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/`

10 August 2024
Version 1.14

Title word cross-reference

(-1) [519]. $(1-2u^3)$ [185]. $(17,4,5)$ [622, 598]. $(4n,2,4n,2n)$ [225]. $(k,R,1)$ [428]. $(n,n-1)$ [240]. $(n,n-2)$ [240]. $(p^n,p^n,p^n,1)$ [35]. $(q^m+1)/\lambda$ [682]. $(r,\leq 2)$ [15]. (σ,δ) [453]. $(x^{pm}-x+\delta)^s+x^{pm}+x$ [237]. 1 [273, 174]. 105 [129]. 128 [288]. 16 [381]. $1\frac{1}{2}$ [357]. 2 [244, 243, 142, 203, 273, 182, 654, 231, 293, 403, 438]. 22 [232]. $24k+10$ [310]. 2^k [172, 430]. 2^n [138, 191]. $2p^n$ [521]. $2p^s$ [439]. 3 [236]. 30 [68]. 4 [240, 432, 181, 179, 163]. $4k+2$ [310]. $4N$ [488]. 4×4 [89]. 5 [173]. 6 [277, 26, 186]. 8 [240]. $8q$ [509]. $[1,0]$ [688]. ^{2} [468]. a [209]. B_2 [667]. c [565, 567, 452, 490]. C^* [301]. $C_n\times Q_8$ [225]. $cx+\mathbf{Tr}_{q^l/q}(x^a)$ [235]. d [404]. ℓ [143]. $\ell^t p^s$ [104]. f^d [373]. f^v [69]. F_p [292]. $F_p[u,v]/\langle u^2-1,v^3-v,uv-vu\rangle$ [292]. G [474]. $G(X)^k-L(X)$ [451]. GF(2^k) [18]. GF(2^n) [44]. GF(l) [124]. GF(q) [645]. $GR(4,m)$ [669]. j [467]. k [148, 7]. l [563, 10]. L_1 [272]. $L_1(x^3)+L_2(x^9)$ [272]. L_2 [272]. m [188, 385, 550]. $M_2(\mathbf{F}_2+u\mathbf{F}_2)$ [265]. $M_4(\mathbf{F}_2+u\mathbf{F}_2)$ [554, 553]. $\mathbf{F}_{2^s}$ [470]. $\mathbf{F}_2^n$ [609, 412]. $\mathbf{F}_2^{n+1}$ [609]. $\mathbf{F}_2\times(\mathbf{F}_2+v\mathbf{F}_2)$ [457, 444]. $\mathbf{F}_{5^n}$ [291]. $\mathbf{F}_p$ [398, 502]. $\mathbf{F}_p+u\mathbf{F}_p$ [195]. $\mathbf{F}_p[u]/\langle u^m-u\rangle$ [224]. $\mathbf{F}_p[u]/\langle u^4-u\rangle$ [185]. $\mathbf{F}_{p^m}$ [242]. $\mathbf{F}_{p^m}+u\mathbf{F}_{p^m}+u^2\mathbf{F}_{p^m}$ [439]. $\mathbf{F}_q$ [549, 682]. $\mathbf{F}_q+u\mathbf{F}_q$ [360]. $\mathbf{F}_{q^2}$ [616]. $\mathbf{F}_{q^2}+u\mathbf{F}_{q^2}$ [513]. $\mathbf{F}_{q^2}+v_1\mathbf{F}_{q^2}+\cdots+v_r\mathbf{F}_{q^2}$ [581]. $\mathbf{F}_{q^n}$ [662]. $\mathbf{F}p^{2m}$ [237]. $\mathbf{P}^3$ [203]. $\mathbf{Q}$ [523]. $\mathbf{R}$ [523]. $\mathbf{Z}_{2^m}$ [127]. $\mathbf{Z}_2\mathbf{Z}_2[u,v]$ [388]. $\mathbf{Z}_4$ [560, 184, 160, 170, 174]. $\mathbf{Z}_4+u\mathbf{Z}_4$

[172, 430, 453]. $\mathbf{Z}_4 + u\mathbf{Z}_4 + v\mathbf{Z}_4$ [621]. $\mathbf{Z}_4[v]/\langle v^2 + 2v\rangle$ [377]. $\mathbf{Z}_{p^2} + u\mathbf{Z}_{p^2}$ [529]. $\mathbf{Z}_{\mathbf{p}}\mathbf{e}$ [282, 330]. $\mathbf{Z}_{p^k}$ [350]. $\mathbf{Z}_p\mathbf{Z}_{p^s}$ [374]. $\mathbf{Z}/(p^e q)$ [142]. $B_{j,k}$ [474]. $\max(R) = 3$ [428]. N [386, 318]. $N-2$ [318]. $n = \frac{q^{2m}-1}{2}$ [369]. $\overline{2}$ [181]. $\overline{3}$ [236]. p [502, 276, 260, 538, 427, 343, 150, 165, 626]. p^n [521, 148]. pq [184, 38]. pq^2 [456]. q [244, 262, 326, 128, 645]. $q-1$ [662]. r [333]. $R[X]/\langle f(X)^{p^s}\rangle$ [606]. S [421, 462]. σ [668]. t [424, 492, 102, 241, 447, 533]. τ [624, 580]. $x + x^{2^l} + \cdots + x^{2^{ml}} = a$ [412]. $x^{2^l+1} + x + a$ [18]. $x^r(1 + ax^{s_1(q-1)} + bx^{s_2(q-1)})$ [616]. $x^r h(x^s)$ [289]. Z [629, 482, 647, 683, 540]. $Z_4[u]/\langle u^k\rangle$ [193]. $Z_r = r$ [316].

-additive [388, 374]. **-adic** [231, 293, 403, 438]. **-ary** [244, 326, 276, 260, 538, 427, 343, 150, 165]. **-boomerang** [567]. **-boxes** [421]. **-byte** [232]. **-codes** [474]. **-complementary** [683, 540, 629, 482, 647]. **-complementary/complementary** [540]. **-constacyclic** [185]. **-D** [654]. **-designs** [424, 492, 533]. **-differential** [565, 452, 490, 519]. **-divisibility** [243]. **-error** [148, 7]. **-errors** [580]. **-Feistel** [209]. **-fold** [182, 102]. **-functions** [240]. **-generator** [174]. **-identifying** [15]. **-intersection** [563]. **-invariant** [467]. **-Linearized** [502]. **-metric** [624]. **-packings** [428]. **-PD** [462]. **-periodic** [456]. **-polynomial** [128]. **-QAM** [381]. **-relative** [225, 35]. **-separable** [181]. **-sequences** [143, 188, 385, 550, 170, 10]. **-Skew** [453]. **-strongly** [236]. **-th** [333, 386]. **-to-** [273]. **-transform** [262]. **-tuple** [241]. **-twisted** [688]. **-uniform** [240, 432, 179]. **-variable** [277]. **-wise** [447].

0 [639]. **0-APN** [639].

16 [294].

2 [329]. **2-Adic** [488, 509]. **2-designs** [461, 511]. **2-rotation** [572]. **2-weight** [594, 593]. **256** [216]. **2D** [661]. **2D-ZCACS** [661].

3-weight [594, 593].

4-adic [674].

64 [91].

7 [75].

8 [294]. **8-bit** [475]. **80** [86].

9 [430].

abelian [455, 324, 45, 690]. **absolute** [304]. **Absorbing** [342]. **accelerator** [63]. **access** [194]. **ACD** [532]. **achieving** [160]. **actions** [652]. **active** [152]. **addition** [138, 491, 191, 421]. **additive** [423, 574, 388, 374]. **Adic** [488, 509, 674, 231, 293, 403, 438]. **adversary** [39]. **AEAD** [531]. **AEAQECCs** [563]. **AES** [99, 250, 4, 471, 441]. **AES-like** [250, 99, 4, 441]. **Affine** [657, 296, 494, 286, 18, 335, 511, 524, 690]. **affine-invariant** [511]. **again** [415]. **against** [86, 257, 114]. **algebra** [111]. **Algebraic** [440, 240, 357, 92, 138, 70, 481, 572, 46, 641, 88, 634, 347, 61, 230]. **algebras** [690]. **algorithm** [144, 273, 232, 531, 36]. **algorithms** [468, 640, 591, 137, 512]. **Almost** [408, 322, 427, 649, 459, 335, 111, 670, 534, 577, 482, 283, 637, 231, 347]. **almost-optimal** [670]. **alphabet** [244]. **alphabets** [233, 583]. **analog** [627]. **Analysis** [623, 254, 141, 300, 475, 458, 252, 51, 678, 59, 209, 601, 8, 189, 211]. **analytic** [33]. **and/or** [643]. **aperiodic** [518, 676, 675, 582, 314]. **APN** [546, 37, 394, 517, 414, 345, 494, 570, 321, 273, 346, 495, 639, 587, 135, 416, 592, 609, 272, 508, 131, 519, 571]. **Application** [144, 507, 42, 250, 460, 9, 647, 490]. **applications** [526, 278, 132, 344, 271, 413, 489, 564, 633, 583, 475, 332, 105, 76, 378, 21, 478, 563, 273, 270, 245, 547, 305, 652, 183, 59, 146, 649, 154, 373, 513, 91]. **Applying** [56, 500]. **approach** [41, 112, 125, 634, 33]. **approaches** [587]. **approximate** [454, 528]. **approximation** [191]. **arbitrary** [560, 269, 605]. **arising** [354]. **arithmetic** [399]. **array** [661, 613, 123, 654, 687]. **arrays** [80, 658, 202, 111, 113, 65]. **ary** [244, 326, 276, 260, 538, 427, 343, 150, 165]. **Ashikhmin** [476]. **aspects** [615]. **assisted** [499, 498, 206]. **associated** [243, 611, 448]. **asymmetric** [555, 477, 372, 371]. **Asymptotic** [19, 82]. **Asymptotically** [181, 323, 113, 410, 574, 436, 374]. **Asynchronous** [290]. **attack** [98, 216, 458, 12, 96, 109, 91, 473]. **Attacking** [527]. **Attacks** [106, 54, 90, 53, 255, 152, 99, 56, 101, 86, 75, 257, 5, 47, 138, 55, 681, 209, 251, 171, 8]. **authenticated** [147]. **Authentication** [227, 147, 23, 102, 182, 87]. **authorization** [644]. **autocorrelation** [408, 233, 202, 117, 509, 674, 387, 283, 630, 665, 677, 231, 403, 649, 488, 38, 382]. **Autocorrelations** [10]. **automata** [41, 274]. **automatic** [258, 539]. **automorphisms** [417]. **Average** [134].

Backtracking [206]. **Backtracking-assisted** [206]. **balanced** [117, 493, 572, 283, 416, 612, 677, 347, 626, 239]. **Barg** [476]. **base** [484]. **Based** [227, 469, 184, 561, 152, 496, 101, 180, 84, 105, 188, 666, 555, 577, 106, 274, 636, 162, 473, 189, 472, 36, 230, 319, 596, 651, 550, 487]. **bases** [25, 26, 454, 27, 77]. **basic** [80]. **BBB** [561]. **BCH** [369, 367, 530, 375, 533, 682, 625]. **BCT** [569]. **beautiful** [31]. **behavior** [517, 452]. **behaviour** [134]. **Belov** [672]. **Bent** [158, 116, 284, 642, 658, 566, 353, 418, 160, 64, 491, 504, 417, 465, 352, 276, 260, 350, 538, 136, 162, 389, 354, 45, 556, 220, 551, 196, 343, 362, 201, 631, 131, 165, 522, 379, 433]. **bent-negabent** [551]. **best** [191]. **Beth** [152]. **between** [363, 643, 592, 508]. **beyond** [215, 257, 249]. **beyond-birthday-bound-secure** [215]. **beyond-the-birthday** [249]. **beyond-the-birthday-bound** [257]. **BGLS** [208]. **bias** [146]. **biased** [175]. **biases** [11]. **bifix** [78, 93]. **big** [273]. **bijective** [137, 608, 601, 656, 89, 421]. **Binary** [600, 629, 315, 222, 393, 318, 376, 623, 462, 521, 214, 247, 332, 567, 411, 64, 664, 148, 387, 525, 401, 535, 361, 622, 598, 476, 557, 302, 677, 231, 403, 383, 329, 523, 488, 687, 646, 456]. **binomials** [662]. **biquadratic** [301]. **birthday** [215, 257, 249]. **bit** [475, 333, 212]. **bits** [345, 97]. **bivariate** [555]. **BKW** [591, 141]. **BKW-style** [591]. **black** [472]. **Block** [71, 147, 99, 666, 573, 249, 528, 503, 441]. **blockchain** [217]. **blockcipher** [106]. **blockcipher-based** [106]. **BLS** [208]. **boolean** [623, 464, 140, 243, 107, 636, 347, 43, 50, 356, 132, 344, 271, 413, 394, 489, 564, 633, 277, 420, 19, 261, 144, 559, 126, 82, 640, 151, 175, 629, 92, 47, 460, 597, 70, 351, 275, 402, 493, 320, 46, 630, 556, 524, 641, 156, 88, 551, 619, 61, 325, 651, 687]. **boomerang** [434, 567, 520, 537]. **bordered** [366, 409]. **both** [100]. **bound** [614, 215, 257, 160, 249, 518, 648, 320, 476, 656, 293, 362]. **boundary** [112]. **Bounds** [635, 72, 667, 267, 236, 624, 328, 356, 247, 290, 23, 312, 6, 326, 602, 689, 407, 15, 654, 524, 288]. **box** [472]. **boxes** [48, 95, 569, 475, 137, 542, 313, 178, 441, 274, 608, 601, 298, 89, 421]. **BP** [123]. **BP-XOR** [123]. **Bracken** [569]. **Bruijn** [219, 241]. **burn** [254]. **burn-in** [254]. **burst** [372, 371]. **Butson** [658]. **butterfly** [345]. **byte** [232, 339, 372, 371]. **bytes** [11].

CAR30 [68]. **Carlitz** [478]. **Cartesian** [391]. **cases** [112, 14]. **CAST** [216]. **CAST-256** [216]. **Categorizing** [470]. **CCZ** [363, 459, 495, 620]. **CCZ-** [363]. **CCZ-equivalence** [495, 620]. **CCZ-inequivalence** [459]. **CDMA** [384, 670]. **cell** [670]. **Cellular** [274]. **central** [35]. **Certain** [399, 547]. **chain** [552, 545, 501, 317, 234, 690]. **Changing** [346]. **channel** [255, 458, 290, 472]. **Character** [197, 689]. **characterising** [171]. **Characteristic** [450, 246, 418, 269, 660, 415, 203, 686, 348, 235, 279, 534, 69, 308, 131]. **Characterization** [107, 686, 616, 398]. **characterizations** [23, 637]. **Characters** [490, 351]. **Cheating** [65]. **Cheating-immune** [65]. **Chebyshev** [544]. **check** [144]. **chi** [256, 636]. **chi-square** [256]. **Chinese** [125]. **Chu** [648]. **Chudnovsky** [468]. **cipher** [147, 68, 173, 215, 75, 119, 12, 13, 83, 60, 88, 49, 58, 650]. **ciphers** [99, 250, 4, 56, 63, 252, 257, 5, 249, 55, 9, 441, 96, 294, 87, 189, 487]. **circuits** [278]. **Circulant** [22, 483, 603, 214, 105, 312, 360]. **circulant-like** [105]. **Circular** [627]. **class** [259, 583, 180, 686, 348, 134, 186, 504, 479, 103, 397, 511, 535, 350, 331, 618, 556, 677, 231, 242, 403, 375, 221, 196, 362, 308, 446, 164, 558, 166, 311, 487]. **Classes** [515, 464, 66, 394, 414, 353, 184, 660, 126, 285, 35, 588, 662, 177, 610, 199, 182, 280, 401, 264, 266, 352, 276, 7, 334, 486, 476, 594, 593, 190, 431, 291, 165, 229, 438, 625]. **classical** [158, 303]. **Classification** [638, 220, 541, 606, 377, 587]. **closed** [334]. **co** [304]. **co-trace** [304]. **coalitions** [114]. **cocyclic** [29, 658]. **Code** [629, 122, 244, 469, 450, 336, 638, 663, 361, 622, 598, 405, 383, 288, 651, 688]. **code-based** [469]. **codebooks** [160, 323, 436]. **coded** [40]. **Codes** [600, 437, 507, 306, 624, 457, 444, 364, 498, 376, 541, 292, 327, 78, 172, 328, 463, 342, 400, 445, 93, 159, 617, 552, 621, 193, 377, 430, 560, 668, 67, 85, 462, 181, 470, 324, 579, 578, 157, 223, 492, 496, 545, 583, 603, 366, 474, 180, 669, 536, 667, 247, 84, 125, 332, 357, 286, 409, 224, 341, 369, 595, 666, 315, 310, 461, 177, 573, 130, 411, 563, 586, 610, 23, 672, 599, 501, 549, 428, 335, 312, 423, 568, 664, 186, 562, 547, 479, 529, 326, 503, 74, 102, 103, 135, 161, 367, 396, 422, 530, 604, 605, 602, 684, 182, 178]. **codes** [238, 280, 401, 511, 535, 222, 265, 264, 266, 128, 477, 442, 453, 585, 162, 643, 334, 309, 510, 410, 407, 476, 554, 553, 123, 15, 317, 448, 594, 593, 331, 339, 372, 371, 185, 447, 14, 607, 440, 104, 155, 127, 228, 574, 195, 268, 388, 359, 360, 480, 532, 671, 234, 548, 439, 628, 242, 375, 221, 590, 190, 176, 163, 319, 431, 446, 497, 581, 645, 174, 543, 673, 685, 149, 164, 443, 533, 631, 150, 165, 513, 522, 287, 166, 311, 646, 374, 690, 167, 236, 449, 682, 625, 65, 499]. **codewords** [74]. **coding** [526, 255, 270, 245, 652, 281, 596]. **coefficient** [690]. **coefficients** [92]. **coherence** [395]. **Cohn** [197]. **collection** [329]. **colliding** [232]. **collision** [98, 232]. **combination** [53]. **Combinatorial** [424, 23, 680, 587, 73, 8]. **Comments** [61]. **Commun** [430]. **communication** [173, 281]. **Communications** [1]. **commutative** [34, 547, 234, 690]. **Comparing** [612]. **compartmented** [194]. **Complementary** [600, 629, 322, 364, 376, 81, 613, 341, 315, 663, 683, 577, 482, 425, 654, 228, 540, 647, 77, 651, 687, 381]. **complementary-dual** [228]. **complementary/complementary** [540]. **Complete** [377, 99, 686, 177, 264, 616, 190, 311, 167, 290, 479, 663, 590, 166]. **completed** [504]. **complex** [25, 24]. **complexes** [607]. **Complexity** [267, 505, 468, 356, 277, 420, 184, 117, 198, 521, 509, 2, 591, 118, 484, 542, 674, 6, 148, 337, 7, 187, 69, 656, 231, 293, 403, 386, 523, 124, 318, 488, 438, 626, 89, 406]. **component** [435]. **component-wise** [435].

components [218, 418]. **composition** [370, 329]. **Compositional** [289]. **compressed** [395, 319, 282]. **compressing** [110, 330]. **computational** [469]. **Computing** [304, 92, 69, 438, 146]. **concatenated** [341]. **concatenation** [313]. **Concrete** [572]. **concurrent** [152]. **Conditional** [129]. **Conditions** [116]. **conflict** [445]. **congruential** [527]. **conjecture** [546, 112, 358]. **conjectures** [133, 387]. **connection** [10]. **connectivity** [567]. **consisting** [2]. **consta** [690]. **consta-Abelian** [690]. **constacyclic** [579, 578, 583, 185, 104, 155, 359, 439, 375, 581, 645, 625]. **constant** [573, 503, 622, 598, 510]. **constraints** [113]. **construct** [239, 200]. **Constructed** [556, 259, 153, 313, 543, 673]. **Constructing** [566, 131, 571, 583, 573, 465]. **Construction** [219, 570, 462, 629, 116, 599, 501, 664, 322, 96, 127, 220, 38, 78, 463, 48, 560, 324, 223, 661, 341, 655, 380, 528, 576, 663, 683, 670, 102, 161, 390, 604, 183, 162, 510, 653, 77, 149]. **Constructions** [240, 577, 298, 168, 499, 498, 395, 72, 366, 536, 667, 290, 409, 503, 422, 602, 684, 70, 518, 323, 477, 136, 493, 572, 368, 73, 637, 628, 319, 436, 488, 651, 287, 236, 449, 680, 200, 381]. **containing** [530, 581]. **Contemporary** [643]. **context** [90]. **continued** [523]. **conversely** [284]. **convolutional** [309]. **cookie** [251]. **Correcting** [430, 180, 306, 326, 477, 361, 331, 339, 372, 371]. **Correction** [457, 499, 579, 270, 676, 622, 554, 594, 372]. **Correlation** [53, 262, 54, 98, 81, 19, 506, 613, 385, 118, 333, 153, 663, 518, 676, 675, 659, 113, 170, 398, 653, 582, 379, 314]. **correlation-immune** [19, 398]. **correlations** [654, 393]. **cosets** [638]. **cost** [458]. **Costas** [627]. **Counting** [126, 171, 134, 33]. **covering** [328, 145, 288]. **CRC** [227]. **criteria** [4, 139]. **criterion** [29]. **cross** [78, 93, 683, 659, 654, 653, 393].

cross-bifix-free [78, 93]. **cross-correlation** [659, 653]. **cross-correlations** [654]. **crosscorrelation** [677]. **Cryptanalysis** [207, 531, 60, 294, 267, 487, 129, 296, 46, 253, 61]. **Cryptogr** [430]. **Cryptographic** [42, 175, 620, 88, 421, 256, 278, 640, 137, 64, 597, 422, 183, 146, 96, 643, 634]. **Cryptographically** [227, 105, 139]. **Cryptography** [295, 101, 204, 1]. **cryptosystems** [301]. **cube** [56, 320]. **CubeHash** [59]. **cubic** [50, 66, 402, 584]. **cumulative** [65]. **curves** [451, 505, 98, 527, 562, 467]. **Cusick** [112]. **cut** [109]. **cycle** [269, 373]. **cycles** [58]. **Cyclic** [193, 186, 265, 553, 234, 292, 159, 617, 621, 377, 560, 324, 223, 545, 125, 357, 177, 610, 501, 529, 103, 535, 477, 453, 585, 228, 359, 242, 590, 163, 497, 174, 685, 150, 374, 449, 554]. **cyclotomic** [184, 521, 186, 337, 486, 154, 438, 626]. **cyclotomy** [198, 480, 163].

D [244, 654, 609]. **D-property** [609]. **Data** [267, 257]. **DDT** [569]. **deception** [102]. **Deciding** [514]. **Decimated** [385, 550]. **decimations** [659]. **decision** [302]. **decodable** [39]. **decoding** [423, 568]. **Decomposition** [297, 340]. **decompositions** [486, 584]. **decorrelation** [90]. **defined** [34]. **degree** [240, 404, 641]. **degree-** [404]. **degrees** [123]. **delay** [183]. **Delsarte** [614]. **density** [28]. **depth** [278]. **derivatives** [433]. **derived** [43, 505, 352, 539, 221, 282, 456]. **descendants** [307]. **Design** [198, 252, 441, 640, 20, 46, 647, 61]. **Designed** [367]. **Designing** [63]. **designs** [424, 492, 461, 528, 511, 533]. **detection** [440]. **determinants** [9]. **determine** [7]. **Determining** [148]. **Deterministic** [319, 395]. **developments** [128]. **deviation** [209]. **devices** [466]. **diagrams** [302]. **Difference** [322, 225, 408, 307, 35, 455, 239].

differences [355]. **Differential** [542, 520, 636, 267, 370, 429, 129, 565, 635, 86, 415, 321, 55, 534, 96, 681, 537, 171, 189, 452, 490, 656, 139, 519, 558]. **differentially** [240, 179]. **differing** [67, 85]. **diffusion** [183]. **digit** [246]. **digit-sum** [246]. **digital** [51]. **digits** [484]. **dimension** [126, 573, 26, 454, 503, 510]. **dimensional** [613, 410, 448, 671, 548]. **dimensions** [414, 605, 27]. **Ding** [337, 124, 438]. **Ding-Helleseth** [124]. **direct** [661, 576, 663, 683, 390]. **discrete** [333]. **distance** [336, 411, 396, 268, 242, 497, 150, 646]. **distance-optimal** [396, 646]. **distances** [529, 367]. **distinct** [614]. **distinctness** [426, 142]. **distinguisher** [250]. **distinguishing** [75, 5, 47, 12]. **distorted** [580]. **Distribution** [630, 450, 442, 241, 585, 231, 242, 221, 590, 170, 282]. **distributions** [177, 97]. **divisibility** [112, 243]. **division** [615]. **DNA** [445]. **domain** [119]. **Doppler** [647]. **Double** [409, 603, 106, 372, 371, 360]. **doubly** [113]. **DryGASCON** [531]. **dual** [444, 364, 376, 560, 496, 603, 366, 474, 536, 409, 595, 315, 310, 547, 417, 390, 530, 352, 317, 104, 127, 228, 360, 220, 628, 581, 287, 457]. **dual-containing** [530, 581]. **Duality** [595, 485]. **duals** [668, 136, 446, 497]. **dynamic** [644]. **dynamics** [559].

EA [363, 414, 495, 514, 44, 452]. **EA-** [495]. **EA-classes** [414]. **EA-equivalence** [514, 452]. **EA-equivalences** [363]. **EA-equivalent** [44]. **EAQECCs** [507, 513]. **Eastman** [197]. **edge** [85]. **Editorial** [132, 344, 271, 295, 413, 489, 564, 633, 1, 94, 204, 378, 20, 76, 52, 248]. **Efficient** [210, 486, 46, 61]. **eigenanalysis** [151]. **eight** [337, 405]. **elements** [158, 304, 532, 282]. **ElGamal** [612]. **elliptic** [98, 527, 467]. **embedded** [466]. **embedding** [516]. **Encoding** [568, 123]. **encryption** [207, 147, 213, 87, 596]. **engineering** [99]. **Enhanced** [139]. **ensemble** [130]. **entanglement** [499, 498, 513]. **entanglement-assisted** [499, 498]. **entropy** [217]. **Enumeration** [228, 19]. **enumerators** [617, 479, 264, 190, 166, 311, 167]. **equal** [102]. **equality** [614]. **Equivalence** [66, 35, 126, 321, 495, 514, 620, 592, 452, 24, 508]. **equivalences** [363]. **equivalent** [494, 44]. **erasure** [602]. **Error** [300, 39, 180, 6, 326, 148, 477, 7, 361, 331]. **error-correcting** [326, 477]. **errors** [145, 306, 339, 372, 371, 580]. **Espresso** [173]. **estimate** [521, 524]. **estimation** [641]. **Euclidean** [437]. **Euler** [456]. **Evaluation** [611, 471, 472]. **even** [560, 310, 79, 674, 576, 235, 279, 406]. **evolutionary** [650]. **Exact** [243, 231]. **existence** [120]. **Exotic** [24]. **expander** [210]. **Expansion** [187, 386]. **Explicit** [569, 267, 330]. **exponent** [558]. **exponential** [243, 397]. **exponents** [259, 285, 199, 279, 305, 222, 338, 291]. **Extended** [114, 98, 335, 651]. **extender** [119]. **external** [455].

F [523]. **Factorization** [9, 547, 652, 302, 419]. **fair** [555]. **Families** [657, 307, 459, 384, 385, 455, 397, 136, 113, 508, 443, 433]. **family** [202, 603, 506, 369, 639, 396, 83, 96, 8, 592, 347, 329, 497]. **fast** [54, 481, 46, 171, 61]. **Faster** [232]. **Fault** [51, 473, 255, 101, 441, 96, 681, 189]. **fault-resilient** [441]. **FBCT** [569]. **FBDT** [569]. **FCSR** [41, 6]. **FCSRs** [183]. **feedback** [230]. **feedbacks** [57, 121]. **Feedforward** [365]. **Feistel** [42, 209]. **Fermat** [43, 203]. **few** [37, 614, 280, 162, 393, 164, 443]. **Fibonacci** [180, 589]. **field** [304, 297]. **fields** [451, 327, 468, 269, 579, 578, 223, 198, 544, 125, 478, 9, 479, 235, 289, 279, 367, 689, 684, 442, 187, 368, 407, 155, 228, 574, 656, 308, 131, 168]. **FiLIP** [681]. **filtering** [241]. **Finding** [62].

finite [451, 468, 342, 304, 552, 269, 579, 578, 223, 603, 198, 544, 125, 478, 501, 9, 547, 479, 235, 289, 279, 367, 689, 684, 442, 187, 297, 368, 407, 155, 228, 574, 234, 656, 308, 131, 690, 168]. **FIRE** [99]. **Five** [266, 686, 343, 497]. **flat** [325]. **flexible** [233, 661, 613, 396]. **FLIP** [681]. **flower** [400]. **fold** [102, 182]. **fool** [472]. **form** [451, 92, 235, 289, 616, 237]. **Formal** [485]. **formally** [390]. **forms** [611, 631, 167]. **formula** [172, 430, 478]. **formulae** [228]. **four** [447, 532, 150, 165]. **four-weight** [447]. **Fourier** [398, 33]. **Fourier-analytic** [33]. **fractions** [523]. **Frameproof** [667]. **frames** [392]. **framework** [189]. **free** [78, 445, 93, 130, 110]. **Frequency** [314, 391, 384, 188, 518, 676, 675, 40, 365, 229, 550, 582, 200, 515, 516]. **Frequency-hopping** [314, 391, 188, 229, 550, 582, 200, 515, 516]. **Frobenius** [353, 409]. **full** [404]. **fully** [644]. **Function** [629, 464, 144, 435, 92, 567, 484, 44, 534, 612, 179, 556, 88, 452, 490]. **functional** [544]. **Functions** [116, 158, 632, 240, 43, 218, 429, 658, 566, 565, 623, 50, 140, 37, 356, 66, 132, 344, 271, 413, 394, 489, 564, 633, 575, 414, 277, 420, 19, 261, 243, 353, 418, 494, 559, 126, 82, 157, 424, 640, 151, 415, 175, 17, 459, 321, 262, 160, 47, 340, 478, 672, 273, 64, 460, 346, 495, 587, 134, 597, 491, 504, 417, 471, 107, 103, 135, 422, 465, 534, 620, 70, 352, 276, 481, 260, 350, 538, 636, 136, 162, 351, 275, 389, 402, 493, 572, 643, 416, 16, 354, 46, 284, 45, 630, 556, 171, 524, 637]. **functions** [641, 156, 88, 440, 592, 370, 220, 656, 551, 139, 196, 347, 343, 362, 609, 619, 272, 508, 61, 398, 201, 325, 436, 543, 651, 631, 131, 165, 522, 687, 519, 239, 571, 379, 433, 168]. **Further** [657, 136, 618, 637, 108, 121, 338, 449].

G [173]. **Gabidulin** [423]. **Galois** [579, 578, 669, 507, 605, 487, 512]. **games** [623]. **gaps** [73]. **Gaussian** [448]. **General** [116, 491, 39, 253]. **generalisations** [411]. **generalised** [345, 379]. **generalizations** [301, 75]. **Generalized** [658, 233, 629, 116, 573, 350, 154, 200, 642, 184, 198, 521, 536, 125, 595, 461, 160, 423, 186, 74, 337, 401, 538, 351, 389, 537, 601, 14, 637, 189, 268, 480, 628, 170, 174, 438, 512, 688, 42]. **generate** [336]. **generated** [365]. **generating** [214, 340, 273]. **generation** [81, 137, 486]. **generation/correlation** [81]. **generator** [527, 174]. **generators** [53, 241, 365]. **Generic** [209, 162, 149, 239]. **genetic** [137]. **genus** [505]. **geometries** [342]. **GGHN** [13]. **girth** [299, 405]. **giving** [353]. **GL-S-NFSR** [679]. **Goethals** [614]. **Golay** [496, 613, 577]. **gold** [569, 494, 567, 490]. **Gong** [650]. **Good** [245, 172, 430, 137, 574, 677, 374, 582, 314, 270]. **Goppa** [159]. **grain** [252, 96, 129]. **grain-like** [252]. **graph** [130]. **graphical** [84]. **graphs** [67, 85, 299, 544, 210, 312, 354]. **gray** [93, 669, 224]. **greedy** [169]. **grid** [15]. **Griesmer** [672]. **group** [366, 409, 678, 417]. **groups** [455, 652, 120]. **Grover** [144]. **GRS** [507]. **Guest** [94, 20, 52, 248].

Hadamard [29, 25, 307, 462, 31, 21, 425, 30, 32, 24, 28, 33]. **half** [143]. **half-** [143]. **Hamming** [62, 385, 401, 518, 676, 675, 582, 314]. **hardware** [183, 473]. **hash** [531, 106, 16]. **Hashing** [467]. **having** [390]. **held** [492]. **Helleseth** [133, 337, 124, 438]. **Hermitian** [541, 595, 599, 530, 581, 513]. **High** [55, 240, 198, 572]. **higher** [556, 619]. **higher-order** [556]. **highly** [48, 440]. **hit** [188, 676, 675, 200, 391, 515]. **Hitag2** [88]. **Homogeneous** [669]. **homomorphic** [207]. **hop** [525]. **hopping** [290, 384, 188, 518, 676, 675, 229, 550, 582, 200, 314, 391, 515, 516]. **Horizontal** [98]. **hull** [448, 671, 548]. **Hulls** [437, 507, 668, 579, 578, 605]. **hyper**

[389, 196]. **hyper-bent** [389, 196]. **Hyperbent** [632]. **hyperelliptic** [505]. **hyperovals** [632]. **hyperplane** [203]. **hypotheses** [253].

IDEA [216]. **ideal** [119, 241, 113]. **ideals** [606]. **idempotents** [359]. **identification** [152]. **identifiers** [336]. **identifying** [67, 85, 130, 15]. **identity** [152]. **identity-based** [152]. **If** [345]. **II** [203, 687]. **III/II** [687]. **illustration** [471]. **Image** [355, 669]. **images** [224]. **immune** [19, 262, 107, 398, 65]. **immunity** [70, 481, 572, 88, 347]. **implementation** [141, 46, 61]. **implementations** [95, 471]. **Improved** [119, 597, 512, 96]. **improvement** [689]. **Improving** [524]. **index** [357, 662, 340, 317]. **indicator** [491]. **individual** [97]. **inducing** [504]. **inductive** [463]. **inequivalence** [29, 459]. **infinite** [353, 639, 136, 15, 433]. **infinitely** [394]. **Influence** [138]. **information** [114, 211]. **initialisation** [87]. **initialization** [58]. **injection** [255]. **injective** [330]. **Injectivity** [110, 282]. **inner** [614]. **input** [623, 275]. **inputs** [175]. **inserting** [573, 503]. **instances** [300]. **Integer** [339, 372, 371, 10]. **integers** [110, 270, 245]. **integral** [216, 250]. **integrated** [63]. **inter** [653]. **inter-set** [653]. **interactions** [643]. **intercept** [153]. **interesting** [620]. **interleaved** [118, 674]. **intersection** [563, 447]. **invariant** [467, 652, 511]. **Invariants** [495, 514, 601]. **Inverse** [435, 569, 44, 534, 179, 452]. **inverses** [289]. **invertible** [214]. **Investigation** [475]. **involutions** [465, 352, 368]. **IPM** [470]. **Irreducibility** [227, 203]. **irreducible** [617, 219, 610, 585, 359]. **Isodual** [549]. **Issue** [271, 295, 1, 643, 466, 526, 132, 344, 413, 489, 564, 633, 20, 76, 204, 378]. **iterated** [90]. **iterations** [16]. **iterative** [340].

Jacobi [293]. **Joint** [2, 148]. **Jump** [525].

Karatsuba [205]. **Kasami** [17]. **KATAN32** [91]. **KATAN32/48/64** [91]. **Kendall** [624, 580]. **key** [86, 301, 232, 12, 678, 11, 253, 399, 596]. **keying** [678]. **keystream** [11]. **Kim** [494]. **Kim-type** [494]. **kind** [176]. **king** [15]. **KISS** [212]. **Klein** [286]. **Kloosterman** [426, 594, 593, 221, 196, 343, 303]. **known** [566, 414, 508, 28].

Large [384, 153, 299, 661, 613, 576, 683, 268]. **largest** [320]. **Latin** [27]. **lattice** [527, 36, 230]. **lattice-based** [36, 230]. **lattices** [552]. **layers** [634]. **LCD** [541, 603, 247, 586, 599, 501, 547, 367, 530, 684, 407, 317, 359, 360, 532, 513, 682, 625]. **LDPC** [405]. **leakage** [100]. **leakage-resilient** [100]. **Leander** [569]. **learning** [472]. **least** [333]. **Lee** [529]. **Legendre** [153]. **Lempel** [197]. **length** [172, 617, 193, 430, 560, 181, 509, 369, 310, 306, 576, 663, 106, 361, 104, 540, 439, 57, 36, 121, 170, 163, 288, 645, 38, 236, 682, 406, 381]. **length/space/time** [410]. **Lengths** [629, 79]. **Levenshtein** [160]. **LFSR** [269, 6]. **LFSRs** [183]. **Li** [112]. **Lidl** [635]. **Lifted** [552, 122]. **lightweight** [105, 60]. **like** [99, 4, 475, 105, 252, 441, 386, 250]. **limited** [145, 306]. **limited-magnitude** [145]. **line** [215]. **Linear** [505, 184, 600, 118, 461, 563, 337, 636, 162, 448, 124, 149, 626, 158, 376, 327, 328, 450, 668, 353, 470, 4, 492, 117, 198, 521, 669, 2, 341, 527, 315, 47, 340, 504, 479, 148, 135, 161, 396, 422, 652, 178, 280, 59, 222, 264, 266, 7, 187, 416, 296, 608, 476, 594, 593, 607, 69, 253, 548, 634, 221, 383, 272, 190, 176, 431, 446, 543, 673, 164, 631, 165, 522, 191, 166, 311, 167, 406]. **linearity** [542, 161]. **Linearized** [502, 402]. **linkage** [510]. **local** [377, 547]. **Localised** [192]. **locality** [646]. **Locally** [666, 428, 604, 602]. **location** [159, 312]. **logarithm** [333]. **logarithmic** [120]. **look** [115]. **looking** [62]. **Low**

[565, 458, 675, 278, 395, 202, 415, 506, 188, 153, 387, 183, 283, 540, 38, 200, 515, 676]. **low-depth** [278]. **Low-hit-zone** [675, 188, 200, 515, 676]. **Lower** [6, 654, 326, 320, 656, 293, 362]. **LPN** [141]. **LWE** [300, 591, 596]. **LWE-based** [596].

MAC [561]. **machine** [472]. **magnetic** [649]. **magnitude** [509, 145, 403, 488, 382]. **Maiorana** [504, 350]. **Malleability** [217]. **management** [678]. **manipulation** [440]. **mappings** [330, 558]. **maps** [4, 544, 110, 627]. **Masking** [100, 500, 251]. **mass** [172, 430]. **matched** [159]. **Mathematical** [295, 615]. **mathematics** [466]. **matrices** [22, 71, 483, 29, 658, 25, 395, 31, 214, 105, 655, 21, 30, 32, 24, 319, 33]. **Matrix** [151, 226, 41, 238, 36]. **maximal** [170, 513]. **Maximum** [484, 336, 70, 654, 386, 57, 121, 487]. **maximum-length** [57, 121]. **McFarland** [504, 350]. **MDS** [437, 595, 105, 655, 563, 586, 605, 442, 268, 671, 548, 645, 287]. **measure** [118, 333]. **measures** [140, 6, 156]. **meet** [109, 91]. **meet-in-the-middle** [109, 91]. **Melas** [122]. **memory** [257]. **Menezes** [358]. **Message** [227, 39]. **metaheuristic** [640]. **method** [256, 415, 340, 399, 131, 239, 571]. **Methods** [295, 116, 200]. **metric** [624, 568, 281]. **metrically** [320]. **middle** [109, 91]. **Minimal** [543, 673, 522, 463, 396, 476, 120, 383, 36]. **Minimum** [67, 85, 376, 310, 411, 268, 497, 150]. **Missing** [205]. **mistakes** [430]. **mixed** [583]. **Modeling** [591]. **Modes** [87, 147]. **Modifications** [608]. **Modified** [218, 565, 491, 293]. **modifying** [179]. **modular** [421]. **modulo** [184, 142, 110, 138, 191]. **MOLS** [27]. **Monomial** [471, 50, 126, 103, 362]. **monomials** [639, 150]. **monotone** [261]. **most** [14]. **MUBs** [528, 27]. **Muller** [492, 638, 461, 411, 74, 14, 288]. **Multi** [561, 574, 516, 250, 672, 670, 208, 555, 602, 644, 671]. **multi-cell** [670]. **multi-erasure** [602]. **Multi-party** [516]. **multi-secret** [555, 644]. **multi-structure** [250]. **Multi-twisted** [574, 671]. **Multi-user** [561, 208]. **multi-variable** [672]. **Multidimensional** [47, 91, 253, 627]. **multilevel** [510]. **multinegacirculant** [364]. **multinomials** [34]. **Multiple** [351, 267, 666, 670, 213, 253]. **multiple/multidimensional** [253]. **multiplication** [468, 206]. **Multiplicative** [89, 356, 277, 420, 35, 542, 656, 97]. **multiplier** [549]. **multisecret** [192]. **multisequence** [148]. **multisequences** [2, 230]. **multivariate** [415, 16]. **mutual** [211]. **Mutually** [27, 26, 454, 77, 651]. **mystery** [316].

Near [322, 655, 79, 201, 229]. **near-bent** [201]. **near-MDS** [655]. **Near-Optimal** [322, 229]. **Necessary** [116]. **negabent** [551, 168]. **negacirculant** [603, 360]. **negacyclic** [172, 430, 369]. **neighbourhood** [597]. **nested** [88]. **Network** [42]. **networks** [678]. **NFSR** [657, 57, 121, 373, 679]. **NGG** [12]. **NHZ** [518]. **Niho** [259, 285, 199, 279, 305, 222, 556, 338, 291, 558]. **NLFSR** [487]. **NLFSR-based** [487]. **NLFSRs** [512]. **NMDS** [595, 586]. **no** [391]. **no-hit-zone** [391]. **Non** [45, 327, 244, 400, 144, 324, 545, 455, 501, 577, 354, 108, 540, 677, 532, 234, 381]. **non-abelian** [455]. **non-chain** [545, 501]. **non-commutative** [234]. **non-cyclic** [324]. **non-overlapping** [244]. **non-power-of-two** [540, 381]. **non-prime** [327]. **non-randomness** [108]. **non-resiliency** [144]. **non-standard** [577]. **non-uniform** [400]. **non-unital** [532]. **non-weakly** [354]. **non-zero** [677]. **nonbinary** [233]. **noncommutative** [532]. **nonexistence** [483, 551]. **Nonlinear**

[263, 48, 459, 534, 284, 365, 637, 440, 318]. **nonlinearities** [17, 619]. **Nonlinearity** [156, 432, 140, 261, 82, 333, 178, 275, 402, 572, 556, 524, 139, 362, 57, 121]. **nonlocal** [623]. **norm** [562]. **norm-trace** [562]. **normal** [92]. **normality** [260]. **Note** [589, 256, 426, 383, 287, 558]. **Notes** [401]. **novel** [336]. **NTRUSign** [51]. **null** [432]. **nulls** [40]. **number** [304, 214, 402, 557, 649]. **numbers** [16, 154].

obtained [545, 597, 612]. **OCDMA** [410]. **Octanary** [607]. **odd** [617, 193, 418, 660, 415, 110, 387, 534, 27, 308, 131, 382]. **odd-periodic** [387, 382]. **often** [394]. **old** [133]. **on-line** [215]. **One** [100, 380, 388, 67, 85, 562, 39, 448, 548]. **one-dimensional** [448, 548]. **one-point** [562]. **one-round** [39]. **One-weight** [388]. **ones** [566, 214]. **online** [249]. **open** [112, 133]. **operates** [345]. **operations** [147, 87, 97]. **optical** [410]. **Optimal** [600, 629, 160, 312, 322, 83, 685, 150, 550, 541, 408, 181, 583, 117, 509, 661, 188, 385, 130, 672, 153, 674, 568, 670, 396, 604, 684, 182, 535, 518, 266, 323, 281, 572, 113, 410, 231, 403, 347, 590, 497, 653, 436, 488, 229, 382, 646, 200, 515]. **optimality** [211]. **Optimization** [468]. **orbit** [324]. **order** [17, 333, 484, 186, 55, 534, 337, 402, 556, 386, 362, 619, 154, 124, 163, 288, 433]. **orders** [28]. **orientable** [334]. **oriented** [331]. **orthogonal** [664, 410, 27, 228, 651]. **other** [100]. **output** [623, 97]. **overheads** [281]. **overlapping** [244]. **overview** [5].

packings [666, 428]. **pair** [341, 442, 585, 242]. **pairing** [101]. **Pairs** [600, 81, 613, 563, 232, 390, 577, 647, 687]. **PAM** [40]. **paper** [430]. **PAPR** [540]. **parallel** [109, 510]. **parallel-cut** [109]. **parameters** [639, 367, 396, 535, 83, 582, 682, 515]. **parametrized** [226]. **Paraunitary** [81]. **parity** [589]. **partial** [385, 350, 36, 673, 33]. **Partially** [394, 658]. **particular** [93]. **partitioned** [93, 307]. **partitions** [642]. **party** [623, 516]. **path** [650]. **Patterson** [597]. **pauses** [649]. **PD** [462]. **Perfect** [80, 225, 658, 233, 459, 79, 111, 380, 102, 135, 534, 182, 659, 637, 649]. **perfectly** [39, 493, 572, 347]. **period** [674, 148, 254, 679, 318, 488, 229, 626, 487]. **Periodic** [309, 665, 6, 387, 113, 382, 456]. **periods** [233, 521, 438]. **Permutation** [419, 44, 235, 40, 624, 259, 434, 660, 285, 686, 662, 348, 478, 199, 289, 279, 616, 11, 584, 618, 308, 338, 291, 237]. **Permutations** [451, 504, 546, 432, 517, 353, 570, 561, 459, 349, 520, 465, 136, 297, 284, 179, 584, 580]. **perturbed** [490]. **phase** [72, 482]. **photonics** [458]. **PIR** [469]. **planar** [218, 135]. **plateaued** [429]. **PN** [34]. **POEx** [215]. **point** [562]. **points** [517, 346, 171]. **Polar** [596]. **Poly** [300]. **polyadic** [690]. **Polynomial** [227, 269, 484, 471, 555, 128, 69, 508]. **Polynomials** [502, 451, 159, 434, 219, 635, 611, 18, 610, 335, 419, 547, 44, 235, 289, 652, 689, 402, 16, 486, 616, 584, 237]. **Polyphase** [379, 506]. **power** [415, 478, 520, 663, 30, 584, 27, 556, 540, 592, 508, 229, 519, 558, 381]. **practicability** [211]. **Practical** [183]. **Preface** [526, 157]. **Preferred** [647]. **Prefix** [93]. **Preimages** [502]. **prescribed** [304, 214]. **presemifields** [158]. **PRESENT** [86]. **PRESENT-80** [86]. **prime** [327, 126, 186, 663, 30, 27, 163, 10, 229, 438, 626]. **prime-power** [663, 229]. **primitive** [142, 110, 390, 359, 263, 282, 330]. **primitives** [100, 634]. **privacy** [469, 114]. **private** [114]. **Probabilistic** [641, 189, 524]. **probabilities** [102]. **probability** [153, 253]. **problem** [273, 26]. **problems** [133, 422]. **product** [219, 238, 391]. **products** [614, 438]. **profile** [118]. **profiles** [335]. **Progress** [21]. **progressions** [399]. **projection** [64]. **projective** [652].

Properties [392, 429, 255, 42, 544, 143, 137, 153, 597, 491, 620, 96, 636, 88, 49, 679, 421]. **property** [615, 153, 663, 609, 314]. **proposal** [106]. **protected** [471]. **protocols** [114]. **provable** [257]. **proven** [49]. **proving** [256]. **pseudo** [523]. **pseudo-ultrametric** [523]. **Pseudorandom** [539, 16]. **pseudorandomness** [258]. **public** [561, 301, 596]. **public-key** [301]. **punctured** [411].

QAM [81, 571, 381]. **QC** [405]. **QC-LDPC** [405]. **QS** [670]. **Quadratic** [224, 37, 611, 587, 134, 416, 486, 584, 185, 631, 571, 167]. **quadrinomials** [660, 592]. **Quadruple** [366]. **Quantum** [292, 562, 480, 499, 498, 545, 583, 501, 530, 238, 477, 334, 268, 581]. **quartic** [286]. **Quasi** [159, 135, 322, 477, 125, 357, 610, 453, 317, 654, 228, 174]. **Quasi-Complementary** [322, 654]. **Quasi-cyclic** [159, 477, 125, 357, 610, 453, 228, 174]. **Quasi-perfect** [135]. **quasi-twisted** [317]. **Quaternary** [64, 541, 408, 184, 117, 521, 672, 599, 153, 674, 283, 220, 38, 382, 626, 406]. **quaternions** [80, 225]. **Quiescent** [458]. **quinary** [685]. **quotients** [43, 456].

R [329]. **R-2** [329]. **Rabbit** [59]. **radii** [328]. **radius** [288]. **ramp** [73, 680]. **random** [612, 630, 156]. **randomisation** [253]. **randomness** [525, 108, 329]. **rank** [404, 568, 281]. **rank-metric** [281]. **rate** [249]. **rate-1** [249]. **ratio** [576]. **Rational** [523, 478, 402, 40]. **RC4** [316, 232, 251, 11, 254, 108]. **RC4A** [108]. **Re** [678]. **Re-keying** [678]. **readout** [458]. **real** [454, 528]. **realistic** [56]. **realization** [36]. **REALLY** [31]. **Reconstruction** [580]. **recoverable** [604, 602]. **recovery** [12]. **recurring** [2, 7]. **recursive** [263]. **reduced** [8]. **redundant** [644]. **Reed** [492, 536, 638, 595, 461, 411, 586, 74, 14, 268, 671, 628, 288, 688]. **Reed-Muller** [74, 14]. **registers** [226, 557, 230]. **Regular** [428, 343, 392, 162, 320, 354, 522]. **regularity** [355]. **Related** [116, 623, 86, 18, 133, 530]. **related-key** [86]. **relations** [363]. **Relative** [335, 225, 35, 332, 169, 447]. **remainder** [125]. **remarks** [32]. **repair** [666]. **repairable** [666, 428, 680]. **Repeated** [529, 104, 439, 242]. **Repeated-root** [104, 439, 242]. **representation** [184, 626, 456]. **representations** [151, 309]. **residue** [224, 185]. **Resilience** [75]. **resiliency** [144, 500]. **Resilient** [500, 100, 441, 647]. **resist** [96]. **resistance** [86]. **resistant** [46, 61]. **Resolvable** [528]. **resonance** [649]. **respect** [262, 421]. **restricted** [275]. **Results** [657, 313, 551, 483, 464, 422, 618, 114, 121, 338, 237]. **retrieval** [114]. **reverse** [99]. **reverse-engineering** [99]. **Reversed** [137]. **reversible** [474]. **Revisiting** [90, 232]. **ring** [377, 545, 474, 669, 224, 501, 183, 453, 317, 532, 234, 690, 596]. **rings** [552, 603, 366, 409, 547]. **rise** [353]. **robust** [210, 107, 331]. **Root** [425, 377, 529, 104, 439, 242]. **Root-Hadamard** [425]. **rotation** [50, 66, 559, 126, 572, 551]. **round** [129, 39]. **RSBFs** [96]. **RSSBs** [313]. **Rudin** [386]. **rule** [68].

S [679, 100, 48, 95, 569, 475, 137, 542, 313, 178, 441, 274, 608, 601, 298, 89]. **S-boxes** [48, 95, 569, 475, 137, 542, 313, 178, 441, 274, 608, 601, 298, 89]. **sample** [591]. **scalable** [68]. **scalar** [468]. **SCARE** [99]. **scenarios** [56, 211]. **scheme** [207, 469, 152, 51, 555, 644]. **schemes** [496, 392, 84, 281, 209, 73, 194, 680, 65]. **search** [232, 587, 405]. **Searchable** [213]. **Second** [74, 186, 169, 534, 402, 14, 362, 288, 433]. **second-order** [534, 402, 362]. **Secondary**

[70]. **Secret** [299, 496, 84, 194, 210, 555, 644, 39, 11, 65]. **sections** [203]. **Secure** [227, 215, 249, 39, 281]. **Security** [152, 208, 256, 561, 301, 257, 331, 472]. **Self** [444, 603, 560, 366, 474, 536, 409, 595, 310, 664, 485, 547, 417, 352, 317, 127, 228, 360, 220, 628, 287, 457]. **Self-dual** [444, 603, 560, 366, 474, 536, 409, 595, 310, 547, 417, 352, 317, 127, 228, 360, 220, 628, 287, 457]. **self-orthogonal** [664, 228]. **semifields** [34]. **sensing** [395, 319]. **sensor** [678]. **separable** [181, 667, 336, 236]. **Separation** [464, 332]. **Sequence** [322, 81, 223, 180, 153, 186, 683, 670, 397, 518, 676, 675, 241, 589, 540, 399, 293, 386, 653, 229, 582, 200, 314, 391, 381, 515]. **Sequences** [657, 76, 201, 225, 197, 505, 408, 233, 219, 184, 142, 117, 198, 521, 509, 2, 384, 588, 143, 506, 188, 385, 79, 118, 378, 110, 153, 674, 6, 380, 387, 525, 577, 337, 648, 659, 425, 7, 187, 258, 539, 643, 283, 40, 427, 612, 665, 365, 69, 677, 231, 403, 649, 627, 246, 329, 263, 523, 36, 124, 170, 282, 330, 393, 318, 488, 10, 550, 438, 38, 382, 626, 379, 456, 406, 516]. **server** [469]. **servers** [213]. **Set** [322, 661, 110, 683, 417, 653, 28]. **Sets** [629, 225, 408, 342, 404, 93, 159, 355, 462, 3, 614, 72, 35, 188, 666, 145, 683, 670, 518, 676, 675, 654, 540, 653, 651, 229, 582, 200, 314, 391, 381, 515]. **setting** [208]. **Settling** [316]. **Several** [199, 684, 280, 352, 476, 291, 433, 568, 431, 325]. **SHA** [8]. **SHA-2** [8]. **Shapiro** [386]. **Shapiro-like** [386]. **sharing** [299, 496, 84, 210, 192, 555, 644, 39, 399, 298, 194, 65]. **shift** [226, 557, 230]. **Shifted** [429]. **shortest** [486]. **side** [255, 458, 472]. **side-channel** [255, 472]. **Sidelnikov** [197]. **signal** [72]. **signals** [40]. **signature** [51, 189]. **signatures** [208, 120]. **significant** [105, 333, 139]. **similarities** [63]. **simple** [78, 377, 73, 120, 212, 49]. **simplex** [442, 492]. **simplicial** [607]. **simulating** [591]. **single** [469, 306, 580]. **single-server** [469]. **Singly** [310]. **six** [460, 405]. **six-valued** [460]. **size** [624, 661, 613, 666, 306, 683, 320]. **sizes** [80, 67, 85, 390]. **Skew** [621, 453, 583, 125]. **SKINNY** [475]. **SKINNY-like** [475]. **Small** [278, 3, 95, 414, 252, 684, 671, 649, 421]. **small-state** [252]. **smallest** [405]. **Solomon** [536, 595, 586, 268, 671, 628, 688]. **Solving** [412, 141, 591]. **Some** [31, 247, 662, 116, 491, 182, 283, 407, 32, 268, 163, 533, 158, 505, 172, 617, 426, 517, 434, 430, 611, 638, 459, 520, 270, 245, 547, 401, 585, 7, 616, 167, 682, 211]. **space** [309, 410]. **spaces** [570]. **sparse** [528, 339]. **Special** [466, 344, 271, 295, 413, 489, 564, 633, 157, 76, 204, 378, 643, 526, 159, 424, 20, 317, 132]. **Spectra** [134, 460, 534, 325]. **spectral** [40, 398]. **spectrum** [148, 659, 558]. **spectrums** [520]. **splitting** [23, 102, 182]. **sporadic** [120]. **spread** [642, 350]. **spreads** [158, 673]. **square** [256, 110, 454]. **square-free** [110]. **squares** [27]. **SRAM** [458]. **SRs** [523]. **standard** [577, 209]. **Stanica** [112]. **State** [58, 252, 309, 254]. **state-space** [309]. **Statistical** [255, 216, 250, 143, 251, 329, 473]. **Status** [588]. **stealthy** [473]. **Steiner** [3]. **step** [8]. **stopping** [3]. **stream** [68, 56, 173, 63, 252, 257, 5, 12, 13, 55, 9, 83, 96, 60, 294, 87, 189, 88, 49, 58, 487, 650]. **strikes** [415]. **Strong** [455, 349]. **Strongly** [354, 236]. **structural** [63, 13]. **structure** [269, 42, 250, 357, 373, 679]. **structures** [504, 39, 416, 608, 194]. **study** [545]. **style** [591]. **Sub** [657]. **subclass** [17, 590]. **subcodes** [461]. **subfield** [431, 446, 443]. **subfields** [565, 179]. **submultiples** [40]. **suboptimal** [78]. **subsequences** [484]. **subset** [320]. **subsets** [390]. **subspace** [503, 510, 449]. **Success** [253]. **Sufficient** [116]. **sum** [404, 478, 484, 677, 246]. **sums** [426, 243, 611, 397, 689, 448, 594, 593, 490, 221, 196, 343, 303]. **superclasses** [566].

supersets [648]. **supplementary** [408]. **support** [511]. **supporting** [87]. **surfaces** [334]. **Survey** [537, 54, 640, 101, 305, 538]. **Suzuki** [120]. **swapping** [517]. **switching** [131]. **Symbol** [585, 442, 40, 123, 242]. **Symbol-pair** [585, 442, 242]. **Symbolic** [559]. **symbols** [365]. **symmetric** [50, 356, 66, 559, 126, 509, 313, 107, 572, 213, 634, 551]. **synchronizable** [480]. **synthesis** [230]. **Synthetic** [59]. **system** [670]. **systems** [3, 173, 290, 410].

table [567]. **tables** [62]. **Tangent** [544]. **Tangent-Chebyshev** [544]. **techniques** [527]. **terms** [594, 593, 343]. **ternary** [380, 659, 497, 393, 519, 625]. **Teske** [358]. **Test** [227]. **tests** [525, 524, 329]. **th** [333, 386]. **their** [218, 429, 132, 344, 271, 413, 489, 564, 633, 307, 418, 462, 75, 224, 76, 378, 21, 563, 64, 428, 460, 479, 529, 511, 659, 136, 104, 647, 24, 154, 446, 497, 513, 166]. **theorem** [125]. **theoretic** [557]. **Theoretical** [681, 601]. **theory** [526, 90, 255, 20, 245, 652, 270]. **Third** [17]. **Third-order** [17]. **Three** [395, 660, 482, 332, 588, 387, 222, 264, 410, 195, 590, 176, 685, 165, 166]. **three-dimensional** [410]. **Three-phase** [482]. **three-weight** [332, 590, 176, 166]. **Threshold** [95, 471, 481, 73]. **tight** [392]. **Tighter** [518]. **time** [72, 257, 410]. **time-memory-data** [257]. **time-phase** [72]. **too** [212]. **tool** [256]. **Trace** [456, 304, 184, 562, 436, 626]. **tradeoff** [257]. **transform** [262, 103]. **transformation** [512]. **transforms** [146, 425, 351]. **transition** [254]. **translators** [353]. **transmission** [39]. **treatment** [73]. **trellis** [447]. **trends** [204, 537]. **triads** [482]. **trick** [205]. **trinomials** [259, 285, 686, 662, 348, 199, 235, 279, 618, 308, 338, 291]. **triple** [3]. **Triplicate** [575]. **Trivium** [58]. **Trojan** [473]. **Truncated** [267]. **truth** [62]. **tuple** [241]. **tweakable** [249]. **twin** [130, 30, 438, 152]. **Twin-Beth** [152]. **twin-free** [130]. **twisted** [595, 586, 423, 317, 574, 671, 628, 688]. **Two** [613, 610, 323, 594, 593, 195, 436, 443, 165, 229, 381, 625, 623, 219, 177, 346, 639, 186, 306, 161, 222, 266, 361, 317, 540, 677, 388, 370, 221, 508, 154, 190, 488, 438, 311]. **Two-dimensional** [613]. **two-error-correcting** [361]. **two-party** [623]. **two-prime** [186]. **two-valued** [677]. **two-weight** [266, 388, 221, 311]. **type** [494, 672, 687]. **Type-II** [687]. **Type-III** [687]. **Type-III/II** [687].

ultrametric [523]. **Unbalanced** [42]. **Unbiased** [25, 26, 454, 27, 77]. **unbounded** [80]. **unequal** [390]. **Unicyclic** [349]. **uniform** [240, 432, 400, 435, 179, 298]. **uniformities** [537]. **uniformity** [565, 434, 635, 500, 415, 542, 370, 490, 656, 139, 519]. **Unit** [72]. **unital** [532]. **Universal** [281, 336]. **Upper** [356, 290, 267, 624, 602]. **user** [561, 208, 114]. **user-private** [114]. **users** [114]. **Using** [629, 141, 255, 198, 591, 249, 302, 607, 87, 77]. **UWB** [384].

v1 [129]. **value** [117]. **valued** [460, 677]. **values** [197, 569]. **variable** [277, 672]. **variables** [587]. **variants** [141]. **variations** [205]. **varieties** [203]. **variety** [286]. **various** [140]. **varying** [36]. **vector** [450, 87]. **Vectorial** [418, 631, 82, 151, 636, 263]. **version** [98]. **vertex** [67]. **via** [570, 527, 610, 672, 514, 648, 556, 440, 628, 436, 131, 433]. **view** [557]. **violating** [476]. **VMPC** [108]. **Volume** [1].

Walsh [570, 92, 460, 103, 146]. **Wan** [635]. **watermark** [516]. **watermarks** [111]. **wave** [410]. **wave-length** [410]. **wave-length/space/time** [410]. **waveform** [647]. **weak** [300]. **weakly** [162, 354, 522]. **weakness** [13]. **weighing** [22, 71, 483].

Weight
[617, 450, 332, 310, 177, 335, 479, 74, 169, 264, 266, 442, 585, 622, 598, 594, 593, 447, 14, 195, 388, 221, 590, 190, 176, 166, 311, 167].
Weights
[50, 376, 62, 280, 401, 222, 162, 164, 443, 165].
weightwise [493, 572, 347]. **Weil** [611, 689, 648, 490]. **Welch** [614, 650]. **Weng** [358]. **WG** [83, 60, 294, 75]. **WG-16** [294]. **WG-7** [60, 75]. **WG-8** [294]. **Whiteman** [186, 480]. **Wiedemann** [597]. **wireless** [173, 678]. **wise** [435, 447]. **within** [372, 371]. **without** [62, 227, 504].

XCB [115]. **XOR** [123].

Z [651]. **Z-complementary** [651]. **Zadoff** [648]. **ZCACS** [661]. **ZCPs** [576]. **ZCZ** [576, 670, 653]. **Zeckendorf** [484]. **zero** [404, 570, 613, 663, 534, 677, 653, 239, 379]. **zero-difference** [239]. **zero-sum** [404]. **zeros** [402, 685]. **zone** [613, 188, 663, 676, 675, 653, 379, 200, 391, 515].

References

Carlet:2009:ECC

[1] Claude Carlet. Editorial: *Cryptography and Communications*, volume 1, issue 1. *Cryptography and Communications*, 1(1):1–2, April 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/content/pdf/10.1007/s12095-009-0010-6.pdf`.

Fu:2009:JLC

[2] Fang-Wei Fu, Harald Niederreiter, and Ferruh Özbudak. Joint linear complexity of multisequences consisting of linear recurring sequences. *Cryptography and Communications*, 1(1):3–29, April 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-007-0001-4`.

Colbourn:2009:SSS

[3] Charles J. Colbourn and Yuichiro Fujiwara. Small stopping sets in Steiner triple systems. *Cryptography and Communications*, 1(1):31–46, April 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-008-0002-y`.

Daemen:2009:NCL

[4] Joan Daemen and Vincent Rijmen. New criteria for linear maps in AES-like ciphers. *Cryptography and Communications*, 1(1):47–69, April 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-008-0003-x`.

Hell:2009:ODA

[5] Martin Hell, Thomas Johansson, and Lennart Brynielsson. An overview of distinguishing attacks on stream ciphers. *Cryptography and Communications*, 1(1):71–94, April 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-008-0006-7`.

Kavuluru:2009:LBE

[6] Ramakanth Kavuluru and Andrew Klapper. Lower bounds on error complexity measures for periodic LFSR and FCSR sequences. *Cryptography and Communications*, 1(1):

95–116, April 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-008-0004-9.

Meidl:2009:HDL

[7] Wilfried Meidl. How to determine linear complexity and k-error linear complexity in some classes of linear recurring sequences. *Cryptography and Communications*, 1(1):117–133, April 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-008-0007-6.

Sanadhya:2009:CAR

[8] Somitra Kumar Sanadhya and Palash Sarkar. A combinatorial analysis of recent attacks on step reduced SHA-2 family. *Cryptography and Communications*, 1(2):135–173, September 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-009-0011-5.

Kolokotronis:2009:FDF

[9] Nicholas Kolokotronis, Konstantinos Limniotis, and Nicholas Kalouptsidis. Factorization of determinants over finite fields and application in stream ciphers. *Cryptography and Communications*, 1(2):175–205, September 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-008-0005-8.

Xu:2009:ASP

[10] Hong Xu, Wen-Feng Qi, and Yong-Hui Zheng. Autocorrelations of l-sequences with prime connection integer. *Cryptography and Communications*, 1(2):207–223, September 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-008-0008-5.

Paul:2009:BPK

[11] Goutam Paul and Subhamoy Maitra. On biases of permutation and keystream bytes of RC4 towards the secret key. *Cryptography and Communications*, 1(2):225–268, September 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-008-0009-4.

Kircanski:2009:NDK

[12] Aleksandar Kircanski, Rabeah Al-Zaidy, and Amr M. Youssef. A new distinguishing and key recovery attack on NGG stream cipher. *Cryptography and Communications*, 1(2):269–282, September 2009. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-009-0012-4.

Kircanski:2010:SWG

[13] Aleksandar Kircanski and Amr M. Youssef. On the structural weakness of the GGHN stream cipher. *Cryptography and Communications*, 2(1):1–17, April 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-009-0013-3.

Rolland:2010:SWG

[14] Robert Rolland. The second weight of generalized Reed-Muller codes in most cases. *Cryptography and Communications*, 2(1):19–40, April 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-009-0014-2`.

Pelto:2010:NBI

[15] Mikko Pelto. New bounds for $(r, \leq 2)$-identifying codes in the infinite king grid. *Cryptography and Communications*, 2(1):41–47, April 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-009-0015-1`.

Ostafe:2010:PNH

[16] Alina Ostafe and Igor E. Shparlinski. Pseudorandom numbers and hash functions from iterations of multivariate polynomials. *Cryptography and Communications*, 2(1):49–67, April 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-009-0016-0`.

Gode:2010:TON

[17] Ruchi Gode and Sugata Gangopadhyay. Third-order nonlinearities of a subclass of Kasami functions. *Cryptography and Communications*, 2(1):69–83, April 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-009-0017-z`.

Helleseth:2010:BXR

[18] Tor Helleseth and Alexander Kholosha. $\boldsymbol{x}^{2^l+1} + \boldsymbol{x} + \boldsymbol{a}$ and related affine polynomials over $\mathrm{GF}(2^k)$. *Cryptography and Communications*, 2(1):85–109, April 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-009-0018-y`.

Canfield:2010:AEC

[19] E. Rodney Canfield, Zhicheng Gao, Catherine Greenhill, Brendan D. McKay, and Robert W. Robinson. Asymptotic enumeration of correlation-immune Boolean functions. *Cryptography and Communications*, 2(1):111–126, April 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-010-0019-x`.

Flannery:2010:GES

[20] Dane L. Flannery and Kathryn J. Horadam. Guest editorial for the special issue on design theory. *Cryptography and Communications*, 2(2):127–128, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/content/pdf/10.1007/s12095-010-0035-x.pdf`.

Horadam:2010:HMT

[21] K. J. Horadam. Hadamard matrices and their applications: Progress 2007–2010. *Cryptography and Communications*, 2(2):129–154, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.`

springer.com/accesspage/article/10.1007/s12095-010-0032-0.

Arasu:2010:CWM

[22] Krishnasamy Thiru Arasu and Alex J. Gutman. Circulant weighing matrices. *Cryptography and Communications*, 2 (2):155–171, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0025-z.

Huber:2010:CBC

[23] Michael Huber. Combinatorial bounds and characterizations of splitting authentication codes. *Cryptography and Communications*, 2(2):173–185, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0020-4.

Szollosi:2010:ECH

[24] Ferenc Szöllősi. Exotic complex Hadamard matrices and their equivalence. *Cryptography and Communications*, 2(2):187–198, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0021-3.

Best:2010:UCH

[25] Darcy Best and Hadi Kharaghani. Unbiased complex Hadamard matrices and bases. *Cryptography and Communications*, 2(2):199–209, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0029-8.

Jaming:2010:PMU

[26] Philippe Jaming, Máté Matolcsi, and Péter Móra. The problem of mutually unbiased bases in dimension 6. *Cryptography and Communications*, 2 (2):211–220, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0023-1.

Rao:2010:MOL

[27] Asha Rao, Diane Donovan, and Joanne L. Hall. Mutually orthogonal Latin squares and mutually unbiased bases in dimensions of odd prime power MOLS and MUBs in odd prime power dimensions. *Cryptography and Communications*, 2(2): 221–231, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0027-x.

deLauney:2010:DSK

[28] Warwick de Launey and Daniel M. Gordon. On the density of the set of known Hadamard orders. *Cryptography and Communications*, 2(2): 233–246, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0028-9.

Armario:2010:ICC

[29] José Andrés Armario. On an inequivalence criterion for cocyclic Hadamard matrices. *Cryptography and Communications*, 2(2):247–259, September 2010.

CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0024-0.

OCathain:2010:TPP

[30] Padraig Ó Catháin and Richard M. Stafford. On twin prime power Hadamard matrices. *Cryptography and Communications*, 2(2):261–269, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0030-2.

Dillon:2010:SRB

[31] J. F. Dillon. Some REALLY beautiful Hadamard matrices. *Cryptography and Communications*, 2(2):271–292, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0031-1.

Seberry:2010:SRH

[32] Jennifer Seberry and Marilena Mitrouli. Some remarks on Hadamard matrices. *Cryptography and Communications*, 2(2):293–306, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0036-9.

deLauney:2010:FAA

[33] Warwick de Launey and David A. Levin. A Fourier-analytic approach to counting partial Hadamard matrices. *Cryptography and Communications*, 2(2):307–334, September 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0033-z.

Budaghyan:2011:NCS

[34] Lilya Budaghyan and Tor Helleseth. New commutative semifields defined by new PN multinomials. *Cryptography and Communications*, 3(1):1–16, March 2011. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0022-2.

Farmer:2011:ECM

[35] D. G. Farmer and K. J. Horadam. Equivalence classes of multiplicative central $(p^n, p^n, p^n, 1)$-relative difference sets. *Cryptography and Communications*, 3(1):17–28, March 2011. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0026-y.

Wang:2011:LBM

[36] Li-Ping Wang. A lattice-based minimal partial realization algorithm for matrix sequences of varying length. *Cryptography and Communications*, 3(1):29–42, March 2011. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-010-0037-8.

Bracken:2011:FMQ

[37] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. A few more quadratic APN functions. *Cryptography and Communications*, 3

(1):43–53, March 2011. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-010-0038-7`.

Yang:2011:CQS

[38] Zheng Yang and Pinhui Ke. Construction of quaternary sequences of length pq with low autocorrelation. *Cryptography and Communications*, 3(2):55–64, June 2011. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-010-0034-y`.

Martin:2011:EDS

[39] Keith M. Martin, Maura B. Paterson, and Douglas R. Stinson. Error decodable secret sharing and one-round perfectly secure message transmission for general adversary structures. *Cryptography and Communications*, 3(2):65–86, June 2011. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-010-0039-6`.

Ouahada:2011:PSC

[40] Khmaies Ouahada, Theo G. Swart, and Hendrik C. Ferreira. Permutation sequences and coded PAM signals with spectral nulls at rational submultiples of the symbol frequency. *Cryptography and Communications*, 3(2):87–108, June 2011. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-010-0040-0`.

Arnault:2011:MAF

[41] François Arnault, Thierry P. Berger, and Benjamin Pousse. A matrix approach for FCSR automata. *Cryptography and Communications*, 3(2):109–139, June 2011. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-010-0041-z`.

Choy:2011:CPA

[42] Jiali Choy, Guanhan Chew, Khoongming Khoo, and Huihui Yap. Cryptographic properties and application of a Generalized Unbalanced Feistel Network structure. *Cryptography and Communications*, 3(3):141–164, September 2011. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-011-0042-6`.

Aly:2011:BFD

[43] Hassan Aly and Arne Winterhof. Boolean functions derived from Fermat quotients. *Cryptography and Communications*, 3(3):165–174, September 2011. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-011-0043-5`.

Li:2011:PPE

[44] Yongqiang Li and Mingsheng Wang. Permutation polynomials EA-equivalent to the inverse function over GF(2^n). *Cryptography and Communications*, 3 (3):175–186, September 2011. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.`

springer.com/accesspage/article/10.1007/s12095-011-0045-3.

Poinsot:2012:NAB

[45] Laurent Poinsot. Non Abelian bent functions. *Cryptography and Communications*, 4(1):1–23, March 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-011-0058-y.

Pasalic:2012:DBF

[46] Enes Pasalic. A design of Boolean functions resistant to (fast) algebraic cryptanalysis with efficient implementation. *Cryptography and Communications*, 4(1):25–45, March 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-011-0057-z. See comments [61].

Hermelin:2012:MLD

[47] Miia Hermelin and Kaisa Nyberg. Multidimensional linear distinguishing attacks and Boolean functions. *Cryptography and Communications*, 4(1):47–64, March 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-011-0053-3.

Beelen:2012:NCH

[48] Peter Beelen and Gregor Leander. A new construction of highly nonlinear S-boxes. *Cryptography and Communications*, 4(1):65–77, March 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-011-0052-4.

Si:2012:SSC

[49] Wenpei Si and Cunsheng Ding. A simple stream cipher with proven properties. *Cryptography and Communications*, 4(2):79–104, June 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-011-0059-x.

Bileschi:2012:WBC

[50] Maxwell L. Bileschi, Thomas W. Cusick, and Daniel Padgett. Weights of Boolean cubic monomial rotation symmetric functions. *Cryptography and Communications*, 4(2):105–130, June 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-011-0060-4.

Kamal:2012:FAN

[51] Abdel Alim Kamal and Amr M. Youssef. Fault analysis of the NTRUSign digital signature scheme. *Cryptography and Communications*, 4(2):131–144, June 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-011-0061-3.

Maitra:2012:GE

[52] Subhamoy Maitra and Palash Sarkar. Guest editorial. *Cryptography and Communications*, 4(3–4):145–146, December 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/content/pdf/10.1007/s12095-012-0073-7.pdf.

Canteaut:2012:CAC

[53] Anne Canteaut and María Naya-Plasencia. Correlation attacks on combination generators. *Cryptography and Communications*, 4(3–4): 147–171, December 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0069-3.

Aagren:2012:SFC

[54] Martin Ågren, Carl Löndahl, Martin Hell, and Thomas Johansson. A survey on fast correlation attacks. *Cryptography and Communications*, 4(3–4): 173–202, December 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0062-x.

Knellwolf:2012:HOD

[55] Simon Knellwolf and Willi Meier. High order differential attacks on stream ciphers. *Cryptography and Communications*, 4(3–4):203–215, December 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0071-9.

Dinur:2012:ACA

[56] Itai Dinur and Adi Shamir. Applying cube attacks to stream ciphers in realistic scenarios. *Cryptography and Communications*, 4(3–4): 217–232, December 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0068-4.

Turan:2012:NML

[57] Meltem Sönmez Turan. On the nonlinearity of maximum-length NFSR feedbacks. *Cryptography and Communications*, 4(3–4):233–243, December 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0067-5.

Simpson:2012:SCI

[58] Leonie Simpson and Serdar Boztas. State cycles, initialization and the Trivium stream cipher. *Cryptography and Communications*, 4(3–4): 245–258, December 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0066-6.

Lu:2012:SLA

[59] Yi Lu, Serge Vaudenay, and Willi Meier. Synthetic linear analysis with applications to CubeHash and Rabbit. *Cryptography and Communications*, 4(3–4): 259–276, December 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0064-8.

Orumiehchiha:2012:CWL

[60] Mohammad Ali Orumiehchiha, Josef Pieprzyk, and Ron Steinfeld. Cryptanalysis of WG-7: a lightweight stream cipher. *Cryptography and Communications*, 4(3–4):277–285, December 2012. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/

article/10.1007/s12095-012-0070-x.

Wang:2013:CDB

[61] Wenhao Wang, Meicheng Liu, and Yin Zhang. Comments on "A design of Boolean functions resistant to (fast) algebraic cryptanalysis with efficient implementation". *Cryptography and Communications*, 5(1):1–6, March 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0063-9. See [46].

Cusick:2013:FHW

[62] Thomas W. Cusick. Finding Hamming weights without looking at truth tables. *Cryptography and Communications*, 5(1):7–18, March 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0072-8.

Gupta:2013:DIA

[63] Sourav Sen Gupta, Anupam Chattopadhyay, and Ayesha Khalid. Designing integrated accelerator for stream ciphers with structural similarities. *Cryptography and Communications*, 5 (1):19–47, March 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0074-6.

Jadda:2013:QCB

[64] Zoubida Jadda, Patrice Parraud, and Soukayna Qarboua. Quaternary cryptographic bent functions and their binary projection. *Cryptography and Communications*, 5(1):49–65, March 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0077-3.

delaCruz:2013:CIS

[65] Romar dela Cruz and Huaxiong Wang. Cheating-immune secret sharing schemes from codes and cumulative arrays. *Cryptography and Communications*, 5(1):67–83, March 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0076-4.

Brown:2013:ECC

[66] Alyssa Brown and Thomas W. Cusick. Equivalence classes for cubic rotation symmetric functions. *Cryptography and Communications*, 5(2):85–118, June 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0075-5.

Charon:2013:MSI

[67] Irène Charon, Iiro Honkala, Olivier Hudry, and Antoine Lobstein. Minimum sizes of identifying codes in graphs differing by one vertex. *Cryptography and Communications*, 5(2):119–136, June 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-012-0078-2.

Das:2013:CNS

[68] Sourav Das and Dipanwita RoyChowdhury. *CAR30*: a new scalable

stream cipher with rule 30. *Cryptography and Communications*, 5(2): 137–162, June 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-012-0079-1`.

Salagean:2013:CLC

[69] Ana Sălăgean, Alex J. Burrage, and Raphael C.-W. Phan. Computing the linear complexity for sequences with characteristic polynomial f^v. *Cryptography and Communications*, 5 (2):163–177, June 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-013-0080-3`.

Limniotis:2013:SCB

[70] Konstantinos Limniotis, Nicholas Kolokotronis, and Nicholas Kalouptsidis. Secondary constructions of Boolean functions with maximum algebraic immunity. *Cryptography and Communications*, 5(3):179–199, September 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-013-0081-2`.

Arasu:2013:BWM

[71] K. T. Arasu, Simone Severini, and Edmund Velten. Block weighing matrices. *Cryptography and Communications*, 5 (3):201–207, September 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-013-0083-0`.

Ding:2013:UTP

[72] Cunsheng Ding, Keqin Feng, Rongquan Feng, Maosheng Xiong, and Aixian Zhang. Unit time-phase signal sets: Bounds and constructions. *Cryptography and Communications*, 5(3): 209–227, September 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-013-0085-y`.

Paterson:2013:SCT

[73] Maura B. Paterson and Douglas R. Stinson. A simple combinatorial treatment of constructions and threshold gaps of ramp schemes. *Cryptography and Communications*, 5(4): 229–240, December 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-013-0082-1`.

Leducq:2013:SWC

[74] Elodie Leducq. Second weight codewords of generalized Reed-Muller codes. *Cryptography and Communications*, 5 (4):241–276, December 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-013-0084-z`.

Gong:2013:RDA

[75] Guang Gong, Mark Aagaard, and Xinxin Fan. Resilience to distinguishing attacks on WG-7 cipher and their generalizations. *Cryptography and Communications*, 5(4): 277–289, December 2013. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.`

springer.com/accesspage/article/10.1007/s12095-013-0089-7.

Helleseth:2014:SIE

[76] Tor Helleseth and Jonathan Jedwab. Special issue editorial: Sequences and their applications. *Cryptography and Communications*, 6(1):1–2, March 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/content/pdf/10.1007/s12095-014-0098-1.pdf.

Wu:2014:CCU

[77] Gaofei Wu and Matthew Geoffrey Parker. A complementary construction using mutually unbiased bases. *Cryptography and Communications*, 6 (1):3–25, March 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-013-0095-9.

Bajic:2014:SSC

[78] Dragana Bajic and Tatjana Loncar-Turukalo. A simple suboptimal construction of cross-bifix-free codes. *Cryptography and Communications*, 6(1): 27–37, March 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-013-0088-8.

Hariharan:2014:NNP

[79] Rema Hariharan. New near perfect sequences of even lengths. *Cryptography and Communications*, 6(1): 39–46, March 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-013-0093-y.

Acevedo:2014:PAU

[80] Santiago Barrera Acevedo and Nathan Jolly. Perfect arrays of unbounded sizes over the basic quaternions. *Cryptography and Communications*, 6(1): 47–57, March 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-013-0086-x.

Budisin:2014:PGC

[81] S. Z. Budišin and P. Spasojević. Paraunitary generation/correlation of QAM complementary sequence pairs. *Cryptography and Communications*, 6 (1):59–102, March 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-013-0087-9.

Dib:2014:ANV

[82] Stéphanie Dib. Asymptotic nonlinearity of vectorial Boolean functions. *Cryptography and Communications*, 6 (2):103–115, June 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-013-0090-1.

Mandal:2014:OPW

[83] Kalikinkar Mandal, Guang Gong, Xinxin Fan, and Mark Aagaard. Optimal parameters for the WG stream cipher family. *Cryptography and Communications*, 6(2):117–135, June 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-013-0091-0.

Gao:2014:SSS

[84] Ying Gao and Romar dela Cruz. Secret sharing schemes based on graphical codes. *Cryptography and Communications*, 6(2):137–155, June 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-013-0092-z.

Charon:2014:MSI

[85] Irène Charon, Iiro Honkala, Olivier Hudry, and Antoine Lobstein. Minimum sizes of identifying codes in graphs differing by one edge. *Cryptography and Communications*, 6(2):157–170, June 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-013-0094-x.

Emami:2014:RPA

[86] Sareh Emami, San Ling, Ivica Nikolić, Josef Pieprzyk, and Huaxiong Wang. The resistance of PRESENT-80 against related-key differential attacks. *Cryptography and Communications*, 6(3):171–187, September 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-013-0096-8.

Sarkar:2014:MOE

[87] Palash Sarkar. Modes of operations for encryption and authentication using stream ciphers supporting an initialisation vector. *Cryptography and Communications*, 6(3):189–231, September 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-013-0097-7.

Shan:2014:CPN

[88] Jinyong Shan, Lei Hu, and Xiangyong Zeng. Cryptographic properties of nested functions and algebraic immunity of the Boolean function in Hitag2 stream cipher. *Cryptography and Communications*, 6(3):233–254, September 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-014-0099-0.

Zajac:2014:MCB

[89] Pavol Zajac and Matúš Jókay. Multiplicative complexity of bijective 4×4 S-boxes. *Cryptography and Communications*, 6(3):255–277, September 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-014-0100-y.

Bay:2014:RIA

[90] AslıBay, Atefeh Mashatan, and Serge Vaudenay. Revisiting iterated attacks in the context of decorrelation theory. *Cryptography and Communications*, 6(4):279–311, December 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-014-0101-x.

Zhu:2014:MMM

[91] Bo Zhu and Guang Gong. Multidimensional meet-in-the-middle attack and its applications to KATAN32/48/64. *Cryptography and Communications*, 6

(4):313–333, December 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0102-9`.

Gong:2014:CWC

[92] Xinxin Gong, Bin Zhang, Wenling Wu, and Dengguo Feng. Computing Walsh coefficients from the algebraic normal form of a Boolean function. *Cryptography and Communications*, 6(4): 335–358, December 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0103-8`.

Bernini:2014:PPG

[93] Antonio Bernini, Stefano Bilotta, Renzo Pinzani, Ahmad Sabri, and Vincent Vajnovszki. Prefix partitioned gray codes for particular cross-bifix-free sets. *Cryptography and Communications*, 6 (4):359–369, December 2014. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0105-6`.

Carlet:2015:GE

[94] Claude Carlet and Pierre-Alain Fouque. Guest editorial. *Cryptography and Communications*, 7(1):1–2, March 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/content/pdf/10.1007/s12095-014-0115-4.pdf`.

Bilgin:2015:TIS

[95] Begül Bilgin, Svetla Nikova, Ventzislav Nikov, Vincent Rijmen, Natalia Tokareva, and Valeriya Vitkup. Threshold implementations of small S-boxes. *Cryptography and Communications*, 7(1): 3–33, March 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0104-7`.

Mazumdar:2015:CRI

[96] Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, and Indranil Sengupta. Construction of RSBFs with improved cryptographic properties to resist differential fault attack on grain family of stream ciphers. *Cryptography and Communications*, 7(1):35–69, March 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0108-3`.

Tunstall:2015:DIB

[97] Michael Tunstall and Marc Joye. The distributions of individual bits in the output of multiplicative operations. *Cryptography and Communications*, 7 (1):71–90, March 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0110-9`.

Bauer:2015:HCC

[98] Aurélie Bauer, Eliane Jaulmes, Emmanuel Prouff, Jean-René Reinhard, and Justine Wild. Horizontal collision correlation attack on elliptic curves—extended version. *Cryptography and Communications*, 7(1):91–119, March 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0111-8`.

Clavier:2015:CRE

[99] Christophe Clavier, Quentin Isorez, Damien Marion, and Antoine Wurcker. Complete reverse-engineering of AES-like block ciphers by SCARE and FIRE attacks. *Cryptography and Communications*, 7(1):121–162, March 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0112-7`.

Belaid:2015:MLR

[100] Sonia Belaïd, Vincent Grosso, and François-Xavier Standaert. Masking and leakage-resilient primitives: One, the other(s) or both? *Cryptography and Communications*, 7(1):163–184, March 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0113-6`.

ElMrabet:2015:SFA

[101] Nadia El Mrabet, Jacques J. A. Fournier, Louis Goubin, and Ronan Lashermes. A survey of fault attacks in pairing based cryptography. *Cryptography and Communications*, 7(1):185–205, March 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0114-5`.

Li:2015:CFP

[102] Mingchao Li, Miao Liang, and Beiliang Du. A construction of t-fold perfect splitting authentication codes with equal deception probabilities. *Cryptography and Communications*, 7(2):207–215, June 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0107-4`.

Li:2015:WTC

[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 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0109-2`.

Sharma:2015:RRC

[104] Anuradha Sharma. Repeated-root constacyclic codes of length $\ell^t p^s$ and their dual codes. *Cryptography and Communications*, 7(2):229–255, June 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0106-5`.

Gupta:2015:CSM

[105] Kishan Chand Gupta and Indranil Ghosh Ray. Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications. *Cryptography and Communications*, 7(2):257–287, June 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0116-3`.

Luo:2015:ADL

[106] Yiyuan Luo, Xuejia Lai, and Tiejun Jia. Attacks on a double length

blockcipher-based hash proposal. *Cryptography and Communications*, 7(3): 289–295, September 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0117-2`.

Li:2015:CRI

[107] Yuan Li. Characterization of robust immune symmetric boolean functions. *Cryptography and Communications*, 7 (3):297–315, September 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0120-7`.

Sarkar:2015:FNR

[108] Santanu Sarkar. Further non-randomness in RC4, RC4A and VMPC. *Cryptography and Communications*, 7(3): 317–330, September 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0119-0`.

Nikolic:2015:PCM

[109] Ivica Nikolić, Lei Wang, and Shuang Wu. The parallel-cut meet-in-the-middle attack. *Cryptography and Communications*, 7(3):331–345, September 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0118-1`.

Hu:2015:ICM

[110] Zhi Hu and Lin Wang. Injectivity of compressing maps on the set of primitive sequences modulo square-free odd integers. *Cryptography and Communications*, 7(4):347–361, December 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0121-6`.

Jolly:2015:AAA

[111] Nathan Jolly. An algebra of arrays and almost perfect watermarks. *Cryptography and Communications*, 7(4): 363–377, December 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-015-0123-z`.

Castro:2015:DAO

[112] Francis N. Castro, Oscar E. González, and Luis A. Medina. A divisibility approach to the open boundary cases of Cusick–Li–Stănică's conjecture. *Cryptography and Communications*, 7(4): 379–402, December 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-015-0124-y`.

Ortiz-Ubarri:2015:NFA

[113] José Ortiz-Ubarri. New families of asymptotically optimal doubly periodic arrays with ideal correlation constraints. *Cryptography and Communications*, 7 (4):403–414, December 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-015-0122-0`.

Swanson:2015:ERP

[114] Colleen M. Swanson and Douglas R. Stinson. Extended results on privacy

against coalitions of users in user-private information retrieval protocols. *Cryptography and Communications*, 7(4): 415–437, December 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0125-x.

Chakraborty:2015:ALX

[115] Debrup Chakraborty, Vicente Hernandez-Jimenez, and Palash Sarkar. Another look at XCB. *Cryptography and Communications*, 7(4):439–468, December 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0127-8.

Hodzic:2015:GBF

[116] S. Hodžić and E. Pasalic. Generalized bent functions — some general construction methods and related necessary and sufficient conditions. *Cryptography and Communications*, 7(4): 469–483, December 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0126-9.

Edemskiy:2015:LCB

[117] Vladimir Edemskiy and Andrey Ivanov. The linear complexity of balanced quaternary sequences with optimal autocorrelation value. *Cryptography and Communications*, 7(4):485–496, December 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0130-0.

He:2015:LCP

[118] Jing Jane He, Daniel Panario, Qiang Wang, and Arne Winterhof. Linear complexity profile and correlation measure of interleaved sequences. *Cryptography and Communications*, 7(4): 497–508, December 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0131-z.

Guo:2015:IDE

[119] Chun Guo and Dongdai Lin. Improved domain extender for the ideal cipher. *Cryptography and Communications*, 7 (4):509–533, December 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0128-7.

Rahimipour:2015:EML

[120] A. R. Rahimipour, A. R. Ashrafi, and A. Gholami. The existence of minimal logarithmic signatures for the sporadic Suzuki and simple Suzuki groups. *Cryptography and Communications*, 7 (4):535–542, December 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0129-6.

Wang:2016:FRN

[121] Mingxing Wang, Yupeng Jiang, and Dongdai Lin. Further results on the nonlinearity of maximum-length NFSR feedbacks. *Cryptography and Communications*, 8(1):1–6, January 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/

article/10.1007/s12095-015-0133-x.

Alahmadi:2016:LMC

[122] Adel Alahmadi, Hussain Alhazmi, Tor Helleseth, Rola Hijazi, Najat Muthana, and Patrick Solé. On the lifted Melas code. *Cryptography and Communications*, 8(1):7–18, January 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0135-8.

Paterson:2016:ESD

[123] Maura B. Paterson, Douglas R. Stinson, and Yongge Wang. On encoding symbol degrees of array BP-XOR codes. *Cryptography and Communications*, 8 (1):19–32, January 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0134-9.

Wang:2016:LCD

[124] Qiuyan Wang, Yupeng Jiang, and Dongdai Lin. Linear complexity of Ding-Helleseth sequences of order 2 over GF(l). *Cryptography and Communications*, 8(1):33–49, January 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0138-5.

Gao:2016:CRT

[125] Jian Gao, Linzhi Shen, and Fang-Wei Fu. A Chinese remainder theorem approach to skew generalized quasi-cyclic codes over finite fields. *Cryptography and Communications*, 8 (1):51–66, January 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0140-y.

Cusick:2016:CEC

[126] Thomas W. Cusick and Pantelimon Stănică. Counting equivalence classes for monomial rotation symmetric Boolean functions with prime dimension. *Cryptography and Communications*, 8(1):67–81, January 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0143-8.

Sharma:2016:CSD

[127] Anuradha Sharma and Amit K. Sharma. Construction of self-dual codes over $\mathbf{Z}_{2^m}$. *Cryptography and Communications*, 8(1):83–101, January 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0139-4.

Lv:2016:NDP

[128] Chuan Lv, Tongjiang Yan, and Guozhen Xiao. New developments in q-polynomial codes. *Cryptography and Communications*, 8(1):103–112, January 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0147-4.

Banik:2016:CDC

[129] Subhadeep Banik. Conditional differential cryptanalysis of 105 round Grain v1. *Cryptography and Communications*,

8(1):113–137, January 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0146-5.

Honkala:2016:EOI

[130] Iiro Honkala, Olivier Hudry, and Antoine Lobstein. On the ensemble of optimal identifying codes in a twin-free graph. *Cryptography and Communications*, 8(1):139–153, January 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0148-3.

Xu:2016:CNA

[131] Guangkui Xu, Xiwang Cao, and Shanding Xu. Constructing new APN functions and bent functions over finite fields of odd characteristic via the switching method. *Cryptography and Communications*, 8(1):155–171, January 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0145-6.

Budaghyan:2016:ESI

[132] Lilya Budaghyan, Tor Helleseth, and Alexander Kholosha. Editorial: Special issue on Boolean functions and their applications. *Cryptography and Communications*, 8(2):173–174, April 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/content/pdf/10.1007/s12095-015-0171-4.pdf.

Katz:2016:NOP

[133] Daniel J. Katz and Philippe Langevin. New open problems related to old conjectures by Helleseth. *Cryptography and Communications*, 8(2):175–189, April 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0137-6.

Kasikci:2016:SCQ

[134] Canan Kaşıkcı, Wilfried Meidl, and Alev Topuzoğlu. Spectra of a class of quadratic functions: Average behaviour and counting functions. *Cryptography and Communications*, 8(2):191–214, April 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0142-9.

Li:2016:QPL

[135] Chunlei Li and Tor Helleseth. Quasi-perfect linear codes from planar and APN functions. *Cryptography and Communications*, 8(2):215–227, April 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0132-y.

Mesnager:2016:FCI

[136] Sihem Mesnager. Further constructions of infinite families of bent functions from new permutations and their duals. *Cryptography and Communications*, 8(2):229–246, April 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.

springer.com/accesspage/article/10.1007/s12095-015-0144-7.

Ivanov:2016:RGA

[137] Georgi Ivanov, Nikolay Nikolov, and Svetla Nikova. Reversed genetic algorithms for generation of bijective S-boxes with good cryptographic properties. *Cryptography and Communications*, 8(2):247–276, April 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0170-5.

Kazymyrov:2016:IAM

[138] Oleksandr Kazymyrov, Roman Oliynykov, and Håvard Raddum. Influence of addition modulo 2^n on algebraic attacks. *Cryptography and Communications*, 8(2):277–289, April 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0136-7.

Tan:2016:ECD

[139] Yin Tan, Guang Gong, and Bo Zhu. Enhanced criteria on differential uniformity and nonlinearity of cryptographically significant functions. *Cryptography and Communications*, 8(2):291–311, April 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0141-x.

Boyar:2016:VNM

[140] Joan Boyar, Magnus Gausdal Find, and René Peralta. On various nonlinearity measures for boolean functions. *Cryptography and Communications*, 8(3):313–330, July 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0150-9.

Bogos:2016:SPU

[141] Sonia Bogos, Florian Tramèr, and Serge Vaudenay. On solving LPN using BKW and variants: implementation and analysis. *Cryptography and Communications*, 8(3):331–369, July 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0149-2.

Cheng:2016:DPS

[142] Yuan Cheng, Wen-Feng Qi, Qun-Xiong Zheng, and Dong Yang. On the distinctness of primitive sequences over $\mathbf{Z}/(p^e q)$ modulo 2. *Cryptography and Communications*, 8(3):371–381, July 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0151-8.

Gu:2016:SPH

[143] Ting Gu and Andrew Klapper. Statistical properties of half-ℓ-sequences. *Cryptography and Communications*, 8(3):383–400, July 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0152-7.

Chakraborty:2016:AGA

[144] Kaushik Chakraborty and Subhamoy Maitra. Application of Grover's algorithm to check non-resiliency of a Boolean function. *Cryptography*

and Communications, 8(3):401–413, July 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-015-0156-3`.

Klove:2016:CSL

[145] Torleiv Kløve. On covering sets for limited-magnitude errors. *Cryptography and Communications*, 8(3): 415–433, July 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-015-0154-5`.

Lu:2016:WTC

[146] Yi Lu and Yvo Desmedt. Walsh transforms and cryptographic applications in bias computing. *Cryptography and Communications*, 8(3): 435–453, July 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-015-0155-4`.

Chakraborty:2016:MOB

[147] Debrup Chakraborty and Palash Sarkar. On modes of operations of a block cipher for authentication and authenticated encryption. *Cryptography and Communications*, 8(4):455–511, October 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-015-0153-6`.

Li:2016:DEJ

[148] Fulin Li, Shixin Zhu, Honggang Hu, and Ting Jiang. Determining the k-error joint linear complexity spectrum for a binary multisequence with period p^n. *Cryptography and Communications*, 8(4):513–523, October 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-015-0157-2`.

Xiang:2016:LCG

[149] Can Xiang. Linear codes from a generic construction. *Cryptography and Communications*, 8(4):525–539, October 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-015-0158-1`.

Xu:2016:OAC

[150] Guangkui Xu, Xiwang Cao, and Shanding Xu. Optimal p-ary cyclic codes with minimum distance four from monomials. *Cryptography and Communications*, 8(4):541–554, October 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-015-0159-0`.

Dravie:2016:MRV

[151] Brandon Dravie, Jérémy Parriaux, Philippe Guillot, and Gilles Millérioux. Matrix representations of vectorial Boolean functions and eigenanalysis. *Cryptography and Communications*, 8 (4):555–577, October 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-015-0160-7`.

Chin:2016:TBS

[152] Ji-Jian Chin, Syh-Yuan Tan, Swee-Huay Heng, and Raphael C.-W. Phan. Twin-

Beth: Security under active and concurrent attacks for the Beth identity-based identification scheme. *Cryptography and Communications*, 8(4): 579–591, October 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0162-5.

Jang:2016:LLP

[153] Ji-Woong Jang and Dae-Woon Lim. Large low probability of intercept properties of the quaternary sequence with optimal correlation property constructed by Legendre sequences. *Cryptography and Communications*, 8(4): 593–604, October 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0161-6.

Wang:2016:GCN

[154] Qiuyan Wang and Dongdai Lin. Generalized cyclotomic numbers of order two and their applications. *Cryptography and Communications*, 8(4): 605–616, October 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0165-2.

Sharma:2016:CCF

[155] Anuradha Sharma and Saroj Rani. On constacyclic codes over finite fields. *Cryptography and Communications*, 8 (4):617–636, October 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0163-4.

Schmidt:2016:NMR

[156] Kai-Uwe Schmidt. Nonlinearity measures of random Boolean functions. *Cryptography and Communications*, 8 (4):637–645, October 2016. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0164-3.

Ding:2017:PSF

[157] Cunsheng Ding and Zhengchun Zhou. Preface: Special functions and codes. *Cryptography and Communications*, 9 (1):1–2, January 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/content/pdf/10.1007/s12095-016-0201-x.pdf.

Abdukhalikov:2017:BFL

[158] Kanat Abdukhalikov and Sihem Mesnager. Bent functions linear on elements of some classical spreads and presemifields spreads. *Cryptography and Communications*, 9(1):3–21, January 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-016-0195-4.

Bezzateev:2017:QCG

[159] Sergey Bezzateev and Natalia Shekhunova. Quasi-cyclic Goppa codes with special Goppa polynomials and matched location sets. *Cryptography and Communications*, 9(1):23–39, January 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-016-0196-3.

Heng:2017:OCA

[160] Ziling Heng and Qin Yue. Optimal codebooks achieving the Levenshtein bound from generalized bent functions over $\mathbf{Z}_4$. *Cryptography and Communications*, 9(1):41–53, January 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-016-0194-5`.

Li:2017:CCL

[161] Chengju Li, Sunghan Bae, and Haode Yan. A construction of codes with linearity from two linear codes. *Cryptography and Communications*, 9(1):55–69, January 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-016-0193-6`.

Mesnager:2017:LCF

[162] Sihem Mesnager. Linear codes with few weights from weakly regular bent functions based on a generic construction. *Cryptography and Communications*, 9(1):71–84, January 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-016-0186-5`.

Wang:2017:SCC

[163] Qi Wang. Some cyclic codes with prime length from cyclotomy of order 4. *Cryptography and Communications*, 9(1):85–92, January 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-016-0188-3`.

Xiang:2017:CLC

[164] Can Xiang, Chunming Tang, and Keqin Feng. A class of linear codes with a few weights. *Cryptography and Communications*, 9(1):93–116, January 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-016-0200-y`.

Xu:2017:TCA

[165] Guangkui Xu, Xiwang Cao, and Shanding Xu. Two classes of p-ary bent functions and linear codes with three or four weights. *Cryptography and Communications*, 9(1):117–131, January 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-016-0199-0`.

Yang:2017:CTW

[166] Shudi Yang, Zheng-An Yao, and Chang-An Zhao. A class of three-weight linear codes and their complete weight enumerators. *Cryptography and Communications*, 9(1):133–149, January 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-016-0187-4`.

Zhang:2017:CWE

[167] Dan Zhang, Cuiling Fan, Daiyuan Peng, and Xiaohu Tang. Complete weight enumerators of some linear codes from quadratic forms. *Cryptography and Communications*, 9(1):151–163, January 2017. CODEN

???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-016-0190-9.

Zhou:2017:CNF

[168] Yue Zhou and Longjiang Qu. Constructions of negabent functions over finite fields. *Cryptography and Communications*, 9(2):165–180, March 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0167-0.

Li:2017:SRG

[169] Xin Li and Zihui Liu. On the second relative greedy weight. *Cryptography and Communications*, 9(2):181–197, March 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0168-z.

Wang:2017:CDG

[170] Lisha Wang and Xiaohu Tang. On the correlation distribution of the generalized maximal length $\mathbf{Z}_4$-sequences. *Cryptography and Communications*, 9(2):199–215, March 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0169-y.

Salagean:2017:CCF

[171] Ana Sălăgean and Matei Mandache-Sălăgean. Counting and characterising functions with "fast points" for differential attacks. *Cryptography and Communications*, 9(2):217–239, March 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/content/pdf/10.1007/s12095-015-0166-1.pdf.

Bandi:2017:MFN

[172] Rama Krishna Bandi, Maheshanand Bhaintwal, and Nuh Aydin. A mass formula for negacyclic codes of length 2^k and some good negacyclic codes over $\mathbf{Z}_4 + u\mathbf{Z}_4$. *Cryptography and Communications*, 9(2):241–272, March 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0172-3. See corrections [430].

Dubrova:2017:ESC

[173] Elena Dubrova and Martin Hell. Espresso: A stream cipher for 5G wireless communication systems. *Cryptography and Communications*, 9(2):273–289, March 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0173-2.

Wu:2017:GGQ

[174] Tingting Wu, Jian Gao, and Fang-Wei Fu. 1-generator generalized quasi-cyclic codes over $\mathbf{Z}_4$. *Cryptography and Communications*, 9(2):291–299, March 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0175-0.

Gangopadhyay:2017:CBF

[175] Sugata Gangopadhyay, Aditi Kar Gangopadhyay, Spyridon Pollatos, and

Pantelimon Stănică. Cryptographic Boolean functions with biased inputs. *Cryptography and Communications*, 9 (2):301–314, March 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0174-1.

Wang:2017:KTW

[176] Qiuyan Wang, Kelan Ding, Dongdai Lin, and Rui Xue. A kind of three-weight linear codes. *Cryptography and Communications*, 9(3): 315–322, May 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0180-3.

Heng:2017:CWD

[177] Ziling Heng and Qin Yue. Complete weight distributions of two classes of cyclic codes. *Cryptography and Communications*, 9(3):323–343, May 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0177-y.

Liu:2017:NBL

[178] Jian Liu, Sihem Mesnager, and Lusheng Chen. On the nonlinearity of S-boxes and linear codes. *Cryptography and Communications*, 9(3):345–361, May 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0176-z.

Peng:2017:NDU

[179] Jie Peng and Chik How Tan. New differentially 4-uniform permutations by modifying the inverse function on subfields. *Cryptography and Communications*, 9(3):363–378, May 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-016-0181-x.

Esmaeili:2017:NCF

[180] M. Esmaeili, M. Moosavi, and T. A. Gulliver. A new class of Fibonacci sequence based error correcting codes. *Cryptography and Communications*, 9 (3):379–396, May 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0178-x.

Cheng:2017:AOS

[181] Minquan Cheng, Jing Jiang, and Xiaohu Tang. Asymptotically optimal $\overline{2}$-separable codes with length 4. *Cryptography and Communications*, 9 (3):397–405, May 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-016-0182-9.

Liang:2017:SNC

[182] Miao Liang, Lijun Ji, and Jingcai Zhang. Some new classes of 2-fold optimal or perfect splitting authentication codes. *Cryptography and Communications*, 9(3):407–430, May 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-015-0179-9.

Lin:2017:PCR

[183] Zhiqiang Lin, Dongdai Lin, and Dingyi Pei. Practical construction of ring LFSRs and ring FCSRs with low diffusion delay for hardware cryptographic applications. *Cryptography and Communications*, 9(4):431–443, July 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Chen:2017:LCT

[184] Zhixiong Chen. Linear complexity and trace representation of quaternary sequences over $\mathbf{Z}_4$ based on generalized cyclotomic classes modulo pq. *Cryptography and Communications*, 9(4):445–458, July 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Raka:2017:CCQ

[185] Madhu Raka, Leetika Kathuria, and Mokshi Goyal. $(1-2u^3)$-constacyclic codes and quadratic residue codes over $\mathbf{F}_p[u]/\langle u^4-u\rangle$. *Cryptography and Communications*, 9(4):459–473, July 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Kewat:2017:CCS

[186] Pramod Kumar Kewat and Priti Kumari. Cyclic codes from the second class two-prime Whiteman's generalized cyclotomic sequence with order 6. *Cryptography and Communications*, 9 (4):475–499, July 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Merai:2017:ECL

[187] László Mérai, Harald Niederreiter, and Arne Winterhof. Expansion complexity and linear complexity of sequences over finite fields. *Cryptography and Communications*, 9(4):501–509, July 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Han:2017:NSO

[188] Hongyu Han, Daiyuan Peng, and Udaya Parampalli. New sets of optimal low-hit-zone frequency-hopping sequences based on m-sequences. *Cryptography and Communications*, 9(4):511–522, July 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Sarkar:2017:PSB

[189] Santanu Sarkar, Prakash Dey, Avishek Adhikari, and Subhamoy Maitra. Probabilistic signature based generalized framework for differential fault analysis of stream ciphers. *Cryptography and Communications*, 9(4):523–543, July 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Wang:2017:CWE

[190] Xianfang Wang, Jian Gao, and Fang-Wei Fu. Complete weight enumerators of two classes of linear codes. *Cryptography and Communications*, 9(5):545–562, September 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Xue:2017:BLA

[191] Shuai Xue, Wen-Feng Qi, and Xiao-Yuan Yang. On the best linear approximation of addition modulo 2^n. *Cryptography and Communications*, 9(5):563–580, September 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Laing:2017:LMS

[192] Thalia M. Laing, Keith M. Martin, Maura B. Paterson, and Douglas R. Stinson. Localised multisecret sharing. *Cryptography and Communications*, 9 (5):581–597, September 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Cao:2017:CCO

[193] Yuan Cao and Qingguo Li. Cyclic codes of odd length over $Z_4[u]/\langle u^k \rangle$. *Cryptography and Communications*, 9(5):599–624, September 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Wang:2017:SSS

[194] Xianfang Wang, Can Xiang, and Fang-Wei Fu. Secret sharing schemes for compartmented access structures. *Cryptography and Communications*, 9(5):625–635, September 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Shi:2017:TTW

[195] Minjia Shi, Rongsheng Wu, Yan Liu, and Patrick Solé. Two and three weight codes over $\mathbf{F}_p + u\mathbf{F}_p$. *Cryptography and Communications*, 9(5):637–646, September 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Tang:2017:CHB

[196] Chunming Tang and Yanfeng Qi. A class of hyper-bent functions and Kloosterman sums. *Cryptography and Communications*, 9(5):647–664, September 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

Alaca:2017:CVS

[197] Saban Alaca and Goldwyn Millar. Character values of the Sidelnikov–Lempel–Cohn–Eastman sequences. *Cryptography and Communications*, 9(6):665–682, November 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-016-0208-3`.

Edemskiy:2017:DSH

[198] Vladimir Edemskiy and Xiaoni Du. Design sequences with high linear complexity over finite fields using generalized cyclotomy. *Cryptography and Communications*, 9(6):683–691, November 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-016-0209-2`.

Li:2017:SCP

[199] Nian Li and Tor Helleseth. Several classes of permutation trinomials from Niho exponents. *Cryptography and Communications*, 9(6):693–705, November 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-016-0210-9`.

Zhou:2017:GMC

[200] Limengnan Zhou, Daiyuan Peng, Hongbin Liang, Changyuan Wang, and Hongyu Han. Generalized methods to construct low-hit-zone frequency-hopping sequence sets and optimal constructions. *Cryptography and Communications*, 9(6):707–728, November 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL

http://link.springer.com/article/10.1007/s12095-017-0211-3.

Wolfmann:2017:SBF

[201] J. Wolfmann. Sequences of bent functions and near-bent functions. *Cryptography and Communications*, 9(6):729–736, November 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0212-2.

Dietrich:2017:NFA

[202] Heiko Dietrich and Nathan Jolly. A new family of arrays with low autocorrelation. *Cryptography and Communications*, 9(6):737–748, November 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0214-0.

Ferard:2017:IHS

[203] Eric Férard. On the irreducibility of the hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in characteristic 2. II. *Cryptography and Communications*, 9(6):749–767, November 2017. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0213-1.

Helleseth:2018:ESI

[204] Tor Helleseth and Bart Preneel. Editorial: Special issue on recent trends in cryptography. *Cryptography and Communications*, 10(1):1–3, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0269-y; http://link.springer.com/content/pdf/10.1007/s12095-017-0269-y.pdf.

Scott:2018:MTK

[205] Michael Scott. Missing a trick: Karatsuba variations. *Cryptography and Communications*, 10(1):5–15, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0217-x.

Ferradi:2018:BAM

[206] Houda Ferradi, Rémi Géraud, Diana Maimut, David Naccache, and Hang Zhou. Backtracking-assisted multiplication. *Cryptography and Communications*, 10(1):17–26, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0254-5.

Bogos:2018:CHE

[207] Sonia Bogos, John Gaspoz, and Serge Vaudenay. Cryptanalysis of a homomorphic encryption scheme. *Cryptography and Communications*, 10(1):27–39, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0243-8.

Lacharite:2018:SBB

[208] Marie-Sarah Lacharité. Security of BLS and BGLS signatures in a multi-user setting. *Cryptography and Communications*, 10(1):41–58, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0253-6; http://

link.springer.com/content/pdf/10.1007/s12095-017-0253-6.pdf.

Nachef:2018:GAS

[209] Valérie Nachef, Jacques Patarin, and Emmanuel Volte. Generic attacks with standard deviation analysis on a-Feistel schemes. *Cryptography and Communications*, 10(1):59–77, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0244-7.

Hemenway:2018:ERS

[210] Brett Hemenway and Rafail Ostrovsky. Efficient robust secret sharing from expander graphs. *Cryptography and Communications*, 10(1):79–99, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0215-z.

deCherisey:2018:OPM

[211] Éloi de Chérisey, Sylvain Guilley, Annelie Heuser, and Olivier Rioul. On the optimality and practicability of mutual information analysis in some scenarios. *Cryptography and Communications*, 10(1):101–121, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0241-x.

Rose:2018:KBT

[212] Gregory G. Rose. KISS: A bit too simple. *Cryptography and Communications*, 10(1):123–137, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0225-x; http://link.springer.com/content/pdf/10.1007/s12095-017-0225-x.pdf.

Poh:2018:SSE

[213] Geong Sen Poh, Moesfa Soeheila Mohamad, and Ji-Jian Chin. Searchable symmetric encryption over multiple servers. *Cryptography and Communications*, 10(1):139–158, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0232-y.

Fabsic:2018:GIC

[214] Tomás Fabsic, Otokar Grosek, Karol Nemoga, and Pavol Zajac. On generating invertible circulant binary matrices with a prescribed number of ones. *Cryptography and Communications*, 10(1):159–175, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0239-4.

Forler:2018:PBB

[215] Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel. POEx: A beyond-birthday-bound-secure online cipher. *Cryptography and Communications*, 10(1):177–193, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0250-9.

Cui:2018:SIA

[216] Tingting Cui, Huaifeng Chen, Long Wen, and Meiqin Wang. Statistical integral attack on CAST-256 and IDEA. *Cryptography and Communications*, 10(1):195–209, January 2018.

CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0245-6.

Pierrot:2018:MBE

[217] Cécile Pierrot and Benjamin Wesolowski. Malleability of the blockchain's entropy. *Cryptography and Communications*, 10(1):211–233, January 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0264-3.

Anbar:2018:MPF

[218] Nurdagül Anbar and Wilfried Meidl. Modified planar functions and their components. *Cryptography and Communications*, 10(2):235–249, March 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0218-9.

Chang:2018:CBS

[219] Zuling Chang, Martianus Frederic Ezerman, San Ling, and Huaxiong Wang. Construction of de Bruijn sequences from product of two irreducible polynomials. *Cryptography and Communications*, 10(2):251–275, March 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0219-8.

Sok:2018:CCQ

[220] Lin Sok, MinJia Shi, and Patrick Solé. Classification and construction of quaternary self-dual bent functions. *Cryptography and Communications*, 10(2):277–289, March 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0216-y.

Tan:2018:WDC

[221] Pan Tan, Zhengchun Zhou, Deng Tang, and Tor Helleseth. The weight distribution of a class of two-weight linear codes derived from Kloosterman sums. *Cryptography and Communications*, 10(2):291–299, March 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0221-1.

Luo:2018:BLC

[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 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0220-2.

Ding:2018:SCC

[223] Cunsheng Ding. A sequence construction of cyclic codes over finite fields. *Cryptography and Communications*, 10(2):319–341, March 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0222-0.

Goyal:2018:QRC

[224] Mokshi Goyal and Madhu Raka. Quadratic residue codes over the ring $\mathbf{F}_p[u]/\langle u^m - u\rangle$ and their Gray images. *Cryptography and Communications*, 10(2):343–355, March 2018.

CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0223-z`.

Acevedo:2018:PSQ

[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): 357–368, March 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0224-y`.

Klapper:2018:MPS

[226] Andrew Klapper. Matrix parametrized shift registers. *Cryptography and Communications*, 10(2):369–382, March 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0226-9`.

Dubrova:2018:MAB

[227] Elena Dubrova, Mats Näslund, Göran Selander, and Fredrik Lindqvist. Message authentication based on cryptographically secure CRC without polynomial irreducibility test. *Cryptography and Communications*, 10(2): 383–399, March 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0227-8`; `http://link.springer.com/content/pdf/10.1007/s12095-017-0227-8.pdf`.

Sharma:2018:EFS

[228] Anuradha Sharma and Taranjot Kaur. Enumeration formulae for self-dual, self-orthogonal and complementary-dual quasi-cyclic codes over finite fields. *Cryptography and Communications*, 10(3):401–435, May 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0228-7`.

Xu:2018:TCN

[229] Shanding Xu, Xiwang Cao, Guangkui Xu, and Gaojun Luo. Two classes of near-optimal frequency-hopping sequence sets with prime-power period. *Cryptography and Communications*, 10(3):437–454, May 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0229-6`.

Wang:2018:LBA

[230] Li-Ping Wang and Daqing Wan. On lattice-based algebraic feedback shift registers synthesis for multisequences. *Cryptography and Communications*, 10(3):455–465, May 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0230-0`.

Sun:2018:EAD

[231] Yuhua Sun, Qiang Wang, and Tongjiang Yan. The exact autocorrelation distribution and 2-adic complexity of a class of binary sequences with almost optimal autocorrelation. *Cryptography and Communications*, 10(3):467–477, May 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0233-x`.

Jana:2018:RRK

[232] Amit Jana and Goutam Paul. Revisiting RC4 key collision: Faster search algorithm and new 22-byte colliding key pairs. *Cryptography and Communications*, 10(3):479–508, May 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0231-z.

Boztas:2018:GNS

[233] Serdar Boztas, Ferruh Özbudak, and Eda Tekin. Generalized nonbinary sequences with perfect autocorrelation, flexible alphabets and new periods. *Cryptography and Communications*, 10(3):509–517, May 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0237-6.

Sobhani:2018:CCN

[234] R. Sobhani. Cyclic codes over a noncommutative finite chain ring. *Cryptography and Communications*, 10(3):519–530, May 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0238-5.

Li:2018:PPF

[235] Kangquan Li, Longjiang Qu, Xi Chen, and Chao Li. Permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$ and permutation trinomials over finite fields with even characteristic. *Cryptography and Communications*, 10(3):531–554, May 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0236-7.

Zhang:2018:BCO

[236] Xuli Zhang, Jing Jiang, and Minquan Cheng. Bounds and constructions for $\overline{3}$-strongly separable codes with length 3. *Cryptography and Communications*, 10(3):555–565, May 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0235-8.

Zha:2018:NRP

[237] Zhengbang Zha, Lei Hu, and Zhizheng Zhang. New results on permutation polynomials of the form $(x^{pm} - x + \delta)^s + x^{pm} + x$ over $\mathbf{F}p^{2m}$. *Cryptography and Communications*, 10(3):567–578, May 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0234-9.

Liu:2018:NQC

[238] Xiusheng Liu, Hai Q. Dinh, Hualu Liu, and Long Yu. On new quantum codes from matrix product codes. *Cryptography and Communications*, 10(4):579–589, July 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0242-9.

Yi:2018:GMC

[239] Zongxiang Yi, Zhiqiang Lin, and Lishan Ke. A generic method to construct zero-difference balanced functions. *Cryptography and Communications*, 10(4):591–609, July 2018. CODEN ???? ISSN 1936-2447

(print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0247-4.

Alsalami:2018:CHA

[240] Yousuf Alsalami. Constructions with high algebraic degree of differentially 4-uniform $(n, n-1)$-functions and differentially 8-uniform $(n, n-2)$-functions. *Cryptography and Communications*, 10(4):611–628, July 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0246-5.

Mandal:2018:ITD

[241] Kalikinkar Mandal, Bo Yang, Guang Gong, and Mark Aagaard. On ideal t-tuple distribution of filtering de Bruijn sequence generators. *Cryptography and Communications*, 10(4):629–641, July 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0248-3.

Sun:2018:SPD

[242] Zhonghua Sun, Shixin Zhu, and Liqi Wang. The symbol-pair distance distribution of a class of repeated-root cyclic codes over $\mathbf{F}_{p^m}$. *Cryptography and Communications*, 10(4):643–653, July 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0249-2.

Castro:2018:EDE

[243] Francis N. Castro, Luis A. Medina, and Ivelisse M. Rubio. Exact 2-divisibility of exponential sums associated to boolean functions. *Cryptography and Communications*, 10(4):655–666, July 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0252-7.

Barcucci:2018:NOC

[244] Elena Barcucci, Antonio Bernini, Stefano Bilotta, and Renzo Pinzani. A 2D non-overlapping code over a q-ary alphabet. *Cryptography and Communications*, 10(4):667–683, July 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0251-8.

Jitman:2018:GIS

[245] Somphong Jitman. Good integers and some applications in coding theory. *Cryptography and Communications*, 10(4):685–704, July 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0255-4. See correction [270].

Tuxanidy:2018:CDS

[246] Aleksandr Tuxanidy and Qiang Wang. Characteristic digit-sum sequences. *Cryptography and Communications*, 10(4):705–717, July 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0256-3.

Galvez:2018:SBB

[247] Lucky Galvez, Jon-Lark Kim, Nari Lee, Young Gun Roe, and Byung-Sun Won. Some bounds on binary LCD codes. *Cryptography and Communications*, 10(4):719–728, July

2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0258-1.

Maitra:2018:GE

[248] Subhamoy Maitra. Guest editorial. *Cryptography and Communications*, 10 (5):729–730, September 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0312-7; http://link.springer.com/content/pdf/10.1007/s12095-018-0312-7.pdf.

Jha:2018:RBB

[249] Ashwin Jha and Mridul Nandi. On rate-1 and beyond-the-birthday bound secure online ciphers using tweakable block ciphers. *Cryptography and Communications*, 10(5):731–753, September 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0275-0.

Cui:2018:SID

[250] Tingting Cui, Huaifeng Chen, Sihem Mesnager, Ling Sun, and Meiqin Wang. Statistical integral distinguisher with multi-structure and its application on AES-like ciphers. *Cryptography and Communications*, 10(5):755–776, September 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0286-5.

Paterson:2018:SAC

[251] Kenneth G. Paterson and Jacob C. N. Schuldt. Statistical attacks on cookie masking for RC4. *Cryptography and Communications*, 10(5): 777–801, September 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0280-y; http://link.springer.com/content/pdf/10.1007/s12095-018-0280-y.pdf.

Hamann:2018:DAS

[252] Matthias Hamann, Matthias Krause, Willi Meier, and Bin Zhang. Design and analysis of small-state grain-like stream ciphers. *Cryptography and Communications*, 10(5):803–834, September 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0261-6.

Samajder:2018:SPM

[253] Subhabrata Samajder and Palash Sarkar. Success probability of multiple/multidimensional linear cryptanalysis under general key randomisation hypotheses. *Cryptography and Communications*, 10(5):835–879, September 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0257-2.

Paul:2018:ABP

[254] Goutam Paul and Souvik Ray. Analysis of burn-in period for RC4 state transition. *Cryptography and Communications*, 10(5):881–908, September 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0287-4.

Carlet:2018:SPS

[255] Claude Carlet and Sylvain Guilley. Statistical properties of side-channel and fault injection attacks using coding theory. *Cryptography and Communications*, 10(5):909–933, September 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0271-4.

Bhattacharya:2018:NCS

[256] Srimanta Bhattacharya and Mridul Nandi. A note on the chi-square method: A tool for proving cryptographic security. *Cryptography and Communications*, 10(5):935–957, September 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0276-z.

Hamann:2018:SCP

[257] Matthias Hamann and Matthias Krause. On stream ciphers with provable beyond-the-birthday-bound security against time-memory-data tradeoff attacks. *Cryptography and Communications*, 10(5):959–1012, September 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0294-5.

Merai:2018:PAS

[258] László Mérai and Arne Winterhof. On the pseudorandomness of automatic sequences. *Cryptography and Communications*, 10(6):1013–1022, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0260-7.

Bai:2018:NCP

[259] Tao Bai and Yongbo Xia. A new class of permutation trinomials constructed from Niho exponents. *Cryptography and Communications*, 10(6):1023–1036, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0263-4.

Meidl:2018:NAB

[260] Wilfried Meidl and Ísabel Pirsic. On the normality of p-ary bent functions. *Cryptography and Communications*, 10(6):1037–1049, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0259-0; http://link.springer.com/content/pdf/10.1007/s12095-017-0259-0.pdf.

Carlet:2018:NMB

[261] Claude Carlet. On the nonlinearity of monotone Boolean functions. *Cryptography and Communications*, 10(6):1051–1061, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0262-5.

Gu:2018:CIF

[262] Ting Gu, Zhixiong Chen, and Andrew Klapper. Correlation immune functions with respect to the q-transform. *Cryptography and Communications*, 10(6):1063–1073, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0267-0.

UlHasan:2018:NVP

[263] Sartaj Ul Hasan, Daniel Panario, and Qiang Wang. Nonlinear vectorial primitive recursive sequences. *Cryptography and Communications*, 10(6):1075–1090, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0265-2`.

Luo:2018:CWE

[264] Gaojun Luo and Xiwang Cao. Complete weight enumerators of three classes of linear codes. *Cryptography and Communications*, 10(6):1091–1108, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0270-5`.

Luo:2018:CCM

[265] Rong Luo and Udaya Parampalli. Cyclic codes over $M_2(\mathbf{F}_2 + u\mathbf{F}_2)$. *Cryptography and Communications*, 10(6):1109–1117, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0266-1`.

Luo:2018:FCO

[266] Gaojun Luo and Xiwang Cao. Five classes of optimal two-weight linear codes. *Cryptography and Communications*, 10(6):1119–1135, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0272-3`.

Samajder:2018:MTD

[267] Subhabrata Samajder and Palash Sarkar. Multiple (truncated) differential cryptanalysis: Explicit upper bounds on data complexity. *Cryptography and Communications*, 10(6):1137–1163, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0268-z`.

Shi:2018:SQM

[268] Xueying Shi, Qin Yue, and Yaotsu Chang. Some quantum MDS codes with large minimum distance from generalized Reed–Solomon codes. *Cryptography and Communications*, 10(6):1165–1182, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0274-1`.

Chang:2018:CSL

[269] Zuling Chang, Martianus Frederic Ezerman, San Ling, and Huaxiong Wang. The cycle structure of LFSR with arbitrary characteristic polynomial over finite fields. *Cryptography and Communications*, 10(6):1183–1202, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0273-2`.

Jitman:2018:CGI

[270] Somphong Jitman. Correction to: Good integers and some applications in coding theory. *Cryptography and Communications*, 10(6):1203, November 2018. CODEN ???? ISSN 1936-2447 (print),

1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0314-5; http://link.springer.com/content/pdf/10.1007/s12095-018-0314-5.pdf. See [245].

Budaghyan:2019:ESIa

[271] Lilya Budaghyan, Claude Carlet, and Tor Helleseth. Editorial: Special issue on Boolean functions and their applications. *Cryptography and Communications*, 11(1):1–2, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0341-2; http://link.springer.com/content/pdf/10.1007/s12095-018-0341-2.pdf.

Villa:2019:AFL

[272] Irene Villa. On APN functions $L_1(x^3) + L_2(x^9)$ with linear L_1 and L_2. *Cryptography and Communications*, 11(1):3–20, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0283-8.

Idrisova:2019:AGA

[273] Valeriya Idrisova. On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem". *Cryptography and Communications*, 11(1):21–39, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0310-9.

Mariot:2019:CAB

[274] Luca Mariot, Stjepan Picek, Alberto Leporati, and Domagoj Jakobovic. Cellular automata based S-boxes. *Cryptography and Communications*, 11(1): 41–62, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0311-8.

Mesnager:2019:NBF

[275] Sihem Mesnager, Zhengchun Zhou, and Cunsheng Ding. On the nonlinearity of Boolean functions with restricted input. *Cryptography and Communications*, 11(1):63–76, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0293-6.

Mandal:2019:NCA

[276] Bimal Mandal, Pantelimon Stanica, and Sugata Gangopadhyay. New classes of p-ary bent functions. *Cryptography and Communications*, 11(1):77–92, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0290-9.

Calik:2019:MCV

[277] Çagdas Çalik, Meltem Sönmez Turan, and René Peralta. The multiplicative complexity of 6-variable Boolean functions. *Cryptography and Communications*, 11(1):93–107, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0297-2.

Boyar:2019:SLD

[278] Joan Boyar, Magnus Gausdal Find, and René Peralta. Small low-depth

circuits for cryptographic applications. *Cryptography and Communications*, 11(1):109–127, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0296-3.

Li:2019:NPT

[279] Nian Li and Tor Helleseth. New permutation trinomials from Niho exponents over finite fields with even characteristic. *Cryptography and Communications*, 11(1):129–136, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0321-6.

Liu:2019:SNC

[280] Hongwei Liu and Youcef Maouche. Several new classes of linear codes with few weights. *Cryptography and Communications*, 11(2):137–146, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0277-y.

Martinez-Penas:2019:USR

[281] Umberto Martínez-Peñas. Universal secure rank-metric coding schemes with optimal communication overheads. *Cryptography and Communications*, 11(2):147–166, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0279-4.

Wang:2019:IDE

[282] Lin Wang and Zhi Hu. Injectivity on distribution of elements in the compressed sequences derived from primitive sequences over $\mathbf{Z}_{\mathbf{p}^{\mathbf{e}}}$. *Cryptography and Communications*, 11(2):167–189, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-017-0278-x.

Michel:2019:SNB

[283] Jerod Michel and Qi Wang. Some new balanced and almost balanced quaternary sequences with low autocorrelation. *Cryptography and Communications*, 11(2):191–206, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0281-x.

Pasalic:2019:BFN

[284] Enes Pasalic, Samir Hodžić, Fengrong Zhang, and Yongzhuang Wei. Bent functions from nonlinear permutations and conversely. *Cryptography and Communications*, 11(2):207–225, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0282-9.

Deng:2019:MCP

[285] Huali Deng and Dabin Zheng. More classes of permutation trinomials with Niho exponents. *Cryptography and Communications*, 11(2):227–236, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0284-7.

Geil:2019:AVC

[286] Olav Geil and Ferruh Özbudak. On affine variety codes from the Klein quartic. *Cryptography and Communications*, 11(2):237–257, ???? 2019.

CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0285-6.

Yan:2019:NCM

[287] Haode Yan. A note on the constructions of MDS self-dual codes. *Cryptography and Communications*, 11(2): 259–268, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0288-3.

Wang:2019:NBC

[288] Qichun Wang and Pantelimon Stanica. New bounds on the covering radius of the second order Reed–Muller code of length 128. *Cryptography and Communications*, 11(2):269–277, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0289-2.

Li:2019:CIP

[289] Kangquan Li, Longjiang Qu, and Qiang Wang. Compositional inverses of permutation polynomials of the form $x^r h(x^s)$ over finite fields. *Cryptography and Communications*, 11(2):279–298, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0292-7.

Gao:2019:UBC

[290] Zhe Gao, Chao Li, and Yue Zhou. Upper bounds and constructions of complete asynchronous channel hopping systems. *Cryptography and Communications*, 11(2):299–312, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0295-4.

Wu:2019:SCP

[291] Gaofei Wu and Nian Li. Several classes of permutation trinomials over $\mathbf{F}_{5^n}$ from Niho exponents. *Cryptography and Communications*, 11(2):313–324, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0291-8.

Ashraf:2019:QCC

[292] Mohammad Ashraf and Ghulam Mohammad. Quantum codes over F_p from cyclic codes over $F_p[u,v]/\langle u^2-1, v^3-v, uv-vu\rangle$. *Cryptography and Communications*, 11(2):325–335, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0299-0.

Sun:2019:LBA

[293] Yuhua Sun, Qiang Wang, and Tongjiang Yan. A lower bound on the 2-adic complexity of the modified Jacobi sequence. *Cryptography and Communications*, 11(2):337–349, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0300-y.

Rostami:2019:CWW

[294] Saeed Rostami, Elham Shakour, Mohammad Ali Orumiehchiha, and Josef Pieprzyk. Cryptanalysis of WG-8 and WG-16 stream ciphers. *Cryptography and Communications*, 11(2): 351–362, ???? 2019. CODEN ????

ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0298-1.

Budaghyan:2019:ESIb

[295] Lilya Budaghyan, Chunlei Li, and Matthew G. Parker. Editorial: Special issue on mathematical methods for cryptography. *Cryptography and Communications*, 11(3):363–365, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00356-8; http://link.springer.com/content/pdf/10.1007/s12095-019-00356-8.pdf.

Nyberg:2019:ALC

[296] Kaisa Nyberg. Affine linear cryptanalysis. *Cryptography and Communications*, 11(3):367–377, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0325-2.

Nikova:2019:DPF

[297] Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. Decomposition of permutations in a finite field. *Cryptography and Communications*, 11(3):379–384, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0317-2.

Varici:2019:CBU

[298] Kerem Varici, Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. Constructions of S-boxes with uniform sharing. *Cryptography and Communications*, 11(3):385–398, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0345-y.

Csirmaz:2019:SSL

[299] László Csirmaz and Péter Ligeti. Secret sharing on large girth graphs. *Cryptography and Communications*, 11(3):399–410, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0338-x.

Chen:2019:EAW

[300] Yao Chen, Benjamin M. Case, Shuhong Gao, and Guang Gong. Error analysis of weak Poly–LWE instances. *Cryptography and Communications*, 11(3):411–426, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0301-x.

Felke:2019:SBP

[301] Patrick Felke. On the security of biquadratic C^* public-key cryptosystems and its generalizations. *Cryptography and Communications*, 11(3):427–442, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0337-y.

Raddum:2019:FUB

[302] Håvard Raddum and Srimathi Varadharajan. Factorization using binary decision diagrams. *Cryptography and Communications*, 11(3):443–460, ???? 2019. CODEN ???? ISSN 1936-2447

(print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0304-7.

Zinoviev:2019:CKS

[303] V. A. Zinoviev. On classical Kloosterman sums. *Cryptography and Communications*, 11(3):461–496, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00357-7.

Bojilov:2019:CNF

[304] Assen Bojilov, Lyubomir Borissov, and Yuri Borissov. Computing the number of finite field elements with prescribed absolute trace and co-trace. *Cryptography and Communications*, 11(3):497–507, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0336-z.

Li:2019:SAN

[305] Nian Li and Xiangyong Zeng. A survey on the applications of Niho exponents. *Cryptography and Communications*, 11(3):509–548, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0305-6.

Klove:2019:CLT

[306] Torleiv Kløve. Codes of length two correcting single errors of limited size. *Cryptography and Communications*, 11(3):549–555, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0327-0.

Buratti:2019:HPD

[307] Marco Buratti. Hadamard partitioned difference families and their descendants. *Cryptography and Communications*, 11(4):557–562, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0308-3.

Tu:2019:CPT

[308] Ziran Tu and Xiangyong Zeng. A class of permutation trinomials over finite fields of odd characteristic. *Cryptography and Communications*, 11(4):563–583, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0307-4.

Napp:2019:PSS

[309] Diego Napp, Ricardo Pereira, Raquel Pinto, and Paula Rocha. Periodic state-space representations of periodic convolutional codes. *Cryptography and Communications*, 11(4):585–595, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0313-6.

Harada:2019:SES

[310] Masaaki Harada. Singly even self-dual codes of length $24k + 10$ and minimum weight $4k + 2$. *Cryptography and Communications*, 11(4):597–608, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0303-8.

Yang:2019:CWE

[311] Shudi Yang, Qin Yue, Yansheng Wu, and Xiangli Kong. Complete weight enumerators of a class of two-weight linear codes. *Cryptography and Communications*, 11(4):609–620, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0315-4.

Junnila:2019:OBC

[312] Ville Junnila, Tero Laihonen, and Gabrielle Paris. Optimal bounds on codes for location in circulant graphs. *Cryptography and Communications*, 11(4):621–640, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0316-3.

Kavut:2019:RSB

[313] Selçuk Kavut and Sevdenur Baloglu. Results on symmetric S-boxes constructed by concatenation of RSSBs. *Cryptography and Communications*, 11(4):641–660, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0318-1.

Zhou:2019:FHS

[314] Limengnan Zhou, Daiyuan Peng, Xing Liu, Hongyu Han, and Zheng Ma. Frequency-hopping sequence sets with good aperiodic Hamming correlation property. *Cryptography and Communications*, 11(4):661–675, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0320-7.

Harada:2019:BLC

[315] Masaaki Harada and Ken Saito. Binary linear complementary dual codes. *Cryptography and Communications*, 11(4):677–696, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0319-0.

Dey:2019:SMR

[316] Sabyasachi Dey and Santanu Sarkar. Settling the mystery of $Z_r = r$ in RC4. *Cryptography and Communications*, 11(4):697–715, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0323-4.

Qian:2019:SDL

[317] Liqin Qian, Minjia Shi, and Patrick Solé. On self-dual and LCD quasi-twisted codes of index two over a special chain ring. *Cryptography and Communications*, 11(4):717–734, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0322-5.

Xiao:2019:BSP

[318] Zibi Xiao, Xiangyong Zeng, Chaoyun Li, and Yupeng Jiang. Binary sequences with period N and nonlinear complexity $N - 2$. *Cryptography and Communications*, 11(4):735–757, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0324-3.

Wang:2019:DCC

[319] Gang Wang, Min-Yao Niu, and Fang-Wei Fu. Deterministic constructions of compressed sensing matrices based on codes. *Cryptography and Communications*, 11(4):759–775, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0328-z.

Oblaukhov:2019:LBS

[320] Alexey Oblaukhov. A lower bound on the size of the largest metrically regular subset of the Boolean cube. *Cryptography and Communications*, 11(4):777–791, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0326-1.

Gorodilova:2019:DEA

[321] Anastasiya Gorodilova. On the differential equivalence of APN functions. *Cryptography and Communications*, 11(4):793–813, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0329-y.

Li:2019:CNO

[322] Yu Li, Tongjiang Yan, and Chuan Lv. Construction of a near-optimal quasi-complementary sequence set from almost difference set. *Cryptography and Communications*, 11(4):815–824, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0330-5.

Luo:2019:TCA

[323] Gaojun Luo and Xiwang Cao. Two constructions of asymptotically optimal codebooks. *Cryptography and Communications*, 11(4):825–838, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0331-4.

Climent:2019:CAN

[324] Joan-Josep Climent, Verónica Requena, and Xaro Soler-Escrivà. A construction of Abelian non-cyclic orbit codes. *Cryptography and Communications*, 11(5):839–852, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0306-5.

Wu:2019:BFS

[325] Gaofei Wu and Matthew Geoffrey Parker. On Boolean functions with several flat spectra. *Cryptography and Communications*, 11(5):853–880, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0309-2.

Laaksonen:2019:NLB

[326] Antti Laaksonen and Patric R. J. Östergård. New lower bounds on q-ary error-correcting codes. *Cryptography and Communications*, 11(5): 881–889, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0302-9.

Aydin:2019:NLC

[327] Nuh Aydin, Ghada Bakbouk, and Jonathan G. G. Lambrinos. New linear codes over non-prime fields. *Cryptography and Communications*, 11(5): 891–902, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0333-2.

Bartoli:2019:NBL

[328] Daniele Bartoli, Alexander A. Davydov, Massimo Giulietti, Stefano Marcugini, and Fernanda Pambianco. New bounds for linear codes of covering radii 2 and 3. *Cryptography and Communications*, 11(5):903–920, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0335-0.

Uguz:2019:RCT

[329] Muhiddin Uguz, Ali Doganaksoy, Fatih Sulak, and Onur Koçak. R-2 composition tests: a family of statistical randomness tests for a collection of binary sequences. *Cryptography and Communications*, 11(5):921–949, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0334-1.

Wang:2019:NEI

[330] Lin Wang and Zhi Hu. New explicit injective compressing mappings on primitive sequences over $\mathbf{Z}_{p^e}$. *Cryptography and Communications*, 11(5):951–963, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0332-3.

Rabii:2019:NCS

[331] Hila Rabii and Osnat Keren. A new class of security oriented error correcting robust codes. *Cryptography and Communications*, 11(5):965–978, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0340-3.

Gao:2019:SBR

[332] Ying Gao, Zihui Liu, and Yiwei Liu. The separation of binary relative three-weight codes and its applications. *Cryptography and Communications*, 11(5):979–992, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0339-9.

Hofer:2019:ONC

[333] Richard Hofer and Arne Winterhof. r-th order nonlinearity, correlation measure and least significant bit of the discrete logarithm. *Cryptography and Communications*, 11(5):993–997, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0344-z.

Naghipour:2019:NCQ

[334] Avaz Naghipour. New classes of quantum codes on closed orientable surfaces. *Cryptography and Communications*, 11(5):999–1008, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0347-9.

Johnsen:2019:RPE

[335] Trygve Johnsen and Hugues Verdure. Relative profiles and extended weight polynomials of almost affine codes. *Cryptography and Communications*, 11(5):1009–1020, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0348-8.

Garcia:2019:NMD

[336] Ismael Gutiérrez García, Daladier Jabba Molinares, and Ivan Molina Naizir. A novel maximum distance separable code to generate universal identifiers. *Cryptography and Communications*, 11(5):1021–1035, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0346-x.

Liang:2019:LCD

[337] Yana Liang, Jiali Cao, Xingfa Chen, Shiping Cai, and Xiang Fan. Linear complexity of Ding–Helleseth generalized cyclotomic sequences of order eight. *Cryptography and Communications*, 11(5):1037–1056, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0343-0.

Wang:2019:FRP

[338] Libo Wang, Baofeng Wu, Xiaoqiang Yue, and Yanbin Zheng. Further results on permutation trinomials with Niho exponents. *Cryptography and Communications*, 11(5):1057–1068, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-0349-2.

Radonjic:2019:ICC

[339] Aleksandar Radonjic and Vladimir Vujicic. Integer codes correcting sparse byte errors. *Cryptography and Communications*, 11(5):1069–1077, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-0350-9.

Hodzic:2019:IML

[340] S. Hodžić, E. Pasalic, and A. Chattopadhyay. An iterative method for linear decomposition of index generating functions. *Cryptography and Communications*, 11(5):1079–1102, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-0351-8.

Guneri:2019:CCL

[341] Cem Güneri, Ferruh Özbudak, and Elif Saçikara. A concatenated construction of linear complementary pair of codes. *Cryptography and Communications*, 11(5):1103–1114, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-0354-5.

Beemer:2019:ASC

[342] Allison Beemer, Kathryn Haymaker, and Christine A. Kelley. Absorbing sets of codes from finite geometries. *Cryptography and Communications*, 11(5):1115–1131, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL

http://link.springer.com/article/10.1007/s12095-019-0353-6.

Tang:2019:RAB

[343] Chunming Tang, Yanfeng Qi, and Dongmei Huang. Regular p-ary bent functions with five terms and Kloosterman sums. *Cryptography and Communications*, 11(5):1133–1144, ???? 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-0355-4.

Budaghyan:2019:ESI

[344] Lilya Budaghyan, Claude Carlet, and Tor Helleseth. Editorial: Special issue on Boolean functions and their applications 2018. *Cryptography and Communications*, 11(6):1145–1146, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00409-y; https://link.springer.com/content/pdf/10.1007/s12095-019-00409-y.pdf.

Canteaut:2019:IGB

[345] Anne Canteaut, Léo Perrin, and Shizhu Tian. If a generalised butterfly is APN then it operates on 6 bits. *Cryptography and Communications*, 11(6):1147–1164, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00361-x.

Kaleyski:2019:CAF

[346] Nikolay S. Kaleyski. Changing APN functions at two points. *Cryptography and Communications*, 11(6):1165–1184, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00366-6.

Tang:2019:FWA

[347] Deng Tang and Jian Liu. A family of weightwise (almost) perfectly balanced boolean functions with optimal algebraic immunity. *Cryptography and Communications*, 11(6):1185–1197, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00374-6.

Hou:2019:CPT

[348] Xiang dong Hou. On a class of permutation trinomials in characteristic 2. *Cryptography and Communications*, 11(6):1199–1210, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-018-0342-1.

Gravel:2019:USP

[349] Claude Gravel, Daniel Panario, and David Thomson. Unicyclic strong permutations. *Cryptography and Communications*, 11(6):1211–1231, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00384-4.

Meidl:2019:GBF

[350] Wilfried Meidl and Alexander Pott. Generalized bent functions into $\mathbf{Z}_{p^k}$ from the partial spread and the Maiorana–McFarland class. *Cryptography and Communications*, 11(6):1233–1245, November 2019. CODEN ????

ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00370-w.

Mesnager:2019:MCT

[351] Sihem Mesnager, Constanza Riera, and Pantelimon Stanica. Multiple characters transforms and generalized Boolean functions. *Cryptography and Communications*, 11(6):1247–1260, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00383-5.

Luo:2019:SNC

[352] Gaojun Luo, Xiwang Cao, and Sihem Mesnager. Several new classes of self-dual bent functions derived from involutions. *Cryptography and Communications*, 11(6):1261–1273, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00371-9.

Cepak:2019:FLT

[353] N. Cepak, E. Pasalic, and A. Muratović-Ribić. Frobenius linear translators giving rise to new infinite classes of permutations and bent functions. *Cryptography and Communications*, 11(6):1275–1295, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00395-1.

Ozbudak:2019:SRG

[354] Ferruh Özbudak and RumI MelIh Pelen. Strongly regular graphs arising from non-weakly regular bent functions. *Cryptography and Communications*, 11(6):1297–1306, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00394-2.

Cesarz:2019:ISR

[355] Patrick G. Cesarz and Robert S. Coulter. Image sets with regularity of differences. *Cryptography and Communications*, 11(6):1307–1337, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00358-6.

Brandao:2019:UBM

[356] Luís T. A. N. Brandão, Çagdas Çalik, Meltem Sönmez Turan, and René Peralta. Upper bounds on the multiplicative complexity of symmetric Boolean functions. *Cryptography and Communications*, 11(6):1339–1362, November 2019. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00377-3.

Gao:2020:ASQ

[357] Yun Gao, Weijun Fang, and Fang-Wei Fu. On the algebraic structure of quasi-cyclic codes of index $1\frac{1}{2}$. *Cryptography and Communications*, 12(1):1–18, January 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-0352-7.

Mesnager:2020:MTW

[358] Sihem Mesnager, Kwang Ho Kim, Junyop Choe, and Chunming Tang.

On the Menezes–Teske–Weng conjecture. *Cryptography and Communications*, 12(1):19–27, January 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00359-5.

Shi:2020:PII

[359] Zexia Shi and Fang-Wei Fu. The primitive idempotents of irreducible constacyclic codes and LCD cyclic codes. *Cryptography and Communications*, 12(1):29–52, January 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00362-w.

Shi:2020:SDL

[360] Minjia Shi, Hongwei Zhu, Liqin Qian, Lin Sok, and Patrick Solé. On self-dual and LCD double circulant and double negacirculant codes over $\mathbf{F}_q + u\mathbf{F}_q$. *Cryptography and Communications*, 12(1):53–70, January 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00363-9.

Milshtein:2020:NTE

[361] Moshe Milshtein. A new two-error-correcting binary code of length 16. *Cryptography and Communications*, 12(1):71–75, January 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00365-7.

Tang:2020:NLB

[362] Deng Tang, Haode Yan, Zhengchun Zhou, and Xiaosong Zhang. A new lower bound on the second-order nonlinearity of a class of monomial bent functions. *Cryptography and Communications*, 12(1):77–83, January 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00360-y.

Budaghyan:2020:RBC

[363] L. Budaghyan, Marco Calderini, and I. Villa. On relations between CCZ- and EA-equivalences. *Cryptography and Communications*, 12(1):85–100, January 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00367-5.

Alahmadi:2020:CDM

[364] Adel Alahmadi, Cem Güneri, Buket Özkaya, Hatoon Shoaib, and Patrick Solé. On complementary dual multi-negacirculant codes. *Cryptography and Communications*, 12(1):101–113, January 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00364-8.

Roy:2020:FSS

[365] Suman Roy and Srinivasan Krishnaswamy. On the frequency of symbols in sequences generated by nonlinear feedforward generators. *Cryptography and Communications*, 12(1):115–126, January 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00379-1.

Dougherty:2020:QBC

[366] Steven T. Dougherty, Joseph Gildea, and Abidin Kaya. Quadruple bordered constructions of self-dual codes from group rings. *Cryptography and Communications*, 12(1):127–146, January 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00380-8.

Li:2020:DDP

[367] Fengwei Li, Qin Yue, and Yansheng Wu. Designed distances and parameters of new LCD BCH codes over finite fields. *Cryptography and Communications*, 12(1):147–163, January 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00385-3.

Niu:2020:NCI

[368] Tailin Niu, Kangquan Li, Longjiang Qu, and Qiang Wang. New constructions of involutions over finite fields. *Cryptography and Communications*, 12(2):165–185, March 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00386-2.

Guo:2020:FNB

[369] Guanmin Guo, Ruihu Li, Yang Liu, and Junli Wang. A family of negacyclic BCH codes of length $n = \frac{q^{2m}-1}{2}$. *Cryptography and Communications*, 12(2):187–203, March 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00387-1.

Shuai:2020:DUC

[370] Li Shuai, Lina Wang, Li Miao, and Xianwei Zhou. Differential uniformity of the composition of two functions. *Cryptography and Communications*, 12(2):205–220, March 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00382-6.

Radonjic:2020:ICC

[371] Aleksandar Radonjic and Vladimir Vujicic. Integer codes correcting burst asymmetric within a byte and double asymmetric errors. *Cryptography and Communications*, 12(2):221–230, March 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00388-0. See correction [372].

Radonjic:2020:CIC

[372] Aleksandar Radonjic and Vladimir Vujicic. Correction to: Integer codes correcting burst asymmetric errors within a byte and double asymmetric errors. *Cryptography and Communications*, 12 (2):231, March 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00398-y; http://link.springer.com/content/pdf/10.1007/s12095-019-00398-y.pdf. See [371].

Wang:2020:CSN

[373] Zhongxiao Wang, Qunxiong Zheng, and Wenfeng Qi. The cycle structure of NFSR(f^d) and its applications. *Cryptography and Communications*, 12(2):233–252, March 2020.

CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00392-4.

Yao:2020:MZZ

[374] Ting Yao and Shixin Zhu. $\mathbf{Z}_p\mathbf{Z}_{p^s}$-additive cyclic codes are asymptotically good. *Cryptography and Communications*, 12(2):253–264, March 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00397-z.

Sun:2020:CCB

[375] Zhonghua Sun, Shixin Zhu, and Liqi Wang. A class of constacyclic BCH codes. *Cryptography and Communications*, 12(2):265–284, March 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00401-6.

Araya:2020:MWB

[376] Makoto Araya and Masaaki Harada. On the minimum weights of binary linear complementary dual codes. *Cryptography and Communications*, 12(2): 285–300, March 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00402-5.

Cao:2020:CCS

[377] Yuan Cao and Yonglin Cao. Complete classification for simple root cyclic codes over the local ring $\mathbf{Z}_4[v]/\langle v^2 + 2v\rangle$. *Cryptography and Communications*, 12(2):301–319, March 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/article/10.1007/s12095-019-00403-4.

Helleseth:2020:ESI

[378] Tor Helleseth, Wai Ho Mow, and Zhengchun Zhou. Editorial: Special issue on sequences and their applications 2018. *Cryptography and Communications*, 12(3):321–323, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00433-3.

Zhang:2020:PZC

[379] Dan Zhang, Matthew Geoffrey Parker, and Tor Helleseth. Polyphase zero correlation zone sequences from generalised bent functions. *Cryptography and Communications*, 12(3):325–335, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00413-2.

Krengel:2020:OCP

[380] Evgeny Krengel. One construction of perfect ternary sequences. *Cryptography and Communications*, 12(3):337–347, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00414-1.

Zhou:2020:TCQ

[381] Yajing Zhou, Zhengchun Zhou, and Yong Wang. Two constructions for 16-QAM complementary sequence sets with non-power-of-two length. *Cryptography and Communications*, 12(3):349–362,

May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00406-1.

Yang:2020:NQS

[382] Yang Yang and Chunlei Li. New quaternary sequences with optimal odd-periodic autocorrelation magnitude. *Cryptography and Communications*, 12 (3):363–374, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00407-0.

Tang:2020:NMB

[383] Deng Tang and Xia Li. A note on the minimal binary linear code. *Cryptography and Communications*, 12(3): 375–388, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00412-3.

Gomez-Perez:2020:LFS

[384] Domingo Gómez-Pérez, Ana I. Gómez, and Andrew Tirkel. Large families of sequences for CDMA, frequency hopping, and UWB. *Cryptography and Communications*, 12(3):389–403, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00399-x.

Han:2020:DSF

[385] Hongyu Han, Sheng Zhang, and Xing Liu. Decimated m-sequences families with optimal partial Hamming correlation. *Cryptography and Communications*, 12(3):405–413, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00400-7.

Sun:2020:TMO

[386] Zhimin Sun, Xiangyong Zeng, and Da Lin. On the N-th maximum order complexity and the expansion complexity of a Rudin–Shapiro-like sequence. *Cryptography and Communications*, 12(3):415–426, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00396-0.

Li:2020:TCB

[387] Chunlei Li and Yang Yang. On three conjectures of binary sequences with low odd-periodic autocorrelation. *Cryptography and Communications*, 12(3): 427–442, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00393-3.

Shi:2020:OWT

[388] Minjia Shi, Chenchen Wang, and Yaoqiang Chang. One-weight and two-weight $\mathbf{Z}_2\mathbf{Z}_2[u,v]$ -additive codes. *Cryptography and Communications*, 12(3): 443–454, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00391-5.

Mesnager:2020:GHB

[389] Sihem Mesnager. On generalized hyperbent functions. *Cryptography and Communications*, 12(3):455–468, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00390-6.

Li:2020:DCP

[390] Shuxing Li and Alexander Pott. A direct construction of primitive formally dual pairs having subsets with unequal sizes. *Cryptography and Communications*, 12(3):469–483, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00389-z.

Zhou:2020:FHS

[391] Limengnan Zhou, Hongyu Han, and Xing Liu. Frequency-hopping sequence sets with no-hit-zone through Cartesian product. *Cryptography and Communications*, 12(3):485–497, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00381-7.

Egan:2020:PTF

[392] Malcolm Egan. Properties of tight frames that are regular schemes. *Cryptography and Communications*, 12(3):499–510, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00378-2.

Wu:2020:BTS

[393] Yansheng Wu, Qin Yue, and Xiaomeng Zhu. Binary and ternary sequences with a few cross correlations. *Cryptography and Communications*, 12(3):511–525, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00376-4.

Budaghyan:2020:PAB

[394] Lilya Budaghyan, Nikolay S. Kaleyski, and Pantelimon Stanica. Partially APN Boolean functions and classes of functions that are not APN infinitely often. *Cryptography and Communications*, 12(3):527–545, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00372-8.

Cao:2020:TDC

[395] Xiwang Cao, Gaojun Luo, and Guangkui Xu. Three deterministic constructions of compressed sensing matrices with low coherence. *Cryptography and Communications*, 12(3):547–558, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00375-5.

Li:2020:FDO

[396] Xia Li, Cuiling Fan, and Xiaoni Du. A family of distance-optimal minimal linear codes with flexible parameters. *Cryptography and Communications*, 12(3):559–567, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (elec-

tronic). URL https://link.springer.com/article/10.1007/s12095-019-00373-7.

Li:2020:CES

[397] Chengju Li, Qin Yue, and Wei Peng. A class of exponential sums and sequence families. *Cryptography and Communications*, 12(3):569–584, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00368-4.

Wang:2020:FSC

[398] Zilong Wang, Jinjin Chai, and Guang Gong. The Fourier spectral characterization for the correlation-immune functions over $\mathbf{F}_p$. *Cryptography and Communications*, 12(3):585–595, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00369-3.

Srikanth:2020:CSA

[399] Ch. Srikanth. Certain sequence of arithmetic progressions and a new key sharing method. *Cryptography and Communications*, 12(3):597–612, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00416-z.

Benerjee:2020:NUF

[400] Krishna Gopal Benerjee and Manish K. Gupta. On non-uniform flower codes. *Cryptography and Communications*, 12(3):613–643, May 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00430-6.

Liu:2020:NGH

[401] Zihui Liu and Jinliang Wang. Notes on generalized Hamming weights of some classes of binary codes. *Cryptography and Communications*, 12(4):645–657, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00404-3.

Mesnager:2020:NRZ

[402] Sihem Mesnager, Kwang Ho Kim, and Myong Song Jo. On the number of the rational zeros of linearized polynomials and the second-order nonlinearity of cubic Boolean functions. *Cryptography and Communications*, 12(4):659–674, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00410-5.

Sun:2020:ACC

[403] Yuhua Sun, Tongjiang Yan, and Lianhai Wang. The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude. *Cryptography and Communications*, 12(4):675–683, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00411-4.

Beierle:2020:DZS

[404] Christof Beierle, Alex Biryukov, and Aleksei Udovenko. On degree-d zero-sum sets of full rank. *Cryptography and Communications*, 12(4):685–710, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00415-0.

Singh:2020:SSQ

[405] Jasvinder Singh, Manish Gupta, and Jaskarn Singh Bhullar. On the search of smallest QC-LDPC code with girth six and eight. *Cryptography and Communications*, 12(4):711–723, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00405-2.

Zhao:2020:ALC

[406] Lu Zhao. About the linear complexity of quaternary sequences with even length. *Cryptography and Communications*, 12(4):725–741, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00419-w.

Pang:2020:SNB

[407] Binbin Pang, Shixin Zhu, and Xiaoshan Kai. Some new bounds on LCD codes over finite fields. *Cryptography and Communications*, 12(4):743–755, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00417-y.

Armario:2020:ASD

[408] J. A. Armario and D. L. Flannery. Almost supplementary difference sets and quaternary sequences with optimal autocorrelation. *Cryptography and Communications*, 12(4):757–768, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00418-x.

Gildea:2020:DBC

[409] Joe Gildea, Rhian Taylor, and A. Tylyshchak. Double bordered constructions of self-dual codes from group rings over Frobenius rings. *Cryptography and Communications*, 12(4):769–784, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00420-3.

Ortiz-Ubarri:2020:NAO

[410] José Ortiz-Ubarri. New asymptotically optimal three-dimensional wavelength/space/time optical orthogonal codes for OCDMA systems. *Cryptography and Communications*, 12(4): 785–794, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-019-00422-1.

Hu:2020:MDN

[411] Liqin Hu and Keqin Feng. The minimum distance of new generalisations of the punctured binary Reed–Muller codes. *Cryptography and

Communications, 12(4):795–808, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-019-00421-2`.

Mesnager:2020:S

[412] Sihem Mesnager, Kwang Ho Kim, and Dae Song Go. Solving $x + x^{2^l} + \cdots + x^{2^{ml}} = a$ over $\mathbf{F}_{2^n}$. *Cryptography and Communications*, 12(4):809–817, July 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00425-3`.

Budaghyan:2020:ESI

[413] Lilya Budaghyan and Tor Helleseth. Editorial: Special issue on Boolean functions and their applications. *Cryptography and Communications*, 12(5):819–820, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00454-y`.

Calderini:2020:ECK

[414] Marco Calderini. On the EA-classes of known APN functions in small dimensions. *Cryptography and Communications*, 12(5):821–840, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00427-1`.

Felke:2020:MMS

[415] Patrick Felke. The multivariate method strikes again: New power functions with low differential uniformity in odd characteristic. *Cryptography and Communications*, 12(5):841–857, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00437-z`.

Musukwa:2020:LSB

[416] A. Musukwa and M. Sala. On the linear structures of balanced functions and quadratic APN functions. *Cryptography and Communications*, 12(5):859–880, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00431-5`.

Kutsenko:2020:GAS

[417] Aleksandr Kutsenko. The group of automorphisms of the set of self-dual bent functions. *Cryptography and Communications*, 12(5):881–898, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00438-y`.

Cesmelioglu:2020:VBF

[418] Ayça Çesmelioglu, Wilfried Meidl, and Alexander Pott. Vectorial bent functions in odd characteristic and their components. *Cryptography and Communications*, 12(5):899–912, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00444-0`.

Kalayci:2020:PPF

[419] Tekgül Kalayci, Henning Stichtenoth, and Alev Topuzoglu. Permutation polynomials and factorization. *Cryptography and Communications*, 12(5):913–934, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00446-y.

Calik:2020:BFM

[420] Çagdas Çalik, Meltem Sönmez Turan, and René Peralta. Boolean functions with multiplicative complexity 3 and 4. *Cryptography and Communications*, 12(5):935–946, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00445-z.

Zajac:2020:CPS

[421] Pavol Zajac and Matús Jókay. Cryptographic properties of small bijective S-boxes with respect to modular addition. *Cryptography and Communications*, 12(5):947–963, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00447-x.

Li:2020:RRP

[422] Nian Li and Sihem Mesnager. Recent results and problems on constructions of linear codes from cryptographic functions. *Cryptography and Communications*, 12(5):965–986, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00435-1.

Kadir:2020:DAG

[423] Wrya K. Kadir and Chunlei Li. On decoding additive generalized twisted Gabidulin codes. *Cryptography and Communications*, 12(5):987–1009, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00449-9.

Ding:2020:CDS

[424] Cunsheng Ding and Chunming Tang. Combinatorial t-designs from special functions. *Cryptography and Communications*, 12(5):1011–1033, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00442-2.

Medina:2020:RHT

[425] Luis A. Medina, Matthew G. Parker, and Pantelimon Stanica. Root-Hadamard transforms and complementary sequences. *Cryptography and Communications*, 12(5):1035–1049, September 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00440-4.

Borissov:2020:NDS

[426] Yuri Borissov and Lyubomir Borissov. A note on the distinctness of some Kloosterman sums. *Cryptography and Communications*, 12(5):1051–1056, September 2020. CODEN ???? ISSN 1936-

2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00443-1`.

Ozden:2020:AAS

[427] Büsra Özden and Oguz Yayla. Almost p-ary sequences. *Cryptography and Communications*, 12(6):1057–1069, November 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00423-5`.

Jiang:2020:RPT

[428] Jing Jiang and Minquan Cheng. Regular $(k, R, 1)$-packings with $\max(R) = 3$ and their locally repairable codes. *Cryptography and Communications*, 12(6):1071–1089, November 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00424-4`.

Anbar:2020:SPF

[429] Nurdagül Anbar, Canan Kasikçi, and Alev Topuzoglu. Shifted plateaued functions and their differential properties. *Cryptography and Communications*, 12(6):1091–1105, November 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00426-2`.

Cao:2020:CMP

[430] Yuan Cao, Yonglin Cao, and Fang-Wei Fu. Correcting mistakes in the paper "A mass formula for negacyclic codes of length 2^k and some good negacyclic codes over $\mathbf{Z}_4 + u\mathbf{Z}_4$" [Cryptogr. Commun. (2017) **9**:241–272]. *Cryptography and Communications*, 12(6):1107–1110, November 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00429-z`. See [172].

Wang:2020:SCS

[431] Xiaoqiang Wang and Dabin Zheng. The subfield codes of several classes of linear codes. *Cryptography and Communications*, 12(6):1111–1131, November 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00432-4`.

Beierle:2020:UPN

[432] Christof Beierle and Gregor Leander. 4-uniform permutations with null nonlinearity. *Cryptography and Communications*, 12(6):1133–1141, November 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00434-2`.

Zheng:2020:SNI

[433] Lijing Zheng, Jie Peng, and Yanjun Li. Several new infinite families of bent functions via second order derivatives. *Cryptography and Communications*, 12(6):1143–1160, November 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00436-0`.

Calderini:2020:BUS

[434] Marco Calderini and Irene Villa. On the boomerang uniformity of some permutation polynomials. *Cryptography and Communications*, 12(6):1161–1178, November 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00439-x`.

Gologlu:2020:IFC

[435] Faruk Göloglu. Inverse function is not component-wise uniform. *Cryptography and Communications*, 12(6):1179–1194, November 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00441-3`.

Wu:2020:TCA

[436] Xia Wu, Wei Lu, and Xiwang Cao. Two constructions of asymptotically optimal codebooks via the trace functions. *Cryptography and Communications*, 12(6):1195–1211, November 2020. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00448-w`.

Fang:2021:EHM

[437] Xiaolei Fang, Meiqing Liu, and Jinquan Luo. On Euclidean hulls of MDS codes. *Cryptography and Communications*, 13(1):1–14, January 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00428-0`.

Yan:2021:CAC

[438] Ming Yan, Tongjiang Yan, and Yu Li. Computing the 2-adic complexity of two classes of Ding–Helleseth generalized cyclotomic sequences of periods of twin prime products. *Cryptography and Communications*, 13(1):15–26, January 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00451-1`.

Sriwirach:2021:RRC

[439] Wateekorn Sriwirach and Chakkrid Klin-eam. Repeated-root constacyclic codes of length $2p^s$ over $\mathbf{F}_{p^m} + u\mathbf{F}_{p^m} + u^2\mathbf{F}_{p^m}$. *Cryptography and Communications*, 13(1):27–52, January 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00450-2`.

Shao:2021:AMD

[440] Minfeng Shao and Ying Miao. Algebraic manipulation detection codes via highly nonlinear functions. *Cryptography and Communications*, 13(1):53–69, January 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00453-z`.

Maiti:2021:DFR

[441] Swapan Maiti and Dipanwita Roy Chowdhury. Design of fault-resilient S-boxes for AES-like block ciphers. *Cryptography and Communications*, 13(1):71–100, January 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (elec-

tronic). URL https://link.springer.com/article/10.1007/s12095-020-00452-0.

Ma:2021:SPW

[442] Junru Ma and Jinquan Luo. On symbol-pair weight distribution of MDS codes and simplex codes over finite fields. *Cryptography and Communications*, 13(1):101–115, January 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00455-x.

Xiang:2021:TFS

[443] Can Xiang and Wenjuan Yin. Two families of subfield codes with a few weights. *Cryptography and Communications*, 13(1):117–127, January 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00457-9.

Aksoy:2021:SDC

[444] Refia Aksoy and Fatma Çaliskan. Self-dual codes over $\mathbf{F}_2 \times (\mathbf{F}_2 + v\mathbf{F}_2)$. *Cryptography and Communications*, 13(1): 129–141, January 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00461-z. See correction [457].

Benerjee:2021:CFD

[445] Krishna Gopal Benerjee, Sourav Deb, and Manish K. Gupta. On conflict free DNA codes. *Cryptography and Communications*, 13(1):143–171, January 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00459-7.

Wang:2021:CSC

[446] Xiaoqiang Wang, Dabin Zheng, and Yan Zhang. A class of subfield codes of linear codes and their duals. *Cryptography and Communications*, 13(1):173–196, January 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00460-0.

Rega:2021:WIT

[447] B. Rega, Z. H. Liu, and C. Durairajan. The t-wise intersection and trellis of relative four-weight codes. *Cryptography and Communications*, 13(2):197–223, March 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00456-w.

Qian:2021:LCO

[448] Liqin Qian, Xiwang Cao, and Sihem Mesnager. Linear codes with one-dimensional hull associated with Gaussian sums. *Cryptography and Communications*, 13(2):225–243, March 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00462-y.

Zhang:2021:FCC

[449] He Zhang and Xiwang Cao. Further constructions of cyclic subspace codes. *Cryptography and Communications*, 13(2):245–262, March

2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00463-x`.

Bouyukliev:2021:CVW

[450] Iliya Bouyukliev, Stefka Bouyuklieva, and Paskal Piperkov. Characteristic vector and weight distribution of a linear code. *Cryptography and Communications*, 13(2):263–282, March 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00458-8`.

Anbar:2021:PPF

[451] Nurdagül Anbar and Canan Kasikci. Permutations polynomials of the form $G(X)^k - L(X)$ and curves over finite fields. *Cryptography and Communications*, 13(2):283–294, March 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00465-9`.

Stanica:2021:CDB

[452] Pantelimon Stanica and Aaron Geary. The c-differential behavior of the inverse function under the EA-equivalence. *Cryptography and Communications*, 13 (2):295–306, March 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00466-8`.

Ma:2021:SQC

[453] Fanghui Ma, Jian Gao, and Fang-Wei Fu. (σ, δ)-skew quasi-cyclic codes over the ring $\mathbf{Z}_4 + u\mathbf{Z}_4$. *Cryptography and Communications*, 13(2):307–320, March 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00467-7`.

Kumar:2021:ARM

[454] Ajeet Kumar, Subhamoy Maitra, and Chandra Sekhar Mukherjee. On approximate real mutually unbiased bases in square dimension. *Cryptography and Communications*, 13(2):321–329, March 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-020-00468-6`.

Huczynska:2021:SED

[455] Sophie Huczynska, Christopher Jefferson, and Silvia Nepsinská. Strong external difference families in abelian and non-abelian groups. *Cryptography and Communications*, 13(2):331–341, March 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-021-00473-3`.

Zhang:2021:TRB

[456] Jingwei Zhang, Chuangqiang Hu, and Chang-An Zhao. Trace representation of the binary pq^2-periodic sequences derived from Euler quotients. *Cryptography and Communications*, 13(2): 343–359, March 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-021-00475-1`.

Aksoy:2021:CSD

[457] Refia Aksoy and Fatma Çaliskan. Correction to: Self-dual codes over $\mathbf{F}_2 \times (\mathbf{F}_2 + v\mathbf{F}_2)$. *Cryptography and Communications*, 13(2):361–362, March 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00464-w. See [444].

Faraj:2021:QPS

[458] Mustafa Faraj and Catherine Gebotys. Quiescent photonics side channel analysis: Low cost SRAM readout attack. *Cryptography and Communications*, 13(3):363–376, May 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-020-00469-5.

Gologlu:2021:CIS

[459] Faruk Göloglu and Jirí Pavlụ. On CCZ-inequivalence of some families of almost perfect nonlinear functions to permutations. *Cryptography and Communications*, 13(3):377–391, May 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00476-0.

Jin:2021:BFS

[460] Wengang Jin, Xiaoni Du, and Cuiling Fan. Boolean functions with six-valued Walsh spectra and their application. *Cryptography and Communications*, 13(3):393–405, May 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00484-0.

He:2021:LCD

[461] Zhiwen He and Jiejing Wen. Linear codes of 2-designs as subcodes of the generalized Reed–Muller codes. *Cryptography and Communications*, 13(3):407–423, May 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00472-4.

Chathely:2021:CBH

[462] Briji J. Chathely and Rajendra P. Deore. Construction of binary Hadamard codes and their s-PD sets. *Cryptography and Communications*, 13(3):425–438, May 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00471-5.

Bartoli:2021:ICM

[463] Daniele Bartoli, Matteo Bonini, and Burçin Günes. An inductive construction of minimal codes. *Cryptography and Communications*, 13(3):439–449, May 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00474-2.

Biswas:2021:SRB

[464] Aniruddha Biswas and Palash Sarkar. Separation results for boolean function classes. *Cryptography and Communications*, 13(3):451–458, May 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

URL https://link.springer.com/article/10.1007/s12095-021-00488-w.

Li:2021:MPI

[465] Yubo Li, Kangquan Li, and Longjiang Qu. More permutations and involutions for constructing bent functions. *Cryptography and Communications*, 13 (3):459–473, May 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00482-2.

Aubry:2021:SIM

[466] Yves Aubry, Pierre Barthélémy, and Nadia El Mrabet. Special issue from mathematics to embedded devices. *Cryptography and Communications*, 13(4): 475–477, July 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00502-1.

Koshelev:2021:HEC

[467] Dmitrii Koshelev. Hashing to elliptic curves of j-invariant 1728. *Cryptography and Communications*, 13(4):479–494, July 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00478-y.

Ballet:2021:OSC

[468] Stéphane Ballet, Alexis Bonnecaze, and Thanh-Hung Dang. Optimization of the scalar complexity of Chudnovsky^2 multiplication algorithms in finite fields. *Cryptography and Communications*, 13(4):495–517, July 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00494-y.

Bordage:2021:PCB

[469] Sarah Bordage and Julien Lavauzelle. On the privacy of a code-based single-server computational PIR scheme. *Cryptography and Communications*, 13(4): 519–526, July 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00477-z.

Cheng:2021:CAL

[470] Wei Cheng, Sylvain Guilley, and Jean-Luc Danger. Categorizing all linear codes of IPM over $\mathbf{F}_{2^8}$. *Cryptography and Communications*, 13(4):527–542, July 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00483-1.

Landry:2021:MEP

[471] Simon Landry, Yanis Linge, and Emmanuel Prouff. Monomial evaluation of polynomial functions protected by threshold implementations — with an illustration on AES. *Cryptography and Communications*, 13(4):543–572, July 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00497-9.

VanOuytsel:2021:HFB

[472] Charles-Henry Bertrand Van Ouytsel, Olivier Bronchain, and François-Xavier

Standaert. How to fool a black box machine learning based side-channel security evaluation. *Cryptography and Communications*, 13(4):573–585, July 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-021-00479-x`.

Momin:2021:SHT

[473] Charles Momin, Olivier Bronchain, and François-Xavier Standaert. A stealthy Hardware Trojan based on a Statistical Fault Attack. *Cryptography and Communications*, 13(4):587–600, July 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-021-00480-4`.

Dougherty:2021:EGC

[474] S. T. Dougherty, Joe Gildea, and Serap Sahinkaya. G-codes, self-dual G-codes and reversible G-codes over the ring $B_{j,k}$. *Cryptography and Communications*, 13(5):601–616, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-021-00487-x`.

Fan:2021:IBS

[475] Yanhong Fan, Sihem Mesnager, and Meiqin Wang. Investigation for 8-bit SKINNY-like S-boxes, analysis and applications. *Cryptography and Communications*, 13(5):617–636, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-021-00486-y`.

Pasalic:2021:SCM

[476] Enes Pasalic, René Rodríguez, and Yongzhuang Wei. Several classes of minimal binary linear codes violating the Ashikhmin–Barg bound. *Cryptography and Communications*, 13(5):637–659, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-021-00491-1`.

Lv:2021:QCC

[477] Jingjie Lv, Ruihu Li, and Yu Yao. Quasi-cyclic constructions of asymmetric quantum error-correcting codes. *Cryptography and Communications*, 13(5):661–680, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-021-00489-9`.

Hou:2021:PSF

[478] Xiang dong Hou. A power sum formula by Carlitz and its applications to permutation rational functions of finite fields. *Cryptography and Communications*, 13(5):681–694, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-021-00495-x`.

Kumar:2021:CLC

[479] Pavan Kumar and Noor Mohammad Khan. A class of linear codes with their complete weight enumerators over finite fields. *Cryptography and Communications*, 13(5):695–725, September

2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00496-w.

Shi:2021:QSC

[480] Xiaoping Shi, Qin Yue, and Xinmei Huang. Quantum synchronizable codes from the Whiteman's generalized cyclotomy. *Cryptography and Communications*, 13(5):727–739, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00501-2.

Meaux:2021:FAI

[481] Pierrick Méaux. On the fast algebraic immunity of threshold functions. *Cryptography and Communications*, 13(5):741–762, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00505-y.

Liu:2021:TPC

[482] Chen Liu, Shuaijun Liu, and Zhengchun Zhou. Three-phase Z-complementary triads and almost complementary triads. *Cryptography and Communications*, 13(5):763–773, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00509-8.

Arasu:2021:NNR

[483] K. T. Arasu, Daniel M. Gordon, and Yiran Zhang. New nonexistence results on circulant weighing matrices. *Cryptography and Communications*, 13(5):775–789, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00492-0.

Jamet:2021:MOC

[484] Damien Jamet, Pierre Popoli, and Thomas Stoll. Maximum order complexity of the sum of digits function in Zeckendorf base and polynomial subsequences. *Cryptography and Communications*, 13(5):791–814, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00507-w.

Kolsch:2021:FSD

[485] Lukas Kölsch and Robert Schüler. Formal self duality. *Cryptography and Communications*, 13(5):815–836, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00508-9.

Otal:2021:EGQ

[486] Kamil Otal and Eda Tekin. Efficient generation of quadratic cyclotomic classes for shortest quadratic decompositions of polynomials. *Cryptography and Communications*, 13(5):837–845, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00512-z.

Yao:2021:CCM

[487] Ge Yao and Udaya Parampalli. Cryptanalysis of the class of maximum period Galois NLFSR-based stream ciphers. *Cryptography and Communications*, 13(5):847–864, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00511-0.

Xiao:2021:ACT

[488] Zibi Xiao and Xiangyong Zeng. 2-adic complexity of two constructions of binary sequences with period $4N$ and optimal autocorrelation magnitude. *Cryptography and Communications*, 13(5):865–885, September 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00498-8.

Budaghyan:2021:ESI

[489] Lilya Budaghyan, Claude Carlet, and Kaisa Nyberg. Editorial: Special issue on Boolean functions and their applications 2020. *Cryptography and Communications*, 13(6):887–889, November 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00536-5.

Stanica:2021:CWS

[490] Pantelimon Stanica, Constanza Riera, and Anton Tkachenko. Characters, Weil sums and c-differential uniformity with an application to the perturbed Gold function. *Cryptography and Communications*, 13(6):891–907, November 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00485-z.

Kolomeec:2021:SGP

[491] Nikolay Kolomeec. Some general properties of modified bent functions through addition of indicator functions. *Cryptography and Communications*, 13(6):909–926, November 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00528-5.

Ding:2021:LCE

[492] Cunsheng Ding and Chunming Tang. The linear codes of t-designs held in the Reed–Muller and Simplex codes. *Cryptography and Communications*, 13(6):927–949, November 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00470-6.

Mesnager:2021:CWP

[493] Sihem Mesnager and Sihong Su. On constructions of weightwise perfectly balanced Boolean functions. *Cryptography and Communications*, 13(6):951–979, November 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00481-3.

Chase:2021:KTA

[494] Benjamin Chase and Petr Lisonek. Kim-type APN functions are affine equivalent to Gold functions. *Cryptography and Communications*, 13(6):981–993, November 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00490-2.

Kaleyski:2021:IEC

[495] Nikolay S. Kaleyski. Invariants for EA- and CCZ-equivalence of APN and AB functions. *Cryptography and Communications*, 13(6):995–1023, November 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00541-8.

Ding:2021:SSS

[496] Jian Ding, Changlu Lin, and Sihem Mesnager. Secret sharing schemes based on the dual of Golay codes. *Cryptography and Communications*, 13(6):1025–1041, November 2021. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00531-w.

Wang:2022:FOT

[497] Dandan Wang and Xiwang Cao. A family of optimal ternary cyclic codes with minimum distance five and their duals. *Cryptography and Communications*, 14(1):1–13, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00493-z.

Allahmadi:2022:NCE

[498] A. Allahmadi, A. AlKenani, and P. Solé. New constructions of entanglement-assisted quantum codes. *Cryptography and Communications*, 14(1):15–37, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00499-7. See correction [499].

Allahmadi:2022:CNC

[499] A. Allahmadi, A. AlKenani, and P. Solé. Correction to: New constructions of entanglement-assisted quantum codes. *Cryptography and Communications*, 14 (1):39, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00532-9. See [498].

Dhooghe:2022:RUA

[500] Siemen Dhooghe and Svetla Nikova. Resilient uniformity: applying resiliency in masking. *Cryptography and Communications*, 14(1):41–58, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00515-w.

Islam:2022:CLN

[501] Habibul Islam and Om Prakash. Construction of LCD and new quantum codes from cyclic codes over a finite non-chain ring. *Cryptography and Communications*, 14(1):59–73, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

URL https://link.springer.com/article/10.1007/s12095-021-00516-9.

Kim:2022:PEP

[502] Kwang Ho Kim, Sihem Mesnager, and Dok Nam Lee. Preimages of p-linearized polynomials over $\mathbf{F}_p$. *Cryptography and Communications*, 14(1):75–86, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00514-x.

Lao:2022:NCD

[503] Huimin Lao, Hao Chen, and Xiaoqing Tan. New constant dimension subspace codes from block inserting constructions. *Cryptography and Communications*, 14(1):87–99, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00524-9.

Kudin:2022:PLS

[504] S. Kudin, E. Pasalic, and F. Zhang. Permutations without linear structures inducing bent functions outside the completed Maiorana–McFarland class. *Cryptography and Communications*, 14(1):101–116, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00523-w.

Anupindi:2022:LCS

[505] Vishnupriya Anupindi and László Mérai. Linear complexity of some sequences derived from hyperelliptic curves of genus 2. *Cryptography and Communications*, 14(1):117–134, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00521-y.

Gu:2022:NFP

[506] Zhi Gu, Zhengchun Zhou, and Udaya Parampalli. A new family of polyphase sequences with low correlation. *Cryptography and Communications*, 14(1):135–144, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00522-x.

Fang:2022:NGH

[507] Xiaolei Fang, Renjie Jin, and Wen Ma. New Galois hulls of GRS codes and application to EAQECCs. *Cryptography and Communications*, 14(1):145–159, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00525-8.

Wan:2022:EBT

[508] Qianhong Wan and Chao Li. On equivalence between two known families of APN polynomial functions and APN power functions. *Cryptography and Communications*, 14(1):161–182, January 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00533-8.

Edemskiy:2022:SAC

[509] Vladimir Edemskiy and Yuhua Sun. The symmetric 2-adic complexity of sequences with optimal autocorrelation magnitude and length $8q$. *Cryptography and Communications*, 14(2):183–199, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00503-0.

Niu:2022:NCD

[510] Yongfeng Niu, Qin Yue, and Daitao Huang. New constant dimension subspace codes from parallel linkage construction and multilevel construction. *Cryptography and Communications*, 14(2):201–214, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00504-z.

Liu:2022:CAI

[511] Yan Liu and Xiwang Cao. A class of affine-invariant codes and their support 2-designs. *Cryptography and Communications*, 14(2):215–227, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00506-x.

Yao:2022:ITA

[512] Ge Yao and Udaya Parampalli. Improved transformation algorithms for generalized Galois NLFSRs. *Cryptography and Communications*, 14(2):229–258, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00500-3.

Xu:2022:HLC

[513] Heqian Xu and Wei Du. Hermitian LCD codes over $\mathbf{F}_{q^2} + u\mathbf{F}_{q^2}$ and their applications to maximal entanglement EAQECCs. *Cryptography and Communications*, 14(2):259–269, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00510-1.

Kaleyski:2022:DEE

[514] Nikolay Kaleyski. Deciding EA-equivalence via invariants. *Cryptography and Communications*, 14(2):271–290, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00513-y.

Zhou:2022:COL

[515] Limengnan Zhou, Xing Liu, and Changyuan Wang. Classes of optimal low-hit-zone frequency-hopping sequence sets with new parameters. *Cryptography and Communications*, 14(2):291–306, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00518-7.

Zhou:2022:MPW

[516] Limengnan Zhou and Hanzhou Wu. Multi-party watermark embedding with frequency-hopping sequences. *Cryptography and Communications*, 14(2):307–318, March 2022. CODEN ????

ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00517-8.

Budaghyan:2022:BSA

[517] Lilya Budaghyan, Nikolay Kaleyski, and Pantelimon Stanica. On the behavior of some APN permutations under swapping points. *Cryptography and Communications*, 14(2):319–345, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00520-z.

Liu:2022:NFH

[518] Xing Liu, Shaofang Hong, and Limengnan Zhou. NHZ frequency hopping sequence sets under aperiodic Hamming correlation: Tighter bound and optimal constructions. *Cryptography and Communications*, 14(2):347–356, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00527-6.

Yan:2022:DUT

[519] Haode Yan. On (-1)-differential uniformity of ternary APN power functions. *Cryptography and Communications*, 14(2):357–369, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00526-7.

Jiang:2022:DBS

[520] Sha Jiang, Kangquan Li, and Longjiang Qu. Differential and boomerang spectrums of some power permutations. *Cryptography and Communications*, 14(2):371–393, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00530-x.

Edemskiy:2022:ELC

[521] Vladimir Edemskiy and Nikita Sokolovskiy. The estimate of the linear complexity of generalized cyclotomic binary and quaternary sequences with periods p^n and $2p^n$. *Cryptography and Communications*, 14(2):395–414, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00534-7.

Xu:2022:MLC

[522] Guangkui Xu, Longjiang Qu, and Gaojun Luo. Minimal linear codes from weakly regular bent functions. *Cryptography and Communications*, 14(2):415–431, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00519-6.

Vielhaber:2022:RCB

[523] Michael Vielhaber, Mónica del Pilar Canales Chacón, and Sergio Jara Ceballos. Rational complexity of binary sequences, F$\mathbf{Q}$SRs, and pseudo-ultrametric continued fractions in $\mathbf{R}$. *Cryptography and Communications*, 14(2):433–457, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00539-2.

Salagean:2022:IBP

[524] Ana Salagean and Pantelimon Stanica. Improving bounds on probabilistic affine tests to estimate the nonlinearity of Boolean functions. *Cryptography and Communications*, 14(2):459–481, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00529-4.

Li:2022:JHR

[525] Haitao Li, Yang Liu, and Gang Wang. Jump and hop randomness tests for binary sequences. *Cryptography and Communications*, 14(2):483–502, March 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00538-3.

Barbero:2022:PSI

[526] Ángela Barbero, Vitaly Skachek, and Øyvind Ytrehus. Preface of special issue on coding theory and applications. *Cryptography and Communications*, 14(3):503, May 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00560-z.

Gutierrez:2022:ALC

[527] Jaime Gutierrez. Attacking the linear congruential generator on elliptic curves via lattice techniques. *Cryptography and Communications*, 14(3):505–525, May 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00535-6.

Kumar:2022:RBD

[528] Ajeet Kumar and Subhamoy Maitra. Resolvable block designs in construction of approximate real MUBs that are sparse. *Cryptography and Communications*, 14(3):527–549, May 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00537-4.

Kumar:2022:RRC

[529] Raj Kumar and Maheshanand Bhaintwal. Repeated root cyclic codes over $\mathbf{Z}_{p^2} + u\mathbf{Z}_{p^2}$ and their Lee distances. *Cryptography and Communications*, 14(3):551–577, May 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00540-9.

Li:2022:HDC

[530] Fengwei Li. The Hermitian dual-containing LCD BCH codes and related quantum codes. *Cryptography and Communications*, 14(3):579–596, May 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00543-6.

Liang:2022:CAH

[531] Huicong Liang, Sihem Mesnager, and Meiqin Wang. Cryptanalysis of the AEAD and hash algorithm DryGASCON. *Cryptography and Communications*, 14(3):597–625, May 2022. CODEN ???? ISSN 1936-2447 (print),

1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00542-7.

Shi:2022:LAC

[532] Minjia Shi, Shitao Li, and Patrick Solé. LCD and ACD codes over a noncommutative non-unital ring with four elements. *Cryptography and Communications*, 14(3):627–640, May 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00545-4.

Xiang:2022:SDB

[533] Can Xiang. Some t-designs from BCH codes. *Cryptography and Communications*, 14(3):641–652, May 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00546-3.

Li:2022:SOZ

[534] Xia Li, Qin Yue, and Deng Tang. The second-order zero differential spectra of almost perfect nonlinear functions and the inverse function in odd characteristic. *Cryptography and Communications*, 14(3):653–662, May 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00544-5.

Liu:2022:CBC

[535] Kaiqiang Liu, Qi Wang, and Haode Yan. A class of binary cyclic codes with optimal parameters. *Cryptography and Communications*, 14(3):663–675, May 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00548-1.

Fang:2022:NCS

[536] Weijun Fang, Jun Zhang, and Fang-Wei Fu. New constructions of self-dual generalized Reed–Solomon codes. *Cryptography and Communications*, 14(3):677–690, May 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00549-0.

Mesnager:2022:SRT

[537] Sihem Mesnager, Bimal Mandal, and Mounira Msahli. Survey on recent trends towards generalized differential and boomerang uniformities. *Cryptography and Communications*, 14(4):691–735, July 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00551-6.

Meidl:2022:SAG

[538] Wilfried Meidl. A survey on p-ary and generalized bent functions. *Cryptography and Communications*, 14(4):737–782, July 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00570-x.

Merai:2022:PSD

[539] László Mérai and Arne Winterhof. Pseudorandom sequences derived from automatic sequences. *Cryptography and Communications*, 14(4):783–815, July

2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00556-9.

Shen:2022:NCC

[540] Bingsheng Shen, Yang Yang, and Zhengchun Zhou. New z-complementary/complementary sequence sets with non-power-of-two length and low PAPR. *Cryptography and Communications*, 14 (4):817–832, July 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00550-7.

Araya:2022:CQO

[541] Makoto Araya and Masaaki Harada. On the classification of quaternary optimal Hermitian LCD codes. *Cryptography and Communications*, 14(4):833–847, July 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00552-5.

Jeon:2022:DUL

[542] Yongjin Jeon, Seungjun Baek, and Jongsung Kim. Differential uniformity and linearity of S-boxes by multiplicative complexity. *Cryptography and Communications*, 14(4):849–874, July 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00547-2.

Wu:2022:MLC

[543] Xia Wu, Wei Lu, and Xiwang Cao. Minimal linear codes constructed from functions. *Cryptography and Communications*, 14(4):875–895, July 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-021-00553-4.

Figueiredo:2022:TCM

[544] Ravi B. D. Figueiredo and Juliano B. Lima. Tangent-Chebyshev maps over finite fields: New properties and functional graphs. *Cryptography and Communications*, 14(4):897–908, July 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00565-8.

Dinh:2022:SQC

[545] Hai Q. Dinh, Narendra Kumar, and Abhay Kumar Singh. A study of quantum codes obtained from cyclic codes over a non-chain ring. *Cryptography and Communications*, 14(4):909–923, July 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00567-6.

Bartoli:2022:CAP

[546] Daniele Bartoli and Marco Timpanella. On a conjecture on APN permutations. *Cryptography and Communications*, 14 (4):925–931, July 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00558-7.

Kose:2022:FSP

[547] Seyda Köse and Ferruh Özbudak. Factorization of some polynomials over finite local commutative rings and applications to certain self-dual and LCD codes. *Cryptography and Communications*, 14(4):933–948, July 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00557-8`.

Sok:2022:MLC

[548] Lin Sok. MDS linear codes with one-dimensional hull. *Cryptography and Communications*, 14(5):949–971, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00559-6`.

Izadi:2022:ICM

[549] Maryam Izadi, Arezoo Soufi Karbaski, Rashid Rezaei, and Karim Samei. Isodual codes over $\mathbf{F}_q$ from a multiplier. *Cryptography and Communications*, 14(5):973–982, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00561-y`.

Xu:2022:OFH

[550] Shanding Xu. Optimal frequency-hopping sequences based on the decimated m-sequences. *Cryptography and Communications*, 14(5):983–998, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00569-4`.

Sun:2022:RNB

[551] Lei Sun, Zexia Shi, Jian Liu, and Fang-Wei Fu. Results on the nonexistence of bent-negabent rotation symmetric Boolean functions. *Cryptography and Communications*, 14(5):999–1008, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00575-6`.

Bouzara:2022:LCL

[552] Reguia Lamia Bouzara, Kenza Guenda, and Edgar Martínez-Moro. Lifted codes and lattices from codes over finite chain rings. *Cryptography and Communications*, 14(5):1009–1020, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00568-5`.

Patel:2022:CCM

[553] Shikha Patel, Om Prakash, and Habibul Islam. Cyclic codes over $M_4(\mathbf{F}_2 + u\mathbf{F}_2)$. *Cryptography and Communications*, 14(5):1021–1034, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00572-9`. See correction [554].

Patel:2022:CCC

[554] Shikha Patel, Om Prakash, and Habibul Islam. Correction to: Cyclic codes over $M_4(\mathbf{F}_2 + u\mathbf{F}_2)$. *Cryptography and Communications*, 14(5):1035–1037, September 2022. CODEN ???? ISSN 1936-

2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00584-5. See [553].

Li:2022:NFM

[555] Fulin Li, Yang Liu, Jiayun Yan, and Shixin Zhu. A new fair multi-secret sharing scheme based on asymmetric bivariate polynomial. *Cryptography and Communications*, 14(5):1039–1053, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00576-5.

Saini:2022:HON

[556] Kezia Saini and Manish Garg. On the higher-order nonlinearity of a Boolean bent function class (constructed via Niho power functions). *Cryptography and Communications*, 14(5):1055–1066, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00574-7.

Petrides:2022:NTV

[557] George Petrides. A number theoretic view on binary shift registers. *Cryptography and Communications*, 14(5):1067–1080, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00562-x.

Yan:2022:NDS

[558] Haode Yan and Zhen Li. A note on the differential spectrum of a class of power mappings with Niho exponent. *Cryptography and Communications*, 14(5):1081–1089, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00577-4.

Chirvasitu:2022:SDR

[559] Alexandru Chirvasitu and Thomas Cusick. Symbolic dynamics and rotation symmetric Boolean functions. *Cryptography and Communications*, 14(5):1091–1115, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00563-w.

Cao:2022:CSD

[560] Yuan Cao, Yonglin Cao, San Ling, and Guidong Wang. On the construction of self-dual cyclic codes over $\mathbf{Z}_4$ with arbitrary even length. *Cryptography and Communications*, 14(5):1117–1143, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00579-2.

Chen:2022:MUB

[561] Yu Long Chen, Avijit Dutta, and Mridul Nandi. Multi-user BBB security of public permutations based MAC. *Cryptography and Communications*, 14(5):1145–1177, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00571-w.

Kim:2022:QCO

[562] Boran Kim. Quantum codes from one-point codes on norm-trace curves. *Cryptography and Communications*, 14 (5):1179–1188, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00586-3.

Huang:2022:LIP

[563] Ziteng Huang, Weijun Fang, and Fang-Wei Fu. Linear l-intersection pairs of MDS codes and their applications to AEAQECCs. *Cryptography and Communications*, 14(5):1189–1206, September 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00582-7.

Budaghyan:2022:ESI

[564] Lilya Budaghyan, Claude Carlet, Cunsheng Ding, and Tor Helleseth. Editorial: Special issue on Boolean functions and their applications 2021. *Cryptography and Communications*, 14(6):1207–1209, November 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00609-z.

Bartoli:2022:LDU

[565] Daniele Bartoli, Marco Calderini, Constanza Riera, and Pantelimon Stănică. Low c-differential uniformity for functions modified on subfields. *Cryptography and Communications*, 14(6):1211–1227, November 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00554-x.

Bapic:2022:CNS

[566] Amar Bapić, Enes Pasalic, Fengrong Zhang, and Samir Hodžić. Constructing new superclasses of bent functions from known ones. *Cryptography and Communications*, 14(6):1229–1256, November 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00566-7.

Hasan:2022:BGF

[567] Sartaj Ul Hasan, Mohit Pal, and Pantelimon Stanica. The binary Gold function and its c-boomerang connectivity table. *Cryptography and Communications*, 14(6):1257–1280, November 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00573-8.

Kadir:2022:EDS

[568] Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. Encoding and decoding of several optimal rank metric codes. *Cryptography and Communications*, 14(6):1281–1300, November 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00578-3.

Eddahmani:2022:EVD

[569] Said Eddahmani and Sihem Mesnager. Explicit values of the DDT, the BCT, the FBCT, and the FBDT of the inverse, the gold, and the Bracken–Leander

S-boxes. *Cryptography and Communications*, 14(6):1301–1344, November 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00581-8.

Chase:2022:CAP

[570] Benjamin Chase and Petr Lisonek. Construction of APN permutations via Walsh zero spaces. *Cryptography and Communications*, 14(6):1345–1357, November 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00580-9.

Yu:2022:CMQ

[571] Yuyin Yu and Léo Perrin. Constructing more quadratic APN functions with the QAM method. *Cryptography and Communications*, 14(6):1359–1369, November 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00598-z.

Mesnager:2022:CCW

[572] Sihem Mesnager, Sihong Su, Jingjing Li, and Linya Zhu. Concrete constructions of weightwise perfectly balanced (2-rotation symmetric) functions with optimal algebraic immunity and high weightwise nonlinearity. *Cryptography and Communications*, 14(6):1371–1389, November 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00603-5.

Hong:2023:GBI

[573] Xiaoqin Hong and Xiwang Cao. Generalized block inserting for constructing new constant dimension codes. *Cryptography and Communications*, 15(1):1–15, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00590-7.

Sharma:2023:MTA

[574] Sandeep Sharma and Anuradha Sharma. Multi-twisted additive codes over finite fields are asymptotically good. *Cryptography and Communications*, 15(1):17–33, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00583-6.

Budaghyan:2023:TF

[575] Lilya Budaghyan, Ivana Ivkovic, and Nikolay Kaleyski. Triplicate functions. *Cryptography and Communications*, 15(1):35–83, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00587-2.

Kumar:2023:DCE

[576] Praveen Kumar, Palash Sarkar, Sudhan Majhi, and Subhabrata Paul. A direct construction of even length ZCPs with large ZCZ ratio. *Cryptography and Communications*, 15(1):85–94, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00589-0.

Li:2023:CAC

[577] Min Li, Yajing Zhou, Wei Su, and Yang Yang. Constructions of almost complementary pairs based on non-standard Golay sequences. *Cryptography and Communications*, 15(1):95–110, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00555-w`.

Debnath:2023:GHC

[578] Indibar Debnath, Om Prakash, and Habibul Islam. Galois hulls of constacyclic codes over finite fields. *Cryptography and Communications*, 15(1): 111–127, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00591-6`. See correction [579].

Debnath:2023:CGH

[579] Indibar Debnath, Om Prakash, and Habibul Islam. Correction to: Galois hulls of constacyclic codes over finite fields. *Cryptography and Communications*, 15(1):129–130, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00602-6`. See [578].

Wang:2023:RPD

[580] Xiang Wang. Reconstruction of permutations distorted by single Kendall τ-errors. *Cryptography and Communications*, 15(1):131–144, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00595-2`.

Wang:2023:HDC

[581] Yu Wang, Xiaoshan Kai, Zhonghua Sun, and Shixin Zhu. Hermitian dual-containing constacyclic codes over $\mathbf{F}_{q^2} + v_1\mathbf{F}_{q^2} + \cdots + v_r\mathbf{F}_{q^2}$ and new quantum codes. *Cryptography and Communications*, 15(1):145–158, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00593-4`.

Yin:2023:NFH

[582] Wenjuan Yin, Can Xiang, and Fang-Wei Fu. New frequency-hopping sequence sets with good parameters under aperiodic Hamming correlation. *Cryptography and Communications*, 15(1):159–169, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00596-1`.

Dinh:2023:CSC

[583] Hai Q. Dinh, Tushar Bag, Kanat Abdukhalikov, Sachin Pathak, Ashish K. Upadhyay, Ramakrishna Bandi, and Warattaya Chinnakum. On a class of skew constacyclic codes over mixed alphabets and applications in constructing optimal and quantum codes. *Cryptography and Communications*, 15(1): 171–198, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00594-3`.

Petrides:2023:DPP

[584] George Petrides. On decompositions of permutation polynomials into quadratic and cubic power permutations. *Cryptography and Communications*, 15(1):199–207, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00600-8.

Maouche:2023:SPW

[585] Youcef Maouche. Symbol-pair weight distribution of some irreducible cyclic codes. *Cryptography and Communications*, 15(1):209–220, January 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00599-y.

Huang:2023:MNL

[586] Daitao Huang, Qin Yue, and Yongfeng Niu. MDS or NMDS LCD codes from twisted Reed–Solomon codes. *Cryptography and Communications*, 15(2):221–237, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00564-9.

Kalgin:2023:CQA

[587] Konstantin Kalgin and Valeriya Idrisova. The classification of quadratic APN functions in 7 variables and combinatorial approaches to search for APN functions. *Cryptography and Communications*, 15(2):239–256, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00588-1.

Gong:2023:STC

[588] G. Gong and Z. L. Wang. Status of three classes of sequences. *Cryptography and Communications*, 15(2):257–308, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00585-4.

Shallit:2023:NFP

[589] Jeffrey Shallit. Note on a Fibonacci parity sequence. *Cryptography and Communications*, 15(2):309–315, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00592-5.

Vega:2023:CWD

[590] Gerardo Vega and Félix Hernández. The complete weight distribution of a subclass of optimal three-weight cyclic codes. *Cryptography and Communications*, 15(2):317–330, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00601-7.

Guo:2023:MSS

[591] Qian Guo, Erik Mårtensson, and Paul Stankovski Wagner. Modeling and simulating the sample complexity of solving LWE using BKW-style algorithms. *Cryptography and Communications*, 15(2):331–350, March

2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00597-0.

Shi:2023:EBN

[592] Chenmiao Shi, Jie Peng, Lijing Zheng, and Shihao Lu. On the equivalence between a new family of APN quadrinomials and the power APN functions. *Cryptography and Communications*, 15(2):351–363, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00606-2.

Quan:2023:TCW

[593] Xiaoshan Quan, Qin Yue, Xia Li, and Chengju Li. Two classes of 2-weight and 3-weight linear codes in terms of Kloosterman sums. *Cryptography and Communications*, 15(2):365–380, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00604-4.

Quan:2023:CTC

[594] Xiaoshan Quan, Qin Yue, Xia Li, and Chengju Li. Correction: Two classes of 2-weight and 3-weight linear codes in terms of Kloosterman sums. *Cryptography and Communications*, 15(2):381, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00608-0.

Guo:2023:DGT

[595] Guanmin Guo, Ruihu Li, Yang Liu, and Hao Song. Duality of generalized twisted Reed–Solomon codes and Hermitian self-dual MDS or NMDS codes. *Cryptography and Communications*, 15(2):383–395, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00605-3.

Wang:2023:PCR

[596] Jiabo Wang and Cong Ling. Polar coding for Ring–LWE-based public key encryption. *Cryptography and Communications*, 15(2):397–431, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00607-1.

Kavut:2023:ICP

[597] Selçuk Kavut. Improved cryptographic properties of Boolean functions obtained from the neighbourhood of Patterson–Wiedemann functions. *Cryptography and Communications*, 15(2):433–442, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00610-6.

Milshtein:2023:NBC

[598] Moshe Milshtein. A new binary $(17, 4, 5)$ constant weight code. *Cryptography and Communications*, 15(2):443–453, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/

article/10.1007/s12095-022-00611-5. See correction [622].

Ishizuka:2023:CQH

[599] Keita Ishizuka. Construction of quaternary Hermitian LCD codes. *Cryptography and Communications*, 15(2): 455–467, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00614-2.

Choi:2023:OBL

[600] Whan-Hyuk Choi, Cem Güneri, Jon-Lark Kim, and Ferruh Özbudak. Optimal binary linear complementary pairs of codes. *Cryptography and Communications*, 15(2):469–486, March 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00612-4.

Rodriguez:2023:TAG

[601] René Rodríguez, Yongzhuang Wei, and Enes Pasalic. A theoretical analysis of generalized invariants of bijective S-boxes. *Cryptography and Communications*, 15(3):487–512, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00615-1.

Li:2023:NUB

[602] Fagang Li, Hao Chen, Huimin Lao, and Shanxiang Lyu. New upper bounds and constructions of multi-erasure locally recoverable codes. *Cryptography and Communications*, 15(3):513–528, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00618-y.

Dinh:2023:SDL

[603] Hai Q. Dinh, Bhanu Pratap Yadav, Tushar Bag, Daniel Panario, and Ashish Kumar Upadhyay. Self-dual and LCD double circulant and double negacirculant codes over a family of finite rings $\mathbf{F}_q[v_1, v_2, \ldots, v_t]$. *Cryptography and Communications*, 15(3):529–551, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00616-0.

Li:2023:COL

[604] Xiaoru Li and Ziling Heng. A construction of optimal locally recoverable codes. *Cryptography and Communications*, 15(3):553–563, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00619-x.

Li:2023:MCG

[605] Yang Li, Shixin Zhu, and Ping Li. On MDS codes with Galois hulls of arbitrary dimensions. *Cryptography and Communications*, 15(3):565–587, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00621-3.

Boudine:2023:CIR

[606] Brahim Boudine, Jamal Laaouine, and Mohammed Elhassani Charkani. On the classification of ideals over $R[X]/\langle f(X)^{p^s}\rangle$ when $R = \mathbf{F}_{p^m} + u\mathbf{F}_{p^m} + \ldots + u^n\mathbf{F}_{p^m}$. *Cryptography and Communications*, 15(3):589–598, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00620-4.

Sagar:2023:OLC

[607] Vidya Sagar and Ritumoni Sarma. Octanary linear codes using simplicial complexes. *Cryptography and Communications*, 15(3):599–616, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00617-z.

Nyberg:2023:MBB

[608] Kaisa Nyberg. Modifications of bijective S-boxes with linear structures. *Cryptography and Communications*, 15(3):617–625, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00631-9.

Taniguchi:2023:DPA

[609] Hiroaki Taniguchi. D-property for APN functions from $\mathbf{F}_2^n$ to $\mathbf{F}_2^{n+1}$. *Cryptography and Communications*, 15(3):627–647, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00627-5.

Huang:2023:TCQ

[610] Daitao Huang, Qin Yue, and Fengwei Li. Two classes of quasi-cyclic codes via irreducible polynomials. *Cryptography and Communications*, 15(3):649–659, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00629-3.

Chen:2023:EWS

[611] Ruikai Chen and Sihem Mesnager. Evaluation of Weil sums for some polynomials and associated quadratic forms. *Cryptography and Communications*, 15(3):661–673, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00628-4.

Panario:2023:CBS

[612] Daniel Panario, Lucas Pandolfo Perin, and Brett Stevens. Comparing balanced sequences obtained from ElGamal function to random balanced sequences. *Cryptography and Communications*, 15(3):675–707, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00623-1.

Gu:2023:TDG

[613] Zhi Gu, Zhengchun Zhou, Avik Ranjan Adhikary, and Pingzhi Fan. Two-dimensional Golay complementary array pairs with flexible size and large zero correlation zone. *Cryptography and Communications*, 15(3):709–717, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic).

URL `https://link.springer.com/article/10.1007/s12095-023-00633-7`.

Datta:2023:WBE

[614] Somantika Datta. Welch bound equality sets with few distinct inner products from Delsarte–Goethals sets. *Cryptography and Communications*, 15(3): 719–729, May 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00635-5`.

Hebborn:2023:MAD

[615] Phil Hebborn, Gregor Leander, and Aleksei Udovenko. Mathematical aspects of division property. *Cryptography and Communications*, 15(4):731–774, July 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00622-2`.

Ozbudak:2023:CCS

[616] Ferruh Özbudak and Burcu Gülmez Temür. Complete characterization of some permutation polynomials of the form $x^r(1 + ax^{s_1(q-1)} + bx^{s_2(q-1)})$ over $\mathbf{F}_{q^2}$. *Cryptography and Communications*, 15(4):775–793, July 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00641-7`.

Bishnoi:2023:WES

[617] Monika Bishnoi and Pankaj Kumar. Weight enumerators of some irreducible cyclic codes of odd length. *Cryptography and Communications*, 15(4):795–809, July 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00637-3`.

Rai:2023:FRC

[618] Amritanshu Rai and Rohit Gupta. Further results on a class of permutation trinomials. *Cryptography and Communications*, 15(4):811–820, July 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00640-8`.

Tiwari:2023:HON

[619] Sampada Tiwari and Deepmala Sharma. On higher order nonlinearities of Boolean functions. *Cryptography and Communications*, 15(4):821–830, July 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00643-5`.

Li:2023:CFI

[620] Yanjun Li, Haibin Kan, Jie Peng, and Lijing Zheng. Cryptographic functions with interesting properties from CCZ-equivalence. *Cryptography and Communications*, 15(4):831–844, July 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00646-2`.

Caliskan:2023:SCC

[621] Basri Çaliskan, Nuh Aydin, and Peihan Liu. Skew cyclic codes over $\mathbf{Z}_4 + u\mathbf{Z}_4 + v\mathbf{Z}_4$. *Cryptography and*

Communications, 15(4):845–858, July 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00645-3.

Milshtein:2023:CNB

[622] Moshe Milshtein. Correction: A new binary $(17, 4, 5)$ constant weight code. *Cryptography and Communications*, 15 (4):859, July 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00638-2. See [598].

Basak:2023:ABF

[623] Jyotirmoy Basak, Subhamoy Maitra, Prabal Paul, and Animesh Roy. Analysis of boolean functions related to binary input binary output two-party nonlocal games. *Cryptography and Communications*, 15(5):861–890, September 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00648-0.

Abdollahi:2023:NUB

[624] Alireza Abdollahi, Javad Bagherian, Fatemeh Jafari, Maryam Khatami, Farzad Parvaresh, and Reza Sobhani. New upper bounds on the size of permutation codes under Kendall τ-metric. *Cryptography and Communications*, 15(5):891–903, September 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00642-6.

Zhou:2023:TCT

[625] Yajing Zhou, Xiaoshan Kai, and Shixin Zhu. Two classes of ternary LCD constacyclic BCH codes. *Cryptography and Communications*, 15(5):905–919, September 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00655-1.

Yang:2023:LCT

[626] Zhiye Yang, Zibi Xiao, and Xiangyong Zeng. Linear complexity and trace representation of balanced quaternary cyclotomic sequences of prime period p. *Cryptography and Communications*, 15(5):921–940, September 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00649-z.

Torres:2023:CCM

[627] Jaziel Torres and Ivelisse Rubio. Circular Costas maps: A multidimensional analog of circular Costas sequences. *Cryptography and Communications*, 15(5):941–958, September 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00654-2.

Sui:2023:NCS

[628] Junzhen Sui, Qin Yue, and Fuqing Sun. New constructions of self-dual codes via twisted generalized Reed–Solomon codes. *Cryptography and Communications*, 15(5):959–978, September 2023. CODEN ???? ISSN 1936-

2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00644-4.

Ghosh:2023:COB

[629] Gobinda Ghosh, Sudhan Majhi, and Subhabrata Paul. Construction of optimal binary Z-complementary code sets with new lengths using generalized Boolean function. *Cryptography and Communications*, 15(5):979–993, September 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00658-y.

Rodier:2023:DAR

[630] François Rodier, Florian Caullery, and Eric Férard. Distribution of the autocorrelation of random Boolean functions. *Cryptography and Communications*, 15(5):995–1009, September 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00653-3.

Xie:2023:VBF

[631] Xianhong Xie, Yi Ouyang, and Ming Mao. Vectorial bent functions and linear codes from quadratic forms. *Cryptography and Communications*, 15(5):1011–1029, September 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00664-0.

Abdukhalikov:2023:HFH

[632] Kanat Abdukhalikov and Duy Ho. Hyperbent functions from hyperovals. *Cryptography and Communications*, 15(5):1031–1048, September 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00668-w.

Budaghyan:2023:ESI

[633] Lilya Budaghyan, Claude Carlet, Tor Helleseth, and Wilfried Meidl. Editorial: Special issue on Boolean functions and their applications 2022. *Cryptography and Communications*, 15(6):1049–1051, November 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00678-8.

Subroto:2023:AAS

[634] Robert Christian Subroto. An algebraic approach to symmetric linear layers in cryptographic primitives. *Cryptography and Communications*, 15(6):1053–1067, November 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00630-w.

Chen:2023:BDU

[635] Li-An Chen and Robert S. Coulter. Bounds on the differential uniformity of the Wan–Lidl polynomials. *Cryptography and Communications*, 15(6):1069–1085, November 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00634-6.

Mella:2023:DLP

[636] Silvia Mella, Alireza Mehrdad, and Joan Daemen. Differential and linear properties of vectorial boolean functions based on chi. *Cryptography and Communications*, 15(6):1087–1116, November 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00639-1`.

Salagean:2023:FCC

[637] Ana Salagean and Ferruh Özbudak. Further constructions and characterizations of generalized almost perfect nonlinear functions. *Cryptography and Communications*, 15(6):1117–1127, November 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00647-1`.

Gillot:2023:CSC

[638] Valérie Gillot and Philippe Langevin. Classification of some cosets of the Reed–Muller code. *Cryptography and Communications*, 15(6):1129–1137, November 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00652-4`.

Kaleyski:2023:IFA

[639] Nikolay Kaleyski, Kjetil Nesheim, and Pantelimon Stanica. An infinite family of 0-APN monomials with two parameters. *Cryptography and Communications*, 15(6):1139–1169, November 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00651-5`.

Djurasevic:2023:SMA

[640] Marko Djurasevic, Domagoj Jakobovic, Luca Mariot, and Stjepan Picek. A survey of metaheuristic algorithms for the design of cryptographic Boolean functions. *Cryptography and Communications*, 15(6):1171–1197, November 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00662-2`.

Salagean:2023:PEA

[641] Ana Salagean and Percy Reyes-Paredes. Probabilistic estimation of the algebraic degree of Boolean functions. *Cryptography and Communications*, 15(6):1199–1215, November 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00660-4`.

Anbar:2023:GSB

[642] Nurdagül Anbar, Tekgül Kalayci, and Wilfried Meidl. On generalized spread bent partitions. *Cryptography and Communications*, 15(6):1217–1234, November 2023. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00670-2`.

Mesnager:2024:SIC

[643] Sihem Mesnager. Special issue on contemporary interactions between codes, cryptographic functions and/

or sequences. *Cryptography and Communications*, 16(1):1–2, January 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00696-0.

Li:2024:FDM

[644] Fulin Li, Hang Hu, Shixin Zhu, and Jiayun Yan. A fully dynamic multi-secret sharing scheme with redundant authorization. *Cryptography and Communications*, 16(1):3–20, January 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00613-3.

Wang:2024:MCC

[645] Xiaoqiang Wang, Cunsheng Ding, Hongwei Liu, and Dabin Zheng. MDS constacyclic codes of length $q+1$ over GF(q). *Cryptography and Communications*, 16(1):21–48, January 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-022-00624-0.

Yang:2024:LBD

[646] Ruipan Yang, Ruihu Li, Qiang Fu, Sen Yang, and Yi Rao. On locality of binary distance-optimal codes. *Cryptography and Communications*, 16(1):49–69, January 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00626-6.

Shen:2024:PZC

[647] Bingsheng Shen, Yang Yang, and Pingzhi Fan. Preferred Z-complementary pairs and their application in Doppler resilient waveform design. *Cryptography and Communications*, 16(1):71–87, January 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00636-4.

Liu:2024:NSZ

[648] Shilu Liu, Zhengchun Zhou, Avik Ranjan Adhikary, and Yang Yang. New supersets of Zadoff–Chu sequences via the Weil bound. *Cryptography and Communications*, 16(1):89–108, January 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00632-8.

Tekin:2024:APA

[649] Eda Tekin, Oliver Wilhelm Gnilke, Ferruh Özbudak, Bernhard Blümich, and Marcus Greferath. Almost perfect autocorrelation sequences with small number of pauses for applications in magnetic resonance. *Cryptography and Communications*, 16(1):109–127, January 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00659-x.

Zidaric:2024:WGS

[650] N. Zidarič, K. Mandal, G. Gong, and M. Aagaard. The Welch–Gong stream cipher — evolutionary path. *Cryptography and Com-*

munications, 16(1):129–165, January 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00656-0`.

Xiao:2024:NCM

[651] Hongyang Xiao and Xiwang Cao. New constructions of mutually orthogonal complementary sets and Z-complementary code sets based on extended Boolean functions. *Cryptography and Communications*, 16(1):167–184, January 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00673-z`.

Li:2024:FIP

[652] Xia Li, Qin Yue, and Daitao Huang. Factorization of invariant polynomials under actions of projective linear groups and its applications in coding theory. *Cryptography and Communications*, 16(1):185–207, January 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00675-x`.

Wang:2024:NCO

[653] Zheng Wang, Zhifan Ye, Chunming Tang, and Yang Yang. New construction of optimal ZCZ sequence sets with inter-set zero cross-correlation zone. *Cryptography and Communications*, 16(1): 209–228, January 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00685-9`.

Roy:2024:LBM

[654] Abhishek Roy and Sudhan Majhi. Lower bounds on the maximum cross-correlations of 2-D quasi-complementary array sets. *Cryptography and Communications*, 16(2):229–247, March 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00665-z`.

Gupta:2024:CNM

[655] Kishan Chand Gupta, Sumit Kumar Pandey, and Susanta Samanta. On the construction of near-MDS matrices. *Cryptography and Communications*, 16(2):249–283, March 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00667-x`.

Steiner:2024:LBD

[656] Matthias Johann Steiner. A lower bound for differential uniformity by multiplicative complexity & bijective functions of multiplicative complexity 1 over finite fields. *Cryptography and Communications*, 16(2):285–308, March 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-023-00661-3`.

Che:2024:FRA

[657] Cheng Che and Tian Tian. Further results on affine sub–families of NFSR sequences. *Cryptography and Communications*, 16(2):309–321, March 2024. CODEN ???? ISSN 1936-

2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00663-1.

Armario:2024:GPB

[658] J. A. Armario, R. Egan, and D. L. Flannery. Generalized partially bent functions, generalized perfect arrays, and cocyclic Butson matrices. *Cryptography and Communications*, 16(2):323–337, March 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00657-z.

Lv:2024:CCS

[659] Xinxin Lv, Cuiling Fan, and Yanyan Wang. The cross-correlation spectrum of ternary perfect sequences and their decimations. *Cryptography and Communications*, 16(2):339–349, March 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00671-1.

Chen:2024:TCP

[660] Changhui Chen, Haibin Kan, Jie Peng, Lijing Zheng, and Yanjun Li. Three classes of permutation quadrinomials in odd characteristic. *Cryptography and Communications*, 16(2):351–365, March 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00672-0.

Ghosh:2024:DCO

[661] Gobinda Ghosh, Sudhan Majhi, and Shubhabrata Paul. A direct construction of optimal 2D-ZCACS with flexible array size and large set size. *Cryptography and Communications*, 16(2):367–385, March 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00669-9.

Gupta:2024:SCP

[662] Rohit Gupta, Luciane Quoos, and Qiang Wang. Some classes of permutation binomials and trinomials of index $q-1$ over $\mathbf{F}_{q^n}$. *Cryptography and Communications*, 16(2):387–402, March 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00674-y.

Kumar:2024:DCCa

[663] Nishant Kumar, Sudhan Majhi, and Ashish K. Upadhyay. A direct construction of complete complementary code with zero correlation zone property for prime-power length. *Cryptography and Communications*, 16(2):403–426, March 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00676-w.

Kai:2024:CBS

[664] Xiaoshan Kai, Jiayuan Zhang, Ping Li, and Shixin Zhu. Construction of binary self-orthogonal codes. *Cryptography and Communications*, 16(2):427–444, March 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00677-9.

Rodier:2024:PAS

[665] François Rodier, Florian Caullery, and Eric Férard. Periodic autocorrelation of sequences. *Cryptography and Communications*, 16(2):445–458, March 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00680-0.

Han:2024:LRC

[666] Xiaopan Han, Guojun Han, Han Cai, and Linxin Yin. Locally repairable codes with multiple repair sets based on packings of block size 4. *Cryptography and Communications*, 16(3):459–479, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00681-z.

Fernandez:2024:FCS

[667] Marcel Fernandez, John Livieratos, and Sebastià Martín. Frameproof codes, separable codes and B_2 codes: Bounds and constructions. *Cryptography and Communications*, 16(3):481–506, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00682-y.

Cao:2024:SDS

[668] Meng Cao, Jing Yang, and Fuchuan Wei. On the σ duals and σ hulls of linear codes. *Cryptography and Communications*, 16(3):507–530, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00679-7.

Eyvazi:2024:HGI

[669] Hamidreza Eyvazi, Karim Samei, and Batoul Savari. The Homogeneous Gray image of linear codes over the Galois ring $GR(4, m)$. *Cryptography and Communications*, 16(3):531–540, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00683-x.

Kumar:2024:NCA

[670] Nishant Kumar, Sudhan Majhi, and Sushant K. Jha. A new construction of almost-optimal multiple ZCZ sequence sets for multi-cell QS–CDMA system. *Cryptography and Communications*, 16(3):541–556, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00684-w.

Singh:2024:MMT

[671] Harshdeep Singh and Kapish Chand Meena. MDS multi-twisted Reed–Solomon codes with small dimensional hull. *Cryptography and Communications*, 16(3):557–578, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00688-6.

Hyun:2024:GCB

[672] Jong Yoon Hyun, Nayoung Han, and Yoonjin Lee. The Griesmer codes of Belov type and optimal quaternary

codes via multi-variable functions. *Cryptography and Communications*, 16(3): 579–600, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00686-8.

Wu:2024:MLC

[673] Xia Wu, Wei Lu, Xiwang Cao, and Gaojun Luo. Minimal linear codes constructed from partial spreads. *Cryptography and Communications*, 16(3): 601–611, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00689-5.

Jing:2024:ACI

[674] Xiaoyan Jing and Zhefeng Xu. The 4-adic complexity of interleaved quaternary sequences of even period with optimal autocorrelation. *Cryptography and Communications*, 16(3):613–628, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00690-y.

Liu:2024:LHZ

[675] Xing Liu. Low-hit-zone frequency hopping sequence sets under aperiodic Hamming correlation. *Cryptography and Communications*, 16(3):629–645, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00691-x. See [676].

Liu:2024:CLH

[676] Xing Liu. Correction: Low-hit-zone frequency hopping sequence sets under aperiodic Hamming correlation. *Cryptography and Communications*, 16 (3):647, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00714-1. See correction [675].

Shen:2024:CBB

[677] Shuhui Shen and Xiaojun Zhang. A class of balanced binary sequences with two-valued non-zero autocorrelation sum and good crosscorrelation sum. *Cryptography and Communications*, 16(3): 649–663, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00692-w.

Kumari:2024:RKA

[678] Prity Kumari and Karam Ratan Singh. Re-keying analysis in group key management of wireless sensor networks. *Cryptography and Communications*, 16 (3):665–677, May 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-023-00693-9.

Wang:2024:NNN

[679] Xiao-Juan Wang, Tian Tian, and Wen-Feng Qi. GL-S-NFSR: a new NFSR structure and its period properties. *Cryptography and Communications*, 16 (4):679–698, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.

com/article/10.1007/s12095-024-00694-2.

Zhao:2024:CCR

[680] Jinghui Zhao, Xiuling Shan, and Zihong Tian. Combinatorial constructions of repairable ramp schemes. *Cryptography and Communications*, 16(4):699–719, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00695-1.

Meaux:2024:TDF

[681] Pierrick Méaux and Dibyendu Roy. Theoretical differential fault attacks on FLIP and FiLIP. *Cryptography and Communications*, 16(4):721–744, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00698-y.

Zhang:2024:PSL

[682] Hanglong Zhang and Xiwang Cao. On the parameters of some LCD BCH codes over $\mathbf{F}_q$ with length $(q^m + 1)/\lambda$. *Cryptography and Communications*, 16(4):745–765, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00697-z.

Kumar:2024:DCCb

[683] Praveen Kumar, Sudhan Majhi, and Subhabrata Paul. A direct construction of cross z-complementary sequence sets with large set size. *Cryptography and Communications*, 16(4):767–777, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00700-7.

Li:2024:SCO

[684] Shitao Li, Minjia Shi, and Huizhou Liu. Several constructions of optimal LCD codes over small finite fields. *Cryptography and Communications*, 16(4):779–800, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00699-x.

Wu:2024:OQC

[685] Tingting Wu, Shixin Zhu, Li Liu, and Lanqiang Li. Optimal quinary cyclic codes with three zeros. *Cryptography and Communications*, 16(4):801–823, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00703-4.

Grassl:2024:CCC

[686] Markus Grassl, Ferruh Özbudak, Buket Özkaya, and Burcu Gülmez Temür. Complete characterization of a class of permutation trinomials in characteristic five. *Cryptography and Communications*, 16(4):825–841, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00705-2.

Xue:2024:BFB

[687] Erzhong Xue, Zilong Wang, and Jinjin Chai. Boolean functions of binary Type-II and Type-III/II complementary array pairs. *Cryptography and*

Communications, 16(4):843–855, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00701-6.

Zhu:2024:TGR

[688] Canze Zhu and Qunying Liao. The $[1, 0]$-twisted generalized Reed–Solomon code. *Cryptography and Communications*, 16 (4):857–878, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00704-3.

Li:2024:IWB

[689] Fengwei Li, Fanhui Meng, Ziling Heng, and Qin Yue. An improvement on Weil bounds for character sums of polynomials over finite fields. *Cryptography and Communications*, 16(4):879–887, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00706-1.

Yilmazguc:2024:ACA

[690] Gülsüm Gözde Yilmazgüç, Javier de la Cruz, and Edgar Martínez-Moro. Abelian and consta-Abelian polyadic codes over affine algebras with a finite commutative chain coefficient ring. *Cryptography and Communications*, 16(4):889–907, July 2024. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL https://link.springer.com/article/10.1007/s12095-024-00707-0.