

Contents

Bitcoin and Payment

Authenticated Key Exchange over Bitcoin	3
<i>Patrick McCorry, Siamak F. Shahandashti, Dylan Clarke, and Feng Hao</i>	
Tap-Tap and Pay (TTP): Preventing the Mafia Attack in NFC Payment.	21
<i>Maryam Mehrnezhad, Feng Hao, and Siamak F. Shahandashti</i>	

Protocol and API

Robust Authenticated Key Exchange Using Passwords and Identity-Based Signatures	43
<i>Jung Yeon Hwang, Seung-Hyun Kim, Daeseon Choi, Seung-Hun Jin, and Boyeon Song</i>	
Non-repudiation Services for the MMS Protocol of IEC 61850.	70
<i>Karl Christoph Ruland and Jochen Sassmannshausen</i>	
Analysis of the PKCS#11 API Using the Maude-NPA Tool.	86
<i>Antonio González-Burgueño, Sonia Santiago, Santiago Escobar, Catherine Meadows, and José Meseguer</i>	

Analysis on Cryptographic Algorithm

How to Manipulate Curve Standards: A White Paper for the Black Hat http://bada55.cr.yp.to	109
<i>Daniel J. Bernstein, Tung Chou, Chitchanok Chuengsatiansup, Andreas Hülsing, Eran Lambooj, Tanja Lange, Ruben Niederhagen, and Christine van Vredendaal</i>	
Security of the SM2 Signature Scheme Against Generalized Key Substitution Attacks.	140
<i>Zhenfeng Zhang, Kang Yang, Jiang Zhang, and Cheng Chen</i>	
Side Channel Cryptanalysis of Streebog.	154
<i>Gautham Sekar</i>	

Privacy

Improving Air Interface User Privacy in Mobile Telephony	165
<i>Mohammed Shafiul Alam Khan and Chris J. Mitchell</i>	

Generating Unlinkable IPv6 Addresses	185
<i>Mwawi Nyirenda Kayuni, Mohammed Shafiul Alam Khan, Wanpeng Li, Chris J. Mitchell, and Po-Wah Yau</i>	
Trust and Formal Analysis	
A Practical Trust Framework: Assurance Levels Repackaged Through Analysis of Business Scenarios and Related Risks.	203
<i>Masatoshi Hokino, Yuri Fujiki, Sakura Onda, Takeaki Kaneko, Natsuhiko Sakimura, and Hiroyuki Sato</i>	
First Results of a Formal Analysis of the Network Time Security Specification.	218
<i>Kristof Teichel, Dieter Sibold, and Stefan Milius</i>	
Formal Support for Standardizing Protocols with State.	246
<i>Joshua D. Guttman, Moses D. Liskov, John D. Ramsdell, and Paul D. Rowe</i>	
Author Index	267

Security Standardisation Research

Second International Conference, SSR 2015, Tokyo,

Japan, December 15-16, 2015, Proceedings

Chen, L.; Matsuo, S. (Eds.)

2015, X, 267 p. 41 illus. in color., Softcover

ISBN: 978-3-319-27151-4