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/

03 June 2022
Version 1.11

Title word cross-reference

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 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. Permuta-

tion 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 autocorrela-

tion, 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 non-commutative 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.

Hasan: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 $\mathbf{Z_{pe}}$. *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 cotrace. *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 asymptoti-

cally 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 (electronic). 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, Novem-

ber 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 (electronic). 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 Com-*

munications, 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. Characteris-

tic 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 Pavlu. 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**Q**SRs, and pseudo-ultrametric continued fractions in **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`.