Communications in Computer and Information Science 448

Zbigniew Kotulski Bogdan Księżopolski
Katarzyna Mazur (Eds.)

Cryptography and Security Systems

Third International Conference, CSS 2014
Lublin, Poland, September 22-24, 2014
Proceedings

Springer

Volume Editors

Zbigniew Kotulski
Warsaw University of Technology, Poland
E-mail: zkotulsk@tele.pw.edu.pl

Bogdan Księżopolski
Maria Curie-Skłodowska University in Lublin, Poland
and
Polish-Japanese Institute of Information Technology
Warsaw, Poland
E-mail: bogdan.ksiezopolski@acm.org

Katarzyna Mazur
Maria Curie-Skłodowska University in Lublin, Poland
E-mail: katarzyna.mazur@umcs.pl

ISSN 1865-0929 e-ISSN 1865-0937
ISBN 978-3-662-44892-2 e-ISBN 978-3-662-44893-9
DOI 10.1007/978-3-662-44893-9
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014948498

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Cryptography and security systems are two fields of security research that strongly interact and complement each other. The series of International Conferences on Cryptography and Security Systems (CSS) is a forum for presentation of theoretical and applied research papers, case studies, implementation experiences, as well as work-in-progress results in these two disciplines. The conference especially invites young researchers and PhD students who have an opportunity to share their results with colleagues, invited keynote lecturers, and the Program Committee members actively participating in conference sessions.

The present volume of the *Communications in Computer and Information Science* series contains 17 papers selected from 43 submissions to the Third International Conferences on Cryptography and Security Systems (CSS 2014) held during September 22–24, 2014, in Lublin, Poland. Seven of these papers concern different areas of cryptography, while the remaining ten deal with recent problems of cryptographic protocols.

The "Numerical Semigroups and Bounds on Impossible Differential Attacks on Generalized Feistel Scheme" by Alexander Toktarev and Maria Pudovkina opens the cryptographic section of this volume. The authors investigate a class of ciphers described as a generalized Feistel scheme. Using the graph theory and the number theory, they provide upper and lower bounds for the maximum number of rounds when an impossible differential technique is applicable. These bounds do not depend on a type of Feistel scheme and a number of nonlinear functions or blocks in the register. In the next paper, entitled "Encrypting Huffman-Encoded Data by Substituting Pairs of Code Words Without Changing the Bit Count of a Pair," Marek Parfieniuk and Piotr Jankowski present a method of combining the Huffman coding with encryption. The encryption is based on replacing the codewords, pair-by-pair, in such a way that the sums of the codeword lengths of an original pair and its substitute are equal. The method preserves the structures and lengths of the bitstreams, which is an advantage if such a bit stream is embedded in a higher-level data container, like a multimedia file. "On Multivariate Cryptosystems Based on Polynomially Compressed Maps with Invertible Decomposition" by Vasyl Ustimenko and Urszula Romańczuk-Polubiec is the third paper in the volume. It presents the concept and the explicit construction of the family of polynomially compressed multivariate maps by relations of degree k with invertible decomposition. Such a construction is based on the edge-transitive family of graphs and uses the equations of a connected component of the graph. The approach introduced by the authors allows one to obtain an effective multivariate public key cryptosystem. An extensively studied problem of pseudo-random number generation is the subject of "Statistical Analysis of the Chaos-Driven Elliptic Curve Pseudo-random Number Generators" by Omar Reyad and Zbigniew Kotulski. The authors pro-

pose a method improvement of the well-known Elliptic Curve Pseudo-Random Number Generator by combining it with a Chaotic Pseudo-Random Number Generator. The resultant algorithm has better statistical properties and is computationally more effective than separate component algorithms. Another recent extensively studied problem, which is identity-based cryptography, is discussed in "Identity-Based Cryptography in Credit Card Payments" by Kimmo Halunen and Mirko Sailio. The authors propose a method of how to apply identity-based cryptography to credit card payments, to reduce the possibility of credit card fraud that is prevalent on the Internet. Since the method requires some changes to the functionality of the credit cards standards, it is not an immediate remedy, but rather a recommendation for the future. And finally, the papers concluding the cryptographic track of this volume are devoted to two different applications of graphs. The paper "On a Cipher Based on Pseudo-random Walks on Graphs" by Wit Foryś, Piotr Oprocha, and Łukasz Jęda presents a cryptosystem that uses wandering on a graph in the process of encryption and also exploits some ideas of dynamical systems (symbolic dynamics), while the paper "On LDPC Codes Based on Families of Expanding Graphs of Increasing Girth Without Edge-Transitive Automorphism Groups" by Monika Polak and Vasyl Ustimenko introduces new examples of low-density parity check codes connected with new families of regular graphs of bounded degree and increasing girth.

The second section of this volume represents cryptographic protocols, which dominated the submissions at CSS 2014. It covers both theoretical models of cryptographic protocols, e.g., secure secret sharing schemes or key establishment protocols and protocols in practically used networks (peer-to-peer, wireless sensor networks, real-time transmissions), and Web services, e.g., electronic payments or Bitcoin. Thus, the first paper in this section, prepared by Jakub Muszyński, Sebastien Sébastien, Juan Luis Jiménez Laredo, and Pascal Bouvry, entitled "Analysis of the Data Flow in the Newscast Protocol for Possible Vulnerabilities," deals with a simple, peer-to-peer data exchange protocol. The authors analyze the robustness of the data flow within the Newscast model against a set of vulnerabilities that have not been taken into account in previous analysis. They demonstrate the attack based on a cache content corruption that is able to defeat the protocol by breaking the network connectivity and perform experiments using a framework that implements both the protocol and a corruption model. The next paper, "Efficient Verifiable Multi-secret Sharing Based on Y.C.H Scheme," by Appala Naidu Tentu and Appa Rao Allam, presents an efficient verifiable multi-secret sharing protocol employing an identity based signature scheme, that uses the identities of the participants in this scheme. This scheme does not require the pre-secure communication between dealer and participants or the exponential functions for the verification, and efficiently resists the dealer/participant(s)' cheating behavior. A new lightweight authentication protocol for RFID systems based on non-linear feedback shift register sequences generated by the position digit algebra function is proposed in the paper of Ferucio Laurenţiu Ţiplea entitled "A Lightweight Authentication Protocol for RFID." The applied function uses only *radix r* additions, which makes the protocol com-

putationally efficient. Aditionally, random sequences generated by this function have a large average period, which results in good privacy and security properties of the protocol. The following "Long-Term Secure Two-Round Group Key Establishment from Pairings," authored by Kashi Neupane, deals with the concept of the long-term security of a protocol, which means resistance against attacks even if later, after completion of the protocol, some security assumptions become invalid. It proposes an authenticated two-round group key establishment protocol, which remains secure if a Computational Bilinear Diffie-Hellman problem is hard, or a server, that shares a symmetric key with each user, is uncorrupted. The paper "Optimizing SHA256 in Bitcoin Mining," written by Nicolas Courtois, Rahuk Naik, and Marek Grajek, revisits the cryptographic process that allows one to make money by producing new bitcoins. It reformulates this problem as a specific sort of constrained input and small output (CISO) hashing problem and reduces it to a pure block cipher problem. The proposed optimizations enable bitcoin miners to save countless millions of dollars per year in electricity bills. Another paper dealing with electronic money is "Protocol for Detection of Counterfeit Transactions in Electronic Currency Exchange" authored by Marek Ogiela and Piotr Sułkowski. The authors present an improvement to Chaum's anonymous currency exchange protocol, and show its vulnerability to serious fraud by both the client and the seller after an electronic coin is spent at least twice. They also propose an improved system based on its original offline version. The next paper by Imed El Fray, Tomasz Hyla, Mirosław Kurkowski, Witold Maćków, and Jerzy Pejaś, "Practical Authentication Protocols for Protecting and Sharing Sensitive Information on Mobile Devices," presents an architecture of the MobInfoSec system for sharing documents with sensitive information using fine-grained access rules described by general access structures. They allow one to establish secure communication channels between different system components, which is exploited in the proposed conference protocol with key transport and key establishment mechanisms. In the paper "Secure Multihop Key Establishment Protocols for Wireless Sensor Networks," Ismail Mansour, Gérard Chalhoub, and Pascal Lafourcade propose four secure multihop key establishment protocols based on elliptic curve cryptography (ECC). For each protocol, they make a formal security proof using the automatic tool Scyther, and, in order to evaluate their performances, present results of implementation on testbeds using TelosB motes and TinyOS. The discussion of protocol' modelling languages is the subject of the paper "Comparison and Assessment of Security Modeling Approaches in Terms of the QoP-ML" by Katarzyna Mazur and Bogdan Ksiezopolski. The authors focus on their capabilities to model relevant information during different phases of the security analysis of protocols. To assess and compare miscellaneous modelling systems, they use a systematic methodology to point out their promiscuous aspects in the context of the QoP-ML language. The last paper in the section on cryptographic protocols is "Context-Aware Secure Routing Protocol for Real-Time Services" by Grzegorz Oryńczak and Zbigniew Kotulski. It proposes a context-aware secure routing protocol suitable for real-time services. The introduced framework systemizes the roles of all actors in establishing optimally

secure network connections for such services. Apart from selecting an optimal route, the framework also supports an additional optimization techniques (e.g., fast packet retransmission, redundant routing etc.), and implements necessary security mechanisms, including both standard hard-security mechanisms, such as private key encryption and soft security techniques, e.g., trust and reputation management for detecting and blocking malicious nodes.

To conclude this short overview of the papers presented at the Third International Conferences on Cryptography and Security Systems (CSS 2014) and published in volume 448 of Springer's *Communications in Computer and Information Science* series, we observe the wide spectrum of research topics covered by papers submitted to the conference, as well as several common directions unifying the submissions such as application of modern cryptography (elliptic curves, multinomial cryptography, bilinear pairing, and identity-based cryptography) and the strong effort to make theoretical models applicable. We hope that the material presented in this volume will contribute toward fruitful future research.

September 2014

Zbigniew Kotulski
Bogdan Księżopolski

Organization

Third International Conference on Cryptography and Security Systems (CSS 2014) was organized by the Faculty of Mathematics, Physics and Computer Science, Maria Sklodowska-Curie University of Lublin, Poland, and the Faculty of Electronics and Information Technology, Warsaw University of Technology, Poland.

Conference Chair

Zbigniew Kotulski	Warsaw University of Technology, Poland
Bogdan Księżopolski	Maria Sklodowska-Curie University and Polish-Japanese Institute of Information Technology, Poland

Technical Volume Editor

Katarzyna Mazur	Maria Sklodowska-Curie University, Poland

Organizing Committee

Bogdan Księżopolski - Chair	Maria Sklodowska-Curie University and Polish-Japanese Institute of Information Technology, Poland
Zbigniew Kotulski	Warsaw University of Technology, Poland
Damian Rusinek	Maria Sklodowska-Curie University, Poland
Katarzyna Mazur	Maria Sklodowska-Curie University, Poland
Urszula Romańczuk-Polubiec	Maria Sklodowska-Curie University, Poland

Program Committee

Pascal Bouvry	University of Luxembourg, Luxembourg
Nicolas T. Courtois	University College London, UK
Stefan Dziembowski	University of Warsaw, Poland, and University of Rome, Italy
Krzysztof Gaj	George Mason University, USA
Piotr Gajewski	Military University of Technology, Poland
Janusz Górski	Gdańsk University of Technology, Poland
Jaime Gutierrez	University of Cantabria, Spain

Table of Contents