A Complete Bibliography of Publications in *Designs, Codes, and Cryptography*

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: https://www.math.utah.edu/~beebe/

29 September 2023  
Version 2.50

Title word cross-reference

(0, 1) [628]. (0, 2) [962]. (0, 2, t) [637]. (0, α) [696, 844]. (1, −1) [518]. (1, 2) [1269]. (17, 9) [351]. (17q, 17, 2) [364]. (2) [1198]. (2, 2) [1179]. (2, 23) [1431]. (2, 7) [1432]. (2, 8) [667, 1133]. (2, n) [904]. (2, p, p) [2430]. (2, q) [1432]. (2, qn) [1231]. (255, k) [657]. (25q, 25, 3) [364]. (28, 12, 11) [117]. (2n) [1270]. (3, 3) [1452]. (3, 4) [1788, 1872]. (3, 5, v) [578]. (3, 8) [667]. (3, L) [2848]. (3, p3) [635]. (3, t) [1550]. (31, 10, 3) [34]. (36, 16, 12) [117]. (4) [659]. (4, 4) [634, 741]. (4, 8) [1133]. (49, 9, 6) [142]. (5, 2) [1138]. (6, 3) [835]. (6, q) [642]. (64, 237, 12) [236]. (8, 2) [451]. (96, 20, 4) [803]. (Ck ⊕ G, k) [251]. (d, σ) [2976]. (G, k, 1) [251]. (k) [1634]. (k, 3) [1963]. (k, n) [478, 1214, 2066]. (k, n)∗ [1982]. (k, p) [425]. (λ + m)Kv+uλKv [1803]. (m, 40n) [2522]. (m, n) [151]. (m, n, 4, 2) [2260]. (m − 1)/pm [167]. (n, 3) [1644]. (n, 4) [1467]. (n, m) [2394, 2556]. (n, q) [636]. (n × m, 3, 2, 1) [2391]. (v, 5, 5) [872]. (v, 6, λ) [901]. (p, v, p, v, p−1) [139]. (p2, p2, p, 1) [605]. (q) [362]. (q + t, t) [637]. (q, 6, 1) [342]. (Q−(5,q)) [1643]. (q2 + q + 2, q + 2) [540]. (q2 − q + 8)/2 [1125]. (q2, 2) [1541]. (qm) [362]. (r, s, t) [2958]. (r, λ) = 1 [2034]. (r, t) [2864]. (t, k) [1160]. (t, L) [2420]. (t, m, s) [814, 1332]. (t, n) [892, 1153, 1360, 2068]. (t − 1) [1534]. (θ, ϑ) [2840]. (v, {2, 4}, 1) [245]. (v, 3, 1) [581]. (v, 4, 1) [2859]. (v, 4, 2, 1) [1285]. (v, k, 1) [1835, 3020]. (v, k, 2) [2283]. (v, k, 3) [2273]. (v, k, 4) [1237]. (v, k, k − 1) [1892, 2346]. (v, k, k − 2, k − 1) [2525].
$F_2 + uF_2 + vF_2 + uvF_2 + u^2F_2 + uv^2F_2$
$[2577, F_2(u)/(u^4) [2668]. F_{2^m} [439]. F_{2^n} [831]. F_{2p+1} [1822]. F_2 \times F_2 [618]. F_4 + vF_4 [1991]. F_5 [675, 1024, 1051, 1159]. F_p [912].$
$F_7 + uF_p [2322]. F_{p^n} [1809]. F_{p^m} [922, 2506]. F_q [742, 1163]. F_q(u)/u^w [834]. F_q(x)/(x^2) [2327]. F_{q^n} [83]. F_{222} [978]. \frac{1}{3} [225]. \frac{1}{3} [1935].$
$\sum_{q=1}^{2} [2467]. \sum_{m=1}^{2} [2503]. G$
$[989, 1019, 1047, 2291, 2691]. G(1, n, q) [909].$
$g(x) = x^3 + bx + c [2853]. G(b) [2863]. g^xu [1327]. g^o = 1 [743, 1759]. G_{1, 2} [717]. G(1, n, q) [2838]. G(19) [2838]. G(23) [2838].$
$G(2^2m) [1654]. G(2^{2m+1}) [1654]. G(2^k) [315]. G(2^n) [948]. G(4) [1308]. G(5) [485]. G(p) [75, 2038]. G(q) [485].$
$[15, 1298, 2125]. G(q^2) [15]. GL(n + 1, q) [692]. GR(4, n) [1738]. GR(p, q) [581, 1022, 1836, 1902, 2117, 1903].$
$H [995, 1218, 1269, 1938].
$H(2d - 1, q^2) [1658]. H(n, 2) [2111]. H(q) [1221].$
$h^t = 1 [995, 1671]. h = 0 \text{ mod } 12 [1671]. j [1422]. j = 0 [2774]. K [206, 261, 912, 949, 1214, 1252, 1298, 1430, 1539, 1614, 1633, 1655, 1694, 2410, 2412, 2677, 2689, 2761, 2767, 2883, 2896, 2944, 3027, 3038].$
$k > 2 [22]. L [988].
$[244, 352, 989, 1232, 2677]. \lambda = 1 [2885].$
$\lambda = 2, 4, 8 [573]. \lambda = 2^n [475]. \lambda > 1 [901].$
$\leq k [2900]. M [36, 186, 374, 501, 743, 1022, 1111, 1613, 1705, 2229]. m + 1 [2295].$
$m > n/2 [2394]. M_{13} [373]. Mat_{n,s}(Z_k) [721]. F_{2s} [1917]. F_{2s} [2041]. F_{2w} [2058].$
$F_{2w} [2049, 2485, 2764]. F_{2r}(u)/u^w [2980]. F_{3w} [1730]. F_{4} [1561, 2902]. F_p [1919]. F_q [1868, 2503, 2744, 2864, 2911].$
$F_q^q(u)/u^w [1774]. F_{q^n} [1868]. F_{q^n} [1959]. F_{q^n} [2941]. G_1 [3031].$
$G_2 [3031]. G_3 [3031]. Z [2514].$
$Z/\mathbb{Z} \times Z/MZ [1992]. Z_{16} [2019]. Z_2 [2202]. Z_{2k} [2242, 2622]. Z_{2w} [1806]. Z_{2} [2067].$
$Z_{2} Z_{2w} [2754]. Z_{2} Z_{4} [1666, 2175, 2829].$
$Z_{4} [1471, 2116, 2244, 2387, 2445, 2573, 2969].$
$Z_{4} [u]/(u^2 - 1) [2244]. Z_{8} [2019, 2819]. Z_{m} [2067, 3037]. Z_{m} [2555, 2954]. Z_{p}(u)/(u^3) [2560]. Z_{p}(u)/u^k [1747]. Z_{p} [2076]. Z_{p^2} [2788]. Z_{p^2} [2920]. Z_{q} [2146]. Z_{2}[32 - 1] [1771]. C [2869]. D_{2} \cap M_{#} [2869].$
$\mathbb{G}^{M_{#}}(\mathbb{C}) [1775]. H(\mathbb{R}, \mathbb{H}^{\infty}) [1703].$
$\mathbb{M}_{#} [2869]. Q^{+}(\mathbb{N}). \mathbb{H}_{2} [931]. R.F [2993]. S_{c} [2358]. P(2, q) [2880]. P(2, q^2) [1852].$
$P(3, 2) [1968]. P(3, q) [2718]. P(4, q) [1988, 2483]. P(n, q) [2410, 2523, 2761].$
$P(n, q) \times P(n, q) [1768]. P(2, 2^m) [2695]. CENCAPP [2806]. LWE [2470]. MP [2470]. MD2 [283]. N$
$[23, 143, 261, 501, 646, 783]. n = 1 [2453, 2486]. n = 5p^r [1141]. n = p_{-1} [1715]. n > 1 [1231]. n > 5 [2910]. n = 0 \text{ mod } 16 [1170]. N = 5 \text{ mod } 8 [2775]. N \geq 4 [881]. N P [607]. n [145]. n \equiv 0 [1865]. N^0 [8, 2] [300]. O_{c_{1}}(3, 5)^{-} [1662]. X [2024]. D [2146]. P$
$P(3, q) [174, 320, 845, 1220]. P(3, q, q = 2 \text{ mod } 3) [1125]. P(4, 2) [472]. P(4, 4) [366]. P(9, 2) [717]. P(d, q^2) [2240]. P(n, m) [44]. P(n, 2) [472]. 773, 1000, 1409]. P(n, 4) [1741]. P(n, p^r) [1534]. P(n, q) [528, 909, 1031, 1065, 1411]. P(n, q, n > 3 [718]. P(n, q, n \geq 3 [474]. P(n, q^3) [1252]. P(n, q^3) [692]. P((r, q) [2642]. P^* [931]. PGL(2, 2^f) [13]. PGL(n, q) [2830]. PGL(n, q) [629]. P(2, q) [2670, 2996].
PSL(n + 1, q) [692]. PSL_2(q) [879].
Q(4, q) [1532]. Q(3, q) [2668]. q + 1 [985].
q = 19 [107]. Q^+(4n + 1, 3) [883]. Q^+(7, q) [778]. Q^{-}(5, 1) [410]. Q^{-}(7, q) [1191]. q^2 [985].
q^2 - 2q - 2q + 1 ≤ d ≤ q^2 - 2q - q [797]. q^m [505]. q^a [98]. R [1061, 1330, 2466, 2896].
R(1, 7) [275]. R(1, 9) [192]. R(4, 9) [192].
r > λ(k - 3) [2779]. R^n [628, 812]. R_3 [1783].
R_k [1407]. r ≥ 3 [2642]. → k [767]. RM(3, 7) [2183].
S [291, 333, 468, 2469, 2647, 2674, 3003].
S(2, 4, 3^{-1/2}) [2467]. S(3, 7, 3^1 + 1) [2802].
s(u) [12]. S_{1,1,1}(2)S_{1,1,1}(2) [1387]. S_9 [1143].
σ [2520]. SL(2, 5) [232, 980, 1067]. SL(2, 2^n) [1628].
SL(n + 1, q) [692]. SL_2 [2011].
SQS(16) [1069]. STS(31) [899]. sv [15].
t - (v, k, λ) [740]. t = 3 [2855]. T_{32}(q) [683]. τ [1004, 1290, 2093, 2173, 2733].
F_2 × F_2 [3040].
F_4 [3040]. θ [620]. TR + D [2466]. U(6) [55].
u^2 [1017]. U_5 [2237]. U_{14}(q) [1869].
v [15, 585, 1133]. v - 1 [585]. v = 4(k - λ) + 2 [1695].
v = r + c - 1 [822]. v_{k} [1980]. v = 0, 1 (mod 8) [1133]. w [990]. W(2n + 1, q) [684].
W_5(q) [977]. u_{min}/u_{max} < 1/2 [2496]. X [1000, 1121].
X^# [1000]. x^{-1} + g(x) [1315].
x^3g(x^q-1) [2853]. x^6 + ax [652]. x^a mod N [303].
x^{-1} ∈ F_q[x] [1875]. x^t g(x^a) [2266].
x^t h(x^a) [2554]. x^t h(x^{-1}) [2302].
x(x^{-a} - y) [2941].
y^{q^2} - y = γx^{q+1} - α [159].
Z [994, 1075, 1238, 1501, 2907]. Z/(Z^{22} - 1) [1602]. Z/2K [789]. Z_2 + uZ_2 [954].
Z_2 + uZ_2 + u^2Z_2 [954]. Z_2^2 [959]. Z_2^2 [794, 1523]. Z_2k [559]. Z_2 × Z_4 [1348].
Z_2Z_2[u] [2253]. Z_2Z_4 [1203, 1236, 1842, 2079].
Z_4 [343, 346, 375, 401, 622, 658, 869, 1348, 1486, 1559, 2206].
Z_q^2 [439]. Z_q × Z_4 [664].
Z_8 [929]. Z_9 [929]. Z_m [1108].
Z_p^r × Z_p^{r+1} × · · · × Z_p^{r^n} [181]. Z_p^{r^n} [1120]. Z_p^k [922]. Z_q [1202].

* [1614]. *-visual [1614].
[2629, 2673, 2821]. -dimension [75, 783]. -dimensional
[1044, 1347, 1422, 1667, 1786, 2432]. -double [2202]. -Elusive [2674]. -error
achievability
Action
Accurate
absolutely
above
Admissible
Adaptive
active
actor
Adaptable
Admissibly
Adaptively
Add
adder
Addition
adic
Adjacency
adjacent
Admissible
Admitting
Adversarial
Adversary
AES
AES-like
AES-based
Affine
Affine-like
Affine-Invariant
Affine-type
against
aggregate
aided
alarms
Algebra
Algebraic
Algebraic-geometry
Algebraically
Algebras
Algorithm
Almost
almost-perfect
Alphabet
alphabet-optimal
alignment
all-but-many
anonymity
Annihilator
Annihilators
anonymous
Anniversary
Anonymity
Annul
Annulled
Annulment
Annulus
Annuluses
Annulus
Annuluses
Annuluses
Annuluses
Annuluses
Annuluses
Annuluses
bytes [1083].


36

1508, 1609, 1670, 1973, 1990, 2772, 2860].
quasi-Feistel [1283]. Quasi-Frobenius [448]. quasi-Galois [2980]. Quasi-Multiple
[520]. quasi-orthogonal [2444].
quasi-perfect [911, 1093, 1307, 2865].
Quasi-Symmetric [20, 30, 39, 71, 116, 117, 142, 520, 604, 616, 617, 926, 934, 1137, 1286, 1404, 1882, 2750].
Quasi-Twisted [548, 1844, 2431, 2473].
Quasideterminant [310].
quasidivisible [1965]. quasifields [1647].
Quasigroups [36, 815, 825, 1052, 1445].
quasiprimitive [1542, 2283].
quasiregular [8]. Quaternary [88, 167, 723, 839, 1186, 1281, 1309, 1310, 1384, 1585, 1687, 1717, 1929, 2026, 2233, 2614, 2722, 2775, 2778, 2958, 2959, 2972].
Quaterni0n [824, 2301]. Question [55, 406].
quintic [717]. Quotient [830].
Quotients [1437, 1524].
R [1513]. Rabin [314, 359].
Rabin-type [359]. Rabin-Williams [314].
Rackoff [876, 2720]. Radii [72, 418, 507, 943, 1356].
Radius [3, 40, 192, 224, 302, 316, 357, 603, 727, 772, 917, 1026, 1061, 1209, 1307, 1555, 1651, 2044, 2183, 2466, 2865].
Rado [1642, 1658, 1819, 2345].
rank-based [2516]. rank-distance [2527].
Rank-metric [1983, 2176, 2517, 2679, 2785].
Rao [1830, 2277, 2330]. Rate [146, 167, 225, 257, 510, 1308, 1595, 1609, 2942].
ratio [1692, 2382, 2798]. Rational [263, 277, 458, 739, 874, 1217, 1398, 1570, 1897, 1959, 2102, 2240, 2509, 2529, 2595, 2862, 3032].
RC4 [1068, 1083, 1873, 2048, 2215, 2625]. re [1845, 2312]. re-encryption [2312].
re-evaluation [1845]. reaching [2327].
Real [163, 2608, 3040]. realizability [1130].
Realization [367, 1595]. realizing [1960].
Receiver [478, 2945]. receivers [2383].
Reciprocal [736, 858, 2270, 2822].
Reconciliation [649]. Reconstructed [552]. reconstructing [2198].
Recoverable [2599, 2600, 2605, 2714, 2783, 2958, 2984].
Recovery [158, 1728, 1743, 2243, 2254, 2600, 2762, 2876, 2823]. rectangle [2539].
Rectangles [125, 1008, 1144, 1857].
Rectilinear [466]. recurrence [1820].
recurring [2894]. recursions [1092].
Recursive [296, 776, 1075, 1335, 1734, 2045, 2051, 2095, 2241, 2368, 2390, 2469, 2538, 2804, 2968, 2980].
Redefining [2046]. Rédei [2390, 2578].
Reduced [535, 1596, 1800, 2094, 2214, 2248, 2530, 2823].
reduced-round [1596, 2214, 2823].
reducibility [1258, 1446]. reducible [1300, 1425, 1594, 1859].
reductions [1602, 1771, 1825]. Redundancy [335, 1184].
Redundant [162, 932, 1290].
Ree [228, 290, 790, 1027, 1044]. Reed [28, 40, 72, 165, 275, 467, 507, 529, 582, 948, 952, 1064, 1072, 1097, 1202, 1210, 1498, 1556, 1558, 1620, 1682, 1707, 1709, 1723, 2183, 2393, 2421, 2438, 2446, 2515, 2581, 2617, 2627, 2633, 2709, 2717, 2758, 2861, 2874, 2901, 2966].
Reflection [97, 2040]. Reflections [1896].
reflexive [1824]. Regev [2873].
Register [91, 682, 1581, 1740, 2041]. Registers
Related [105, 116, 165, 233, 348, 413, 492, 577, 635, 737, 803, 824, 886, 979, 1028, 1135, 1199, 1278, 1300, 1305, 1311, 1333, 1420, 1433, 1442, 1495, 1549, 1719, 1822, 1846, 1848, 1873, 2059, 2115, 2133, 2150, 2185, 2234, 2330, 2354, 2390, 2391, 2485, 2539, 2700, 2839, 2927, 2959, 2993].

Related-key [1311, 1333, 2539].

Relating [428, 1306].

relations [51, 1166, 1326, 1750, 1820, 2663, 2947].

Relativity [650, 1459].

Relative [10, 139, 185, 266, 294, 345, 404, 605, 665, 780, 804, 1057, 1147, 1569, 1652, 1653, 1660, 1697, 1796, 1802, 2013, 2111, 2356, 2547, 2553].

relatively [2141].

release [2177].

remaining [2899].

Remarks [22, 1559].

Relativism [155].

repair [2462].

repairability [2186].

reparable [2199, 2800].

repeated [854, 999, 1235, 1670].

repeated-root [999].

Replication [2533, 2922].

Representation [550, 624, 647, 933, 948, 1257, 1308, 1593, 1827, 2050, 2097, 2509, 2590, 2626].

Representations [162, 215, 608, 888, 940, 1004, 1164, 1399, 1871, 2435, 2542].

reprint [188, 189].

repudiation [808].

Required [264].

Requirements [157].

research [1903].

Residually [641].

residuals [90].

Residue [444, 938, 1811, 2379, 2832].

residuosity [2630].

Resilience [1701, 2661].

resiliency [3028].

Resource [157].

Resident [264].

Residues [157].

Resistant [1342, 2942].

Resmini [1514].

Resolutions [593, 1069, 2241].

resolvability [1269].

Resolvable [86, 252, 258, 581, 711, 774, 775, 931, 1053, 1218, 1256, 2121, 2133, 2320, 2469, 2536, 2566, 2647, 2656, 2855, 3003].

Respect [715, 757, 834, 1220, 1743, 2617].

Restricted [628, 1368, 1434, 1925, 2355, 2780].

restrictions [1439, 2972].

Result [98, 610, 938, 993, 1190, 1220, 1343, 1410].

Results [60, 72, 331, 355, 558, 635, 748, 772, 1088, 1104, 1212, 1270, 1285, 1353, 1363, 1427, 1496, 1519, 1520, 1562, 1587, 1659, 1736, 1771, 1814, 1897, 1959, 2002, 2091, 2115, 2328, 2341, 2458, 2476, 2491, 2522, 2897, 3012].

Retracted [2920].

retransmission [1481].

retrieval [2197, 2456].

retrospective [1894].

Reusable [2308, 2666].

reveal [1757].

Reversible [2863].

Review [100, 481, 1122, 2857].

Revisited [187, 876, 965, 1491, 1498, 1627, 1701, 1752, 1950, 2132, 2471, 2508, 2725, 2886, 2975].

Revisiting [1696, 2048, 2586].

Revocable [2145, 2303, 2689, 2704].

Revocation [762, 1151].

rewinding [2136].

RFID [1142].

Richard [1469].

Rick [1470].

Rights [1085, 1647].

rigidity [97].

Rigorous [584].

Rijndael [2047, 2087].

Rijndael-160 [2047].

Rijndael-224 [2047].

Ring [319, 367, 442, 526, 566, 893, 999, 1048, 1112, 1401, 1488, 1489, 1747, 2226, 2257, 2323, 2560, 2669, 2752, 2851, 2918, 2919, 2980].

ring-like [2323].

ring-linear [1489].

Ring-Valued [566].

Rings [185, 236, 448, 514, 525, 543, 569, 654, 789, 874, 936, 954, 955, 974, 1001, 1003, 1103, 1131, 1238, 1265, 1375, 1381, 1495, 1507, 1541, 1601, 1617].
1676, 1678, 1688, 1699, 1738, 1794, 1855, 2085, 2291, 2296, 2317, 2379, 2480, 2520, 2526, 2568, 2636, 2650, 2691, 2732, 2828, 2921.
RIPEMD [2530]. RIPEMD-160 [2530].

Roos [2048]. Root [330, 999, 1022, 1124, 1383, 1670, 1820, 2182].
Roots [563, 608, 625, 686, 854, 1014, 2103].

Round-efficient [1413]. round-optimal [2752]. round-reduced [2094, 2248, 2530].
Ruud [2589].


SEEDs [1731, 1734]. Segre
Self-Complementary [90, 604, 934].
Self-conjugacy [347].
Self-embeddings [1816]. Self-Healing [691]. Self-Orthogonal [14, 204, 703, 833, 1112, 1552, 1717, 2141, 2561, 2675, 2791, 2837, 2918, 2919, 2980, 3011].
Self-Reciprocal [736, 858, 2270].
semi-primitive [2989]. Semi-Regula
sets
[6, 10, 23, 26, 27, 29, 85, 103, 139, 181, 345, 914, 960, 971, 983, 988, 1002, 1021, 1037, 1050, 1076, 1104, 1111, 1119, 1141, 1162, 1164, 1212, 1220, 1239, 1242, 1244, 1252, 1259, 1268, 1288, 1289, 1367, 1384, 1507, 1544, 1565, 1642, 1655, 1658, 1665, 1675, 1677, 1700, 1735, 1818, 1819, 1856, 1931, 1932, 1962, 1985, 2072, 2140, 2156, 2161, 2166, 2191, 2207, 2252, 2294, 2309, 2332, 2347, 2378, 2397, 2437, 2443, 2466, 2517, 2521, 2555, 2642, 2664, 2671, 2693, 2735, 2767, 2773, 2794, 2882, 2884, 2890, 2897, 2907, 2908, 2917, 2985, 3012, 3030]. Setting
[735, 2570, 2684, 2945]. seven
[2818]. Several
[732, 770, 1172, 2332, 2494, 2905, 2929, 2934, 2993, 3023]. Severely
[137]. SFLASH
[1728]. SHA
[1318]. SHA-1
[1318]. Shannon
[1487, 2110, 2228, 2417]. Shared
[328, 339, 1263, 2588, 2915]. Shares
[762]. Sharpening
[64]. Sharp
[1398, 2405, 2600]. Sharper
[2809]. sharply
[23]. sharpness
[1675]. Shen
[961]. Shift
[91, 131, 218, 682, 1287, 1581, 1740, 1810, 2041, 2070, 2085, 2092, 2509, 2511, 2619]. Shift-inequivalent
[2511]. shift-register
[1581]. Short
[608, 1235, 1299, 1399, 1465, 1767, 1864, 1901, 1942, 2011, 2516, 2552, 2563, 2646, 2973, 2988]. shortened
[1266, 1320, 1450, 1558]. Shorter
[1342, 1739, 2000, 2303]. shortest
[1883, 2085]. shot
[2194]. show
[1398]. Shrinking
[508]. shuffle
[2991]. side
[908, 1573]. side-channel
[1573]. Sidelnikov
[639, 843, 912, 1304, 1785, 2442, 2451, 2511]. Sides
[1085]. Sidon
[2891, 2943]. Sierpinski
[1562]. Sieve
[416]. Signal
[446, 2294]. Signature
[158, 359, 519, 563, 575, 619, 651, 660, 672, 735, 836, 945, 1134, 1200, 1223, 1293, 1920, 2009, 2057, 2160, 2260, 2433, 2489, 2516, 2609, 2667, 2712, 2845, 2915]. Signatures
[893, 1229, 1312, 1337, 1864, 1869, 1887, 1975, 2295, 2384, 2428, 2508, 2669, 2782, 2795, 2913, 2930, 2973, 2987]. Signcryption
[808, 1600, 1624]. Signed
[267, 272, 402, 940, 2497, 2739, 2985]. signed-digit
[2739]. Significance
[567]. significant
[1270]. SIMD
[1610]. SIMECK
[2713]. Simmon
[720]. SIMON
[2094, 2702]. Simple
[7, 207, 334, 491, 872, 1114, 1300, 1379, 1522, 1556, 1626, 1662, 1854, 1859, 2095, 2241, 2392, 2428, 2533, 2697, 2987]. Simplectic
[982]. Simplex
[266, 1488, 1793, 2592, 2624, 2962]. simplicial
[1679, 2293]. Singularity
[2898]. Simulation
[2383, 2765]. Simulation-based
[2383]. simulators
[2136]. Simultaneous
[1967, 2331]. Singer
[612, 695, 731, 862, 886, 1287, 1431]. Singh
[2249, 2388]. Single
[57, 88, 941, 1052, 2089, 2261, 2319, 2381, 2579, 2977]. single-deletion-correcting
[2579]. single-error
[941]. single-error-correcting
[88]. single-permutation
[2319]. Singleton
[2402, 2403]. Singly
[191, 209]. Singly-Even
[150, 209]. singular
[12, 1251, 1640, 2483]. Six
[460, 595, 1515, 1861, 2541]. six-weight
[1861]. sixty
[2776]. sixty-four
[2776]. Size
[60, 73, 121, 145, 150, 244, 254, 258, 287, 311, 366, 498, 573, 577, 587, 737, 743, 835, 931, 1045, 1061, 1158, 1198, 1204, 1227, 1233, 1253, 1278, 1297, 1300, 1313, 1364, 1380, 1423, 1455, 1606, 1658, 1759, 1762, 1859, 1936, 2027, 2098, 2463, 2477, 2484, 2551, 2866, 3018, 3026]. Sized
[572]. Sizes
[129, 240, 648, 786, 811, 941, 1023, 1218, 1256,

Theorem [9, 183, 207, 391, 393, 397, 486, 565, 751, 853, 1156, 1163, 1171, 1174, 1175, 1376, 1378, 1448, 1463, 1476, 1598, 1773, 2016, 2043, 2118, 2201, 2232, 2345, 2379, 2389, 2460, 2473, 2490, 2517, 2550, 2599, 2632, 2711, 2829, 2833, 2846, 2917, 2923, 2948, 2958, 2959, 2993].

Theorems [9, 183, 207, 391, 393, 397, 486, 565, 751, 853, 1156, 1163, 1171, 1174, 1175, 1376, 1378, 1448, 1463, 1476, 1598, 1773, 2016, 2043, 2118, 2201, 2232, 2345, 2379, 2389, 2460, 2473, 2490, 2517, 2550, 2599, 2632, 2711, 2829, 2833, 2846, 2917, 2923, 2948, 2958, 2959, 2993].

Theorem [1098].

Theorem [9, 183, 207, 391, 393, 397, 486, 565, 751, 853, 1156, 1163, 1171, 1174, 1175, 1376, 1378, 1448, 1463, 1476, 1598, 1773, 2016, 2043, 2118, 2201, 2232, 2345, 2379, 2389, 2460, 2473, 2490, 2517, 2550, 2599, 2632, 2711, 2829, 2833, 2846, 2917, 2923, 2948, 2958, 2959, 2993].

Theorem [9, 183, 207, 391, 393, 397, 486, 565, 751, 853, 1156, 1163, 1171, 1174, 1175, 1376, 1378, 1448, 1463, 1476, 1598, 1773, 2016, 2043, 2118, 2201, 2232, 2345, 2379, 2389, 2460, 2473, 2490, 2517, 2550, 2599, 2632, 2711, 2829, 2833, 2846, 2917, 2923, 2948, 2958, 2959, 2993].

Theorem [1098].

Theorem [1098].

Theorem [1098].
triple-cycle [2554]. triple-error-correcting [1659].

Triples [352, 592, 1445, 1473, 2205]. triply [182, 1450]. triply-shortened [1450].

Trivial [491, 2947]. Trivium [1393, 2341, 2634]. True [532, 799].


tweak [2936]. tweakable [1781, 2209, 2702, 2720, 2936]. Tweaking [2321]. twenty [1894]. twenty-year [1894].


two-to-one [1119, 2923]. Two-Transitive [489, 985]. Two-Weight [462, 916, 1048, 1946, 2242, 2573, 2705, 2969].

Twofold [2101]. Type [151, 307, 359, 370, 371, 375, 475, 502, 521, 541, 559, 587, 637, 656, 664, 671, 743, 789, 915, 995, 1037, 1109, 1162, 1229, 1288, 1327, 1331, 1354, 1374, 1396, 1401, 1419, 1423, 1431, 1456, 1466, 1494, 1542, 1543, 1594, 1650, 1671, 1759, 1778, 1835, 2182, 2213, 2266, 2280, 2289, 2421, 2435, 2439, 2591, 2660, 2699, 2841]. Type-1 [475].

types [1651, 2501].

Ubiquity [1683]. Unbalanced [1164, 1303].


uniformity [2263, 2394, 2559, 2616, 2629, 2673, 2737, 2808]. uniformly [1053, 1256]. unions [2356].

Unique [723, 1468, 1593, 1725, 2986].

Uniquely [386, 451, 3041]. Uniqueness [321, 634, 747, 977, 1117, 2115, 2413, 2435, 2441, 2776].

Unital [55, 228, 1027, 2851, 2918, 2919]. Unitals [242, 290, 313, 348, 399, 860, 1213, 1230, 1338, 1645, 2362, 2474, 2956].

Unitary [52, 242, 512, 1177, 1869, 2335, 2887].


unrestricted [812]. unsigncryption [1600]. Untransferability [190]. Untrusted [878].

Unweighted [2279]. updatable [1942].


Use [497, 763, 876, 902]. User [446, 735, 1932, 2321, 2966, 2570].

user-irrepressible [1932]. uses [2464].

[2574, 2687]. Wide-sense [2574].
Wiedemann [1081]. Wieferich [1187].
Williams [314]. Williamson [382, 769, 1035, 1374]. Wilson [1469, 1470].
window [950]. wire [2289]. wire-tap [2289]. wireless [933]. Wiretap [1718].
Moorhouse:1991:BNC
Tietavainen:1991:CRD
LaMacchia:1991:CDL
Lamken:1991:FPB
Ho:1991:SRO
[6] Chat Yin Ho. Some remarks on orders of projective planes, planar difference sets and multipliers. Designs, Codes,


DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).


REFERENCES

Cohen:1992:ECI


Stinson:1992:CCA


Blokhuis:1992:QSD


Hou:1992:SIA


Hamada:1992:CCM


Fellows:1992:SWP


Colbourn:1992:CMA


Shaw:1992:CP


Arasu:1992:EPC


Pott:1992:ADS

References

- **Landrock:1992:CCI**

- **Beth:1992:DMA**

- **Melone:1992:RTI**

- **Gao:1992:ONB**

- **Wan:1992:CCA**

- **Stinson:1992:ESS**

- **deCaen:1992:RIM**

- **Schmidt:1992:NQB**

- **Hare:1993:CBI**
  [56] Donovan R. Hare and William McCuaig. The connectivity of the block-intersection graphs of designs. *Designs, Codes, and Cryptography*, 3


[77] Josep Rifa-Coma. How to avoid the cheaters succeeding in the key sharing scheme. Designs, Codes, and
REFERENCES


O'Keefe:1993:SGD


Carlet:1993:AGD


Hamalainen:1993:BBM


Bitan:1993:LPN


Dougherty:1993:NTC


Geiselmann:1993:SDB


Klapper:1993:CCG


Davis:1993:NNS


Teirlinck:1994:SNR


Mitchell:1994:DPM

Conway:1994:QCB


Kennedy:1994:DFS


Dodunekov:1994:BSC


Johansson:1994:SRC


Jackson:1994:GSS


Dempwolff:1994:TPO


Dougherty:1994:CTS


Hachenberger:1994:CFE


Sabin:1994:RCC


Sali:1994:RSD


REFERENCES


Naccache:1995:CMP


Paterson:1995:PFB


Peeters:1995:RNG


Suchower:1995:NCS


Carpentieri:1995:PTS


Colbourn:1995:TTD

[127] Charles J. Colbourn, Jeffrey H. Dinitz, and Mieczyslaw Wojtas. Thwarts in
REFERENCES


Craigen:1995:SWM


Etzion:1995:BSC


Gopalakrishnan:1995:TCN


Munemasa:1995:PSC


OKeefe:1995:KDP


Trung:1995:CAS


Key:1995:ECS


Bours:1995:CPD


REFERENCES


[161] Xian-Mo Zhang and Yuliang Zheng. Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vec-

Gollmann:1996:RIR


Scheidler:1996:KER


Key:1996:CCS


Ashikhmin:1996:FDA


Berger:1996:AGA


Gulliver:1996:NGR


VanEupen:1996:NTC


REFERENCES


REFERENCES


[193] Heeralal Janwa and Oscar Moreno. McEliece public key cryptosystems us-


REFERENCES


Colbourn:1996:CDM


Kimura:1996:HMD


Monroe:1996:SOG


Pinelis:1996:MNE


Thas:1996:AHP


Trung:1996:GTD


Walker:1996:NAM

REFERENCES


REFERENCES


Gacs:1997:TRB


Hamada:1997:NSC


Hiss:1997:IMR


vanEupen:1997:CSO


vanZanten:1997:LOL


Jungnickel:1997:P


Bonisoli:1997:SMD


Bouzette:1997:TNP


Broecker:1997:CCS

[234] Claudia Broecker, Ralph-Hardo Schulz, and Gernot Stroth. Check character systems using Chevalley groups. Designs, Codes, and Cryptography, 10(2):
REFERENCES


Metsch:1997:ELS


Erdmann:1997:ADM


Abel:1997:EIT


Faldum:1997:CSD


Batten:1997:BSD


Houston:1997:LMD


Wan:1997:SSC


Buratti:1997:DF

[251] Marco Buratti. From a $(G,k,1)$ to a $(Ck \oplus G,k,1)$ difference family. Designs, Codes, and Cryptography, 11
REFERENCES


REFERENCES


[302] Tsonka Stefanova Baicheva. The covering radius of ternary cyclic codes
References


REFERENCES


He:1998:SSR


Langevin:1998:WAC


Paterson:1998:RCD


Stinson:1998:SNR


vanDijk:1998:USG


Siemon:1998:ENT


Betten:1998:SDS


DePrisco:1998:LBR


Chen:1998:WHL

[336] Wende Chen and Torleiv Kløve. Weight hierarchies of linear codes satisfying the chain condition. Designs, Codes,

Gehrmann:1998:MUS


Kurosawa:1998:NCB


Anderson:1998:HBR


Carlet:1998:CBF


Chen:1998:NCD


Chen:1998:EDF


Helleseth:1998:IFD


Kaikkonen:1998:CAP

Perera:1998:CGH

Cocyclic generalised Hadamard matrices and central relative difference
CREC. ISSN 0925-1022 (print), 1573-
wkap.nl/oasis.htm/181765.

Yang:1998:TNI

[346] Kyeongcheol Yang and Tor Helleseth.
Two new infinite families of 3-designs
from Kerdock codes over \( \mathbb{Z}_4 \).
Designs, Codes, and Cryptography, 15
(2):201–214, 1998. CODEN DC-
CREC. ISSN 0925-1022 (print), 1573-
wkap.nl/oasis.htm/181767.

Arasu:1998:ADS

Abelian difference sets without self-conjugacy. Designs,
Codes, and Cryptography, 15(3):
223–230, December 1998. CODEN DC-
CREC. ISSN 0925-1022 (print), 1573-
wkap.nl/oasis.htm/185600.

Ball:1998:PUR

[348] Simeon Ball.
Partial unitals and related
structures in Desarguesian planes. Designs,
Codes, and Cryptography, 15(3):
231–236, December 1998. CODEN DC-
CREC. ISSN 0925-1022 (print), 1573-
wkap.nl/oasis.htm/186357.

Bhandari:1998:LBC

On lower bounds for covering codes. Designs,
Codes, and Cryptography, 15(3):237–
243, December 1998. CODEN DC-
CREC. ISSN 0925-1022 (print), 1573-
wkap.nl/oasis.htm/185601.

Landjev:1998:NSO

[350] Ivan N. Landjev.
The nonexistence of some optimal ternary codes of
dimension five. Designs, Codes, and
Cryptography, 15(3):245–258, December
1998. CODEN DCCREC. ISSN
0925-1022 (print), 1573-7586 (elec-
tronic). URL http://www.wkap.nl/
oasis.htm/185603.

Ohmori:1998:CWM

[351] Hiroyuki Ohmori and Takashi Miyamoto.
Construction of weighing matrices
\((17,9)\) having the intersection number
8. Designs, Codes, and Cryptography,
0925-1022 (print), 1573-7586 (elec-
tronic). URL http://www.wkap.nl/
oasis.htm/185604.

Shalaby:1998:NOP

[352] Nabil Shalaby and Jianxing Yin.
Nested optimal \( \lambda \)-packings and \( \lambda \)-
coverings of pairs with triples. Designs,
Codes, and Cryptography, 15(3):
271–278, December 1998. CODEN DC-
CREC. ISSN 0925-1022 (print), 1573-
wkap.nl/oasis.htm/185607.

Stevens:1998:LBT

[353] Brett Stevens, Lucia Moura, and
Eric Mendelsohn.
Lower bounds for transversal covers. Designs,
Codes, and Cryptography, 15(3):
279–299, December 1998. CODEN DCCREC. ISSN
REFERENCES


[362] Keisuke Shiromoto. The weight enumerator of linear codes over GF($q^m$)

Barg:1999:BMD


Buratti:1999:SBC


Camion:1999:CIR


Edel:1999:LSC


Norton:1999:MRF


Phelps:1999:SEC


vanZanten:1999:CCC


Batten:1999:SST

Bonnecaze:1999:JPT


Chateauneuf:1999:CAS


Egner:1999:HP


Friedlander:1999:CBS


Gaborit:1999:CET


Martin:1999:DPA


Smeltzer:1999:PCD


Anonymous:1999:GE


Key:1999:EFA

Anonymous:1999:EA


Bruen:1999:LBL


Schmidt:1999:WMC


Chen:1999:FCE


Ward:1999:IDC


Charpin:1999:MDN


Cohen:1999:CLU


Thas:1999:EFG


Calkin:1999:MWD


REFERENCES


vanLint:1999:PTC


Szonyi:1999:EAM


Dinitz:2000:HCR


Vance:2000:GGC


Zhang:2000:RDD


Koblitz:2000:GE


Blake-Wilson:2000:ISM


Lenstra:2000:IF


Odlyzko:2000:DLP

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[475] Akos Seress. All lambda-designs with λ = 2^p are type-1. Designs, Codes, and Cryptography, 22(1):5–17, January 2001. CODEN DCCREC. ISSN
REFERENCES


[484] D. R. Stinson. Something about all or nothing (transforms). Designs, Codes, and Cryptography, 22(2):

Ward:2001:NCG


Tanabe:2001:NPA


Dizon-Garciano:2001:SSA


Maruta:2001:NAL


Johnson:2001:TTP


Dempwolff:2001:PRG


Sebille:2001:TES


Ahlswede:2001:PCR


Scheidler:2001:CQF

REFERENCES


[502] Blessilda P. Raposa. Some triple block intersection numbers of Paley 2-designs of QN-type. *Designs, Codes,
REFERENCES


REFERENCES


Cooperstein:2001:HSK


Edel:2001:LCS


Akiyama:2001:CSR


Krasikov:2001:DDB


Buratti:2001:PCD


Thas:2001:CTG


Koukouvinos:2001:VMI


Howgrave-Graham:2001:LAD

REFERENCES


[528] István Kovács. On the internal nuclei of sets in PG\((n, q)\), \(q\) is odd. Designs, Codes, and Cryptography, 24(1):


[554] Etsuko Bannai and Mitsuhiro Sawano. Symmetric designs attached to four-
REFERENCES


Brozovic:2002:CIM


Blackmore:2002:LBS


Arasu:2002:CCH


Ferret:2002:MLC


Georgiou:2002:ODT


Cabello:2002:SSS

REFERENCES


Abel:2002:BIB


Bilous:2002:EBS


Blake:2002:SDS


Blundo:2002:CBU


Buratti:2002:CDB


Cao:2002:KPD

REFERENCES

Charnes:2002:HBF


Chang:2002:GCD


Colbourn:2002:EKS


Ding:2002:SPG


deResmini:2002:AOA


Drmota:2002:RPW

REFERENCES


REFERENCES

Stevens:2002:PAP


Phelps:2002:PCR


Jha:2002:TFT


Tzeng:2002:NAV


Murphy:2002:KDB


Ostergaard:2002:DCS


Ashikhmin:2002:BCR

REFERENCES


REFERENCES

Govaerts:2003:PCM


Abatangelo:2003:DDT


Arasu:2003:NFC


Hou:2003:BRF


Law:2003:EPA


Konyagin:2003:LCD


Mavron:2003:QSD

[616] V. C. Mavron, T. P. McDonough, and M. S. Shrikhande. Quasi-symmetric

**Bouyuklieva:2003:ESD**


**Betsumiya:2003:ESD**


**Xu:2003:SDS**


**Nikova:2003:IDB**


**Guillermo:2003:PAU**


**Shin:2003:DGC**

[622] Dong-Joon Shin, P. Vijay Kumar, and Tor Helleseth. 3-designs from the $\mathbb{Z}_4$-Goethals codes via a new Kloosterman sum identity. *Designs, Codes, and
REFERENCES

121

Helleseth:2003:HDD


Masson:2003:DRS


Huber:2003:TRM


Ahlswede:2003:FVH


Blokhuis:2003:FG


Aguglia:2003:CSH


Ferret:2003:RMP


Gacs:2003:MPS


Gacs:2003:AT


Govaerts:2003:SNM


Kyureghyan:2003:LCS


Landjev:2003:OCF


Leemans:2003:RWP

[641] Dimitri Leemans. The residually weakly primitive geometries of

Luyckx:2003:SQE


vanMaldeghem:2003:SRS


Metsch:2003:CFH


Thas:2003:SGQ


Tonchev:2003:NMC


Ng:2003:RFS

REFERENCES


REFERENCES

Kharaghani:2003:CSB


Dalan:2003:NET


Sala:2003:UBD


Tanabe:2003:CDC


Kim:2003:DAC


Nguyen:2003:IEC

REFERENCES


[667] J. Barát, A. Del Fra, S. Innamorati, and L. Storme. Minimal blocking sets in $\text{PG}(2,8)$ and maximal partial...

Schaathun:2004:LBG


Glynn:2004:OGC


Golic:2004:CAA


Shin:2004:AMT


Biehl:2004:EUS


Trung:2004:CTC


REFERENCES


Klapper:2004:RSA


Brown:2004:SFO


Metsch:2004:SPS


Rinaldi:2004:KDP


Muller:2004:CSR


Avgustinovich:2004:CSP


Anonymous:2004:P

REFERENCES

[Anonymous:2004:LP]

[Blundo:2004:DSH]

[Brown:2004:AG]

[Chu:2004:CPC]

[Colbourn:2004:CFF]

[Cossidente:2004:RSC]
REFERENCES


ings of the Third Pythagorean Conference.


REFERENCES

Korchmaros:2004:HOF


Kucucukccifcci:2004:MCH


Labbate:2004:ACB


Laue:2004:RD


Ma:2004:BCF


Martirosyan:2004:CA


Mellinger:2004:LCT

REFERENCES


[721] Steven T. Dougherty and Keisuke Shiromoto. Maximum distance codes in $Mat_{n,s}(Z_k)$ with a non-Hamming metric and uniform distributions. *Designs, Codes, and Cryptography*, 33


REFERENCES


Yucas:2004:SRI


Maruta:2005:MSS


Marti-Farre:2005:SSS


Ozbudak:2005:EPO


Braun:2005:SCA


Harada:2005:SNG


Dey:2005:LCC


Ge:2005:GDD


Blokhuis:2005:P
REFERENCES


[754] Ákos Seress. Square-free non-Cayley numbers. on vertex-transitive non-Cayley graphs of square-free order. Designs, Codes, and Cryptography, 34(2–


[764] Olgica Milenkovic. Support weight enumerators and coset weight distributions of isodual codes. *Designs, Codes,
REFERENCES


Hess:2005:LCM

Brown:2005:GGC

Bialota:2005:MAG

Maruta:2005:ETL

Xia:2005:NMC

Carvalho:2005:GCW

Trung:2005:NCI

Ostergaard:2005:NRC

Lisonek:2005:FCC

Haanpaa:2005:NRD
[774] Harri Haanpää and Petteri Kaski. The near resolvable $2 - (13,4,3)$ designs and thirteen-player whist tournaments. Designs, Codes, and Cryptography, 35

Gennian:2005:RMP


Ionin:2005:RCN


Cimato:2005:OCT


Luyckx:2005:TSQ


Barwick:2005:GAR


Galati:2005:NES


Ciet:2005:ECC


Bracken:2005:CSD
REFERENCES


[790] Shenglin Zhou. Block primitive $2-(v,k,1)$ designs admitting a Ree group of characteristic two. Designs, Codes, and Cryptography, 36
REFERENCES


Leung:2005:FDM


Carlet:2005:CIF


Jha:2005:LSL


Gupta:2005:LCM


Brown:2005:HCC


Martin:2005:DED


Cheon:2005:NCA

[797] E. J. Cheon, T. Kato, and S. J. Kim. Nonexistence of $[n, 5, d_q]$ codes attaining the Griesmer bound for $q^4 - 2q^2 - 2q + 1 \leq d \leq q^4 - 2q^2 - q$. Designs, Codes, and Cryptography, 36(3):


REFERENCES


REFERENCES


Ahlswede:2005:FVH


Ang:2005:SWM


Belyavskaya:2005:CCSa


Safavi-naini:2005:MH


Phelps:2005:KKA


DeBruyn:2005:SNP

REFERENCES


**Yin:2005:CDP**


**Suetake:2005:CST**


**Spera:2005:AGC**


**Mcsorley:2005:DATb**


**Barwick:2005:OMT**


**Dorofeev:2005:MGR**


**Belyavskaya:2005:CCSb**
REFERENCES


Cheon:2005:MLS


Wispelaere:2005:CGH


Carlet:2005:PCB


Gulliver:2005:NEF


Matthews:2005:WSC


Ahmadi:2005:NTO


Bohli:2005:WKM


Lavrauw:2006:SPO


Heden:2006:FRP


Ball:2006:OPQ


Meidl:2006:SNL


deClerck:2006:DRR


Cauchie:2006:CCH


Scott:2006:GMM

REFERENCES


[854] San Ling, Harald Niederreiter, and Patrick Solé. On the algebraic structure of quasi-cyclic codes IV:

**Grolmusz:2006:COC**


**Wang:2006:NCO**


**Weng:2006:LMA**


**Ahmadi:2006:SRI**


**Arazi:2006:CCT**


**Dover:2006:SSH**


**Khatirinejad:2006:CCC**
REFERENCES


Cossidente:2006:AGP


Feng:2006:EZC


Garciano:2006:RDS


Dougherty:2006:CAI


DeWinter:2006:GQA


Masucci:2006:SMS


Shparlinski:2006:RMP
Dougherty:2006:CCE


Aly:2006:LCP


Giudici:2006:CCW


Chen:2006:SSD


Ciet:2006:TIM


Bini:2006:CRF


Guneri:2006:IGH

REFERENCES


REFERENCES

Maffre:2006:WKT


Homma:2006:TPCb


OBrien:2006:BCD


Aguglia:2006:BSC


Homma:2006:CDM


Grabner:2006:NOB


Dalai:2006:BTC


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[938] Chong-Dao Lee, Yaotsu Chang, and Trien-Kien Truong. A result on

Roelse:2007:DCP


Ebeid:2007:BSD


Litsyn:2007:ILB


Kim:2007:SWC


Chigira:2007:ESD


Cossidente:2007:VET

REFERENCES


[966] Aggelos Kiayias and Moti Yung. Cryptanalyzing the polynomial-reconstruction
REFERENCES


[973] Maria Bras-Amorós. Algebraic-geometry codes, one-point codes, and evaluation codes. Designs, Codes, and Cryptography, 43(2–3):
REFERENCES


REFERENCES


[iii98]


[iii99]


[iii100]


[iii101]


REFERENCES

175


[Carvalho:2007:CCT]


[Hana:2007:SC]


[Momihara:2007:NSC]


[Skachek:2008:PAF]


[1023] Boris Skorić, Stefan Katzenbeisser, and Mehmet U. Celik. Symmet-

Abatangelo:2008:ENM


Britz:2008:DSS


Keri:2008:CRE


Montinaro:2008:RU


Yin:2008:GBT


Cossidente:2008:GST


Potechin:2008:MC

REFERENCES


Donati:2008:ITS


Bierbrauer:2008:CB


Cuaresma:2008:HFJ


Ustaoglu:2008:OSE


Holzmann:2008:WMO


Kolokotronis:2008:CPN


Ji:2008:IQC


Blinco:2008:VSP


Blayer:2008:IVT


Thas:2008:NET


Ding:2008:P


Liu:2008:RGH


Xia:2008:UEP

REFERENCES


Hyun:2008:MDS

Prince:2008:FTP

Klein:2008:ARS

deVries:2008:ORC

Gong:2008:SIA

Dempwolff:2008:DSD

Geil:2008:SWG


REFERENCES


[1093] Danyo Danev and Stefan Dodunekov. A family of ternary quasi-perfect...
REFERENCES


Brinkmann:2008:CAF


Nojima:2008:SSM


Siqueira:2008:FTL


Fourquet:2008:ILD


Bey:2008:BFS


Garaschuk:2008:BKS


Homma:2009:SGH

[1100] Masaaki Homma and Seon Jeong Kim. The second generalized Ham-


[1107] Frédéric A. B. Edoukou. Codes defined by forms of degree 2 on non-degenerate Hermitian varieties in $\mathbb{P}^1(F_q)\mathbb{P}^1(F_q)$. *Designs, Codes, and Cryptography*, 50(1):135–146, January 2009. CODEN DCCREC.
REFERENCES


REFERENCES


REFERENCES


[1135] Iliya Bouyukliev, Veerle Fack, and Joost Winne. 2 – (31, 15, 7), 2 –

Cossidente:2009:SCH


Jungnickel:2009:PQS


Shaw:2009:CSV


Bamberg:2009:HNG


Collins:2009:UBP


Feng:2009:DSN


Lee:2009:ERA


[1149] José Joaquín Bernal, Ángel del Río, and Juan Jacobo Simón. An intrin-
REFERENCES

195

Burkhart:2009:FFE

Martin:2009:EBE

Marti-Farre:2009:ISS

Harn:2009:DIC

Colbourn:2009:LHF

Grassl:2009:CSD


REFERENCES

Cheon:2009:NET

Heuberger:2009:UDS

Dorbec:2009:WCL

Paterson:2009:RBN

Prince:2009:PPP

Tian:2009:LPB

Curtin:2009:SAS
Mishima:2009:OCA


Caranti:2009:AOS


Carlet:2009:FPS


Nuida:2009:IDT


Kim:2009:GGP


Moody:2009:DHP


Coulter:2009:SSD

REFERENCES

Roy:2009:UDC

Yang:2009:IAB

Owsiejczuk:2009:CGG

Alderson:2009:MLC

Heden:2009:NSC

Kavuluru:2009:CPB

Carvalho:2009:AAC


Bierbrauer:2010:NSP


Dokovic:2010:NYN


Abe:2010:EHE


Petelczyc:2010:TFS


Davydov:2010:LCC


Schillewaert:2010:MCR


Vandendriessche:2010:SLD


[1219] Ronald C. Mullin and Rainer Steinwandt. Special issue dedicated to


Colbourn:2010:CAC

Abreu:2010:AMP

Huber:2010:BTD

Singhi:2010:MLS

Baker:2010:EOB

Korchmaros:2010:IFL

Newman:2010:EFC

Buratti:2010:FPD
[1233] Marco Buratti and Anita Pasotti. Further progress on difference fam-

Hiramine:2010:MGH


Glebsky:2010:SCR


Fernandez-Cordoba:2010:LCR


OReilly-Regueiro:2010:RPF


Nevins:2010:NRB


Leung:2010:LCD


DeBeule:2010:GGA

[1240] Jan De Beule, Yves Edel, Emilia Käsper, Andreas Klein, Svetla Nikova,

Ball:2010:MAG


Lavrauw:2010:LSP


Cossidente:2010:STC


Marino:2010:OBS


Fanali:2010:SOP


Barreto:2010:WNC


Edel:2010:MCF

REFERENCES


Aguglia:2010:MBS


DeBruyn:2010:HPS


Yoshiara:2010:NAF


Edoukou:2010:SWC


Harrach:2010:SPS


Shum:2010:TAB


Fuelberth:2010:ISN

[1254] John Fuelberth, Athula Gunawardena, and C. David Shaffer. On


[1261] Shenglin Zhou and Huili Dong. Alternating groups and flag-transitive triplanes. Designs, Codes, and
REFERENCES


Blinovsky:2010:WDM


Zaverucha:2010:ASS


Fernandez-Cordoba:2010:MDG


Byrne:2010:NBC


Krotov:2010:BCP


Park:2010:MDH


Zhou:2010:OPD

Zhengchun Zhou and Xiaohu Tang. Optimal and perfect difference systems of sets from q-ary sequences with difference-balanced property. Designs, Codes, and Cryptography, 57(2):


REFERENCES


REFERENCES

Yun:2011:LMQ


Yun:2011:LMQ


OCathain:2011:CHM


Buratti:2011:NRO


Pawale:2011:QSD


Ghorpade:2011:PPS


Glynn:2011:IMS
Avanzi:2011:RAE


Betsuniya:2011:HMO


Glynn:2011:CAM


Park:2011:IPE


Li:2011:EEC


Yildiz:2011:CC


Poulakis:2011:EVD


See[1134]
REFERENCES


Sarkar:2011:TBC


Zhou:2011:ELC


Lee:2011:IHV


Zhang:2011:CRS


Parker:2011:E


Blondeau:2011:AED


Bogdanov:2011:UFN

[1303] Andrey Bogdanov. On unbalanced Feistel networks with contracting MDS diffusion. Designs,
REFERENCES


[1310] Richard G. Gibson and Jonathan Jedwab. Quaternary Golay se-

Harris:2011:CRK


Joye:2011:HDS


Klove:2011:LBS


Langevin:2011:CAB


Leander:2011:BDA


Lisonek:2011:ZKS


Maitra:2011:SOH

REFERENCES


REFERENCES

Tu:2011:CAB

Kim:2011:NRR

Chang:2011:PDG


Yutaka Hiramine. A family of non class-regular symmetric transversal designs of spread type. Designs, Codes, and Cryptography, 60(1):91–99, July 2011. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http:
REFERENCES


Menegatto:2011:EPD


Donovan:2011:DHP


Zhou:2011:GMG


Carrillo-Pacheco:2011:LGC

Lee:2011:DPA

Marino:2011:TCR

Bilal:2011:MDS

Batra:2011:SCC

Avanzi:2011:DCN

Prazmowska:2011:SPC

Plagne:2011:ACT

Liu:2011:FRS


Cheon:2011:NEG


Han:2011:BFS


Chee:2011:LDS


Marti-Farre:2011:OCS


Bierbrauer:2011:CSP


Cordero:2011:FDS
Koga:2011:GMC


Edemskiy:2011:ACL


Bracken:2011:EQA


Abel:2011:EGB


Kyureghyan:2011:ICP


Krotov:2011:WDP

[1366] Denis S. Krotov. On weight distributions of perfect colorings and completely regular codes. *Designs,
REFERENCES

Wang:2011:LSF  

Jesso:2011:HCR  

Lamberger:2012:MNC  

Fan:2012:ESD  

Guenda:2012:NMS  

Christopoulou:2012:GPC  

Bonvicini:2012:SPE  
Simona Bonvicini, Marco Buratti, Gloria Rinaldi, and Tommaso Traetta. Some progress on the existence of 1-rotational Steiner triple systems. *Designs, Codes, and Cryptography*, 62
REFERENCES


[1380] Xiande Zhang, Hui Zhang, and Gen-nian Ge. Optimal constant weight covering codes and nonuniform group divisible 3-designs with block size four. Designs, Codes, and Cryptography, 62


REFERENCES


Kim:2012:BES


Ostafe:2012:PVS


Mavron:2012:QSD


Wang:2012:EFC


Kiah:2012:NCC


Dougherty:2012:CCR


Csirmaz:2012:LSS


Zhi Hu, Patrick Longa, and Maozhi Xu. Implementing the 4-dimensional GLV method on GLS elliptic curves with $j$-invariant 0. *Designs, Codes, and Cryptography*, 63(3):331–343,
REFERENCES

Silvesan:2012:CBD


Huang:2012:TCO


Ballico:2012:SCC


Simone:2012:APT


Weng:2012:FRP


Panario:2012:DPF


Bonisoli:2012:PGC


REFERENCES


Marquardt:2012:PNG


Grosek:2012:QFA


Cao:2012:RSC


Fu:2012:CHN


Pun:2012:GPT


Heden:2012:ESS


Krotov:2012:BCP

Zhou:2012:CCE


Sajadieh:2012:CIM


Cossidente:2012:HHP


vanDam:2012:PGA


Ball:2012:SVF


Jungnickel:2012:HTC


Jurisic:2012:ECD

[1457] Aleksandar Jurisić and Janos Vidal. Extremal 1-codes in distance-


Bahattin Yildiz. A lemma on binomial coefficients and applications to Lee weights modulo $2^e$ of codes over $\mathbb{Z}_4$. Designs, Codes, and Cryptography, 65


Tom Høholdt and Heeralal Janwa. Eigenvalues and expansion of bipartite graphs. *Designs, Codes,

Hernando:2012:PCS


Hernando:2012:PCS

Katz:2012:TDM


Katz:2012:TDM

Dinitz:2012:CRP


Balachandran:2012:FCS


Singhi:2012:SDM


Baldi:2012:BAH


Augot:2013:E

REFERENCES


REFERENCES


[1496] Santanu Sarkar and Subhamoy Maitra.


REFERENCES


Yamada:2013:DSG


Cao:2013:CQC


Tang:2013:CBB


Leemans:2013:BCS


Bose:2013:KPS


Armknecht:2013:GHE

Wang:2013:FRE

Goldberg:2013:AOW

Hong:2013:SEF

Nagata:2013:MFS

Chen:2013:LCB

Ke:2013:LCA
<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
</table>
| [1533]    | L. Beukemann and K. Metsch. Small tight sets of hyperbolic quadrics. De-


[1541] Thomas Honold and Michael Kiermaier. The existence of maximal $(q^2,2)$-arcs in projective Hjelmslev...


REFERENCES


Munuera:2013:GHC

Hernando:2013:DSS

Lunardon:2013:RSS

Yankov:2013:NOS

Martinez-Moro:2013:ASM

Gravier:2013:NRV

Abel:2013:GSG


REFERENCES


[1579] Padmapani Seneviratne. Codes associated with circulant graphs and permutation decoding. *Designs, Codes,


REFERENCES

Feulner:2014:CNR


Borges:2014:NFC


Tomlinson:2014:NBC


Pinero:2014:SSH


Bernal:2014:ISA


Galindo:2014:ECD


Marquez-Corbella:2014:URV


Khan:2014:MNT


Zheng:2014:DMR


Bogdanov:2014:LHC


Ozbudak:2014:FNF


Lopez:2014:ACC


Bartoli:2014:FCD


Wu:2014:CRS

REFERENCES


REFERENCES


REFERENCES

Stokes:2014:LST

Stokes:2014:ELS

Ogata:2014:CDT


Bamberg:2014:ESI

Ghinelli:2014:RPD

Blokhuis:2014:KPG
REFERENCES


References


[1663] Megan Adams and Junhua Wu. 2-ranks of incidence matrices associated
REFERENCES


[1671] Hengjia Wei and Gennian Ge. Kirkman frames having hole type \(h^m\) for

Xiong:2014:WDC


Horiguchi:2014:SDE


Leung:2014:PCW


Landjev:2014:SBB


Cengellenmis:2014:CIF


Ding:2014:CAD


Liu:2014:KIS

REFERENCES


Cossidente:2014:NIF


Fang:2014:NSQ


Li:2014:NAS


Geil:2014:ESW


Budaghyan:2014:ESI


Ballet:2014:LWC

REFERENCES


Liang:2014:CFP


Ma:2014:NOC


Lin:2014:EPS


Feng:2014:DSF


Herranz:2014:NRA


Adhikari:2014:LAT


Momihara:2014:DDF


Chen:2014:SIB

278

REFERENCES


Raaphorst:2014:CSC


Gavrilyuk:2014:CLL


Yankov:2014:NBS


Bulygin:2014:FAP


Ballico:2014:NCC


Horiguchi:2014:ESD


Klove:2014:ELC

REFERENCES


[1761] Bocong Chen, Hongwei Liu, and Guanghui Zhang. A class of mini-

[Feng:2015:SCH]


[Albrecht:2015:CBA]


[Yang:2015:SDC]


[Dokovic:2015:CPC]


[Torezzan:2015:OCG]


[Lee:2015:AHS]


[Lavrauw:2015:EMD]

Michel Lavrauw, John Sheekey, and Corrado Zanella. On embeddings of minimum dimension of $\text{PG}(n,q) \times \text{PG}(n,q)$. Designs, Codes, and Cryptography, 74(2):427–440, February 2015. CODEN DCCREC. ISSN
REFERENCES


REFERENCES

Doliskani:2015:CDT

Yankov:2015:CSD

Chen:2015:PTS

Danielsen:2015:GCP

Li:2015:OAS

Minematsu:2015:BBS

Schmidt:2015:HNF

Karadeniz:2015:NEB
Matsui:2015:GMP


Su:2015:LCL


Csirmaz:2015:SSD


Lin:2015:CIB


Fazio:2015:HLP

Nelly Fazio, Kevin Iga, Antonio R. Nicolosi, Ludovic Perret, and William E. Skeith III. Hardness of learning prob-

Zieve:2015:PFP


Kovacevic:2015:PCD


Britz:2015:DMC


Shum:2015:OTD


Liu:2015:RCW


Ugolini:2015:SIP


Han:2015:NLB


Horak:2015:SDH

[1799] Peter Horak and Zsolt Tuza. Speeding up deciphering by hypergraph ordering. Designs, Codes, and Cryptography,
Yang:2015:OPK


Ma:2015:ASF


Cossidente:2015:NFR


Newman:2015:CD


Zheng:2015:WDF

REFERENCES


[1815] Yeow Meng Chee, Gennian Ge, Hui Zhang, and Xiande Zhang. Hanani triple packings and optimal $q$-ary


Simone:2015:FPP  

Gluesing-Luerssen:2015:FRP  

Langlois:2015:WCA  

Kotsireas:2015:FCA  

Villanueva:2015:ERB  

Duck:2015:HDL  

Hoholdt:2015:OCT  

Geil:2015:IFR  
REFERENCES

290


REFERENCES


REFERENCES


REFERENCES

Hong:2015:MLS


Qian:2015:EAQ


Winter:2015:LRS


Bao:2015:CDO


Sarkar:2015:PTA


Zeng:2015:SGC


Martinez:2015:EF


Blake:2015:GES

REFERENCES


REFERENCES


[1891] Jeffrey Hoffstein and Joseph H. Silverman. PASS-Encrypt: a pub-

Lamken:2015:AED


Zhang:2015:BVC


Koblitz:2015:ROM


McGuire:2015:FRN


Ng:2016:DDF


Niederreiter:2016:SSA


Pott:2016:APP


Moura:2016:FFC


Schmidt:2016:SSC


Fragouli:2016:SLN


Etzion:2016:GGC


Etzion:2016:GGC


Chen:2016:GCI


Cossidente:2016:SC


Wu:2016:SIP


Gauravaram:2016:BIC


Lavrauw:2016:BCF


Caullery:2016:EPP


Steinbach:2016:CQL

Carlet:2016:QZD


Anonymous:2016:WES


DeBeule:2016:NFT


Lo:2016:PUI


delaCruz:2016:AGE


Montanari:2016:ECM


Ji:2016:EOS


Miezaki:2016:UBV

[1937] Tsuyoshi Miezaki and Hiroyuki Nakasora. An upper bound of the value of \(t\) of the support \(t\)-designs of extremal binary doubly even self-dual codes. Designs, Codes, and Cryptography, 79(1):37–46, April 2016. CODEN DCCREC. ISSN 0925-1022 (print),


Byrne:2016:TWC


Compton:2016:UHM


Ozen:2016:GWB


Moody:2016:IIS


Albrecht:2016:PCR


Jiang:2016:SSC


Hiramine:2016:AGD


Alavi:2016:SDA

[1953] Seyed Hassan Alavi, Mohsen Bayat, and Ashraf Daneshkhah. Symmetric


REFERENCES


References

Cossidente:2016:NLM


Hui:2016:ESI


Cooper:2016:TH


Fancsali:2016:HPS


Chen:2016:NBM


Moreira:2016:ASA


Hofheinz:2016:TSS

Shparlinski:2016:SGB


Jedwab:2016:CCE


Krotov:2016:PCD


Guo:2016:GCS


Davydov:2016:CPS


Chen:2016:GCD


Dutta:2016:CAS

REFERENCES


[1989] Yarkin Doröz, Yin Hu, and Berk


REFERENCES


Nowak:2016:PGD


Ballico:2016:NSS


Li:2016:MMA


Lee:2016:CPT


Gong:2016:EDS


Alahmadi:2016:LZC

REFERENCES

Hachenberger:2016:AER

Guo:2016:EMM

Ku-Cauich:2016:ACB

Stones:2016:LSA

Yan:2016:TCC

Kendall:2016:GTD

Abiad:2016:SSG

Cheng:2016:PBS


Banin:2016:RSD


Mullan:2016:HHF


Guo:2016:SIK


Bamberg:2016:NIS


Braun:2016:NIS


Zhou:2016:LCT

Meidl:2016:MHJ

Liu:2016:FVF

Cheng:2016:BCS

Abel:2016:GHD

Wang:2016:NCD

Eid:2016:SIC


Carvalho:2016:NWH


Zhan:2016:FTN


Wan:2016:IBC


Kageyama:2016:GCO


Cossidente:2016:VSC

REFERENCES

Zhou:2016:TPC

Zheng:2016:LCP

Chen:2016:IAM

Kim:2016:CIS

Chaparin:2017:ESI

Boura:2017:RC

Ronjom:2017:IAA
[2041] Sondre Rønjom. Improving algebraic attacks on stream ciphers based on linear feedback shift register over \( F_{2^k} \). Designs, Codes, and Cryptography, 82(1–2):27–41, January 2017. CODEN DC-CREC. ISSN 0925-1022 (print),


Sarkar:2017:RNR


Bhattacharya:2017:SPB


Tibouchi:2017:IEC


Gupta:2017:TGC


Dyachkov:2017:CFC


Dyachkov:2017:SDL


Dyachkov:2017:ACF

[2054] Arkadii D’yachkov, Ilya Vorobyev, Nikita Polyanskii, and Vladislav Shchukin. Almost cover-free codes and designs. Designs, Codes, and
REFERENCES


Guneri:2017:HWB

Anbar:2017:IPQ

Gritsenko:2017:SCN

Maitin-Shepard:2017:OSI

Michel:2017:GCD

Jiang:2017:ASF
REFERENCES


Yang:2017:CWE

Huggan:2017:SLA

Li:2017:AGS

Peng:2017:CDR

Zheng:2017:DCL

Lu:2017:AIS
REFERENCES


[2080] Xiaotian Chen and Yue Zhou. Asynchronous channel hopping systems from difference sets. Designs, Codes, and Cryptography, 83(1):179–196, April 2017. CODEN DCCREC. ISSN 0925-1022 (print),


Hao:2017:TDB


vanTrung:2017:SDR


Zhang:2017:QMC


Erzurumluoglu:2017:TTS


Jin:2017:CBL

REFERENCES


REFERENCES


[2120] Sebastian M. Cioaba, Willem H. Haemers, and Jason R. Vermette. The graphs with all but two eigenvalues equal to $-2$ or 0. Designs, Codes, and Cryptography, 84(1–2):153–163, July


REFERENCES

DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).


REFERENCES

Steinke:2017:CFA


Isik:2017:CMC


Horak:2017:CPR


Chen:2017:SAK


Chen:2017:NSA


Yuan:2017:CQC


Otal:2017:CSC


Yoshiara:2017:EAP


Zhou:2017:COL

Tonchev:2017:LED


Zhou:2017:BCS


Kurosawa:2017:ALR


Chen:2017:NOO


Fan:2017:NFD


Dong:2017:CBS


Cuitino:2017:SPS


Alhakim:2017:SBS

REFERENCES

Kolomeec:2017:GMD


Zheng:2017:LSK


Chen:2017:SBS


Tzanakis:2017:CAM


Cossidente:2017:SRG


Li:2017:NTC


Hagiwara:2017:CCC


Egan:2017:ENG

REFERENCES


Jongkil Kim, Willy Susilo, Fuchun Guo, and Man Ho Au. Functional encryption for computational hiding in prime order groups via pair encodings.
References


REFERENCES


REFERENCES


Borges:2018:DCC

Feltz:2018:SSA

Han:2018:TCS

Drapal:2018:FAT

Barrolleta:2018:PPD

Jungnickel:2018:ESA

Bierbrauer:2018:FSO

Lee:2018:CTM
[2209] Jooyoung Lee, Atul Luykx, Bart Mennink, and Kazuhiko Minematsu. Connecting tweakable and multi-key block-


Fengwei Li and Qin Yue. The primitive idempotents and weight distributions of irreducible constacyclic codes.
Moreira:2018:CAS


Zhang:2018:CCP


Olmez:2018:LBC


Vega:2018:CDW


Ding:2018:NCM


Polak:2018:NNC


Sudha:2018:CPM


REFERENCES


[2239] Antonio Cossidente and Francesco Pavese. On intriguing sets of finite sym-


REFERENCES

346


REFERENCES


[2261] Sen-Peng Wang, Bin Hu, and Yan Liu. The autocorrelation properties of single cycle polynomial $T$-functions. De-


[2269] Konstantinos Limniotis and Nicholas Kolokotronis. Boolean functions with...

Fernando:2018:SRP


Shangguan:2018:NUB


Li:2018:COS


Liang:2018:FTP


Blanco-Chacon:2018:RMC


Yoshida:2018:ENI


Augot:2018:GGC

REFERENCES

Farran:2018:SFRa


Mesnager:2018:ACB


Bibak:2018:ULC


Zhang:2018:FTP


Rifa:2018:HFP


Sun:2018:ZCA


Koga:2018:CED

REFERENCES


Schmidt:2018:NIG


Otmani:2018:ICR


Xu:2018:SCM


Ravagnani:2018:DCS


delaCruz:2018:GCC


Johnsen:2018:FAA


Fan:2018:FTB


[2298] Chengju Li. Hermitian LCD codes from cyclic codes. *Designs, Codes,
REFERENCES


Carlet:2018:EHL


Mogilnykh:2018:EMW


Torres-Jimenez:2018:CAS


Zhang:2018:MCB


Antrobus:2018:LFP


Tan:2018:GIW


Cogliati:2018:ASP


Costa:2018:FDF


Egan:2019:PUG

[2335] Ronan Egan. Phased unitary Go-
lay pairs, Butson Hadamard matrices and a conjecture of Ito’s. De-
signs, Codes, and Cryptography, 87
DCCREC. ISSN 0925-1022 (print),
1573-7586 (electronic). URL https:
//link.springer.com/article/10.
1007/s10623-018-0485-2.

Mefenza:2019:PIG

[2336] Thierry Mefenza and Damien Vergnaud.
Polynomial interpolation of the gen-
eralized Diffie–Hellman and Naor–
Reingold functions. Designs, Codes,
and Cryptography, 87(1):75–85, Jan-
uary 2019. CODEN DCCREC.
ISSN 0925-1022 (print), 1573-7586
springer.com/article/10.1007/s10623-
018-0486-1.

Shi:2019:HMW

[2337] Minjia Shi, Hongwei Zhu, Patrick Solé,
and Gérard D. Cohen. How many
weights can a linear code have? De-
signs, Codes, and Cryptography, 87
(1):87–95, January 2019. CODEN
DCCREC. ISSN 0925-1022 (print),
1573-7586 (electronic). URL https:
//link.springer.com/article/10.
1007/s10623-018-0488-z.

Cheng:2019:IBF

[2338] Minquan Cheng, Jing Jiang, and
Qiang Wang. Improved bounds on 2-
frameproof codes with length 4. De-
signs, Codes, and Cryptography, 87
DCCREC. ISSN 0925-1022 (print),
1573-7586 (electronic). URL https:
//link.springer.com/article/10.
1007/s10623-018-0489-y.

Zhang:2019:COF

[2339] Tao Zhang and Gennian Ge. Con-
structions of optimal Ferrers diagram rank metric codes. Designs, Codes,
and Cryptography, 87(1):107–121, January
2019. CODEN DCCREC. ISSN 0925-

Soleimanian:2019:PVS

[2340] Azam Soleimanian and Shahram Khaz-
aei. Publicly verifiable searchable symmetric encryption based on efficient cryptographic components. Designs, Codes, and Cryptography, 87
(1):123–147, January 2019. CODEN
DCCREC. ISSN 0925-1022 (print),
1573-7586 (electronic). URL https:
//link.springer.com/article/10.
1007/s10623-018-0492-3.

Chen:2019:BBF

[2341] Shiyong Zhang and Gongliang Chen.
New results on the state cycles of Triv-
ium. Designs, Codes, and Cryptog-
CODEN DCCREC. ISSN 0925-1022
1007/s10623-018-0493-2.

Chen:2019:BBF

REFERENCES


[2350] Daniele Bartoli, Massimo Giulietti, and Maria Montanucci. Linear codes from Denniston maximal arcs. *Designs, Codes, and Cryptography*, 87
DeWinter:2019:MAE


Pinero:2019:WSC


Jungnickel:2019:CST


Rousseva:2019:LCC


Shparlinski:2019:CCR


Blokhuis:2019:RBS


DeBeule:2019:CC


Taniguchi:2019:VDH


Guo:2019:BBS

Farras:2019:LBO

Huang:2019:SBS

Derler:2019:KHS

Chang:2019:EFD

Bartoli:2019:MWC

Shi:2019:TCB

Ihringer:2019:CMM

Kapetanakis:2019:VPN


Fu:2019:RCP


Feng:2019:ODO


Meng:2019:SEL

REFERENCES


[2403] Xing Liu and Liang Zhou. Correction to: Improved Singleton bound on frequency hopping sequences and optimal constructions. Designs,
REFERENCES

Ducas:2019:PTB


Wang:2019:TSS


Shiromoto:2019:CRM


Cheraghchi:2019:NOR


Liu:2019:WPB


Hou:2019:OBC


Blokhuis:2019:CLS

REFE RENCES

1007/s10623-018-0583-1. See correction [2761].


Cossidente:2019:LCF


Liang:2019:FPA


Carvalho:2019:PRM


Wang:2019:TOB


Zhou:2019:CLR


Shi:2019:NDR


Shi:2019:CND

Bereg:2019:NLB


Vandendriessche:2019:KAN


Maxwell:2019:SSM


Shi:2019:DCP


Wang:2019:LAE


Aydin:2019:ECC


Bai:2019:TGW


[2439] Hadi Kharaghani and Sho Suda. Linked systems of symmetric group divisible designs of type II. Designs, Codes, and Cryptography, 87(10):2341–2360, October 2019. CODEN DCCREC. ISSN 0925-1022 (print),


REFERENCES


[2454] Yi Ouyang and Xianhong Xie. Linear complexity of generalized cyclotomic sequences of period $2p^m$. *Designs,
References

Mesnager:2019:FSM


Zhang:2019:GPI


Xu:2019:NTB


Garefalakis:2019:FRM


Michel:2019:PGD


Byrnes:2019:MLC


Yang:2019:PSA


Carlet:2019:SAO


vanTrung:2019:RCR

Tran van Trung. Recursive constructions for s-resolvable t-designs.
References


REFERENCES

Singh:2020:CGQ


Mesnager:2020:PBK


Bereg:2020:LBP


Duc:2020:NCE


Kolbl:2020:TTC


Pan:2020:OOO


Guenda:2020:LIP


Bereg:2020:CPA


Xu:2020:CEC


vandeKamp:2020:MAA


Mariot:2020:MOL


Ling:2020:CNS


DeBruyn:2020:FCA


Hyun:2020:RGE


REFERENCES


REFERENCES


[2528] Jing Jiang, Yujie Gu, and Minquan Cheng. Multimedia IPP codes with efficient tracing. *Designs, Codes, and Cryptography*, 88...


Shi:2020:NRS

Guillevic:2020:CPC

Sun:2020:PTM

Zhao:2020:GRK

Fang:2020:NMS

Lu:2020:SCA

Budaghyan:2020:PAF
Dong:2020:QAS


Zhao:2020:CIN


Chara:2020:BTC


Wu:2020:LCF


Datta:2020:RGH


Hodzic:2020:GFS


Potapov:2020:ABP


Ong:2020:EZD

Kai Lin Ong and Miin Huey Ang. On equivalency of zero-divisor codes.

Gu:2020:PIS


Yasuda:2020:ADR


Zhu:2020:RDJ


Wu:2020:CCT


Elsholtz:2020:CPF


Zheng:2020:CPF


Boyadzhyska:2020:EEM

[2557] Simona Boyadzhyska, Shagnik Das, and Tibor Szabó. Enumerating extensions of mutually orthogonal Latin

Lambin:2020:LEB


Mesnager:2020:BUQ


Kim:2020:CSD


Gao:2020:LCS


Liu:2020:PDC


Ekeraa:2020:PPQ

Alavi:2020:SB


Chee:2020:ABS


Xu:2020:DRS


Bibak:2020:DCC


Guneri:2020:LCP


Gong:2020:FCL


Lee:2020:TCS


Huang:2020:BPL

[2571] Xinmei Huang, Qin Yue, Yansheng Wu, Xiaoping Shi, and Jerod Michel. Binary...


Choi:2020:CSD


Kolsch:2020:IKB


Lavauzelle:2020:CSB


Chirvasițu:2020:AEQ


Randrianarisoa:2020:GAR


Shao:2020:OWA


Jia:2020:ITS

Grassi:2020:RGK


Ma:2020:SPC


Jiang:2020:LSS


Beelen:2020:FSI


Fadavi:2020:UEE


Britz:2020:WTD


Martínez-Penas:2020:HSC

REFERENCES

Galvez:2020:CSD


Couvreur:2020:PEL


Castellanos:2020:WSR


Bras-Amoros:2020:IDF


Christensen:2020:SEQ


Garcia-Marco:2020:HDA


Lopez:2020:MCC


Marquez-Corbella:2020:CSR

[2600] Irene Márquez-Corbella, Edgar Martínez-Moro, and Carlos Munuera. Computing sharp recovery structures for locally recoverable codes. Designs,
REFERENCES


REFERENCES

Dey:2020:PBS


Deneuville:2020:CCB


Salagean:2020:CBF


Egorova:2020:NBT


Matsumoto:2020:MRS


Matthews:2020:CLC


Rousseva:2020:GAE

REFERENCES


Meidl:2021:BBF


Wang:2021:IUB


Grezet:2021:CHL


Chakraborty:2021:FCM


Bamiloshin:2021:CIM


Oblaukhov:2021:MRR


Ballico:2021:SSC


[2651] Zhongxiao Wang, Qunxiong Zheng, Xiaoxin Zhao, and Xintao Feng. Grain-like structures with minimal and maximal period sequences. Designs, Codes, and Cryptography, 89


REFERENCES


[2666] Nan Cui, Shengli Liu, Dawu Gu, and Jian Weng. Robustly reusable fuzzy

**Shafieinejad:2021:SPQ**


**Ankur:2021:SDC**


**Feng:2021:TRS**


**Dong:2021:FTD**


**Guo:2021:CLS**


**Yan:2021:DSC**


**Zha:2021:SCP**


Polujan:2021:CCB


Lopez:2021:DEC


Shi:2021:BLC


Sajadieh:2021:CTM


Yang:2021:CLI


Zhang:2021:WMB


Abdukhalikov:2021:ECN


REFERENCES


REFERENCES


Heng:2021:FPT


Wang:2021:BLC


Chen:2021:CGP


Kharaghani:2021:BSO


Ghasemi:2021:IHS

REFERENCES


REFERENCES


REFERENCES


REFERENCES

Dougherty:2022:NGB


Fernandez:2022:SSP


Demirbas:2022:ICK


Dempwolff:2022:CCE


Geil:2022:PDA


Xu:2022:RCP

[2764] Xiaofang Xu, Xiangyong Zeng, and Shasha Zhang. Regular complete permutation polynomials over $\mathbb{F}_2^n$. Designs, Codes, and Cryptography, 90

Liu:2022:EQH


Wiese:2022:MCD


DeBeule:2022:CLK


Zhao:2022:TSC


Tan:2022:LCS


Lau:2022:DSL


Yuan:2022:SRH


Rajput:2022:LQC

[2772] Charul Rajput and Maheshanand Bhaintwal. On the locality of quasi-


REFERENCES


REFERENCES


[2802] Can Xiang, Chunming Tang, and Qi Liu. An infinite family of antiprimitive cyclic codes supporting

Kiermaier:2022:PAF


Dose:2022:HOE


Senel:2022:AGA


Bhattacharjee:2022:MCB


Kim:2022:PQB


Wen:2022:SBF


Wen:2022:SBF


Alhakim:2022:DPF


Ma:2022:CMS


Eyvazi:2022:LCG


Horsley:2022:BAP


Yan:2022:DSP


Cakiroglu:2022:NIP


Liu:2022:IKR


Zhou:2022:EES

[2824] Zhaocun Zhou, Dengguo Feng, and Bin Zhang. Efficient and extensive search for precise linear

Janusz:2022:CPP


Ji:2022:CCS


Huffman:2022:GEC


Gao:2022:WDD


Wu:2022:MZZ


Martinez:2022:SFS


Chakraborty:2022:VJP

REFERENCES


[2839] Vladimir D. Tonchev. On Pless symmetry codes, ternary QR codes,


REFERENCES


Ball:2022:ELC


vanTrung:2022:MCR


Crnkovic:2022:SD


Tonchev:2022:BRD


Bao:2022:LSD


Zhang:2022:CTG

Bereg:2022:UPR


Korban:2022:RGC


Wang:2022:LCM


Romanov:2022:NEQ


Bibak:2022:MSS


Cheon:2022:ACD


Mashahdi:2022:NIP

Kudin:2022:CCM


Azimi:2022:BVD


Wang:2022:GOC


Abreu:2022:SRC


Boudgoust:2022:VMR


Sui:2022:MNM


Ball:2022:CAB

DeBruyn:2022:CCC


Haemers:2022:SSC


Janzer:2022:CLH


Abiad:2022:NGF


Lavrauw:2022:CIN


Bailey:2022:DGA


Longobardi:2022:SST


Blokhuis:2022:SBE


Denaux:2022:CSS


Kantor:2022:ASD


Betten:2022:EPC


Tan:2022:AUD


Amarra:2022:DDP


Blokhuis:2022:ECL


Kolsch:2023:ISP

[2891] He Zhang and Chunming Tang. Constructions of large cyclic constant dimension codes via Sidon spaces. Designs, Codes, and Cryptography, 91
REFERENCES

Kharaghani:2023:COC


Khaefi:2023:SPC


Gadouleau:2023:BFP


Tan:2023:MLL


Aguirre:2023:APN


Wang:2023:NRV


Carlet:2023:SCB

Venema:2023:SCP

Li:2023:PCC

Caruso:2023:DLR

Shi:2023:ACD

Jiang:2023:RBS

Lavorante:2023:NHH

Xie:2023:SCB

Armario:2023:BFP
REFERENCES


Shen:2023:NCZ


Zhang:2023:DFA


Katsumata:2023:DCB


Beierle:2023:GFS


Byrne:2023:CNM


Hong:2023:IGB


Bidoux:2023:CBS

REFERENCES


Anbar:2023:GSS


Feneuil:2023:SPS


Doulgerakis:2023:IVL


Kiernmaier:2023:SWR


Shi:2023:SOC


Shi:2023:CSO


Shi:2023:RAM

REFERENCES

Liu:2023:LGC


Shen:2023:FTD


Mesnager:2023:FPB


Datta:2023:CSP


Akre:2023:GCC


Correll:2023:DBS


Araya:2023:HMR


Meng:2023:WDQ

[2928] Xiangrui Meng, Jian Gao, Fang-Wei Fu, and Fanghui Ma. Weight distributions of Q2DC codes over finite fields.
REFERENCES


Montanucci:2023:GWS


Kim:2023:PDG


DeBoeck:2023:EAP


Tong:2023:ETS


Na:2023:GBS


Guo:2023:SSM


Bouvier:2023:ADI


Li:2023:CCD


Fang:2023:PLO


Huang:2023:RSO


Xu:2023:CCP


Gill:2023:PMO


Satake:2023:CSG


Mo:2023:IHS


Mora:2023:DSS

Zeng:2023:CSC


Shi:2023:SDB


Sun:2023:ISP


Lavorante:2023:EPC


Elsholtz:2023:LSM


Iurlano:2023:GPS


Xu:2023:OQR

[2958] Li Xu, Zhengchun Zhou, Jun Zhang, and Sihem Mesnager. Optimal quaternary $(r, \delta)$-locally recoverable codes: their structures and complete classi-
REFERENCES

442

Hollmann:2023:SBC


Sun:2023:OQH


Su:2023:FSC


Ducoat:2023:RWH


Attrapadung:2023:MCP


REFERENCES


Datta:2023:SAB


Li:2023:CCL


Wang:2023:DNC


Durante:2023:DVS


Han:2023:CMP


Lavrauw:2023:SDS


Gyarmati:2023:SSR


Lemos:2023:APF


Feng:2023:FGQ


Pasalic:2023:EIF


Wang:2023:TFN


Ding:2023:FTC


Stanojkovski:2023:SCS


Shparlinski:2023:FPS


Delgado:2023:SNT

[3002] Moises Delgado, Heeralal Janwa, and Carlos Agrinsoni. Some new techniques and progress towards the resolution of the conjecture of exceptional APN functions and absolutely

vanTrung:2023:PME


Bannai:2023:NAM


Kobayashi:2023:TLB


Li:2023:IMC


Pavone:2023:SSB


Chen:2023:CNO


Lu:2023:GCR


REFERENCES


[3025] S. P. Glasby, Ferdinand Ihringer, and Sam Matthews. The proportion of


[3032] Daniele Bartoli, Giuliana Fatabbi, and Francesco Ghiandoni. On the ex-


[3040] Livia Betti, Jim Brown, Fernando Gaitan, Aiyana Spear, and Japheth Varlack. Lattices in real quadratic fields