

# Contents

## PUFs and Applications

Security Evaluation and Enhancement of Bistable Ring PUFs .....	3
<i>Xiaolin Xu, Ulrich Rührmair, Daniel E. Holcomb, and Wayne Burleson</i>	
On the Scaling of Machine Learning Attacks on PUFs with Application to Noise Bifurcation .....	17
<i>Johannes Tobisch and Georg T. Becker</i>	
ReSC: RFID-Enabled Supply Chain Management and Traceability for Network Devices .....	32
<i>Kun Yang, Domenic Forte, and Mark Tehranipoor</i>	

## Side-Channels and Countermeasures

Side-Channel Assisted Modeling Attacks on Feed-Forward Arbiter PUFs Using Silicon Data .....	53
<i>Raghavan Kumar and Wayne Burleson</i>	
Sharing is Caring—On the Protection of Arithmetic Logic Units against Passive Physical Attacks .....	68
<i>Hannes Gross</i>	

## RFID System Attacks

Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited .....	87
<i>José Vila and Ricardo J. Rodríguez</i>	
Algebraic Cryptanalysis and RFID Authentication .....	104
<i>Carlos Cid, Loic Ferreira, Gordon Procter, and Matt J.B. Robshaw</i>	
An RFID Skimming Gate Using Higher Harmonics .....	122
<i>René Habraken, Peter Dolron, Erik Poll, and Joeri de Ruiter</i>	

## Efficient Implementations

Efficient E-cash with Attributes on MULTOS Smartcards .....	141
<i>Gesine Hinterwälder, Felix Riek, and Christof Paar</i>	

Efficient and Secure Delegation of Group Exponentiation to a Single  
Server ..... 156  
    *Bren Cavallo, Giovanni Di Crescenzo, Delaram Kahrobaei,*  
    *and Vladimir Shpilrain*

**Author Index** ..... 175

Radio Frequency Identification

11th International Workshop, RFIDsec 2015, New York,

NY, USA, June 23-24, 2015, Revised Selected Papers

Mangard, S.; Schaumont, P. (Eds.)

2015, X, 175 p. 57 illus., Softcover

ISBN: 978-3-319-24836-3