

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbruecken, Germany*

Ari Juels Christof Paar (Eds.)

# RFID Security and Privacy

7th International Workshop, RFIDSec 2011  
Amherst, MA, USA, June 26-28, 2011  
Revised Selected Papers

## Volume Editors

Ari Juels  
RSA Laboratories/EMC  
11 Cambridge Center  
Cambridge, MA 02142, USA  
E-mail: [ajuels@rsa.com](mailto:ajuels@rsa.com)

Christof Paar  
Ruhr University Bochum  
Horst Görtz Institute for IT-Security  
44780 Bochum, Germany  
E-mail: [christof.paar@rub.de](mailto:christof.paar@rub.de)

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-25285-3 e-ISBN 978-3-642-25286-0  
DOI 10.1007/978-3-642-25286-0  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011944230

CR Subject Classification (1998): C.2, K.6.5, D.4.6, E.3, H.4, J.1

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

*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](http://www.springer.com))

# Preface

RFIDSec 2011, the 7th workshop on RFID Security and Privacy, was held in Amherst and Northampton, Massachusetts, USA, during June 26–28, 2011.

The workshop attracted 21 submissions, of which the Program Committee selected 12 for publication in the workshop proceedings. The accepted papers dealt with the topics of on-tag cryptography, attacks, security through physics, and protocol-level security. The Program Committee included 26 subject-matter experts from 14 countries, and represented academia, industry, and government.

An excellent array of invited talks complemented the paper sessions. Adi Shamir of the Weizmann Institute of Science (Israel) gave the RFIDSec 2011 keynote talk, “Minimalism in Cryptography,” an overview of his recent results in the theory of cipher design. Srdjan Capkun highlighted the limitations of logical-layer privacy protections in his invited talk, “On Physical-Layer Identification of RFID Tags.” At the workshop banquet, Collin Mulliner gave an update on NFC security (“Hacking Your NFC Phone and Service: The Good News and the Bad News”). Offering an industry perspective on the work of RFID (and other) standards bodies, Ravi Pappu informed and regaled workshop attendees with a talk entitled “The Making of Camels.”

For the first time, RFIDSec offered tutorials in highly relevant areas. The four tutorials preceding the workshop were: Matt Reynolds and Ravi Pappu taught “The Physics of RFID,” David Oswald and Timo Kasper, “Hands-on Side Channel Attacks Against Smart Cards and Other Tokens,” Shane Clark, Ben Ransford, Mastooreh Salajegheh, and Hong Zhang, “Hands-on Programming of Batteryless, RFID-Scale Computers with Sensors,” and Ari Juels, “Introduction to RFID Security and Privacy.”

We wish to thank the generous sponsors of RFIDSec 2011: Microsoft Research, Mocana, Cryptography Research, the National Science Foundation, the Institute for Information Infrastructure Protection (I3P), the *RFID Journal*, DIFRwear, and UMass Amherst. Deep thanks are also due to Kevin Fu for his outstanding organizational efforts as General Chair, and to Wendy Cooper for her tireless support as Conference Coordinator.

August 2011

Ari Juels  
Christof Paar



## External Reviewers

T. Akishita	P. Peris-Lopez	M. Valis
M.A. Bingol	B. Martin	M.G. Vasco
X. Carpent	A. Mirhoseini	J. Voris
T. Halevi	J.M. Seguí	A. Vosoughi
Y. Hanatani	J. Takahashi	Y. Oren
C.H. Kim	R. Trujillo-Rasúa	

## RFIDSec 2011 Sponsors

Cryptography Research	Mocana
DIFRwear	National Science Foundation
I3P	RFID Journal
Microsoft Research	UMass Amherst

## RFIDSec Steering Committee

Manfred Aigner	TU Graz, Austria
Gildas Avoine (Chair)	UCL, Louvain-la-Neuve, Belgium
Kevin Fu	UMass Amherst, USA
Yingjiu Li	Singapore Management University, Singapore
Christof Paar	Ruhr University Bochum, Germany
Bart Preneel	KU Leuven, Belgium
Vincent Rijmen	TU Graz, Austria; KU Leuven, Belgium

# Table of Contents

KLEIN: A New Family of Lightweight Block Ciphers .....	1
<i>Zheng Gong, Svetla Nikova, and Yee Wei Law</i>	
The Hummingbird-2 Lightweight Authenticated Encryption Algorithm.....	19
<i>Daniel Engels, Markku-Juhani O. Saarinen, Peter Schweitzer, and Eric M. Smith</i>	
Elliptic Curve Cryptography on the WISP UHF RFID Tag.....	32
<i>Christian Pendl, Markus Pelnar, and Michael Hutter</i>	
Exploring the Feasibility of Low Cost Fault Injection Attacks on Sub-threshold Devices through an Example of a 65nm AES Implementation.....	48
<i>Alessandro Barenghi, Cédric Hocquet, David Bol, François-Xavier Standaert, Francesco Regazzoni, and Israel Koren</i>	
Side-Channel Analysis of Cryptographic RFIDs with Analog Demodulation .....	61
<i>Timo Kasper, David Oswald, and Christof Paar</i>	
A Novel RFID Distance Bounding Protocol Based on Physically Unclonable Functions.....	78
<i>Süleyman Kardaş, Mehmet Sabir Kiraz, Muhammed Ali Bingöl, and Hüseyin Demirci</i>	
Security Analysis of Two Distance-Bounding Protocols .....	94
<i>Mohammad Reza Sohizadeh Abyaneh</i>	
An Automatic, Time-Based, Secure Pairing Protocol for Passive RFID .....	108
<i>George T. Amariuca, Clifford Bergman, and Yong Guan</i>	
BUPLE: Securing Passive RFID Communication through Physical Layer Enhancements .....	127
<i>Qi Chai and Guang Gong</i>	
A Scalable RFID Authentication Protocol Supporting Ownership Transfer and Controlled Delegation.....	147
<i>Albert Fernández-Mir, Rolando Trujillo-Rasua, Jordi Castellà-Roca, and Josep Domingo-Ferrer</i>	

ROTIV: RFID Ownership Transfer with Issuer Verification . . . . .	163
<i>Kaoutar Elkhiyaoui, Erik-Oliver Blass, and Refik Molva</i>	
Hierarchical ECC-Based RFID Authentication Protocol . . . . .	183
<i>Lejla Batina, Stefaan Seys, Dave Singelée, and Ingrid Verbauwhede</i>	
<b>Author Index</b> . . . . .	203