

# Contents

## Information Flow

|                                                                                                  |    |
|--------------------------------------------------------------------------------------------------|----|
| Faceted Dynamic Information Flow via Control and Data Monads . . . . .                           | 3  |
| <i>Thomas Schmitz, Dustin Rhodes, Thomas H. Austin, Kenneth Knowles,<br/>and Cormac Flanagan</i> |    |
| Asymmetric Secure Multi-execution with Declassification . . . . .                                | 24 |
| <i>Iulia Boloşteanu and Deepak Garg</i>                                                          |    |
| A Taxonomy of Information Flow Monitors . . . . .                                                | 46 |
| <i>Nataliia Bielova and Tamara Rezk</i>                                                          |    |
| On Improvements of Low-Deterministic Security . . . . .                                          | 68 |
| <i>Joachim Breitner, Jürgen Graf, Martin Hecker, Martin Mohr,<br/>and Gregor Snelting</i>        |    |
| Tool Demonstration: JOANA . . . . .                                                              | 89 |
| <i>Jürgen Graf, Martin Hecker, Martin Mohr, and Gregor Snelting</i>                              |    |

## Models and Applications

|                                                                                                             |     |
|-------------------------------------------------------------------------------------------------------------|-----|
| Towards Fully Automatic Logic-Based Information Flow Analysis:<br>An Electronic-Voting Case Study . . . . . | 97  |
| <i>Quoc Huy Do, Eduard Kamburjan, and Nathan Wasser</i>                                                     |     |
| Towards a Comprehensive Model of Isolation for Mitigating<br>Illicit Channels . . . . .                     | 116 |
| <i>Kevin Falzon and Eric Bodden</i>                                                                         |     |
| Correct Audit Logging: Theory and Practice. . . . .                                                         | 139 |
| <i>Sepehr Amir-Mohammadian, Stephen Chong, and Christian Skalka</i>                                         |     |
| The Value of Attack-Defence Diagrams . . . . .                                                              | 163 |
| <i>Holger Hermanns, Julia Krämer, Jan Krčál, and Mariëlle Stoelinga</i>                                     |     |

## Protocols

|                                                                 |     |
|-----------------------------------------------------------------|-----|
| Composing Protocols with Randomized Actions . . . . .           | 189 |
| <i>Matthew S. Bauer, Rohit Chadha, and Mahesh Viswanathan</i>   |     |
| Bounding the Number of Agents, for Equivalence Too . . . . .    | 211 |
| <i>Véronique Cortier, Antoine Dallon, and Stéphanie Delaune</i> |     |

AIF- $\omega$ : Set-Based Protocol Abstraction with Countable Families . . . . . 233  
    *Sebastian Mödersheim and Alessandro Bruni*

Computational Soundness Results for Stateful Applied  $\pi$  Calculus . . . . . 254  
    *Jianxiong Shao, Yu Qin, and Dengguo Feng*

**Author Index** . . . . . 277