

Springer

1st
edition

2012, XVI, 356 p.

Printed book

Hardcover

Printed book

Hardcover

ISBN 978-3-642-29655-0

£ 119,99 | CHF 165,50 | 139,99 € |
153,99 € (A) | 149,79 € (D)

Available

Discount group

Science (SC)

Product category

Monograph

Series

Information Security and Cryptography

Other renditions

Softcover

ISBN 978-3-642-43677-2

Softcover

ISBN 978-3-642-29657-4

Computer Science : Data Structures and Information Theory

Joye, Marc, Tunstall, Michael (Eds.)

Fault Analysis in Cryptography

- **First comprehensive treatment of this topic covering theory, practice and countermeasures**
- **Will help establish fault defence as standard practice**
- **Authors are among the leading academic and industrial researchers in this field**

In the 1970s researchers noticed that radioactive particles produced by elements naturally present in packaging material could cause bits to flip in sensitive areas of electronic chips. Research into the effect of cosmic rays on semiconductors, an area of particular interest in the aerospace industry, led to methods of hardening electronic devices designed for harsh environments. Ultimately various mechanisms for fault creation and propagation were discovered, and in particular it was noted that many cryptographic algorithms succumb to so-called fault attacks. Preventing fault attacks without sacrificing performance is nontrivial and this is the subject of this book. Part I deals with side-channel analysis and its relevance to fault attacks. The chapters in Part II cover fault analysis in secret key cryptography, with chapters on block ciphers, fault analysis of DES and AES, countermeasures for symmetric-key ciphers, and countermeasures against attacks on AES. Part III deals with fault analysis in public key cryptography, with chapters dedicated to classical RSA and RSA-CRT implementations, elliptic curve cryptosystems and countermeasures using fault detection, devices resilient to fault injection attacks, lattice-based fault attacks on signatures, and fault attacks on pairing-based cryptography. Part IV examines fault attacks on stream ciphers and how faults interact with countermeasures used to prevent power analysis attacks. Finally, Part V contains chapters that explain how fault attacks are implemented, with chapters on fault injection technologies for microprocessors, and fault injection and key retrieval experiments on a widely used evaluation board. This is the first book on this topic and will be of interest to researchers and practitioners engaged with cryptographic engineering.

Order online at springer.com/book sellers**Springer Nature Customer Service Center GmbH**

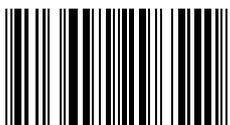
Customer Service

Tiergartenstrasse 15-17

69121 Heidelberg

Germany

T: +49 (0)6221 345-4301

row-book sellers@springernature.com

ISBN 978-3-642-29655-0 / BIC: UMB / SPRINGER NATURE: SCI15009

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.