

Table of Contents

Invited Paper

Sweet Dreams and Nightmares: Security in the Internet of Things	1
<i>Timo Kasper, David Oswald, and Christof Paar</i>	

Cryptography and Cryptanalysis

A Security Analysis of Key Expansion Functions Using Pseudorandom Permutations	10
<i>Ju-Sung Kang, Nayoung Kim, Wangho Ju, and Ok-Yeon Yi</i>	

Towards More Practical Time-Driven Cache Attacks	24
<i>Raphael Spreitzer and Benoît Gérard</i>	

Orthogonal Direct Sum Masking: A Smartcard Friendly Computation Paradigm in a Code, with Builtin Protection against Side-Channel and Fault Attacks	40
<i>Julien Bringer, Claude Carlet, Hervé Chabanne, Sylvain Guilley, and Houssein Maghrebi</i>	

Smart Cards and Embedded Devices

New Countermeasures against Fault and Software Type Confusion Attacks on Java Cards	57
<i>Guillaume Barbu and Christophe Giraud</i>	

A Pre-processing Composition for Secret Key Recovery on Android Smartphone	76
<i>Yuto Nakano, Youssef Souissi, Robert Nguyen, Laurent Sauvage, Jean-Luc Danger, Sylvain Guilley, Shinsaku Kiyomoto, and Yutaka Miyake</i>	

Privacy

Usable Privacy for Mobile Sensing Applications	92
<i>Delphine Christin, Franziska Engelmann, and Matthias Hollick</i>	

A Secure Genetic Algorithm for the Subset Cover Problem and Its Application to Privacy Protection	108
<i>Dan Bogdanov, Keita Emura, Roman Jagomägis, Akira Kanaoka, Shin'ichiro Matsuo, and Jan Willemson</i>	

End-to-End Secure and Privacy Preserving Mobile Chat Application ... 124
Raja Naeem Akram and Ryan K.L. Ko

Short Papers

S-box, SET, Match: A Toolbox for S-box Analysis 140
Stjepan Picek, Lejla Batina, Domagoj Jakobović, Barış Ege, and Marin Golub

Policy-Based Access Control for Body Sensor Networks 150
Charalampos Maniavas, Konstantinos Fysarakis, Konstantinos Rantos, Konstantinos Kagiambakis, and Ioannis Papaefstathiou

Personal Identification in the Web Using Electronic Identity Cards and a Personal Identity Provider 160
André Zúquete, Hélder Gomes, and Cláudio Teixeira

CAN Bus Risk Analysis Revisit 170
Hafizah Mansor, Konstantinos Markantonakis, and Keith Mayes

AU2EU: Privacy-Preserving Matching of DNA Sequences 180
Tanya Ignatenko and Milan Petković

Early DDoS Detection Based on Data Mining Techniques 190
Konstantinos Xylogiannopoulos, Panagiotis Karampelas, and Reda Alhajj

Author Index 201