Boolean Functions for Cryptography and Coding Theory

Boolean functions are essential to systems for secure and reliable communication. This comprehensive survey of Boolean functions for cryptography and coding covers the whole domain and all important results, building on the authors influential articles with additional topics and recent results. A useful resource for researchers and graduate students, the book balances detailed discussions of properties and parameters with examples of various types of cryptographic attacks that motivate the consideration of these parameters. It provides all the necessary background on mathematics, cryptography, and coding and an overview of recent applications, such as side-channel attacks on smart cards and hardware, cloud computing through fully homomorphic encryption, and local pseudorandom generators. The result is a complete and accessible text on the state of the art in single- and multiple-output Boolean functions that illustrates the interaction among mathematics, computer science, and telecommunications.

CLAUDE CARLET is Professor Emeritus of Mathematics at the University of Paris 8, France, and member of the Bergen University Department of Computer Science. He has contributed to 16 books, and published more than 130 papers in international journals and more than 70 papers in international proceedings. He has been a member of 80 program committees of international conferences and served as cochair for 10 of them. He has overseen the research group Codage-Cryptographie, which gathers all French researchers in coding and cryptography, and is editor-in-chief of the journal *Cryptography and Communications*. He has been an invited plenary speaker at 20 international conferences and the invited speaker at 30 other international conferences and workshops.

Boolean Functions for Cryptography and Coding Theory

Claude Carlet
University of Bergen, Norway, and University of Paris 8, France

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314-321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India

79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108473804
DOI: 10.1017/9781108606806

First published 2020

Printed in the United Kingdom by TJ Books Limited, Padstow Cornwall

A catalogue record for this publication is available from the British Library.

Library of Congress Cataloging-in-Publication Data
Names: Carlet, Claude, author.
Title: Boolean functions for cryptography and coding theory / Claude Carlet.
Description: Cambridge ; New York, NY : Cambridge University Press, 2020. |
Includes bibliographical references and index.
Identifiers: LCCN 2020002605 (print) | LCCN 2020002606 (ebook) |
ISBN 9781108473804 (hardback) | ISBN 9781108606806 (epub)
Subjects: LCSH: Algebra, Boolean. | Cryptography. | Coding theory.
Classification: LCC QA10.3 .C37 2020 (print) | LCC QA10.3 (ebook) |
DDC 003/.5401511324–dc23
LC record available at https://lccn.loc.gov/2020002605
LC ebook record available at https://lccn.loc.gov/2020002606

ISBN 978-1-108-47380-4 Hardback

Cambridge University Press
978-1-108-47380-4 — Boolean Functions for Cryptography and Coding Theory
Claude Carlet
Frontmatter
More Information

Contents

Preface

The present monograph is a merged, reorganized, significantly revised, and extensively completed version of two chapters, entitled “Boolean Functions for Cryptography and Error Correcting Codes” [236] and “Vectorial Boolean Functions for Cryptography” [237], which appeared in 2010 as parts of the book *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* [394] (editors, Yves Crama and Peter Hammer). It is meant for researchers but is accessible to anyone who knows basics in linear algebra and general mathematics. All the other notions needed are introduced and studied (even finite fields are, in the Appendix).

Since these chapters were written in 2009, about 1,500 papers have been published that deal with this twofold topic (which is broad, as we see), and this version is updated with the main references and their main results (with corrections in the rare cases where they were needed). It also contains original results.

New notions on Boolean and vectorial functions and new ways of using them have also emerged. A chapter devoted to these recent and/or not enough studied directions of research has been included.

In the limit of a book, we tried to be as complete as possible. Of course, we could not go into details as much as do papers, but we made our best to ensure a good trade-off between completeness in scope and in depth. The choice of those papers that are referred to and of those results that are developed may seem subjective; it has been difficult, given the large number of papers. We tried, within the imposed length limit, to give the proof of a result each time it was short and simple enough, and when it provided a vision (we tried to avoid giving too technical proofs whose only – but of course important – value would have been to convince the reader that the result is true). We would have liked to avoid, when presenting arguments and observations, to refer to results (and concepts) to come later in the text, but the large number of results has made this necessary; otherwise, it would have been impossible to gather in a same place all the facts related to a same notion.

We have limited ourselves to Boolean and vectorial functions in characteristic 2, since these fit better with applications in coding and cryptography, and since dealing with p-ary and generalized functions would have reduced the description of the results on binary functions.

Acknowledgments

The author wishes to thank Cambridge University Press for publishing this monograph, and in particular Kaitlin Leach, Amy He, and Mark Fox for their kind help. He deeply thanks Lilya Budaghyan, from the Selmer Center, University of Bergen, for her kind support and her precious and numerous bits of information, in particular on almost perfect nonlinear (APN) functions, which allowed me to improve several chapters, making them more accurate, complete, and up-to-date, and Sihem Mesnager, from the University of Paris 8 and the Laboratoire Analyse, Géométrie et Applications (LAGA), for her careful reading of the whole book during the time it was written, for her supporting advice, and for her detailed additive proposals, which improved the completeness. I also thank very much Victor Chen, Sylvain Guilley, Pierrick Méaux, Lauren De Meyer, Stjepan Picek, Emmanuel Prouff, Sondre Rønjom, and Deng Tang, each of whom helped with completing and correcting a part of a section of the book or even several. Many thanks also to the anonymous reviewers invited by Cambridge University Press, whose comments have been helpful.

Research is a collective action and a too-long list of names should be cited to acknowledge all the stimulating discussions, collaborations, and information that contributed to this book. A few names are the 10 previously mentioned and Kanat Abdukhalikov, Benny Applebaum, Thierry Berger, Marco Calderini, Xi Chen, Robert Coulter, Diana Davidova, Ulrich Dempwolff, John Dillon, Cunsheng Ding, the late Hans Dobbertin, Yves Edel, Keqin Feng, Caroline Fontaine, Rafael Fourquet, Philippe Gaborit, Faruk Göloglu, Guang Gong, Aline Gouget, Cem Güneri, Tor Helleseth, Xiang-dong Hou, Nikolay Kaleyski, William Kantor, Selçuk Kavut, Jenny Key, Alexander Kholosha, Andrew Klapper, Nicholas Kolokotronis, Gohar Kyureghyan, Philippe Langevin, Gregor Leander, Alla Levina, Chunlei Li, Nian Li, Konstantinos Limniotis, Mikhail Lobanov, Luca Mariot, Subhamoy Maitra, the late James Massey, Gary McGuire, Wilfried Meidl, Willi Meier, Harald Niederreiter, Svetla Nikova, Kaisa Nyberg, Ferruh Özbudak, Daniel Panario, Matthew Parker, Enes Pasalic, George Petrides, Alexander Pott, Mathieu Rivain, Thomas Roche, François Rodier, Neil Sloane, François-Xavier Standaert, Henning Stichtenoth, Yin Tan, Chunming Tang, Horacio Tapia-Recillas, Faina Solov'eva, Pante Stănică, Yuriy Tarannikov, Cédric Tavernier, Alev Topuzoğlu, Irene Villa, Arne Winterhof, Satoshi Yoshiara, Xiangyong Zeng, Fengrong Zhang, and Victor Zinoviev, as well as the members of the National Institute for Research in Computer Science and Automation (INRIA) team, whose CODES project (now called SECRET) has been a nice research environment and has supported me during my thesis and many years after, and the Bergen Selmer Center team, which does the same now, with a spirit of kindness and generosity, for my great scientific benefit.

I also wish to acknowledge that gathering the bibliography has been considerably eased by websites such as dblp: computer science bibliography (https://dblp.uni-trier.de), ResearchGate (www.researchgate.net), and Google Scholar (https://scholar.google.fr/schhp?hl=fr&tab=Xs).

Last but not least, I am so grateful to my wife Madeleine and my family for their support, patience, and understanding of what a researcher's work is. This is even more true for the last three years, during which the writing of this book, the reviewing of the numerous published papers, and the copyediting took so much of my time. I dedicate my book to them, with a special thought for my children and grandchildren, who will have to face the world we leave them.

Notation

$\|I\|$	size of a set I,
$\lfloor u \rfloor$	integer part (floor) of a real number u,
$\lceil u \rceil$	ceiling of u (the smallest integer larger than or equal to u),
$\phi^{-1}(u)$	preimage of u by a function ϕ,
1_E	indicator (or characteristic) function of a set E: $1_E(x) = \begin{cases} 1 \text{ if } x \in E \\ 0 \text{ otherwise,} \end{cases}$
δ_a	the Dirac (or Kronecker) symbol at a (*i.e.* the indicator of $\{a\}$),
$\mathbb{F}_2$	the finite field with two elements 0, 1 (bits),
$\mathbb{F}_2^n$	the n-dimensional vector space over $\mathbb{F}_2$ (sometimes identified with $\mathbb{F}_{2^n}$),
$\mathcal{L}_{n,m}$	the vector space of linear (n, m)-functions,
0_n	zero vector in $\mathbb{F}_2^n$ or in $\mathbb{F}_q^n$, $n > 1$ (in other groups, we just write 0),
1_n	vector $(1, \ldots, 1)$ in $\mathbb{F}_2^n$,
$+$	addition in characteristic 0 (*e.g.*, in $\mathbb{R}$), and in $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ for $n > 1$,
$\sum_i$	multiple sum of $+$,
$\oplus$	addition in $\mathbb{F}_2$ (*i.e.*, modulo 2); direct sum of two vector spaces,
$\bigoplus_i$	multiple sum of $\oplus$,
$\overline{x}$	$x + 1_n$, where $x \in \mathbb{F}_2^n$,
$a \cdot x$	inner product in $\mathbb{F}_2^n$,
$\ell_a(x)$, $t_a(x)$	$= a \cdot x$, resp. $x + a$, where "$\cdot$" is an inner product in $\mathbb{F}_2^n$,
$\mathbb{F}_2^I$	the vector space over $\mathbb{F}_2$ of all binary vectors whose indices range in I,
$\mathbb{F}_{2^n}$	the finite (Galois) field of order 2^n, identified with $\mathbb{F}_2^n$ as a vector space,
$tr_m^n(x)$	$= x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{n-m}}$, trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ $(m \mid n)$,
$tr_n(x)$	$= tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ the absolute trace function,
$\mathbb{F}_{2^n}^*$	$\mathbb{F}_{2^n} \setminus \{0\}$, where 0 denotes the zero element of $\mathbb{F}_{2^n}$,
α	primitive element of $\mathbb{F}_{2^n}$,
$\otimes$	convolutional product of two functions over $\mathbb{F}_2^n$ (see page 60),
$f, g, h, \ldots$	Boolean functions,
$\mathcal{BF}_n$	the $\mathbb{F}_2$-vector space of all n-variable Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$,
$F, G, H, \ldots$	vectorial functions,
$\mathcal{G}_F$	graph of a vectorial function: $\mathcal{G}_F = \{(x, F(x));\ x \in \mathbb{F}_2^n\}$,
$w_H()$	Hamming weight (of a vector, of a function),
$d_H(,)$	Hamming distance (between two vectors, two functions),
$d(C)$	minimum (Hamming) distance of code C,

$supp()$	the support (of a vector, of a function),
$x \preceq y$	"x is covered by y" (*i.e.*, $supp(x) \subseteq supp(y)$),
$x \vee y$	vector such that $supp(x \vee y) = supp(x) \cup supp(y)$,
$x \wedge y$	vector such that $supp(x \wedge y) = supp(x) \cap supp(y)$,
e_i	ith vector of the canonical basis of $\mathbb{F}_2^n$,
x^I, x^u	$\prod_{i\in I} x_i$, $I \subseteq \{1,\dots,n\}$, $\prod_{i=1}^n x_i^{u_i}$, $u \in \mathbb{F}_2^n$,
$f \mapsto f^\circ$	binary Möbius transform ($f^\circ : u \mapsto a_u$, coef. of x^u in the ANF of f),
$\widehat{\varphi}$	Fourier–Hadamard transform of a real-valued function φ over $\mathbb{F}_2^n$,
f_χ	sign function of a Boolean function f, that is, $x \mapsto (-1)^{f(x)}$,
$W_f()$	Walsh transform of a Boolean function f (*i.e.*, $\widehat{f_\chi}$),
$W_F(,)$	Walsh transform of a vectorial function F,
$supp(W_f)$	support of W_f: $\{u \in \mathbb{F}_2^n;\ W_f(u) \neq 0\}$,
N_{W_f}	cardinality of the support of W_f,
$\mathcal{F}(f)$	$\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)}(= W_f(0_n))$,
$nl()$	nonlinearity of a Boolean or vectorial function,
$nl_r()$	r-th order nonlinearity of a Boolean function,
ln, $\log_2$	natural (Neperian) logarithm, base 2 logarithm,
$d_{alg}(f)$	the algebraic degree of f (*i.e.*, the degree of its ANF),
$d_{num}(f)$	the numerical degree of f (*i.e.*, the degree of its NNF),
$w_2(j)$	2-weight of integer j (see page 45),
(n,m,t)-function	t-resilient (n,m)-function,
$AI()$	algebraic immunity of a function,
$M_{f,d}$	matrix of the system of equations $\bigoplus_{\substack{I\subseteq\{1,\dots,n\}\\ \lvert I\rvert\le d}} a_I u^I = 0$, $u \in supp(f)$,
$rk(M)$	the rank of a matrix M,
$FAC()$	fast algebraic complexity of a function,
$FAI()$	fast algebraic immunity of a function,
$D_a f, D_a F$	derivatives in the direction a: $x \mapsto f(x) \oplus f(x+a)$, $F(x)+F(x+a)$,
Δ	the symmetric difference between two sets,
$\Delta_f(a)$	autocorrelation function $\Delta_f(a) = \sum_{x\in\mathbb{F}_2^n}(-1)^{D_a f(x)}$,
Δ_f	absolute indicator of f: $\Delta_f = \max_{a\in\mathbb{F}_2^n\setminus\{0_n\}} \lvert\Delta_f(a)\rvert$,
$\mathcal{V}(f)$	sum-of-squares indicator of f: $\sum_{e\in\mathbb{F}_2^n}\mathcal{F}^2(D_e f)$,
$\mathcal{E}_f$	linear kernel of a Boolean function f,
$RM(r,n)$	Reed–Muller code of order r and length 2^n,
$\rho(r,n)$	covering radius of $RM(r,n)$,
β_f	the symplectic form associated to a quadratic function f,
$\widetilde{f}$	dual of a bent Boolean function (Definition 51, page 197),
$\mathcal{M}$	Maiorana–McFarland's class,
$\mathcal{PS}$	partial spread class,
L^*	adjoint operator of a linear automorphism L,
$Im(F)$	the range (*i.e.*, image set) $F(\mathbb{F}_2^n)$ of an (n,m)-function,
$An(f)$	the $\mathbb{F}_2$-vector space of annihilators of a Boolean function f,
$An_d(f)$	restriction of $An(f)$ to those functions of algebraic degree at most d,
$B_{k,l}(f)$	$= \{g \in \mathcal{BF}_n;\ d_{alg}(g) \le k \text{ and } d_{alg}(fg) \le l\}$,

f	defined by $f(x) = \mathrm{f}(w_H(x))$, when f is symmetric,
$\sigma_i(x)$	elementary symmetric Boolean fct., of ANF: $\bigoplus_{I\subseteq\{1,\dots,n\}/\ \lvert I\rvert=i} x^I$,
$S_i(x)$	elementary symmetric pseudo-Boolean fct. NNF: $\sum_{I\subseteq\{1,\dots,n\}/\ \lvert I\rvert=i} x^I$,
δ_F	differential uniformity of an (n,m)-function F,
Nb_F	imbalance of an (n,m)-function (see page 113),
NB_F	derivative imbalance of an (n,m)-function (see page 138),
$\mathbf{x}$	a sharing of x (see page 436),
$\mathbf{F}$	a threshold implementation of function F (see page 436),
$E_{n,k}$	$= \{x \in \mathbb{F}_2^n;\ w_H(x) = k\}$,
$w_H(f)_k$	Hamming weight of the restriction of function f to $E_{n,k}$,