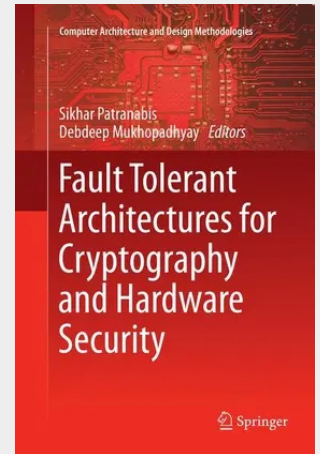


Fault Tolerant Architectures for Cryptography and Hardware Security

This book uses motivating examples and real-life attack scenarios to introduce readers to the general concept of fault attacks in cryptography. It offers insights into how the fault tolerance theories developed in the book can actually be implemented, with a particular focus on a wide spectrum of fault models and practical fault injection techniques, ranging from simple, low-cost techniques to high-end equipment-based methods. It then individually examines fault attack vulnerabilities in symmetric, asymmetric and authenticated encryption systems. This is followed by extensive coverage of countermeasure techniques and fault tolerant architectures that attempt to thwart such vulnerabilities. Lastly, it presents a case study of a comprehensive FPGA-based fault tolerant architecture for AES-128, which brings together of a number of the fault tolerance techniques presented. It concludes with a discussion on how fault tolerance can be combined with side channel security to achieve protection against implementation-based attacks. The text is supported by illustrative diagrams, algorithms, tables and diagrams presenting real-world experimental results.

Reviews exhaustively the recent key research into fault tolerant architectures in hardware security and cryptography softwareDiscusses the latest fault attacks on a wide variety of cryptographic implementations, such as biased fault attacks, algebraic fault attacks, and attacks on authenticated encryption based ciphersOffers hands-on and practical demonstrations for handling complex secure cryptographic architectures, complementing the theoretical analysis



149,79 €

139,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9789811338199

Medium: Buch

ISBN: 978-981-13-3819-9

Verlag: Springer

Erscheinungstermin: 25.12.2018

Sprache(n): Englisch

Auflage: Softcover Nachdruck of the original 1. Auflage 2018

Serie: Computer Architecture and Design Methodologies

Produktform: Kartoniert

Gewicht: 388 g

Seiten: 240

Format (B x H): 155 x 235 mm

