Review of the book

Cryptographic Engineering

by Çetin Kaya Koç, Editor

Springer, 2009

ISBN: 978-0-387-71816-3

RAMRAMI Azzeddine
CryptoDisk/France

21th of December, 2009

1 About this book

This book is the first complete introduction to a new area called **Cryptographic Engineering**. Cryptographic Engineering refers to the theory and practice of engineering of cryptographic systems, including encryption and decryption engines, digital signature and authentication systems, true random number generators, and the design, implementation, testing, and validation of cryptographic systems.

2 Detailed Summary

Cryptographic Engineering is a comprehensive text that is suitable as a handbook for hardware and software engineers who are interested in building secure systems using cryptographic techniques. This book addresses cryptanalysis of security systems for the purpose of checking their robustness and their strength against attacks, and building countermeasures in order to thwart such attacks by reducing their probability of success. The material includes four important parts, intimately interconnected :

① Detailed description of true random number generators,

② Detailed algorithmic treatment of public-key cryptographic systems and emphasis on the engineering of systems,

③ ASIC and FPGA hardware design for cryptography, and

④ Side-channel attacks on cryptographic systems and design of countermeasures.

This book starts with a brief chapter (chapter 1) introducing the new area of *Cryptographic Engineering*, and explains the organization of the rest of chapter.
The following subsections explain in detail the four parts of this book.

Random number generators exposed

The first part starts from chapter 2 to chapter 4, explain all things concerning the random number generators. The role and evaluation of the random number generators are explained. I found this part very interesting and useful, because all information needed about the random number generators are explained in this book.
A dedicated chapter is reserved for true random number generators (TRNG). A good explanation on how to implement TRNG on ASIC and FPGA is given with the different implementation scenarios.

Public key cryptosystem

The second parts start from chapter 5 to chapter 9, is a good course and reference on implementation (hardware and software) of public key algorithms and cryptosystems, such as RSA, Diffie-Hellman and elliptic curve cryptography. A mathematical concept for elliptic curve, Galois Fields and Fast Fourier Transform is exposed in this part.

AES on FPGA and ASIC hardware

The third part starts from chapter 10 to chapter 12, is a good course and reference on implementation (hardware and software) of secret key algorithms and cryptosystems. Everything is explained : ECB, CBS, CCM modes, AES. Complete details on ASIC and FPGA realizations are presented. Two chapters explain in details the AES algorithm, chapters 10 and 12.

Side-channel attacks

The fourth part starts from chapter 13 to chapter 18. This is the longest part and focuses on side-channel attacks and countermeasures against these attacks.
Chapter 13 explains the basic of side-channel analysis like timing analysis, simple power analysis and differential power analysis (DPA). Some countermeasures are presented to protect an implementation against those attacks.
Chapter 14 describes improved techniques for side-channel analysis like :

① CMOS Device : side-channel leakage perspectives

② Characterizing side-channel leakage using maximum likelihood

③ Template attacks

④ Improved DPA/DEMA metric

⑤ Multichannel attacks

Chapter 15 presents in some details the electromagnetic attacks (EM attacks) and the corresponding countermeasures. The following themes are discussed in this chapter :

① Background on EM

② EM capturing equipment

③ EM Leakage

④ Multiplicity of EM channels and comparison with DPA

Also Instruction Set Extensions (ISE) for cryptography are discussed for AES and ECC.
Chapter 16 discusses the leakage from Montgomery multiplication and chapter 17 present the randomized exponentiation algorithms attacks.
This book ends with a chapter on cryptoarchitectural attacks and countermeasures. Chapter 18 starts with a brief history and discusses cache analysis and branch prediction analysis.
This book is very interesting for students and professors, since every chapter ends with a list of exercises and projects for the propose of checking the reader's understanding. An extensive list of references end each chapter for further reading. I hope in the next edition, the authors could present some tools to hand-on all the techniques presented in this book. I suggest adding a CD-ROM or DVD-ROM containing all necessary software.

3 Would you recommend this book ?

The books is written for graduate students and researchers in cryptography and engineers working in the following area :

① implementation of cryptography on FPGA and ASIC,

② development of TRNG on ASIC.

I really recommend this book to students and engineers working on implementations of cryptography in real life. It could help them to use efficient techniques on different platforms from embedded system to high level cryptographic software running on database, operating system and more. As a cryptographic hardware level (ASIC and FPGA) designer, I am going to use *Cryptographic Engineering* as a reference in my daily work.

The reviewer is an IT Security Architect at Capgemini/France and CTO of Cryptodisk/France,a hardware real-time hard disk encryption ASIC/FPGA manufacturer and designer.