Computer Science : Data Structures and Information Theory

Alvim, M.S., Chatzikokolakis, K., McIver, A., Morgan, C., Palamidessi, C., Smith, G., Universidade Federal de Minas Gerais, Belo Horizonte, Brazil

# The Science of Quantitative Information Flow

- **Computer systems that process sensitive information should preserve that information's confidentiality, but our current cyber-infrastructure is failing to achieve this goal: reports of massive-scale information disclosures are distressingly frequent**
- **Written by an international team of six experts, with diverse research backgrounds, whose work was recognized with the NSA's Best Scientific Cybersecurity Paper Award in 2015**
- **Unified, self-contained, and comprehensive presentation, with numerous exercises, suitable for students and researchers**

This book presents a comprehensive mathematical theory that explains precisely what information flow is, how it can be assessed quantitatively – so bringing precise meaning to the intuition that certain information leaks are small enough to be tolerated – and how systems can be constructed that achieve rigorous, quantitative information-flow guarantees in those terms. It addresses the fundamental challenge that functional and practical requirements frequently conflict with the goal of preserving confidentiality, making perfect security unattainable. Topics include: a systematic presentation of how unwanted information flow, i.e., "leaks", can be quantified in operationally significant ways and then bounded, both with respect to estimated benefit for an attacking adversary and by comparisons between alternative implementations; a detailed study of capacity, refinement, and Dalenius leakage, supporting robust leakage assessments; a unification of information-theoretic channels and information-leaking sequential programs within the same framework; and a collection of case studies, showing how the theory can be applied to interesting realistic scenarios.

Springer

1st edition

Due 2020-08-08
1st ed. 2020, Approx. 280 p.

Printed book
Hardcover

Printed book
Hardcover
ISBN 978-3-319-96129-3
Ca. $ 69,99

Planned

Discount group
Professional Books (2)

Product category
Graduate/advanced undergraduate textbook

Series
Information Security and Cryptography

Order online at springer.com/booksellers
**Springer Nature Customer Service Center LLC**
233 Spring Street
New York, NY 10013
USA
**T**: +1-800-SPRINGER NATURE
(777-4643) or 212-460-1500
customerservice@springernature.com

Prices and other details are subject to change without notice. All errors and omissions excepted. Americas: Tax will be added where applicable. Canadian residents please add PST, QST or GST. Please add $5.00 for shipping one book and $ 1.00 for each additional book. Outside the US and Canada add $ 10.00 for first book, $5.00 for each additional book. If an order cannot be fulfilled within 90 days, payment will be refunded upon request. Prices are payable in US currency or its equivalent.

ISBN 978-3-319-96129-3 / BIC: UMB / SPRINGER NATURE: SCI15009