Cryptographic Engineering

Çetin Kaya Koç
Editor

Cryptographic Engineering

Springer

Editor
Çetin Kaya Koç
City University of Istanbul
Tophane, Istanbul
Turkey
and
University of California Santa Barbara
Santa Barbara, CA
USA

ISBN: 978-0-387-71816-3 e-ISBN: 978-0-387-71817-0
DOI 10.1007/978-0-387-71817-0

Library of Congress Control Number: 2008935379

Printed on acid-free paper

springer.com

To all scientists and engineers whose ideas gave birth to modern cryptography, particularly, Claude Shannon, Whit Diffie, Martin Hellman, Ralph Merkle, Don Coppersmith, Ron Rivest, Adi Shamir, Len Adleman, and Neal Koblitz.

Preface

Cryptography is an ancient art. Chinese, Roman, and Arab cultures often used ciphers to protect military and state communications or secret society documents. Cryptographic engineering, on the other hand, is a relatively new subject. A cryptographic engineer designs, implements, tests, validates, and sometimes reverse-engineers or attempts to break cryptographic systems. The designers of Enigma, an electromechanical cipher machine, were cryptographic engineers; so was Alan Turing who contributed to its cryptanalysis. In our view, anyone who designs and builds electromechanical, electronic, or quantum-mechanical systems in order to encrypt, decrypt, sign or authenticate data is a cryptographic engineer. However, in this book we have narrowed our definition to only electronic systems, specifically, hardware and software systems.

Cryptographic engineering is a complicated, multidisciplinary field. It encompasses mathematics (algebra, finite groups, rings, and fields), electrical engineering (hardware design, ASIC, FPGAs) and computer science (algorithms, complexity theory, software design, embedded systems). It is rather difficult to be a master of all subjects; one usually has to be content with being a master of one. In order to practice state-of-the-art cryptographic design, mathematicians, computer scientists, and electrical engineers need to collaborate.

This book was born out of the class notes of the lecturers who have been meeting since 2002 in Lausanne, Switzerland, at the campus of EPFL, to teach a one-week course to graduate students, faculty, and researchers from academia, and engineers from industry. In order to create this book, I compiled the lecture notes together, wrote some of the material, and also invited other prominent researchers to contribute. This book is intended to constitute a first step towards becoming a cryptographic engineer. We hope that it will successfully serve its purpose.

Istanbul & Santa Barbara *Çetin Kaya Koç*

Contents

Acronyms

2DEM	2D-Encryption Mode
ABC	Accumulated Block Chaining
ABL	Arbitrary Block Length
ACM	Association for Computing Machinery
AES	Advanced Encryption Standard
AE	Authenticated Encryption
AEAD	Authenticated Encryption with Associated Data
AIS	Anwendungshinweise und Interpretationen zum Schema
AIS	Application Notes and Interpretation of the Scheme
ALU	Arithmetic Logic Unit
ANSI	American National Standards Institute
ARK	Add Round Key
ASIC	Application Specific Integrated Circuits
BPA	Branch Prediction Analysis
BPU	Branch Prediction Unit
BTB	Branch Target Buffer
BS	Byte Substitution
CASR	Cellular Automata Shift Register
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CHES	Cryptographic Hardware and Embedded Systems
CISC	Complex Instruction Set Computer
CLB	Configurable Logic Block
CMAC	Cipher Based MAC
CMC	CBC Mask CBC
CMOS	Complementary Metal-Oxide Semiconductor
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit
CRT	Chinese Remainder Theorem
CS	Cipher State

CTR	Counter Mode
CWC	Carter Wegman with Counter
das	digitized analog signal
DE	Disk Encryption
DEA	Data Encryption Algorithm
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DPA	Differential Power Analysis
DRM	Digital Rights Management
DRNG	Deterministic Random Number Generator
DSA	Digital Signature Algorithm
DLP	Discrete Logarithmic Problem
DSS	Digital Signature Standard
EAX	Conventional Authenticated-Encryption Mode
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EME	ECB Mix ECB
FEAL	Fast Data Encipherment Algorithm
FFSEM	Feistel Finite Set Encryption Mode
FFT	Fast Fourier Transform
FIGARO	Fibonacci Galois Ring Oscillator
FIPS	Federal Information Processing Standard
FIPS PUB	Federal Information Processing Standard Publication
FPGA	Field Programmable Gate Array
FPLD	Field Programmable Logic Device
gcd	Greatest Common Divisor
GCM	Galois Counter Mode
GF	Galois Field
HCH	Hash Encrypt Hash
HCTR	Hash Counter Hash
HECC	Hyperelliptic Curve Cryptography
HEH	Hash ECB Hash
IACBC	Integrity Aware Cipher Block Chaining
IAPM	Integrity Aware Parallelizable Mode
IEEE	Institute of Electrical and Electronics Engineers
IDEA	International Data Encryption Algorithm
IDFT	Inverse Discrete Fourier Transform
IGE	Infinite Garble Extension
iid	independent and identically distributed
IMA	Institute of Mathematics and its Applications
ISA	Instruction Set Architecture
ISE	Instruction Set Extension
KFB	Key Feedback Mode

LFSR	Linear Feedback Shift Register
LNCS	Lecture Notes in Computer Science
LRU	Least Recently Used
LRW	Liskov Rivest Wagner
LT	LaGrande Technology
LUT	Lookup Table
MA	Microarchitectural Analysis
MAC	Message Authentication Code
MC	Mixed Columns
MD	Message Digest
MDC	Manipulation Detection Code
MMX	Multimedia Extension
MSMP	Modified Spectral Modular Product
MULGF	Multiply in Galois Field
MULGF2	Multiply in Galois Field Base 2
NACSIM	National Communications Security Information Memorandum
NACSEM	National Communications Security Emanation Memorandum
NTT	Number Theoretical Transform
NIST	National Institute of Standards and Technology
NPTRNG	Non-Physical Random Number Generator
NSA	National Security Agency
NSTISSI	National Training Standard for Information Systems Security
OCB	Offset Code Book
OEF	Optimal Extension Fields
OFB	Output Feedback
OMAC	One-Key CBC
ONB	Optimal Normal Basis
OS	Operating System
PC	Personal Computer
PCFB	Propagating Cipher Feedback
PEP	Polynomial Hash Encrypt Polynomial Hash
PKC	Public Key Cryptography
PKCS	Public Key Cryptography Standards
PL	Phase Locked Loop
PMAC	Parallelizable Message Authentication Code
PNT	Pseudo Number Transform
PRNG	Physical Random Number Generator
PTRNG	Physical True Random Number Generator
PUF	Physically Unclonable Functions
RAM	Random Access Memory
RAMB	Block RAM
RFID	Radio Frequency Identification Device
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RISC	Reduced Instruction Set Computer
RMAC	Randomized MAC

RNG	Random Number Generator
RSA	Rivest Shamir Adleman
RSD	Redundant Signed Digit
SBPA	Simple Branch Prediction Analysis
SCA	Side Channel Analysis
SEMA	Simple Electromagnetic Analysis
SFU	Shared Functional Units
SHA	Secure Hash Algorithm
SIAM	Society for Industrial and Applied Mathematics
SIMD	Single Instruction Multiple Data
SIV	Synthetic IV
SME	Spectral Modular Exponentiation
SMM	Spectral Modular Multiplication
SMP	Spectral Modular Product
SMT	Simultaneous Multithreading
SPA	Simple Power Analysis
SPRP	Strong Pseudo Random Permutation
SR	Shift Rows
TDEA	Triple Data Encryption Algorithm
TEMPEST	Transient Electromagnetic Pulse Emanation Standard
TET	Hash ECB Hash
TMAC	Two-Key CBC MAC
TRNG	True Random Number Generator
TXT	Trusted Execution Technology
VCO	Voltage Controlled Oscillator
VHDL	Very High Level Hardware Description Language
VLIW	Very Long Instruction Word
VT	Virtualization Technology
WAIFI	Workshop on the Arithmetic of Finite Fields
XCB	Extended Code Book
XCBC	Extended Cipher Block Chaining
XECB	Extended Electronic Code Book