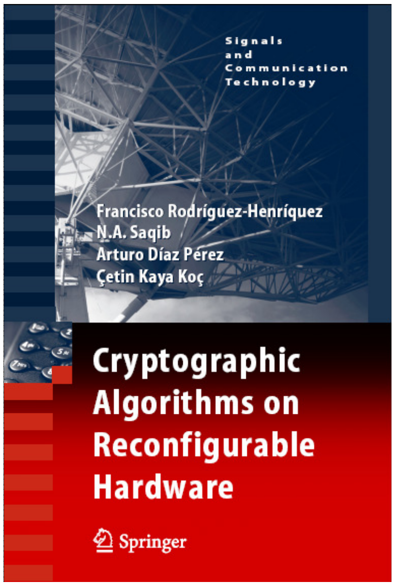
Signals and Communication Technology
Francisco Rodríguez-Henríquez
N.A. Saqib
Arturo Díaz Pérez
Çetin Kaya Koç
Cryptographic Algorithms on Reconfigurable Hardware
Springer

Francisco Rodriguez-Henriquez, Centro de Investigación y de Estudios Avanzados del IPN (CINVESTAV), Col. San Pedro Zacatenco, Mexico D.F., Mexico; Nazar Abbas Saqib, Centro de Investigación y de Estudios Avanzados del IPN (CINVESTAV), Col. San Pedro Zacatenco, Mexico D.F., Mexico; Arturo Díaz Pérez, Centro de Investigación y de Estudios Avanzados del IPN (CINVESTAV), Col. San Pedro Zacatenco, Mexico D.F., Mexico; Cetin Kaya Koc, Oregon State University, Corvallis, OR, USA

Cryptographic Algorithms on Reconfigurable Hardware

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. The concepts and techniques to be reviewed in this book will make special emphasis on the practical aspects of reconfigurable hardware design, explaining the basic mathematics related and giving a comprehensive description of state-of-the-art implementation techniques. Thus, the main goal of this monograph is to show how high-speed cryptographic algorithms implementations can be achieved on reconfigurable hardware devices without posing prohibited high requirements for hardware resources.

Content: Introduction.- A Brief Introduction to Modern Cyptography.- Reconfigurable Hardware Technology.- Mathematical Background.- Prime Finite Field Arithmetic.- Binary Finite Field Arithmetic.- Reconfigurable Hardware Implementation of Hash Functions.- General Guidelines for Implementing Block Ciphers in FPGAs.- Architectural Designs for Advanced Encryption Standard.- Elliptic Curve Cryptography.

_____ copies Rodriguez-Henriquez et al., Cryptographic Algorithms on Reconfigurable Hardware
ISBN-10: 0-387-33883-7 / ISBN-13: 978-0-387-33883-5 • **$ 89.95**

2007 362 p. Hardcover
Signals and Communication Technology
• **$ 89.95**
ISBN-10: 0-387-33883-7
ISBN-13: 978-0-387-33883-5
available

○ Check / money order enclosed ○ Please charge my credit card: ○ Mastercard ○ VISA ○ AmericanExpress

Card No. □□□□ □□□□ □□□□ □□□□ □□□ Expiration Date □□□□

Springer
Order Department
PO Box 2485
Secaucus, NJ 07096-2485

Tel: 1-800-Springer, 8:30 am – 5:30 pm ET
Fax: 1-201-348-4505
Email: orders-ny@springer.com