Lai-Massey Cipher Designs

Jorge Nakahara Jr.

Lai-Massey Cipher Designs

History, Design Criteria and Cryptanalysis

Springer

Jorge Nakahara Jr.
São Paulo, Brazil

Additional material for this book can be downloaded from http://extras.springer.com.

ISBN 978-3-319-68272-3 ISBN 978-3-319-68273-0 (eBook)
https://doi.org/10.1007/978-3-319-68273-0

Library of Congress Control Number: 2018957428

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

This book is dedicated to my parents
Jorge Nakahara and Misao Nakahara.
In memoriam

Preface

This book presents the first comprehensive account of the history, design and analysis of cryptographic block ciphers following the Lai-Massey design paradigm, which started with the PES and IDEA ciphers in 1990/1991.

The fact that these ciphers were originally designed by X. Lai and J.L. Massey led to the terminology *Lai-Massey cipher designs* to denote these and other ciphers that follow in one way or another the design guidelines set by Lai and Massey for PES and IDEA.

Other ciphers discussed in this book include: the MESH cipher family (including MESH-64, MESH-96, MESH-128, MESH-64(8) and MESH-128(8)), RIDEA, WIDEA-n, YBC, the FOX/IDEA-NXT cipher family, REESSE3+, IDEA* and Bel-T.

Lai-Massey cipher designs differ structurally from Feistel Network ciphers such as the DES, and from Substitution-Permutation Network (SPN) ciphers such as the AES. Lai-Massey ciphers have their own unique features such as: (i) complete text diffusion in a single round; (ii) they usually repeat a rather strong round function a small number of times, instead of repeating a comparatively weak round function a large number of times; (iii) originally, only three group operations are used as building blocks, such as bitwise exclusive-or, modular addition and modular multiplication (in a finite field); (iv) originally, they did not employ S-boxes nor MDS codes to achieve optimal confusion and diffusion, respectively.

This book consolidates research and cryptanalysis results in the publicly-available literature on Lai-Massey ciphers covering a 28-year period from 1990 to 2017. An extensive bibliographic research has been performed to collect the most relevant conference papers, journal articles, PhD and MSc theses and technical reports dealing with mathematical and computational aspects of Lai-Massey ciphers. Therefore, this book may serve as a useful resource for students, researchers and practitioners willing to understand, design and deploy ciphers based on the Lai-Massey design paradigm.

The attacks listed in this book cover both published, new, updated and revised papers. The attacks include: Differential Cryptanalysis, Linear Crypt-

analysis, Square/Multiset, Impossible Differential, Truncated Differential, Biryukov-Demirci, Demirci, Slide, Advanced Slide, Boomerang, Biclique, Differential-Linear, Key-Dependent, BDK, Meet-in-the-Middle and Related-Key attacks.

Although we tried to be as accurate as possible, any errors, mistakes and inconsistencies are the author's sole responsibility. Any comments, corrections or suggestions for improvement are welcome. Please, forward them to

jorge.nakahara@springer.com

Many people helped and supported this book project over the years. To mention a few: Bart Preneel, Vincent Rijmen, Joos Vandewalle, Christian Cachin, Pela Noé, Beverley Ford, Alfred Hofmann, Ronan Nugent and Xuejia Lai.

The author appreciates the kind permission to include parts of papers, articles and theses that have been published (and are copyrighted) by Springer, by the Katholieke Universiteit Leuven (KUL), by the International Association for Cryptologic Research (IACR) or by other institutions, scientific societies or companies.

Some data concerning attack details of some Lai-Massey ciphers could not fit in this book due to space limitations. Please, follow the instructions on the book's webpage to access this information:

http://www.springer.com/978-3-319-68272-3

Finally, I would like to dedicate this book to my family, without whom nothing would have ever been accomplished at all.

São Paulo, Brazil *Jorge Nakahara Jr.*
January 2018

List of Acronyms

ACPC	Adaptively-Chosen Plaintext and Ciphertext
AES	Advanced Encryption Standard
AMX	Addition, Multiplication, eXclusive-or
ARX	Addition, bitwise-Rotation, eXclusive-or
ASR	All-Subkey Recovery
AX	Addition-eXclusive-or (layer)
BDK	Biham-Dunkelman-Keller
CBC	Cipher Block Chaining (mode)
CC	Chosen Ciphertext
CCACP	Chosen-Ciphertext Adaptively-Chosen Plaintext
CFB	Cipher FeedBack (mode)
CP	Chosen Plaintext
CPACC	Chosen-Plaintext Adaptively-Chosen Ciphertext
CPCC	Chosen-Plaintext (non-adaptively)-Chosen Ciphertext
CO	Ciphertext Only
CPU	Central Processing Unit
CTR	Counter (mode)
DES	Data Encryption Standard
DFR	Distinguish-From-Random
ECB	Electronic Code Book (mode)
ES	Exhaustive Search
EKS	Exhaustive Key Search
GCD	Greatest Common Divisor
HW	Hamming Weight
IBA	Impossible-Boomerang Attack
IDEA	International Data Encryption Algorithm
IND-KPA	Indistinguishable under Known-Plaintext Attack
IND-CPA	Indistinguishable under Chosen-Plaintext Attack
IND-CCA1	Indistinguishable under non-adaptive Chosen-Ciphertext Attack
IND-CCA2	Indistinguishable under adaptive Chosen-Ciphertext Attack
io	inverse orthomorphism (function)
IPES	Improved Proposed Encryption Standard
IV	Initial Value(s)
KK	Known Key
KM	Key-Mixing (layer)
KP	Known Plaintext
KR	Key Recovery

KW	Key Whitening (layer)
KSA	Key Schedule Algorithm
LCM	Least Common Multiple
LFSR	Linear Feedback Shift Register
lsb	Least Significant Bit
MA	Memory Access or Multiplication-Addition (layer)
MA-box	Multiplication-Addition box
MAC	Message Authentication Code
MDS	Maximum Distance Separable (code)
MITM	Meet-in-the-Middle
msb	Most Significant Bit
NESSIE	New European Schemes for Signature, Integrity and Encryption
NIST	(US) National Institute of Standards and Technology
NLFSR	NonLinear Feedback Shift Register
OFB	Output FeedBack (mode)
OPP	Offline Pre-Processing
or	orthomorphism function
OT	Output Transformation
OTP	One-Time Pad
PES	Proposed Encryption Standard
PGP	Pretty Good Privacy
PRF	PseudoRandom Function
PRP	PseudoRandom Permutation
RK-CP	Related-Key Chosen-Plaintext
RK-KP	Related-Key Known-Plaintext
S-box	Substitution box
SPN	Substitution Permutation Network
SPRP	Strong PseudoRandom Permutation
TDC	Truncated Differential Cryptanalysis
TEA	Tiny Encryption Algorithm
TLU	Table LookUp
TMDTO	Time-Memory-Data Trade-Off
TMTO	Time-Memory Trade-Off
UD	Unicity Distance
WCU	whole codebook used
WKC	Weak-Key Class

List of Symbols

$\text{lsb}_i(x)$	the i-th least significant bit of x
$\text{msb}_i(x)$	the i-th most significant bit of x
$x \ll y$	the value of x left-shifted by y bits
$x \gg y$	the value of x right-shifter by y bits
$x \lll y$	the value of x left-rotated by y bits
$x \ggg y$	the value of x right-rotated by y bits
$\oplus$	bitwise exclusive-or operation
$\boxplus$	modular addition in $\mathbb{Z}_{2^w}$, $w \in \{2, 4, 8, 16\}$
$\boxminus$	modular subtraction in $\mathbb{Z}_{2^w}$, $w \in \{2, 4, 8, 16\}$
$\odot$	modular multiplication in GF$(2^w + 1)$, $w \in \{2, 4, 8, 16\}$
$\oslash$	modular division in GF$(2^w + 1)$, $w \in \{2, 4, 8, 16\}$
$\mathbb{Z}_{2^n}$	the ring of integer modulo 2^n
GF$(2^{16} + 1)$	the finite field of $2^{16} + 1$ elements and such that $0 \equiv 2^{16}$
GF$(2^8 + 1)$	the finite field of $2^8 + 1$ elements and such that $0 \equiv 2^8$
GF(2^n)	the finite field of 2^n elements i.e. GF$(2)[x]/p(x)$ where $p(x)$ is an irreducible polynomial in GF(2) of degree n
subscript x	denotes an hexadecimal value e.g. $1a_x = 26$
subscript 2	denotes a binary value e.g. $1100_2 = 12$
1^m	denotes a sequence of m bits 1
0^t	denotes a sequence of t bits 0
$\|x\|$	the magnitude, length or the absolute value of x
$\mathbb{Z}_m^t$	the cartesian product of $\mathbb{Z}_m$ with itself t times: $\mathbb{Z}_m \times \mathbb{Z}_m \times \ldots \times \mathbb{Z}_m$
Λ-set	a multiset of 2^m n-bit text blocks

Contents