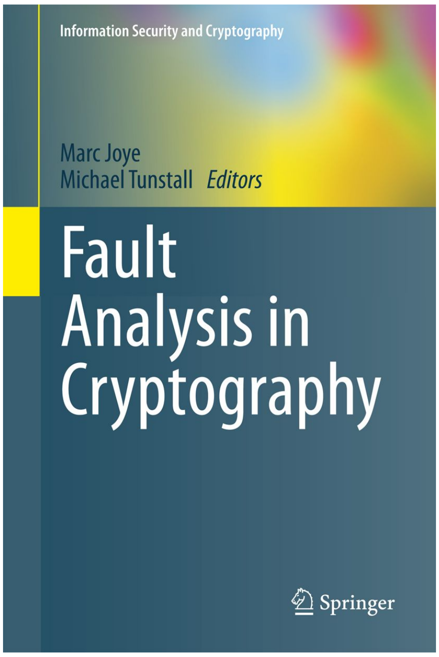
Springer

springer.com



Information Security and Cryptography

Marc Joye
Michael Tunstall *Editors*

Fault Analysis in Cryptography

Springer

2012, XVI, 356 p.

Printed book

Hardcover

139,99 € | £119.99 | $169.99
[1]149,79 € (D) | 153,99 € (A) | CHF 165,50

Softcover

139,99 € | £119.99 | $169.99
[1]149,79 € (D) | 153,99 € (A) | CHF 165,50

eBook

117,69 € | £95.50 | $129.00
[2]117,69 € (D) | 117,69 € (A) | CHF 132,00

Available from your library or springer.com/shop

MyCopy [3]

Printed eBook for just
€ | $ 24.99
springer.com/mycopy

Marc Joye, Michael Tunstall (Eds.)

Fault Analysis in Cryptography

Series: Information Security and 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 / or for the Americas call (toll free) 1-800-SPRINGER /
or email us at: customerservice@springernature.com. / For outside the Americas call +49 (0) 6221-345-4301 /
or email us at: customerservice@springernature.com.

The first € price and the £ and $ price are net prices, subject to local VAT. Prices indicated with [1] include VAT for books; the €(D) includes 7% for Germany, the €(A) includes 10% for Austria. Prices indicated with [2] include VAT for electronic products; 19% for Germany, 20% for Austria. All prices exclusive of carriage charges. Prices and other details are subject to change without notice. All errors and omissions excepted. [3] No discount for MyCopy.