## Contents

### Invited Contribution

Quantitative Approaches to the Protection of Private Information: State of the Art and Some Open Challenges .......................... 3  
*Catuscia Palamidessi*

### Information Flow and Security Types

IFC Inside: Retrofitting Languages with Dynamic Information Flow Control ................................................................. 11  
*Stefan Heule, Deian Stefan, Edward Z. Yang, John C. Mitchell, and Alejandro Russo*

Very Static Enforcement of Dynamic Policies ................................................. 32  
*Bart van Delft, Sebastian Hunt, and David Sands*

The Foundational Cryptography Framework ............................................. 53  
*Adam Petcher and Greg Morrisett*

On the Flow of Data, Information, and Time .................................... 73  
*Martín Abadi and Michael Isard*

### Risk Assessment and Security Policies

Pareto Efficient Solutions of Attack-Defence Trees ......................... 95  
*Zaruhi Aslanyan and Flemming Nielson*

Analysis of XACML Policies with SMT ........................................ 115  
*Fatih Turkmen, Jerry den Hartog, Silvio Ranise, and Nicola Zannone*

### Protocols

Automatically Checking Commitment Protocols in ProVerif without False Attacks ................................................................. 137  
*Tom Chothia, Ben Smyth, and Chris Staite*

Generalizing Multi-party Contract Signing .................................... 156  
*Sjouke Mauw and Saša Radomirović*

Leakiness is Decidable for Well-Founded Protocols .......................... 176  
*Sibylle Pröschle*
Abstractions for Security Protocol Verification .......................... 196
   Binh Thanh Nguyen and Christoph Sprenger

Hardware and Physical Security

Automated Backward Analysis of PKCS#11 v2.20 .......................... 219
   Robert Künemann

A Safe Update Mechanism for Smart Cards .............................. 239
   Kristian Beilke and Volker Roth

Discrete vs. Dense Times in the Analysis of Cyber-Physical Security Protocols ................................................. 259
   Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov, and Carolyn Talcott

   Vincent Cheval and Véronique Cortier

Privacy and Voting

Type-Based Verification of Electronic Voting Protocols .................. 303
   Véronique Cortier, Fabienne Eigner, Steve Kremer, Matteo Maffei, and Cyrille Wiedling

Composing Security Protocols: From Confidentiality to Privacy .......... 324
   Myrto Arapinis, Vincent Cheval, and Stéphanie Delaune

PriCL: Creating a Precedent, a Framework for Reasoning about Privacy Case Law ................................................................. 344
   Michael Backes, Fabian Bendun, Jörg Hoffmann, and Ninja Marnau

Author Index ........................................................................... 365