

Springer

1st
edition

2007, XXVI, 362 p.

Printed book

Hardcover

Printed book

Hardcover

ISBN 978-0-387-33883-5

\$ 199,99

Available

Discount group

Professional Books (2)

Product category

Professional book

Series

Signals and Communication Technology

Other renditions

Softcover

ISBN 978-1-4419-4156-5

Engineering : Electrical Engineering

Rodríguez-Henríquez, F., Saqib, N.A., Díaz Pérez, A., Koc, C.K., Centro de Investigación y de Estudios Avanzados del IPN, Mexico, Mexico

Cryptographic Algorithms on Reconfigurable Hardware

- Presents a comprehensive methodology for efficient implementation of cryptographic algorithms on reconfigurable hardware devices
- Special emphasis on the practical aspects of reconfigurable hardware design and a comprehensive description of state-of-the-art implementation techniques
- Demonstrates how high-speed cryptographic algorithm implementations can be achieved on reconfigurable hardware devices without posing prohibitive requirements on hardware resources

Cryptographic solutions using software methods can be used for those security applications where data traffic is not too large and low encryption rate is tolerable. On the other hand, hardware methods offer high-speed solutions making them highly suitable for applications where data traffic is fast and large data is required to be encrypted in real time. VLSI (also known as ASIC), and FPGAs (Field Programmable Gate Arrays) are two alternatives for implementing cryptographic algorithms in hardware. FPGAs offer several benefits for cryptographic algorithm implementations over VLSI as they offer high flexibility. Due to its reconfigurable property, keys can be changed rapidly. Moreover, basic primitives in most cryptographic algorithms can efficiently be implemented in FPGAs. Since the invention of the Data Encryption Standard (DES), some 40 years ago, a considerable amount of cryptographic algorithm implementation literature has been produced both, for software and hardware platforms. Unfortunately, virtually there exists no book explaining how the main cryptographic algorithms can be implemented on reconfigurable hardware devices. This book will cover the study of computational methods, computer arithmetic algorithms, and design improvement techniques needed to implement efficient cryptographic algorithms in FPGA reconfigurable hardware platforms.

Order online at springer.com/booksellers**Springer Nature Customer Service Center LLC**

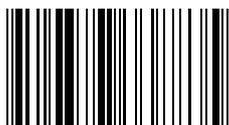
233 Spring Street

New York, NY 10013

USA

T: +1-800-SPRINGER NATURE

(777-4643) or 212-460-1500

customerservice@springernature.com

ISBN 978-0-387-33883-5 / BIC: THR / SPRINGER NATURE: SCT24000

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.

Part of **SPRINGER NATURE**