Research output

Experiments in information flow analysis

Program algebra for quantitative information flow

An axiomatization of information flow measures

Abstract Hidden Markov Models: a monadic account of quantitative information flow

Generalised differential privacy for text document processing

Proving that programs are differentially private

Categorical information flow

Preface

Schedulers and finishers: on generating and filtering the behaviours of an event structure

A new proof rule for almost-sure termination
An algebraic approach for reasoning about information flow

Conditioning in probabilistic programming

Preface

Processing text for privacy: an information flow perspective

Privacy in elections: How small is "small"?

Algebra for quantitative information flow

Formal analysis of the information leakage of the DC-nets and crowds anonymity protocols

Reasoning about distributed secrets

Probabilistic rely-guarantee calculus

Axioms for information leakage

Program refinement, perfect secrecy and information flow
Schedulers and finishers: On generating the behaviours of an event structure

Conditioning in Probabilistic Programming

Abstract hidden Markov models: a monadic account of quantitative information flow

Hidden-Markov program algebra with iteration


Additive and multiplicative notions of leakage, and their capacities

Hopscotch - reaching the target hop by hop

Operational versus weakest pre-expectation semantics for the probabilistic guarded command language

Abstractions of non-interference security: Probabilistic versus possibilistic

Abstract channels and their robust information-leakage ordering

Towards a formal analysis of information leakage for signature attacks in preferential elections
An event structure model for probabilistic concurrent Kleene algebra

Prinsys - On a quest for probabilistic loop invariants

Probabilistic concurrent Kleene algebra

Statistical model checking of wireless mesh routing protocols

Preface: Special issue QFM 2009

A Kantorovich-monadic powerdomain for information hiding, with probability and nondeterminism

A process algebra for wireless mesh networks

A rigorous analysis of AODV and its variants

Automated analysis of AODV using UPPAAL

Operational versus weakest precondition semantics for the probabilistic guarded command language

Compositional refinement in agent-based security protocols
Model exploration and analysis for quantitative safety refinement in probabilistic B

Continual and explicit comparison to promote proactive facilitation during second computer language learning

On probabilistic Kleene algebras, automata and simulations

Preface

Towards an algebra of routing tables

An expectation transformer approach to predicate abstraction and data independence for probabilistic programs

Compositional closure for Bayes risk in probabilistic noninterference

Linear-invariant generation for probabilistic programs: Automated support for proof-based methods

The Thousand-and-one cryptographers

YAGA: automated analysis of quantitative safety specifications in probabilistic B

Graphical modelling for simulation and formal analysis of wireless network protocols

Security, probability and nearly fair coins in the cryptographers’ café
Sums and lovers: Case studies in security, compositionality and refinement

The secret art of computer programming

Using probabilistic Kleene algebra pKA for protocol verification

CaVi - Simulation and model checking for wireless sensor networks

Proofs and refutations for probabilistic refinement

Results on the quantitative μ-calculus qμ

Automating refinement checking in probabilistic system design

Formal techniques for the analysis of wireless networks

A Novel Stochastic Game Via the Quantitative μ-calculus

Developing and reasoning about probabilistic programs in pGCL

Programming-logic analysis of fault tolerance: expected performance of self-stabilisation
Probabilistic models for the guarded command language

Unifying wp and wlp

Probabilistic Predicate Transformers

Refinement-oriented probability for CSP

Software, who needs it?

A question of identity

Finitely generated non-Hopf modules

Enumerating finite groups