Signals and Communication Technology

Francisco Rodríguez-Henríquez
N.A. Saqib
Arturo Díaz Pérez
Çetin Kaya Koç

Cryptographic Algorithms on Reconfigurable Hardware

Springer

2007, XXVI, 362 p.

Printed book

Hardcover
159,99 € | £139.99 | $199.99
[1]171,19 € (D) | 175,99 € (A) | CHF 189,00

Softcover
130,83 € | £99.99 | $149.99
[1]139,99 € (D) | 143,91 € (A) | CHF 154,50

eBook

107,09 € | £79.50 | $109.00
[2]107,09 € (D) | 107,09 € (A) | CHF 123,50

Available from your library or springer.com/shop

MyCopy [3]

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

F. Rodriguez-Henriquez, N.A. Saqib, A. Díaz Pérez, C.K. Koc

Cryptographic Algorithms on Reconfigurable Hardware

Series: Signals and Communication Technology

- 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.

Part of **SPRINGER NATURE**