the team from Springer Nature's production department for their extensive efforts during the phases of this project and the timely fashion in which the book was produced by.

Finally, it is acknowledged the support in part by the 111 Center of Mobile Internet Security, Xidian University and China 111 project (No. B16037).

Contents

Stateful Public-Key Encryption: A Security Solution for Resource-Constrained Environment	1
Joonsang Baek, Willy Susilo, Khaled Salah, Jun Su Ha, Ernesto Damiani and Ilsun You	
Non-intrusive Load Monitoring Algorithms for Privacy Mining in Smart Grid	23
Zijian Zhang, Jialing He, Liehuang Zhu and Kui Ren	
Accountable Anonymous Credentials	49
Zuoxia Yu, Man Ho Au and Rupeng Yang	
CAPTCHA Design and Security Issues	69
Yang-Wai Chow, Willy Susilo and Pairat Thorncharoensri	
Ring Signature	93
Joseph K. Liu	
Data Authentication with Privacy Protection	115
Jianghua Liu, Yang Xiang, Wanlei Zhou, Xinyi Huang and Jinhua Ma	
A Methodology for Retrofitting Privacy and Its Application to e-Shopping Transactions	143
Jesus Diaz, Seung Geol Choi, David Arroyo, Angelos D. Keromytis, Francisco B. Rodriguez and Moti Yung	
Pseudonymous Signature Schemes	185
Przemysław Błażkiewicz, Lucjan Hanzlik, Kamil Klucznik, Łukasz Krzywiecki, Mirosław Kutylowski, Marcin Słowik and Marta Wszola	