A Complete Bibliography of Publications in Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA
Tel: +1 801 581 5254
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/

02 October 2019
Version 1.06

Title word cross-reference

(1 - 2u^3) [185]. (4n, 2, 4n, 2n) [225].
(n, n - 1) [240]. (n, n - 2) [240]. (p^n, p^n, p^n, 1) [35]. (r, \leq 2) [15]. (x^{pm} - x + \delta)^s + x^{pm} + x [237]. 1 [273, 174]. 105 [129]. 128 [288]. 2 [244, 243, 142, 203, 273, 182, 231, 293]. 22 [232]. 24k + 10 [310]. 2k [172]. 2^n [138, 191]. 3 [236]. 30 [68]. 4 [240, 181, 179, 163]. 4k + 2 [310]. 4 \times 4 [89]. 5 [173]. 6 [277, 26, 186]. 8 [240]. a [209]. C^* [301]. C_n \times Q_8 [225]. cx + Tr_{q'/q}(x^n) [235]. \ell [143]. \ell^p x^n [104]. f^n [69]. F_p [292].
F_p[u, v]/\langle u^2 - 1, v^3 - v, uv - vu \rangle [292].
GF(2^k) [18]. GF(2^n) [44]. GF(l) [124]. k [148, 7]. l [10]. L_1 [272]. L_1(x^3) + L_2(x^3) [272]. L_2 [272]. m [188]. M_2(F_2 + uF_2) [265].

-adic [231, 293]. -ary
[244, 326, 276, 260, 343, 150, 165]. -byte
232. -constacyclic [185]. -divisibility
243. -error [148, 7]. -Feistel [209]. -fold
182, 102. -functions [240]. -generator
174. -identifying [15]. -polynomial [128].
-relative [225, 35]. -separable [181].

16 [294].
2 [329]. 256 [216].
64 [91].
7 [75].
8 [294]. 80 [86].

Abelian [324, 45]. absolute [304].
Absorbing [342]. accelerator [63]. access [194]. achieving [160]. active [152].
addition [138, 191].adic [231, 293].
against [86, 257, 114]. algebra [111].
approximation [191]. arbitrary [269]. array [123]. arrays [80, 202, 111, 113, 65].
ary [244, 326, 276, 260, 343, 150, 165].
assisted [206]. associated [243].
Asymptotic [19, 82]. Asymptotically [181, 323, 113]. Asynchronous [290].
Autocorrelations [10]. automata [41, 274]. automatic [258]. Average [134].
Backtracking [206].
beyond-birthday [249].
Birthday [215, 257, 249]. bit [333, 212]. bits [97].
BKW [141]. Block [71, 147, 99, 249].
blockchain [217]. blockcipher [106].
blockcipher-based [106]. BLS [208].
boolean [140, 243, 107, 43, 50, 132, 271, 277, 19, 261, 144, 126, 82, 151, 175, 92, 47, 70, 275, 320, 46, 156, 88, 61, 325]. both [100].
bound [215, 257, 160, 249, 320, 293].
boundary [112]. Bounds [72, 267, 236, 328, 247, 290, 23, 312, 6, 326, 15, 288]. boxes [48, 95, 137, 313, 178, 274, 298, 89].
burn [254]. burn-in [254]. byte [232, 339].

CAR30 [68]. cases [112, 14]. CAST [216].
Character [197]. characterising [171].
Characteristic [246, 269, 203, 235, 279, 69, 308, 131].
Characterization [107]. characterizations
deviation [209]. diagrams [302].
Difference [322, 225, 307, 35, 239].
Differential
[267, 129, 86, 321, 55, 96, 171, 189, 139].
differentially [240, 179]. differing [67, 85].
diffusion [183]. digit [246]. digit-sum [246].
digital [51]. dimension [126, 26].
dimensions [27]. Ding [337, 124].
Ding-Helleseth [124].
distinctness [142].
distinguisher [250]. distinguishing [75, 5, 47, 12].
distribution [241, 231, 242, 221, 170, 282].
distributions [177, 97]. divisibility [112, 243].
domain [119]. double [106]. doubly [113]. dual
[345, 310, 317, 104, 127, 228, 220, 287].
duals [136].

EA [44]. EA-equivalent [44]. Eastman
[197]. edge [85]. Editorial
[132, 271, 295, 1, 94, 204, 20, 76, 52, 248].
Efficient [210, 46, 61]. eigenanalysis [151].
eight [337]. elements [158, 304, 282].
elliptic [98]. encoding [123]. encryption
[207, 147, 213, 87]. engineering [99].
Enhanced [139]. ensemble [130]. entropy
[217]. Enumeration [228, 19].
enumerators [264, 190, 166, 311, 167].
equal [102]. Equivalence
[66, 35, 126, 321, 24]. equivalent [44].
Error [300, 39, 180, 6, 326, 148, 7, 331].
error-correcting [326]. errors
[310, 79, 235, 279]. Exact [243, 231].
existence [120]. Exotic [24]. expander
[210]. Expansion [187]. Explicit [267, 330].
exponential [243]. exponents
Extended [114, 98, 335]. extender [119].

Factorization [9, 302]. families
[307, 136, 113]. family [202, 83, 96, 8, 329].
fast [54, 46, 171, 61]. Faster [232]. Fault
[51, 255, 101, 96, 189]. FCSR [41, 6].

FCSRs [183]. feedback [230]. feedbacks
[57, 121]. Feistel [42, 209]. Fermat
[43, 203]. few [37, 280, 162, 164]. Fibonacci
[180]. field [304, 297]. fields
[327, 269, 223, 198, 125, 9, 235, 289, 279, 187,
155, 228, 308, 131, 168]. filtering [241].
Finding [62]. finite
[342, 304, 269, 23, 198, 125, 9, 235, 289, 279,
187, 297, 155, 228, 308, 131, 168]. FIRE
[99]. Five [266, 343]. flat [325]. flexible
[233]. fold [102, 182]. form
[92, 235, 289, 237]. forms [167]. formula
[172]. formulae [228]. four [150, 165].
Fourier [33]. Fourier-analytic [33].
framework [189]. free [78, 93, 130, 110].
Frequency [314, 188, 40, 229, 200].
Frequency-hopping [314, 188, 229, 200].
function [144, 92, 44, 179, 88]. Functions
[116, 158, 240, 43, 218, 50, 140, 37, 66, 132,
271, 277, 19, 261, 243, 126, 82, 157, 151, 175,
17, 321, 262, 160, 47, 340, 273, 64, 134, 107,
103, 135, 70, 276, 260, 136, 162, 275, 16, 46,
284, 45, 171, 156, 88, 220, 139, 196, 343, 272,
61, 201, 325, 131, 165, 239, 168]. Further
[136, 108, 121, 338].

G [173]. gaps [73]. General [116, 39, 253].
gereralizations [301, 75]. Generalized
[233, 116, 154, 200, 184, 198, 125, 160, 186,
74, 337, 14, 189, 268, 170, 174, 42]. generate
[336]. generating [214, 340, 273].
generation [81, 137].
generation/correlation [81]. generator
[174]. generators [53, 241]. Generic
[209, 162, 149, 239]. genetic [137].
geometries [342]. GGHN [13]. girth [299].
Good [245, 172, 137, 314, 270]. Goppa
[159]. grain [252, 96, 129]. grain-like [252].
graph [130]. graphical [84]. graphs
[67, 85, 299, 210, 312]. gray [93, 224].
greedy [169]. grid [15]. groups [120].
Grover [144]. Guest [94, 20, 52, 248].

Hadamard


Jacobi [293]. Joint [2, 148].


Multidimensional [47, 91, 253].
multinomials [34]. Multiple
[267, 213, 253].
multiple/multidimensional [253].
multiplication [206]. Multiplicative
[89, 277, 35, 97]. multisecret [192].
multisequence [148]. multisequences
[2, 230]. multivariate [16]. mutual [211].
Mutually [27, 26, 77]. mystery [316].
Near [322, 79, 201, 229]. near-bent [201].
Near-Optimal [322, 229]. Necessary [116].
egnegabent [168]. negacyclic [172]. nested
[88]. Network [42]. NFSR [57, 121]. NGG
[12]. Niho
[259, 285, 199, 279, 305, 222, 338, 291]. Non
[45, 327, 244, 144, 324, 108, 234].
non-commutative [234]. non-cyclic [324].
non-overlapping [244]. non-prime [327].
non-randomness [108]. non-resiliency
[144]. nonbinary [233]. Nonlinear
[263, 48, 284, 318]. nonlinearities [17].
Nonlinearity
[156, 140, 261, 82, 333, 178, 275, 139, 57, 121].
normal [92]. normality [260]. note
[256, 287]. novel [336]. NTRUSign [51].
nulls [40]. number [304, 214]. numbers
[16, 154].
odd [193, 110, 27, 308, 131]. old [133].
on-line [215]. One [100, 67, 85, 39].
one-round [39]. ones [214]. online [249].
on [112, 133]. operations [147, 87, 97].
Optimal
[160, 312, 322, 83, 150, 181, 117, 188, 130,
153, 182, 266, 323, 281, 113, 231, 229, 200].
optimality [211]. orbit [324]. order
[17, 333, 186, 55, 337, 154, 124, 163, 288].
orders [28]. oriental [334]. oriented
[331]. orthogonal [27, 228]. other [100].
output [97]. overheads [281]. overlapping
[244]. overview [5].
pair [341, 242]. pairing [101]. pairs
[81, 232]. PAM [40]. parallel [109].
parallel-cut [109]. parameters [83].
parametrized [226]. Paraunitary [81].
partial [36, 33]. particular [93].
partitioned [93, 307]. Perfect
[80, 225, 233, 79, 111, 102, 135, 182].
perfectly [39]. period [148, 254, 318, 229].
Periodic [309, 6, 113]. periods [233].
Permutation [44, 235, 40, 259, 285, 199,
permutations [136, 297, 284, 179]. phase
[72]. planar [218, 135]. PN [34]. POEx
[215]. points [171]. Poly [300]. Polynomial
[227, 269, 128, 69]. polynomials
[159, 219, 18, 335, 44, 235, 289, 16, 237].
power [30, 27, 229]. practicability [211].
proscribed [304, 214]. presemifields [158].
PRESENT [86]. PRESENT-80 [86].
prime [327, 126, 186, 30, 27, 163, 10, 229].
prime-power [229]. primitive
[142, 263, 110, 282, 330]. primitives [100].
privacy [114]. private [114]. Probabilistic
[189]. probabilities [102]. probability
[153, 253]. problem [273, 26]. problems
[133]. product [219, 238]. profile [118].
profiles [335]. Progress [21]. projection
[64]. properties
[255, 42, 143, 137, 153, 96, 88, 49]. property
provable [257]. proven [49]. proving [256].
Pseudorandom [16]. pseudorandomness
[258]. public [301]. public-key [301].
QAM [81]. Quadratic
[224, 37, 134, 185, 167]. Quantum
[292, 238, 334, 268]. quartic [286]. Quasi
[159, 135, 322, 125, 317, 228, 174].
Quasi-Complementary [322].
Quasi-cyclic [159, 125, 228, 174].
Quasi-perfect [135]. quasi-twisted [317].
Quaternary [64, 184, 117, 153, 283, 220, 38].
quaternions [80, 225]. quotients [43].
References


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Kamal:2012:FAN


Maitra:2012:GE


Canteaut:2012:CAC


Aagren:2012:SFC


Knellwolf:2012:HOD


Dinur:2012:ACA


Turan:2012:NML

[58] Leonie Simpson and Serdar Boztas. State cycles, initialization and the
REFERENCES


Lu:2012:SLA


Orumiehchiha:2012:CWL


Wang:2013:CDB


Gupta:2013:DIA


Jadda:2013:QCB


delaCruz:2013:CIS

REFERENCES


Maura B. Paterson and Douglas R. Stinson. A simple combinatorial treat-
REFERENCES

18


Leducq:2013:SWC


Gong:2013:RDA


Helleseth:2014:SIE


Wu:2014:CCU


Bajic:2014:SSC


Hariharan:2014:NNP


Acevedo:2014:PAU


Budisin:2014:PGC

[81] S. Z. Budišin and P. Spasojević. Paraunitary generation/correlation of

Dib:2014:ANV


Mandal:2014:OPW


Gao:2014:SSS


Charon:2014:MSI


Emami:2014:RP


Sarkar:2014:MOE


Shan:2014:CPN

REFERENCES

Zajac:2014:MCB


Bay:2014:RIA


Zhu:2014:MMM


Gong:2014:CWC


Bernini:2014:PPG


Carlet:2015:GE


Bilgin:2015:TIS


Mazumdar:2015:CRI

REFERENCES


[103] Chengju Li and Qin Yue. The Walsh transform of a class of monomial functions and cyclic codes. *Cryptography and Communications*, 7(2):217–228, June 2015. CODEN ????. ISSN 1936-2447 (print), 1936-2455
REFERENCES


REFERENCES

Castro:2015:DAO

Castro:2015:DAO

Ortiz-Ubarri:2015:NFA

Ortiz-Ubarri:2015:NFA

Swanson:2015:ERP

Swanson:2015:ERP

Chakraborty:2015:ALX

Chakraborty:2015:ALX

Hodzic:2015:GBF

Hodzic:2015:GBF

Edemskiy:2015:LCB

Edemskiy:2015:LCB

He:2015:LCP

He:2015:LCP


Thomas W. Cusick and Pantelimon Stănică. Counting equivalence classes for monomial rotation symmetric Boolean functions with prime dimen-
REFERENCES


REFERENCES


27


[149] Can Xiang. Linear codes from a generic construction. Cryptogra-
REFERENCES

Xu:2016:OAC


Dravie:2016:MRV


Chin:2016:TBS


Jang:2016:LLP


Wang:2016:GCN


Sharma:2016:CCF


Schmidt:2016:NMR

REFERENCES


Xu:2017:TCA


Yang:2017:CTW


Zhang:2017:CWE


Zhou:2017:CNF


Li:2017:SRG


Wang:2017:CDG


Salagean:2017:CCF


Bandi:2017:MFN

Rama Krishna Bandi, Maheshanand Bhaintwal, and Nuh Aydin. A mass formula for negacyclic codes.
REFERENCES


[188] Hongyu Han, Dajiyuan Peng, and Udaya Parampalli. New sets of optimal low-hit-zone frequency-hopping sequences...

Sarkar:2017:PSB


Wang:2017:CWE


Xue:2017:BLA


Laing:2017:LMS


Cao:2017:CCO


Wang:2017:SSS


Shi:2017:TTW


Tang:2017:CHB


Alaca:2017:CVS


REFERENCES


CODEN ????? ISSN 1936-2447 (print), 1936-2455 (electronic). URL

[222] Gaojun Luo, Xiwang Cao, Shanding Xu, and Jiafu Mi. Binary linear
codes with two or three weights from Niho exponents. Cryptography and
Communications, 10(2):301–318, March 2018. CODEN ????? ISSN 1936-2447

[223] Cunsheng Ding. A sequence construction of cyclic codes over finite
CODEN ????? ISSN 1936-2447 (print), 1936-2455 (electronic). URL
http://link.springer.com/article/10.1007/s12095-017-0222-0.

[224] Mokshi Goyal and Madhu Raka. Quadratic residue codes over the ring
$F_p[u]/(u^m - u)$ and their Gray images. Cryptography and Communications,

[225] Santiago Barrera Acevedo and Heiko Dietrich. Perfect sequences over the
quaternions and $(4n,2,4n,2n)$-relative
difference sets in $C_n \times Q_8$. Cryptography and Communications, 10(2):

[226] Andrew Klapper. Matrix parametrized shift registers. Cryptography and
Communications, 10(2):369–382, March 2018. CODEN ????? ISSN 1936-2447


[228] Anuradha Sharma and Taranjot Kaur. Enumeration formulae for self-dual,
self-orthogonal and complementary-
dual quasi-cyclic codes over finite
38 REFERENCES


[244] Elena Barucci, Antonio Bernini, Stefano Bilotta, and Renzo Pinzani. A

Jitman:2018:GIS


Tuxanidy:2018:CDS


Galvez:2018:SBB


Maitra:2018:GE


Jha:2018:RBB


Cui:2018:SID


Paterson:2018:SAC


REFERENCES

Shi:2018:SQM


Chang:2018:CSL


Jitman:2018:CGI


Budaghyan:2019:ESIa


Villa:2019:AFL


Idrisova:2019:AGA


Mariot:2019:CAB


Mesnager:2019:NBF

[275] Sihem Mesnager, Zhengchun Zhou, and Cunsheng Ding. On the nonlinearity of Boolean functions with restricted
REFERENCES


Mandal:2019:NCA


Calik:2019:MCV


Boyar:2019:SLD


Li:2019:NPT


Liu:2019:SNC


Martinez-Penas:2019:USR


Wang:2019:IDE


Michel:2019:SNB

[283] Jerod Michel and Qi Wang. Some new balanced and almost balanced quaternary sequences with low autocor-

Pasalic:2019:BFN


Deng:2019:MCP


Geil:2019:AVC


Yan:2019:NCM


Wang:2019:NBC


Li:2019:CIP


Gao:2019:UBC


Wu:2019:SCP


REFERENCES


Chen:2019:EAW


Felke:2019:SBP


Raddum:2019:FUB


Zinoviev:2019:CKS


Bojilov:2019:CNF


Li:2019:SAN


Klove:2019:CLT


Buratti:2019:HPD


Dey:2019:SMR


Qian:2019:SDL


Xiao:2019:BSP


Wang:2019:DCC


Oblaukhov:2019:LBS


Gorodilova:2019:DEA


Li:2019:CNO


Luo:2019:TCA

REFERENCES


REFERENCES


Gao:2019:SBR


Hofer:2019:ONC


Naghipour:2019:NCQ


Johnsen:2019:RPE


Garcia:2019:NMD


Liang:2019:LCD


Wang:2019:FRP


Radonjic:2019:ICC


Hodzic:2019:IML


Guneri:2019:CCL


Beemer:2019:ASC


Tang:2019:RAB