Preface

This volume presents the set of papers accompanying some of the lectures of the 10th International School on Formal Methods for the Design of Computer, Communication and Software Systems (SFM).

This series of schools addresses the use of formal methods in computer science as a prominent approach to the rigorous design of the above mentioned systems. The main aim of the SFM series is to offer a good spectrum of current research in foundations as well as applications of formal methods, which can be of help for graduate students and young researchers who intend to approach the field.

SFM 2010 was devoted to formal methods for quantitative aspects of programming languages and covered several topics including probabilistic and timed models, model checking, static analysis, quantum computing, real-time and embedded systems, and security.

This volume comprises four articles. The paper by Di Pierro, Hankin, and Wiklicky investigates the relation between the operational semantics of probabilistic programming languages and discrete-time Markov chains and presents a framework for probabilistic program analysis inspired by classical abstract interpretation. Broadbent, Fitzsimons, and Kashefi review the mathematical model underlying measurement-based quantum computation, a novel approach to quantum computation where measurement is the main driving force of computation instead of the unitary operations of the more traditional quantum circuit model. The paper by Malacaria and Heusser illustrates the information-theoretical basis of quantitative information flow by showing the relationship between lattices, partitions, and information-theoretical concepts, as well as their applicability to quantify leakage of confidential information in programs. Finally, Wolter and Reinecke discuss the tradeoff between performance and security by formulating metrics that explicitly express the tradeoff and by showing how to find system parameters that optimize those metrics.

We believe that this book offers a useful view of what has been done and what is going on worldwide in the field of formal methods for quantitative aspects of programming languages. We wish to thank all the speakers and all the participants for a lively and fruitful school. We also wish to thank the entire staff of the University Residential Center of Bertinoro for the organizational and administrative support.

June 2010

Alessandro Aldini
Marco Bernardo
Alessandra Di Pierro
Herbert Wiklicky

Table of Contents

Probabilistic Semantics and Program Analysis

Alessandra Di Pierro, Chris Hankin, Herbert Wiklicky

Measurement-based and Universal Blind Quantum Computation

Anne Broadbent, Joseph Fitzsimons, Elham Kashefi

Information Theory and Security: Quantitative Information Flow

Pasquale Malacaria, Jonathan Heusser

Performance and Security Tradeoff

Katinka Wolter, Philipp Reinecke

Author Index