Publication List of Tor Helleseth

1 Edited Books, Proceedings and Journal Special Issues (22)

SEquences and Their Applications (SETA)

[1] T. Helleseth and J. Jedwab, Eds., *Sequences and Their Applications - SETA 2012*, vol. 7280, ser. Lecture Notes in Computer Science, Cover, Front Matter, Link, Berlin: Springer-Verlag, 2012.

[2] G. Gong, T. Helleseth, H.-Y. Song, and K. Yang, Eds., *Sequences and Their Applications - SETA 2006*, vol. 4086, ser. Lecture Notes in Computer Science, Cover, Front Matter, Link, Berlin: Springer-Verlag, 2006.

[3] T. Helleseth, D. Sarwate, H.-Y. Song, and K. Yang, Eds., *Sequences and Their Applications - SETA 2004*, vol. 3486, ser. Lecture Notes in Computer Science, Cover, Front Matter, Link, Berlin: Springer-Verlag, 2005.

[4] T. Helleseth, P. V. Kumar, and K. Yang, Eds., *Sequences and Their Applications - SETA '01*, ser. Discrete Mathematics and Theoretical Computer Science, Cover, Berlin: Springer-Verlag, 2002.

[5] C. Ding, T. Helleseth, and H. Niederreiter, Eds., *Sequences and Their Applications*, ser. Discrete Mathematics and Theoretical Computer Science, Cover, Berlin: Springer-Verlag, 1999.

Cryptography and Coding Theory

[1] L. Budaghyan, C. Carlet, and T. Helleseth, "Editorial: Special issue on boolean functions and their applications," *Cryptography and communications*, vol. 11, no. 1, pp. 1–2, 2019, PDF.

[2] T. Helleseth and B. Preneel, "Editorial: Special issue on recent trends in cryptography," *Cryptography and Communications*, vol. 10, no. 1, pp. 1–3, 2018, PDF.

[3] T. Helleseth and B. Preneel, Eds., *Editorial: Special issue on Recent Trends in Cryptography, Cryptography and Communications*, vol. 10, 1, 2018, PDF.

[4] L. Budaghyan, T. Helleseth, and M. Parker, Eds., *Special issue of Designs, Codes and Cryptography: Coding and Cryptography*, vol. 73, 2, Nov. 2014, Editorial.

[5] O. Grošek, T. Helleseth, A. Kholosha, and K. Nemoga, Eds., *Nilcrypt '10*, vol. 45, ser. Tatra Mountains Mathematical Publications, Bratislava: Mathematical Institute, Slovak Academy of Sciences, 2010.

[6] C. Ding, T. Helleseth, and Ø. Ytrehus, Eds., *Special issue of Designs, Codes and Cryptography dedicated to Professor Torleiv Kløve for his 65th birthday*, vol. 48, 2, Aug. 2008, Preface.

[7] T. Helleseth, Ed., *Advances in Cryptology - EUROCRYPT '93*, vol. 765, ser. Lecture Notes in Computer Science, Front Matter, Link, Berlin: Springer-Verlag, 1994.

Sequenece and Discrete Mathematics

[1] L. Budaghyan, T. Helleseth, and A. Kholosha, Eds., *Editorial: Special issue on Boolean Functions and their Applications*, vol. 8, 2, 2016, PDF.

[2] T. Helleseth and J. Jedwab, Eds., *Special issue of Cryptography and Communications: Sequences and Their Applications*, vol. 6, 1, Mar. 2014, Editorial.

[3] M. A. Hasan and T. Helleseth, Eds., *Arithmetic of finite fields*, vol. 6087, ser. Lecture Notes in Computer Science, Cover, Front Matter, Link, Berlin: Springer-Verlag, 2010.

[4] S. Golomb, G. Gong, T. Helleseth, and H.-Y. Song, Eds., *Sequences, Subsequences, and Consequences*, vol. 4893, ser. Lecture Notes in Computer Science, Cover, Front Matter, Link, Berlin: Springer-Verlag, 2007.

[5] T. Helleseth, P. V. Kumar, and Ø. Ytrehus, Eds., *Proceedings of the 2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks*, Cover, Front Matter, IEEE, Jul. 2007.

[6] J.-S. No, H.-Y. Song, T. Helleseth, and P. V. Kumar, Eds., *Mathematical properties of sequences and other combinatorial structures*, ser. The Kluwer International Series in Engineering and Computer Science. Dordrecht: Kluwer Academic Publishers, 2003, Cover.

[7] A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, Eds., *Difference Sets, Sequences and their Correlation Properties*, ser. NATO Science Series, Series C: Mathematical and Physical Sciences. Dordrecht: Kluwer Academic Publishers, 1999, vol. 542, Cover.

Master and PhD Thesis

[1] T. Helleseth, *Krysskorrelasjonsfunksjonen mellom maksimale sekvenser over $GF(q)$. Hovedoppgave i ren matematikk*, Universitetet i Bergen, Matematisk Institutt, Våren 1971.

[2] ——, "Weight distribution problems in codes," Consists of Introduction and [21], [18], [103], [20], [19], [17], [101], [100], [102], PhD thesis, Department of Pure Mathematics, University of Bergen, Bergen, Norway, 1979.

2 Chapters in Books (31)

Encyclopedia of Cryptography and Security

[1] T. Helleseth, "Autocorrelation," in *Encyclopedia of Cryptography and Security, 2nd ed.* 2011, p. 68. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5_334.

[2] ——, "Cross-correlation," in *Encyclopedia of Cryptography and Security, 2nd ed.* 2011, p. 277. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5_341.

[3] ——, "De bruijn sequence," in *Encyclopedia of Cryptography and Security, 2nd ed.* 2011, pp. 315–316. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5_344.

[4] ——, "Gap," in *Encyclopedia of Cryptography and Security, 2nd ed.* 2011, pp. 508–509. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5_350.

[5] ——, "Golomb's randomness postulates," in *Encyclopedia of Cryptography and Security, 2nd ed.* 2011, pp. 516–517. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5_351.

[6] ——, "Maximal-length sequences," in *Encyclopedia of Cryptography and Security, 2nd ed.* 2011, pp. 763–766. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5_359.

[7] ——, "Pseudo-noise sequences (pn-sequences)," in *Encyclopedia of Cryptography and Security, 2nd ed.* 2011, p. 992. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5_364.

[8] ——, "Run," in *Encyclopedia of Cryptography and Security, 2nd ed.* 2011, pp. 1072–1073. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5_367.

[9] ——, "Sequences," in *Encyclopedia of Cryptography and Security, 2nd ed.* 2011, pp. 1185–1188. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5_372.

[10] ——, "Cross correlation," in *Encyclopedia of Cryptography and Security*, H. C. van Tilborg, Ed., Berlin: Springer-Verlag, 2005, pp. 113–113.

[11] ——, "De Bruijn sequence," in *Encyclopedia of Cryptography and Security*, H. C. van Tilborg, Ed., Berlin: Springer-Verlag, 2005, pp. 138–140.

[12] ——, "Gap," in *Encyclopedia of Cryptography and Security*, H. C. van Tilborg, Ed., Berlin: Springer-Verlag, 2005, pp. 239–239.

[13] ——, "Golomb's randomness postulates," in *Encyclopedia of Cryptography and Security*, H. C. van Tilborg, Ed., Berlin: Springer-Verlag, 2005, pp. 242–242.

[14] ——, "Maximal-length linear sequence," in *Encyclopedia of Cryptography and Security*, H. C. van Tilborg, Ed., Berlin: Springer-Verlag, 2005, pp. 372–375.

[15] ——, "Pseudo-noise sequence (PN-sequence)," in *Encyclopedia of Cryptography and Security*, H. C. van Tilborg, Ed., Berlin: Springer-Verlag, 2005, pp. 483–483.

[16] ——, "Run," in *Encyclopedia of Cryptography and Security*, H. C. van Tilborg, Ed., Berlin: Springer-Verlag, 2005, pp. 539–539.

[17] ——, "Sequences," in *Encyclopedia of Cryptography and Security*, H. C. van Tilborg, Ed., Berlin: Springer-Verlag, 2005, pp. 560–563.

Coding Theory

[1] T. Helleseth and T. Kløve, "Algebraic coding theory," in *Wiley encyclopedia of computer science and engineering*, J. G. Webster, Ed., vol. 1, Chichester: John Wiley & Sons, Inc., 2009, pp. 80–94.

[2] P. Charpin and T. Helleseth, Eds., *Special issue of designs, codes and cryptography: Coding and cryptography. in memory of hans dobbertin*, vol. 49, 1-3, Dec. 2008, Editorial.

[3] T. Helleseth and T. Klve, "Algebraic coding theory," in *Wiley encyclopedia of computer science and engineering*, 2008. DOI: 10.1002/9780470050118.ecse011. [Online]. Available: https://doi.org/10.1002/9780470050118.ecse011.

[4] T. Helleseth, "Optical orthogonal codes," in *Handbook of combinatorial designs*, ser. Discrete Mathematics and its Applications, C. J. Colbourn and J. H. Dinitz, Eds., Second, .V, London: Chapman & Hall/CRC, 2007, ch. 9, pp. 321–322.

[5] T. Helleseth and T. Kløve, "Algebraic coding theory," in *Wiley encyclopedia of electrical and electronics engineering*, J. G. Webster, Ed., vol. 1, PDF, Chichester: John Wiley & Sons, Inc., 1999, pp. 402–415.

[6] T. Helleseth and P. V. Kumar, "Sequences with Low Correlation," in *Handbook in coding theory*, V. S. Pless and W. C. Huffman, Eds., vol. II.3, PDF, Amsterdam: Elsevier Science B.V., 1998, ch. 21, pp. 1765–1853.

Sequence Design for Communication

[1] G. Garg, T. Helleseth, and P. V. Kumar, "Recent advances in low-correlation sequences," in *New directions in wireless communications research*, V. Tarokh, Ed., PDF, Berlin: Springer-Verlag, 2009, ch. 3, pp. 63–92.

[2] T. Helleseth, "Sequence correlation," in *Handbook of combinatorial designs*, ser. Discrete Mathematics and its Applications, C. J. Colbourn and J. H. Dinitz, Eds., Second, .V, London: Chapman & Hall/CRC, 2007, ch. 7, pp. 313–317.

[3] T. Helleseth and P. V. Kumar, "Pseudonoise sequences," in *The communications handbook*, J. D. Gibson, Ed., Second, PDF, London: CRC Press, 2002, ch. 8, pp. 8-1–8-12.

[4] ——, "Pseudonoise sequences," in *The mobile communications handbook*, ser. The electrical engineering handbook series, J. D. Gibson, Ed., Second, London: CRC Press, 1999, ch. 8.

Discrete Mathematics and Finite Fields

[1] T. Helleseth, "Open problems on the cross-correlation of m-sequences," in *Open problems in mathematics and computational science*, 2014, pp. 163–179. DOI: 10.1007/978-3-319-10683-0_8. [Online]. Available: https://doi.org/10.1007/978-3-319-10683-0_8.

[2] ——, "Correlation and autocorrelation of sequences," in *Handbook of finite fields*, G. L. Mullen and D. Panario, Eds., ser. Discrete Mathematics and its Applications, London: CRC Press, 2013, ch. 10.3, pp. 317–324.

[3] T. Helleseth and A. Kholosha, "Bent functions and their connections to combinatorics," in *Surveys in combinatorics 2013*, S. R. Blackburn, S. Gerke, and M. Wildon, Eds., ser. London Mathematical Society Lecture Note Series, vol. 409, New York: Cambridge University Press, 2013, pp. 91–126.

[4] ——, "Bent functions and their connections to combinatorics," in *Surveys in combinatorics 2013*, 2013, pp. 91–126. DOI: 10.1017/CBO9781139506748.004. [Online]. Available: https://doi.org/10.1017/CBO9781139506748.004.

3 Journal Papers (230)

IEEE Transactions on Information Theory (103)

[1] L. Budaghyan, C. Carlet, T. Helleseth, N. Li, and B. Sun, "On upper bounds for algebraic degrees of APN functions," *IEEE Trans. Information Theory*, vol. 64, no. 6, pp. 4399–4411, 2018, PDF.

[2] G. Gong, T. Helleseth, and P. V. Kumar, "Solomon w. golomb - mathematician, engineer, and pioneer," *IEEE Trans. Information Theory*, vol. 64, no. 4, pp. 2844–2857, 2018, PDF.

[3] Z. Zhou, T. Helleseth, and U. Parampalli, "A family of polyphase sequences with asymptotically optimal correlation," *IEEE Trans. Information Theory*, vol. 64, no. 4, pp. 2896–2900, 2018, PDF.

[4] Z. Zhou, D. Zhang, T. Helleseth, and J. Wen, "A construction of multiple optimal ZCZ sequence sets with good cross correlation," *IEEE Trans. Information Theory*, vol. 64, no. 2, pp. 1340–1346, 2018, PDF.

[5] Z. Sun, X. Zeng, C. Li, and T. Helleseth, "Investigations on periodic sequences with maximum nonlinear complexity," *IEEE Trans. Information Theory*, vol. 63, no. 10, pp. 6188–6198, 2017, PDF.

[6] C. Tang, Z. Zhou, Y. Qi, X. Zhang, C. Fan, and T. Helleseth, "Generic construction of bent functions and bent idempotents with any possible algebraic degrees," *IEEE Trans. Information Theory*, vol. 63, no. 10, pp. 6149–6157, 2017, PDF.

[7] Y. Xia, N. Li, X. Zeng, and T. Helleseth, "On the correlation distribution for a niho decimation," *IEEE Trans. Information Theory*, vol. 63, no. 11, pp. 7206–7218, 2017, PDF.

[8] L. Budaghyan, A. Kholosha, C. Carlet, and T. Helleseth, "Univariate niho bent functions from o-polynomials," *IEEE Trans. Information Theory*, vol. 62, no. 4, pp. 2254–2265, 2016, PDF.

[9] C. Li, X. Zeng, C. Li, T. Helleseth, and M. Li, "Construction of de bruijn sequences from lfsrs with reducible characteristic polynomials," *IEEE Trans. Information Theory*, vol. 62, no. 1, pp. 610–624, 2016, PDF.

[10] C. Tang, N. Li, Y. Qi, Z. Zhou, and T. Helleseth, "Linear codes with two or three weights from weakly regular bent functions," *IEEE Trans. Information Theory*, vol. 62, no. 3, pp. 1166–1176, 2016, PDF.

[11] Y. Xia, N. Li, X. Zeng, and T. Helleseth, "An open problem on the distribution of a Niho-type cross-correlation function," *IEEE Trans. Information Theory*, vol. 62, no. 12, pp. 7546–7554, 2016, PDF.

[12] S. Hong, H. Park, J.-S. No, T. Helleseth, and Y.-S. Kim, "Near-optimal partial Hadamard codebook construction using binary sequences obtained from quadratic residue mapping," *IEEE Trans. Information Theory*, vol. 60, no. 6, pp. 3698–3705, Jun. 2014, PDF.

[13] H. Hu, S. Shao, G. Gong, and T. Helleseth, "The proof of Lin's conjecture via the decimation-Hadamard transform," *IEEE Trans. Information Theory*, vol. 60, no. 8, pp. 5054–5064, Aug. 2014, PDF.

[14] C. Li, X. Zeng, T. Helleseth, C. Li, and L. Hu, "The properties of a class of linear FSRs and their applications to the construction of nonlinear FSRs," *IEEE Trans. Information Theory*, vol. 60, no. 5, pp. 3052–3061, May 2014, PDF.

[15] C. Li, X. Zeng, C. Li, and T. Helleseth, "A class of de Bruijn sequences," *IEEE Trans. Information Theory*, vol. 60, no. 12, pp. 7955–7969, Dec. 2014, PDF.

[16] C. Li, N. Li, T. Helleseth, and C. Ding, "The weight distributions of several classes of cyclic codes from APN monomials," *IEEE Trans. Information Theory*, vol. 60, no. 8, pp. 4710–4721, Aug. 2014, PDF.

[17] N. Li, X. Tang, and T. Helleseth, "New constructions of quadratic bent functions in polynomial form," *IEEE Trans. Information Theory*, vol. 60, no. 9, pp. 5760–5767, Sep. 2014, PDF.

[18] Y. Xia, C. Li, X. Zeng, and T. Helleseth, "Some results on cross-correlation distribution between a p-ary m-sequence and its decimated sequences," *IEEE Trans. Information Theory*, vol. 60, no. 11, pp. 7368–7381, Nov. 2014, PDF.

[19] H. Cai, X. Zeng, T. Helleseth, X. Tang, and Y. Yang, "A new construction of zero-difference balanced functions and its applications," *IEEE Trans. Information Theory*, vol. 59, no. 8, pp. 5008–5015, Aug. 2013, PDF.

[20] C. Ding and T. Helleseth, "Optimal ternary cyclic codes from monomials," *IEEE Trans. Information Theory*, vol. 59, no. 9, pp. 5898–5904, Sep. 2013, PDF.

[21] N. Li, T. Helleseth, A. Kholosha, and X. Tang, "On the Walsh transform of a class of functions from Niho exponents," *IEEE Trans. Information Theory*, vol. 59, no. 7, pp. 4662–4667, Jul. 2013, PDF.

[22] N. Li, T. Helleseth, X. Tang, and A. Kholosha, "Several new classes of bent functions from Dillon exponents," *IEEE Trans. Information Theory*, vol. 59, no. 3, pp. 1818–1831, Mar. 2013, PDF.

[23] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, "Further results on Niho bent functions," *IEEE Trans. Information Theory*, vol. 58, no. 11, pp. 6979–6985, Nov. 2012, PDF.

[24] G. Gong, T. Helleseth, and H. Hu, "A three-valued Walsh transform from decimations of Helleseth-Gong sequences," *IEEE Trans. Information Theory*, vol. 58, no. 2, pp. 1158–1162, Feb. 2012, PDF.

[25] G. Gong, T. Helleseth, H. Hu, and A. Kholosha, "On the dual of certain ternary weakly regular bent functions," *IEEE Trans. Information Theory*, vol. 58, no. 4, pp. 2237–2243, Apr. 2012, PDF.

[26] W. Jia, X. Zeng, T. Helleseth, and C. Li, "A class of binomial bent functions over the finite fields of odd characteristic," *IEEE Trans. Information Theory*, vol. 58, no. 9, pp. 6054–6063, Sep. 2012, PDF.

[27] G. Gong, S. Rønjom, T. Helleseth, and H. Hu, "Fast discrete Fourier spectra attacks on stream ciphers," *IEEE Trans. Information Theory*, vol. 57, no. 8, pp. 5555–5565, Aug. 2011, PDF.

[28] N. Li, X. Tang, and T. Helleseth, "Several classes of codes and sequences derived from a $\mathbb{Z}_4$- valued quadratic form," *IEEE Trans. Information Theory*, vol. 57, no. 11, pp. 7618–7628, Nov. 2011, PDF.

[29] J. Luo and T. Helleseth, "Constant composition codes as subcodes of cyclic codes," *IEEE Trans. Information Theory*, vol. 57, no. 11, pp. 7482–7488, Nov. 2011, PDF.

[30] X. Tang and T. Helleseth, "Generic construction of quaternary sequences of period $2N$ with low correlation from quaternary sequences of odd period N," *IEEE Trans. Information Theory*, vol. 57, no. 4, pp. 2295–2300, Apr. 2011, PDF.

[31] T. Helleseth and A. Kholosha, "New binomial bent functions over the finite fields of odd characteristic," *IEEE Trans. Information Theory*, vol. 56, no. 9, pp. 4646–4652, Sep. 2010, PDF.

[32] T. Helleseth, H. D. L. Hollmann, A. Kholosha, Z. Wang, and Q. Xiang, "Proofs of two conjectures on ternary weakly regular bent functions," *IEEE Trans. Information Theory*, vol. 55, no. 11, pp. 5272–5283, Nov. 2009, PDF.

[33] T. Helleseth, L. Hu, A. Kholosha, X. Zeng, N. Li, and W. Jiang, "Period-different m- sequences with at most four-valued cross correlation," *IEEE Trans. Information Theory*, vol. 55, no. 7, pp. 3305–3311, Jul. 2009, PDF.

[34] A. Johansen and T. Helleseth, "A family of m- sequences with five-valued cross correlation," *IEEE Trans. Information Theory*, vol. 55, no. 2, pp. 880–887, Feb. 2009, PDF.

[35] A. Johansen, T. Helleseth, and A. Kholosha, "Further results on m- sequences with five-valued cross correlation," *IEEE Trans. Information Theory*, vol. 55, no. 12, pp. 5792–5802, Dec. 2009, PDF.

[36] X. Tang, T. Helleseth, L. Hu, and W. Jiang, "Two new families of optimal binary sequences obtained from quaternary sequences," *IEEE Trans. Information Theory*, vol. 55, no. 4, pp. 1833–1840, Apr. 2009, PDF.

[37] A. Johansen, T. Helleseth, and X. Tang, "The correlation distribution of quaternary sequences of period $2(2^n-1)$," *IEEE Trans. Information Theory*, vol. 54, no. 7, pp. 3130–3139, Jul. 2008, PDF.

[38] C. Ding, T. Helleseth, T. Kløve, and X. Wang, "A generic construction of Cartesian authentication codes," *IEEE Trans. Information Theory*, vol. 53, no. 6, pp. 2229–2235, Jun. 2007, PDF.

[39] T. Helleseth, A. Kholosha, and G. J. Ness, "Characterization of m- sequences of lengths $2^{2k}-1$ and 2^k-1 with three-valued crosscorrelation," *IEEE Trans. Information Theory*, vol. 53, no. 6, pp. 2236–2245, Jun. 2007, PDF.

[40] G. J. Ness and T. Helleseth, "A new family of four-valued cross correlation between m- sequences of different lengths," *IEEE Trans. Information Theory*, vol. 53, no. 11, pp. 4308–4313, Nov. 2007, PDF.

[41] ——, "A new family of ternary almost perfect nonlinear mappings," *IEEE Trans. Information Theory*, vol. 53, no. 7, pp. 2581–2586, Jul. 2007, PDF.

[42] S. Rønjom and T. Helleseth, "A new attack on the filter generator," *IEEE Trans. Information Theory*, vol. 53, no. 5, pp. 1752–1758, May 2007, PDF.

[43] P. Charpin, T. Helleseth, and V. A. Zinoviev, "The coset distribution of triple-error-correcting binary primitive BCH codes," *IEEE Trans. Information Theory*, vol. 52, no. 4, pp. 1727–1732, Apr. 2006, PDF.

[44] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums," *IEEE Trans. Information Theory*, vol. 52, no. 2, pp. 613–627, Feb. 2006, PDF.

[45] T. Helleseth and A. Kholosha, "Monomial and quadratic bent functions over the finite fields of odd characteristic," *IEEE Trans. Information Theory*, vol. 52, no. 5, pp. 2018–2032, May 2006, PDF.

[46] H. Molland and T. Helleseth, "Linear properties in T-functions," *IEEE Trans. Information Theory*, vol. 52, no. 11, pp. 5151–5157, Nov. 2006, PDF.

[47] G. J. Ness and T. Helleseth, "A new three-valued cross correlation between m- sequences of different lengths," *IEEE Trans. Information Theory*, vol. 52, no. 10, pp. 4695–4701, Oct. 2006, PDF.

[48] ——, "Cross correlation of m- sequences of different lengths," *IEEE Trans. Information Theory*, vol. 52, no. 4, pp. 1637–1648, Apr. 2006, PDF.

[49] G. J. Ness, T. Helleseth, and A. Kholosha, "On the correlation distribution of the Coulter-Matthews decimation," *IEEE Trans. Information Theory*, vol. 52, no. 5, pp. 2241–2247, May 2006, PDF.

[50] T. Helleseth, T. Kløve, and V. I. Levenshtein, "Error-correction capability of binary linear codes," *IEEE Trans. Information Theory*, vol. 51, no. 4, pp. 1408–1423, Apr. 2005, PDF.

[51] S.-H. Kim, J.-S. No, H. Chung, and T. Helleseth, "New cyclic relative difference sets constructed from d- homogeneous functions with difference-balanced property," *IEEE Trans. Information Theory*, vol. 51, no. 3, pp. 1155–1163, Mar. 2005, PDF.

[52] H. G. Schaathun and T. Helleseth, "The second support weight distribution of the Kasami codes," *IEEE Trans. Information Theory*, vol. 51, no. 8, pp. 2892–2894, Aug. 2005, PDF.

[53] T. Helleseth, T. Kløve, and V. I. Levenshtein, "The simplex codes and other even-weight binary linear codes for error correction," *IEEE Trans. Information Theory*, vol. 50, no. 11, pp. 2818–2823, Nov. 2004, PDF.

[54] T. Helleseth, M. Maas, J. E. Mathiassen, and T. Segers, "Linear complexity over $\mathbb{F}_p$ of Sidel'nikov sequences," *IEEE Trans. Information Theory*, vol. 50, no. 10, pp. 2468–2472, Oct. 2004, PDF.

[55] T. Helleseth and H. G. Schaathun, "On the (2,1)-separating weight of the Kerdock code," *IEEE Trans. Information Theory*, vol. 50, no. 12, pp. 3312–3315, Dec. 2004, PDF.

[56] T. Helleseth and J. F. Voloch, "Double circulant quadratic residue codes," *IEEE Trans. Information Theory*, vol. 50, no. 9, pp. 2154–2155, Sep. 2004, PDF.

[57] J.-W. Jang, Y.-S. Kim, J.-S. No, and T. Helleseth, "New family of p- ary sequences with optimal correlation property and large linear span," *IEEE Trans. Information Theory*, vol. 50, no. 8, pp. 1839–1843, Aug. 2004, PDF.

[58] T. Helleseth, S.-H. Kim, and J.-S. No, "Linear complexity over $\mathbb{F}_p$ and trace representation of Lempel-Cohn-Eastman sequences," *IEEE Trans. Information Theory*, vol. 49, no. 6, pp. 1548–1552, Jun. 2003, PDF.

[59] K. Yang and T. Helleseth, "On the minimum distance of array codes as LDPC codes," *IEEE Trans. Information Theory*, vol. 49, no. 12, pp. 3268–3271, Dec. 2003, PDF.

[60] C. Ding, T. Helleseth, H. Niederreiter, and C. Xing, "The minimum distance of the duals of binary irreducible cyclic codes," *IEEE Trans. Information Theory*, vol. 48, no. 10, pp. 2679–2689, Oct. 2002, PDF.

[61] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation," *IEEE Trans. Information Theory*, vol. 48, no. 11, pp. 2868–2872, Nov. 2002, PDF.

[62] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, and H. M. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Trans. Information Theory*, vol. 47, no. 7, pp. 2934–2943, Nov. 2001, PDF.

[63] C. Ding, T. Helleseth, and H. M. Martinsen, "New families of binary sequences with optimal three-level autocorrelation," *IEEE Trans. Information Theory*, vol. 47, no. 1, pp. 428–433, Jan. 2001, PDF.

[64] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. M. Martinsen, "Ternary m- sequences with three-valued cross-correlation function: New decimations of Welch and Niho type," *IEEE Trans. Information Theory*, vol. 47, no. 4, pp. 1473–1481, May 2001, PDF.

[65] T. Helleseth and V. A. Zinoviev, "Codes with the same coset weight distributions as the $\mathbb{Z}_4$- linear Goethals codes," *IEEE Trans. Information Theory*, vol. 47, no. 4, pp. 1589–1595, May 2001, PDF.

[66] ——, "On coset weight distributions of the $\mathbb{Z}_4$- linear Goethals codes," *IEEE Trans. Information Theory*, vol. 47, no. 5, pp. 1758–1772, Jul. 2001, PDF.

[67] J.-S. No, H. Chung, H.-Y. Song, K. Yang, J.-D. Lee, and T. Helleseth, "New construction for binary sequences of period $p^m - 1$ with optimal autocorrelation using $(z+1)^d + az^d + b$," *IEEE Trans. Information Theory*, vol. 47, no. 4, pp. 1638–1644, May 2001, PDF.

[68] A. Chang, P. Gaal, S. W. Golomb, G. Gong, T. Helleseth, and P. V. Kumar, "On a conjectured ideal autocorrelation sequence and a related triple-error correcting cyclic code," *IEEE Trans. Information Theory*, vol. 46, no. 2, pp. 680–687, Mar. 2000, PDF.

[69] N. Hamada, T. Helleseth, H. M. Martinsen, and Ø. Ytrehus, "There is no ternary $[28, 6, 16]$ code," *IEEE Trans. Information Theory*, vol. 46, no. 4, pp. 1550–1554, Jul. 2000, PDF.

[70] C. Ding and T. Helleseth, "Generalized cyclotomic codes of length $p_1^{e_1} \cdots p_t^{e_t}$," *IEEE Trans. Information Theory*, vol. 45, no. 2, pp. 467–474, Mar. 1999, PDF.

[71] C. Ding, T. Helleseth, and K. Y. Lam, "Several classes of binary sequences with three-level autocorrelation," *IEEE Trans. Information Theory*, vol. 45, no. 7, pp. 2606–2612, Nov. 1999, PDF.

[72] T. Helleseth, B. Hove, and K. Yang, "Further results on generalized Hamming weights for Goethals and Preparata codes over $\mathbb{Z}_4$," *IEEE Trans. Information Theory*, vol. 45, no. 4, pp. 1255–1258, May 1999, PDF.

[73] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings," *IEEE Trans. Information Theory*, vol. 45, no. 2, pp. 475–485, Mar. 1999, PDF.

[74] C. Rong, T. Helleseth, and J. Lahtonen, "On algebraic decoding of the $\mathbb{Z}_4$- linear Calderbank-McGuire code," *IEEE Trans. Information Theory*, vol. 45, no. 5, pp. 1423–1434, Jul. 1999, PDF.

[75] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of Legendre sequences," *IEEE Trans. Information Theory*, vol. 44, no. 3, pp. 1276–1278, May 1998, PDF.

[76] K. Yang and T. Helleseth, "On the weight hierarchy of Goethals codes over $\mathbb{Z}_4$," *IEEE Trans. Information Theory*, vol. 44, no. 1, pp. 304–307, Jan. 1998, PDF.

[77] I. Boukliev, S. M. Dodunekov, T. Helleseth, and Ø. Ytrehus, "On the $[162, 8, 80]$ codes," *IEEE Trans. Information Theory*, vol. 43, no. 6, pp. 2055–2057, Nov. 1997, PDF.

[78] T. Helleseth and T. Kløve, "The Newton radius of codes," *IEEE Trans. Information Theory*, vol. 43, no. 6, pp. 1820–1831, Nov. 1997, PDF.

[79] T. Helleseth, T. Kløve, and V. I. Levenshtein, "On the information function of an error-correcting code," *IEEE Trans. Information Theory*, vol. 43, no. 2, pp. 549–557, Mar. 1997, PDF.

[80] K. Yang and T. Helleseth, "On the weight hierarchy of Preparata codes over $\mathbb{Z}_4$," *IEEE Trans. Information Theory*, vol. 43, no. 6, pp. 1832–1842, Nov. 1997, PDF.

[81] A. R. Calderbank, G. McGuire, P. V. Kumar, and T. Helleseth, "Cyclic codes over $\mathbb{Z}_4$, locator polynomials, and Newton's identities," *IEEE Trans. Information Theory*, vol. 42, no. 1, pp. 217–226, Jan. 1996, PDF.

[82] T. Helleseth and T. Kløve, "The weight hierarchies of some product codes," *IEEE Trans. Information Theory*, vol. 42, no. 3, pp. 1029–1034, May 1996, PDF.

[83] T. Helleseth, P. V. Kumar, O. Moreno, and A. G. Shanbhag, "Improved estimates via exponential sums for the minimum distance of $\mathbb{Z}_4$- linear trace codes," *IEEE Trans. Information Theory*, vol. 42, no. 4, pp. 1212–1216, Jul. 1996, PDF.

[84] P. V. Kumar, T. Helleseth, A. R. Calderbank, and J. A. Roger Hammons, "Large families of quaternary sequences with low correlation," *IEEE Trans. Information Theory*, vol. 42, no. 2, pp. 579–592, Mar. 1996, PDF.

[85] A. G. Shanbhag, P. V. Kumar, and T. Helleseth, "Improved binary codes and sequence families from $\mathbb{Z}_4$- linear codes," *IEEE Trans. Information Theory*, vol. 42, no. 5, pp. 1582–1587, Sep. 1996, PDF.

[86] ——, "Upper bound for a hybrid sum over Galois rings with applications to aperiodic correlation of some q- ary sequences," *IEEE Trans. Information Theory*, vol. 42, no. 1, pp. 250–254, Jan. 1996, PDF.

[87] K. Yang, T. Helleseth, P. V. Kumar, and A. G. Shanbhag, "On the weight hierarchy of Kerdock codes over $\mathbb{Z}_4$," *IEEE Trans. Information Theory*, vol. 42, no. 5, pp. 1587–1593, Sep. 1996, PDF.

[88] T. Helleseth, T. Kløve, V. I. Levenshtein, and Ø. Ytrehus, "Bounds on the minimum support weights," *IEEE Trans. Information Theory*, vol. 41, no. 2, pp. 432–440, Mar. 1995, PDF.

[89] T. Helleseth and P. V. Kumar, "The algebraic decoding of the $\mathbb{Z}_4$-linear Goethals code," *IEEE Trans. Information Theory*, vol. 41, no. 6, Part II, pp. 2040–2048, Nov. 1995, PDF.

[90] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "An upper bound for Weil exponential sums over Galois rings and applications," *IEEE Trans. Information Theory*, vol. 41, no. 2, pp. 456–468, Mar. 1995, PDF.

[91] X. Chen, I. S. Reed, T. Helleseth, and T.-K. Truong, "General principles for the algebraic decoding of cyclic codes," *IEEE Trans. Information Theory*, vol. 40, no. 5, pp. 1661–1663, Sep. 1994, PDF.

[92] ——, "Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance," *IEEE Trans. Information Theory*, vol. 40, no. 5, pp. 1654–1661, Sep. 1994, PDF.

[93] T. Helleseth, T. Kløve, and Ø. Ytrehus, "Generalized Hamming weights of linear codes," *IEEE Trans. Information Theory*, vol. 38, no. 3, pp. 1133–1140, May 1992, PDF.

[94] T. Helleseth and T. Kløve, "The number of cross-join pairs in maximum length linear sequences," *IEEE Trans. Information Theory*, vol. 37, no. 6, pp. 1731–1733, Nov. 1991, PDF.

[95] Ø. Ytrehus and T. Helleseth, "There is no binary $[25, 8, 10]$ code," *IEEE Trans. Information Theory*, vol. 36, no. 3, pp. 695–696, May 1990, PDF.

[96] S. M. Dodunekov, T. Helleseth, N. Manev, and Ø. Ytrehus, "New bounds on binary linear codes of dimension eight," *IEEE Trans. Information Theory*, vol. IT-33, no. 6, pp. 917–919, Nov. 1987, PDF.

[97] T. Helleseth, "Further classifications of codes meeting the Griesmer bound," *IEEE Trans. Information Theory*, vol. IT-30, no. 2, pp. 395–403, Mar. 1984, PDF.

[98] ——, "New constructions of codes meeting the Griesmer bound," *IEEE Trans. Information Theory*, vol. IT-29, no. 3, pp. 434–439, May 1983, PDF.

[99] T. Helleseth and H. C. van Tilborg, "A new class of codes meeting the Griesmer bound," *IEEE Trans. Information Theory*, vol. IT-27, no. 5, pp. 548–555, Sep. 1981, PDF.

[100] T. Helleseth, "No primitive binary t-error-correcting BCH code with $t > 2$ is quasi-perfect," *IEEE Trans. Information Theory*, vol. IT-25, no. 3, pp. 361–362, May 1979, PDF.

[101] ——, "All binary 3-error-correcting BCH codes of length $2^m - i$ have covering radius 5," *IEEE Trans. Information Theory*, vol. IT-24, no. 2, pp. 257–258, Mar. 1978, PDF.

[102] T. Helleseth, T. Kløve, and J. J. Mykkeltveit, "On the covering radius of binary codes," *IEEE Trans. Information Theory*, vol. IT-24, no. 5, pp. 627–628, Sep. 1978, PDF.

[103] T. Helleseth, "Some two-weight codes with composite parity-check polynomials," *IEEE Trans. Information Theory*, vol. IT-22, no. 5, pp. 631–632, Sep. 1976, PDF.

Discrete Mathematics (21)

[1] Z. Tu, X. Zeng, and T. Helleseth, "A class of permutation quadrinomials," *Discrete Mathematics*, vol. 341, no. 11, pp. 3010–3020, 2018, PDF.

[2] P. Charpin, T. Helleseth, and V. A. Zinoviev, "Divisibility properties of classical binary Kloosterman sums," *Discrete Mathematics*, vol. 309, no. 12, pp. 3975–3984, Jun. 2009, PDF.

[3] T. Helleseth and V. A. Zinoviev, "On a new identity for Kloosterman sums and non-linear system of equations over finite fields of characteristic 2," *Discrete Mathematics*, vol. 274, no. 1-3, pp. 109–124, Jan. 2004, PDF.

[4] T. Helleseth, C. Rong, and K. Yang, "New 3-designs from Goethals codes over $\mathbb{Z}_4$," *Discrete Mathematics*, vol. 226, no. 1-3, pp. 403–409, Jan. 2001, PDF.

[5] ——, "On t- designs from codes over $\mathbb{Z}_4$," *Discrete Mathematics*, vol. 238, no. 1-3, pp. 67–80, Jul. 2001, PDF.

[6] D.-J. Shin, P. V. Kumar, and T. Helleseth, "5-designs from the lifted Golay code over $\mathbb{Z}_4$ via an Assmus-Mattson type approach," *Discrete Mathematics*, vol. 241, no. 1-3, pp. 479–487, Oct. 2001, PDF.

[7] C. Ding, T. Helleseth, and K. Y. Lam, "Duadic sequences of prime lengths," *Discrete Mathematics*, vol. 218, no. 1-3, pp. 33–49, May 2000, PDF.

[8] T. Helleseth, C. Rong, and K. Yang, "New infinite families of 3-designs from Preparata codes over $\mathbb{Z}_4$," *Discrete Mathematics*, vol. 195, no. 1-3, pp. 139–156, Jan. 1999, PDF.

[9] E. R. Hauge and T. Helleseth, "DeBruijn sequences, irreducible codes and cyclotomy," *Discrete Mathematics*, vol. 159, no. 1-3, pp. 143–154, Nov. 1996, PDF.

[10] T. Helleseth and P. V. Kumar, "On the weight hierarchy of the semiprimitive codes," *Discrete Mathematics*, vol. 152, no. 1-3, pp. 185–190, May 1996, PDF.

[11] N. Hamada and T. Helleseth, "A characterization of some $\{3v_{\mu+1}, 3v_\mu;\ k-1, q\}$-minihypers and some $[n, k, q^{k-1} - 3q^\mu;\ q]$- codes $(k \geq 3, q \geq 5, 1 \leq \mu < k-1)$ meeting the Griesmer bound," *Discrete Mathematics*, vol. 146, no. 1-3, pp. 59–67, Nov. 1995, PDF.

[12] T. Helleseth and P. V. Kumar, "The weight hierarchy of the Kasami codes," *Discrete Mathematics*, vol. 145, no. 1-3, pp. 133–143, Oct. 1995, PDF.

[13] N. Hamada, T. Helleseth, and Ø. Ytrehus, "Characterization of $\{2(q+1)+2, 2;\ t, q\}$-minihypers in $\mathrm{PG}(t, q)$ $(t \geq 3, q \in \{3, 4\})$," *Discrete Mathematics*, vol. 115, no. 1-3, pp. 175–185, May 1993, PDF.

[14] N. Hamada and T. Helleseth, "A characterization of some $\{2v_{\alpha+1}+v_{\gamma+1}, 2v_\alpha+v_\gamma;\ k-1, 3\}$- minihypers and some $(n, k, 3^{k-1}-2\cdot 3^\alpha-3^\gamma;\ 3)$- codes $(k \geq 3, 0 \leq \alpha < \gamma < k-1)$ meeting the Griesmer bound," *Discrete Mathematics*, vol. 104, no. 1, pp. 67–81, Jun. 1992, PDF.

[15] T. Helleseth, "Projective codes meeting the Griesmer bound," *Discrete Mathematics*, vol. 106-107, pp. 265–271, Sep. 1992, PDF.

[16] T. Helleseth and H. F. M. Jr., "On the cosets of the simplex code," *Discrete Mathematics*, vol. 56, no. 2-3, pp. 169–189, Oct. 1985, PDF.

[17] T. Helleseth, "The weight distribution of the coset leaders for some classes of codes with related parity-check matrices," *Discrete Mathematics*, vol. 28, no. 2, pp. 161–171, Nov. 1979, PDF.

[18] ——, "A note on the cross-correlation function between two binary maximal length linear sequences," *Discrete Mathematics*, vol. 23, no. 3, pp. 301–307, 1978, PDF.

[19] ——, "The weight enumerator polynomials of some classes of codes with composite parity-check polynomials," *Discrete Mathematics*, vol. 20, no. 1, pp. 21–31, 1977, PDF.

[20] T. Helleseth, T. Kløve, and J. J. Mykkeltveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l - 1)/N)$," *Discrete Mathematics*, vol. 18, no. 2, pp. 179–211, 1977, PDF.

[21] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Mathematics*, vol. 16, no. 3, pp. 209–232, Nov. 1976, PDF.

Designs, Codes and Cryptography (20)

[1] V. Edemskiy, C. Li, X. Zeng, and T. Helleseth, "The linear complexity of generalized cyclotomic binary sequences of period p^n," *Des. codes and cryptography*, vol. 87, no. 5, pp. 1183–1197, 2019, PDF. DOI: 10.1007/s10623-018-0513-2. [Online]. Available: https://doi.org/10.1007/s10623-018-0513-2.

[2] Z. Xiao, X. Zeng, C. Li, and T. Helleseth, "New generalized cyclotomic binary sequences of period p^2," *Des. Codes and Cryptography*, vol. 86, no. 7, pp. 1483–1497, 2018, PDF.

[3] X. Xu, C. Li, X. Zeng, and T. Helleseth, "Constructions of complete permutation polynomials," *Des. Codes and Cryptography*, vol. 86, no. 12, pp. 2869–2892, 2018, PDF.

[4] A. Alahmadi, H. Alhazmi, T. Helleseth, R. Hijazi, N. M. Muthana, and P. Solé, "On the lifted zetterberg code," *Des. Codes and Cryptography*, vol. 80, no. 3, pp. 561–576, 2016, PDF.

[5] Z. Zhou, N. Li, C. Fan, and T. Helleseth, "Linear codes with two or three weights from quadratic bent functions," *Des. Codes and Cryptography*, vol. 81, no. 2, pp. 283–295, 2016, PDF.

[6] N. Li, X. Tang, and T. Helleseth, "New M- ary sequences with low autocorrelation from interleaved technique," *Des. Codes and Cryptography*, vol. 73, no. 1, pp. 237–249, Oct. 2014, PDF.

[7] X. Tang, T. Helleseth, and P. Fan, "A new optimal quaternary sequence family of length $2(2^n - 1)$ obtained from the orthogonal transformation of families $\mathcal{B}$ and $\mathcal{C}$," *Des. Codes and Cryptography*, vol. 53, no. 3, pp. 137–148, Dec. 2009, PDF.

[8] T. Helleseth and J. J. Mykkeltveit, "A proof of Simmons' conjecture," *Des. Codes and Cryptography*, vol. 33, no. 1, pp. 39–43, Aug. 2004, PDF.

[9] J.-S. No, D.-J. Shin, and T. Helleseth, "On the p- ranks and characteristic polynomials of cyclic difference sets," *Des. Codes and Cryptography*, vol. 33, no. 1, pp. 23–37, Aug. 2004, PDF.

[10] D.-J. Shin, P. V. Kumar, and T. Helleseth, "An Assmus-Mattson-type approach for identifying 3-designs from linear codes over $\mathbb{Z}_4$," *Des. Codes and Cryptography*, vol. 31, no. 1, pp. 75–92, Jan. 2004, PDF.

[11] T. Helleseth, T. Kløve, and V. I. Levenshtein, "Hypercubic 4 and 5-designs from double-error-correcting BCH codes," *Des. Codes and Cryptography*, vol. 28, no. 3, pp. 265–282, Apr. 2003, PDF.

[12] D.-J. Shin, P. V. Kumar, and T. Helleseth, "3-designs from the $\mathbb{Z}_4$- Goethals codes via a new Kloosterman sum identity," *Des. Codes and Cryptography*, vol. 28, no. 3, pp. 247–263, Apr. 2003, PDF.

[13] T. Helleseth, P. V. Kumar, and H. M. Martinsen, "A new family of ternary sequences with ideal two-level autocorrelation function," *Des. Codes and Cryptography*, vol. 23, no. 2, pp. 157–166, Jul. 2001, PDF.

[14] I. Duursma, T. Helleseth, C. Rong, and K. Yang, "Split weight enumerators for the Preparata codes with applications to designs," *Des. Codes and Cryptography*, vol. 18, no. 1-3, pp. 103–124, Dec. 1999, PDF.

[15] T. Helleseth and V. A. Zinoviev, "On $\mathbb{Z}_4$- linear Goethals codes and Kloosterman sums," *Des. Codes and Cryptography*, vol. 17, no. 1-3, pp. 269–288, Sep. 1999, PDF.

[16] R. Anderson, C. Ding, T. Helleseth, and T. Kløve, "How to build robust shared control systems," *Des. Codes and Cryptography*, vol. 15, no. 2, pp. 111–124, Nov. 1998, PDF.

[17] T. Helleseth, P. V. Kumar, and K. Yang, "An infinite family of 3-designs from Preparata codes over $\mathbb{Z}_4$," *Des. Codes and Cryptography*, vol. 15, no. 2, pp. 175–181, Nov. 1998, PDF.

[18] K. Yang and T. Helleseth, "Two new infinite families of 3-designs from Kerdock codes over $\mathbb{Z}_4$," *Des. Codes and Cryptography*, vol. 15, no. 2, pp. 201–214, Nov. 1998, PDF.

[19] T. Helleseth, P. V. Kumar, and A. G. Shanbhag, "Codes with the same weight distributions as the Goethals codes and the Delsarte-Goethals codes," *Des. Codes and Cryptography*, vol. 9, no. 3, pp. 257–266, Nov. 1996, PDF.

[20] N. Hamada, T. Helleseth, and Ø. Ytrehus, "On the construction of $[q^4+q^2-q, 5, q^4-q^3+q^2-2q;\ q]$- codes meeting the Griesmer bound," *Des. Codes and Cryptography*, vol. 2, no. 3, pp. 225–229, Sep. 1992, PDF.

Finite Fields and Their Applications (14)

[1] Z. Tu, X. Zeng, and T. Helleseth, "New permutation quadrinomials over F_2^{2m}," *Finite fields and their applications*, vol. 50, pp. 304–318, 2018, PDF.

[2] Z. Tu, X. Zeng, C. Li, and T. Helleseth, "A class of new permutation trinomials," *Finite fields and their applications*, vol. 50, pp. 178–195, 2018, PDF.

[3] ——, "Permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over the finite field $GF(p^{2m})$ of odd characteristic," *Finite Fields and Their Applications*, vol. 34, pp. 20–35, 2015, PDF.

[4] N. Li, C. Li, T. Helleseth, C. Ding, and X. Tang, "Optimal ternary cyclic codes with minimum distance four and five," *Finite Fields and Their Applications*, vol. 30, pp. 100–120, Nov. 2014, PDF.

[5] G. Wu, N. Li, T. Helleseth, and Y. Zhang, "Some classes of monomial complete permutation polynomials over finite fields of characteristic two," *Finite Fields and Their Applications*, vol. 28, pp. 148–165, Jul. 2014, PDF.

[6] N. Li, T. Helleseth, and X. Tang, "Further results on a class of permutation polynomials over finite fields," *Finite Fields and Their Applications*, vol. 22, pp. 16–23, Jul. 2013, PDF.

[7] T. Helleseth and A. Kholosha, "On the equation $x^{2^l+1} + x + a = 0$ over $\mathrm{GF}(2^k)$," *Finite Fields and Their Applications*, vol. 14, no. 1, pp. 159–176, Jan. 2008, PDF.

[8] P. Charpin, T. Helleseth, and V. A. Zinoviev, "Propagation characteristics of $x \mapsto x^{-1}$ and Kloosterman sums," *Finite Fields and Their Applications*, vol. 13, no. 2, pp. 366–381, Apr. 2007, PDF.

[9] T. Helleseth, J. Lahtonen, and P. Rosendahl, "On Niho type cross-correlation functions of m- sequences," *Finite Fields and Their Applications*, vol. 13, no. 2, pp. 305–317, Apr. 2007, PDF.

[10] T. Helleseth and P. Rosendahl, "New pairs of m- sequences with 4-level cross-correlation," *Finite Fields and Their Applications*, vol. 11, no. 4, pp. 674–683, Nov. 2005, PDF.

[11] T. Helleseth and V. A. Zinoviev, "New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m," *Finite Fields and Their Applications*, vol. 9, no. 2, pp. 187–193, Apr. 2003, PDF.

[12] C. Ding and T. Helleseth, "New generalized cyclotomy and its applications," *Finite Fields and Their Applications*, vol. 4, no. 2, pp. 140–166, Apr. 1998, PDF.

[13] A. G. Shanbhag, P. V. Kumar, and T. Helleseth, "An upper bound for the extended Kloosterman sums over Galois rings," *Finite Fields and Their Applications*, vol. 4, no. 3, pp. 218–238, Jul. 1998, PDF.

[14] N. Hamada and T. Helleseth, "Construction of some optimal ternary linear codes and the uniqueness of $[294, 6, 195;\ 3]$- codes meeting the Griesmer bound," *Finite Fields and Their Applications*, vol. 1, no. 4, pp. 458–468, Oct. 1995, PDF.

Cryptography and Communications (10)

[1] N. Li and T. Helleseth, "New permutation trinomials from niho exponents over finite fields with even characteristic," *Cryptography and communications*, vol. 11, no. 1, pp. 129–136, 2019, PDF.

[2] P. Tan, Z. Zhou, D. Tang, and T. Helleseth, "The weight distribution of a class of two-weight linear codes derived from kloosterman sums," *Cryptography and Communications*, vol. 10, no. 2, pp. 291–299, 2018, PDF.

[3] N. Li and T. Helleseth, "Several classes of permutation trinomials from Niho exponents," *Cryptography and Communications*, vol. 9, no. 6, pp. 693–705, 2017, PDF.

[4] A. Alahmadi, H. Alhazmi, T. Helleseth, R. Hijazi, N. M. Muthana, and P. Solé, "On the lifted melas code," *Cryptography and Communications*, vol. 8, no. 1, pp. 7–18, 2016, PDF.

[5] L. Budaghyan, T. Helleseth, and A. Kholosha, "Editorial: Special issue on Boolean Functions and their Applications," *Cryptography and Communications*, vol. 8, no. 2, pp. 173–174, 2016, PDF.

[6] C. Li and T. Helleseth, "Quasi-perfect linear codes from planar and APN functions," *Cryptography and Communications*, vol. 8, no. 2, pp. 215–227, 2016, PDF.

[7] T. Helleseth and J. Jedwab, "Special issue editorial: Sequences and their applications," *Cryptography and Communications*, vol. 6, no. 1, pp. 1–2, 2014, PDF.

[8] L. Budaghyan and T. Helleseth, "New commutative semifields defined by new PN multinomials," *Cryptography and Communications*, vol. 3, no. 1, pp. 1–16, Mar. 2011, PDF.

[9] T. Helleseth and A. Kholosha, "Crosscorrelation of m- sequences, exponential sums, bent functions and Jacobsthal sums," *Cryptography and Communications*, vol. 3, no. 4, pp. 281–291, Dec. 2011, PDF.

[10] ——, "$x^{2^l+1} + x + a$ and related affine polynomials over GF(2^k)," *Cryptography and Communications*, vol. 2, no. 1, pp. 85–109, Apr. 2010, PDF.

Mathematica Japonica (5)

[1] N. Hamada and T. Helleseth, "The nonexistence of some ternary linear codes and update of the bounds for $n_3(6, d)$, $1 \leq d \leq 243$," *Mathematica Japonica*, vol. 52, no. 1, pp. 31–43, Jul. 2000.

[2] ——, "A characterization of $\{3\nu_1 + \nu_4, 3\nu_0 + \nu_3;\ 4, 3\}$- minihypers and projective ternary $[78, 5, 51;\ 3]$- codes," *Mathematica Japonica*, vol. 43, no. 2, pp. 253–266, Mar. 1996.

[3] ——, "A characterization of some $\{\nu_1 + \nu_2 + 2\nu_3, \nu_0 + \nu_1 + 2\nu_2;\ 4, 3\}$- minihypers and some $[90, 5, 59;\ 3]$- codes meeting the Griesmer bound," *Mathematica Japonica*, vol. 41, no. 3, pp. 657–672, May 1995.

[4] ——, "A characterization of some q- ary codes ($q > (h-1)^2$, $h \geq 3$) meeting the Griesmer bound," *Mathematica Japonica*, vol. 38, no. 5, pp. 925–940, 1993.

[5] ——, "A characterization of some linear codes over GF(4) meeting the Griesmer bound," *Mathematica Japonica*, vol. 37, no. 2, pp. 231–242, 1992.

Journal of Statistical Planning and Inference (4)

[1] N. Hamada and T. Helleseth, "The nonexistence of ternary $[97, 6, 63]$ codes," *Journal of statistical planning and inference*, vol. 106, no. 1-2, pp. 485–507, Aug. 2002, PDF.

[2] ——, "A characterization of some $\{3v_2 + v_3, 3v_1 + v_2;\ 3, 3\}$- minihypers and some $[15, 4, 9;\ 3]$- codes with $B_2 = 0$," *Journal of statistical planning and inference*, vol. 56, no. 1, pp. 129–146, Dec. 1996, PDF.

[3] ——, "The uniqueness of $[87, 5, 57;\ 3]$- codes and the nonexistence of $[258, 6, 171;\ 3]$- codes," *Journal of statistical planning and inference*, vol. 56, no. 1, pp. 105–127, Dec. 1996, PDF.

[4] ——, "A characterization of some $\{\nu_2 + 2\nu_3, \nu_1 + 2\nu_2;\ k-1, 3\}$- minihypers and some $(\nu_k - 30, k, 3^{k-1} - 21;\ 3)$- codes meeting the Griesmer bound," *Journal of statistical planning and inference*, vol. 34, no. 3, pp. 387–402, Mar. 1993, PDF.

Discrete Applied Mathematics (3)

[1] N. Hamada, T. Helleseth, and Ø. Ytrehus, "A new class of nonbinary codes meeting the Griesmer bound," *Discrete Applied Mathematics*, vol. 47, no. 3, pp. 219–226, Dec. 1993, PDF.

[2] T. Helleseth, "Legendre sums and codes related to QR codes," *Discrete Applied Mathematics*, vol. 35, no. 2, pp. 107–113, Jan. 1992, PDF.

[3] ——, "On the covering radius of cyclic linear codes and arithmetic codes," *Discrete Applied Mathematics*, vol. 11, no. 2, pp. 157–173, Jun. 1985, Russian translation in [21], PDF.

Problems of Information Transmission (3)

[1] L. A. Bassalygo, S. M. Dodunekov, V. A. Zinoviev, and T. Helleseth, "The Grey-Rankin bound for nonbinary codes," *Problems of Information Transmission*, vol. 42, no. 3, pp. 197–203, Sep. 2006, PDF.

[2] V. A. Zinoviev, T. Helleseth, and P. Charpin, "On cosets of weight 4 of binary BCH codes with minimum distance 8 and exponential sums," *Problems of Information Transmission*, vol. 41, no. 4, pp. 331–348, Oct. 2005, PDF.

[3] V. A. Zinoviev and T. Helleseth, "On weight distributions of shifts of Goethals-like codes," *Problems of Information Transmission*, vol. 40, no. 2, pp. 118–134, Apr. 2004, PDF.

IEICE Transactions (3)

[1] Y. Xia, S. Chen, T. Helleseth, and C. Li, "Cross-correlation between a p-aay sequence and its all decimated sequences for $d = (p^m+1)(p^m+p-1)/(p+1)$," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 97-A, no. 4, pp. 964–969, 2014. [Online]. Available: https://doi.org/10.1587/transfun.E97.A.964.

[2] T. Helleseth, "Crosscorrelation of m- sequences, exponential sums and Dickson polynomials," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E93-A, no. 11, pp. 2212–2219, Nov. 2010, PDF.

[3] Y.-S. Kim, J.-W. Jang, J.-S. No, and T. Helleseth, "New constructions of p- ary bent sequences," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E87-A, no. 2, pp. 489–494, Feb. 2004, PDF.

Information and Computation (2)

[1] T. W. Sze, S. T. Chanson, C. Ding, T. Helleseth, and M. G. Parker, "Logarithm Cartesian authentication codes," *Information and Computation*, vol. 184, no. 1, pp. 93–108, Jul. 2003, PDF.

[2] T. Helleseth and H. M. Martinsen, "Binary sequences of period $2^m - 1$ with large linear complexity," *Information and Computation*, vol. 151, no. 1-2, pp. 73–91, May 1999, PDF.

Information and Control (2)

[1] T. Helleseth, "A characterization of codes meeting the Griesmer bound," *Information and Control*, vol. 50, no. 2, pp. 128–159, Aug. 1981, PDF.

[2] T. Helleseth and T. Kløve, "On group-theoretic codes for asymmetric channels," *Information and Control*, vol. 49, no. 1, pp. 1–9, Apr. 1981, PDF.

Applicable Algebra in Engineering, Communication and Computing (2)

[1] T. Helleseth and D. Sandberg, "Some power mappings with low differential uniformity," *Applicable Algebra in Engineering, Communication and Computing*, vol. 8, no. 5, pp. 363–370, Jul. 1997, PDF.

[2] P. V. Kumar and T. Helleseth, "An expansion for the coordinates of the trace function over Galois rings," *Applicable Algebra in Engineering, Communication and Computing*, vol. 8, no. 5, pp. 353–361, Jul. 1997, PDF.

Journal of Combinatorial Theory, Series A (1)

[1] P. Charpin, T. Helleseth, and V. A. Zinoviev, "The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd," *Journal of Combinatorial Theory, Series A*, vol. 114, no. 2, pp. 322–338, Feb. 2007, PDF.

Other Journals (16)

[1] A. Alahmadi, H. Alhazmi, S. Ali, T. Helleseth, R. Hijazi, C. Li, and P. Solé, "An analogue of the $\mathbb{Z}_4$-goethals code in non-primitive length," *J. systems science and complexity*, vol. 30, no. 4, pp. 950–966, 2017, PDF.

[2] N. Li, X. Tang, and T. Helleseth, "A class of quaternary sequences with low correlation," *Advances in math. of comm.*, vol. 9, no. 2, pp. 199–210, 2015, Link.

[3] Y. Xia, T. Helleseth, and C. Li, "Some new classes of cyclic codes with three or six weights," *Advances in math. of comm.*, vol. 9, no. 1, pp. 23–36, 2015, Link.

[4] W. Jia, X. Zeng, C. Li, T. Helleseth, and L. Hu, "Permutation polynomials with low differential uniformity over finite fields of odd characteristic," *Science china mathematics*, vol. 56, no. 7, pp. 1429–1440, Jul. 2013, PDF.

[5] L. Budaghyan and T. Helleseth, "On isotopisms of commutative presemifields and CCZ-equivalence of functions," *International Journal of Foundations of Computer Science*, vol. 22, no. 6, pp. 1243–1258, Sep. 2011, PDF.

[6] P. Charpin, T. Helleseth, and V. A. Zinoviev, "On cosets of weight 4 of BCH$(2^m, 8)$, m even, and exponential sums," *SIAM Journal on Discrete Mathematics*, vol. 23, no. 1, pp. 59–78, 2008, PDF.

[7] T. Helleseth, J. Lahtonen, and K. Ranto, "A simple proof to the minimum distance of $\mathbb{Z}_4$- linear Goethals-like codes," *Journal of Complexity*, vol. 20, no. 2-3, pp. 297–304, Apr. 2004, PDF.

[8] T. Helleseth, "Sekvenser og anvendelser i mobilkommunikasjon," *Nordisk Matematisk Tidsskrift*, vol. 50, no. 3-4, pp. 155–169, 2002, PDF.

[9] ——, "Sequences with good correlations and some open problems," *Electronic Notes in Discrete Mathematics*, vol. 6, pp. 507–517, Apr. 2001, PDF.

[10] N. Hamada and T. Helleseth, "Arcs, blocking sets, and minihypers," *Computers and Mathematics with Applications*, vol. 39, no. 11, pp. 159–168, Jun. 2000, PDF.

[11] C. Ding and T. Helleseth, "On cyclotomic generator of order r," *Information Processing Letters*, vol. 66, no. 1, pp. 21–25, Apr. 1998, PDF.

[12] N. Hamada, T. Helleseth, and Ø. Ytrehus, "On the construction of $[q^4+q^2-q, 5, q^4-q^3+q^2-2q; q]$- codes meeting the Griesmer bound," *RIMS Proceedings*, vol. 853, pp. 187–195, Nov. 1993, (In Japanese) PDF.

[13] ——, "The nonexistence of $[51, 5, 33;\ 3]$- codes," *Ars Combinatoria*, vol. 35, pp. 25–32, Jun. 1993, PDF.

[14] ——, "There are exactly two nonequivalent $[20, 5, 12;\ 3]$- codes," *Ars Combinatoria*, vol. 35, pp. 3–14, Jun. 1993, PDF.

[15] N. Hamada and T. Helleseth, "A characterization of some $\{3v_2, 3v_1;\ t, q\}$- minihypers and some $\{2v_2 + v_{\gamma+1}, 2v_1 + v_\gamma;\ t, q\}$- minihypers ($q = 3$ or 4, $2 \leq \gamma < t$) and its applications to error-correcting codes," *Bulletin of Osaka Women's University*, vol. 27, pp. 49–107, 1990.

[16] ——, "A characterization of some minihypers in a finite projective geometry PG$(t, 4)$," *European Journal of Combinatorics*, vol. 11, no. 6, pp. 541–548, Nov. 1990.

IACR and arXiv papers (22)

[1] S. Rønjom, N. G. Bardeh, and T. Helleseth, "Yoyo tricks with aes," *IACR cryptology eprint archive*, vol. 2017, p. 980, 2017. [Online]. Available: http://eprint.iacr.org/2017/980.

[2] L. Budaghyan, C. Carlet, T. Helleseth, and N. Li, "On the (non-)existence of APN (n, n)-functions of algebraic degree n," *IACR cryptology eprint archive*, 2016.

[3] L. Budaghyan, T. Helleseth, N. Li, and B. Sun, "Some results on the known classes of quadratic apn functions," *IACR cryptology eprint archive*, vol. 2016, p. 1183, 2016. [Online]. Available: http://eprint.iacr.org/2016/1183.

[4] N. Li and T. Helleseth, "Several classes of permutation trinomials from niho exponents," *Corr*, vol. abs/1612.08823, 2016. [Online]. Available: http://arxiv.org/abs/1612.08823.

[5] Y. Xia, N. Li, X. Zeng, and T. Helleseth, "On the correlation distribution for a ternary niho decimation," *Corr*, vol. abs/1612.06686, 2016. [Online]. Available: http://arxiv.org/abs/1612.06686.

[6] Z. Zhou, N. Li, C. Fan, and T. Helleseth, "Linear codes with two or three weights from quadratic bent functions," *Corr*, vol. abs/1506.06830, 2015. [Online]. Available: http://arxiv.org/abs/1506.06830.

[7] L. Budaghyan, A. Kholosha, C. Carlet, and T. Helleseth, "Univariate niho bent functions from o-polynomials," *Corr*, vol. abs/1411.2394, 2014. [Online]. Available: http://arxiv.org/abs/1411.2394.

[8] C. Ding and T. Helleseth, "Optimal ternary cyclic codes from monomials," *Corr*, vol. abs/1305.0061, 2013. [Online]. Available: http://arxiv.org/abs/1305.0061.

[9] H. Hu, S. Shao, G. Gong, and T. Helleseth, "The proof of Lin's conjecture via the decimation-hadamard transform," *Corr*, vol. abs/1307.0885, 2013. [Online]. Available: http://arxiv.org/abs/1307.0885.

[10] C. Li, N. Li, T. Helleseth, and C. Ding, "On the weight distributions of several classes of cyclic codes from APN monomials," *Corr*, vol. abs/1308.5885, 2013. [Online]. Available: http://arxiv.org/abs/1308.5885.

[11] N. Li, C. Li, T. Helleseth, C. Ding, and X. Tang, "Optimal ternary cyclic codes with minimum distance four and five," *Corr*, vol. abs/1309.1218, 2013. [Online]. Available: http://arxiv.org/abs/1309.1218.

[12] G. Wu, N. Li, T. Helleseth, and Y. Zhang, "More classes of complete permutation polynomials over $GF(q)$," *Corr*, vol. abs/1312.4716, 2013. [Online]. Available: http://arxiv.org/abs/1312.4716.

[13] T. Helleseth, A. Kholosha, and S. Mesnager, "Niho bent functions and subiaco/adelaide hyperovals," *Corr*, vol. abs/1210.4732, 2012. [Online]. Available: http://arxiv.org/abs/1210.4732.

[14] L. Budaghyan and T. Helleseth, "On isotopisms of commutative presemifields and ccz-equivalence of functions," *IACR cryptology eprint archive*, vol. 2010, p. 507, 2010. [Online]. Available: http://eprint.iacr.org/2010/507.

[15] M. M. Hassanzadeh and T. Helleseth, "Algebraic attack on the alternating step(r, s) generator," *Corr*, vol. abs/1006.1735, 2010.

[16] T. Helleseth and A. Kholosha, "Sequences, bent functions and Jacobsthal sums," *Corr*, vol. abs/1006.3112, 2010. [Online]. Available: http://arxiv.org/abs/1006.3112.

[17] C. Bracken and T. Helleseth, "Triple-error-correcting BCH-Like codes," *Corr*, vol. abs/0901.1827, 2009. [Online]. Available: http://arxiv.org/abs/0901.1827.

[18] L. Budaghyan and T. Helleseth, "New commutative semifields defined by pn multinomials," *IACR cryptology eprint archive*, vol. 2009, p. 53, 2009. [Online]. Available: http://eprint.iacr.org/2009/053.

[19] T. Helleseth and A. Kholosha, "New binomial bent function over the finite fields of odd characteristic," *Corr*, vol. abs/0907.3348, 2009. [Online]. Available: http://arxiv.org/abs/0907.3348.

[20] ——, "On the equation $x^{2^l} + x + a = 0$ over $GF(2^k)$ (extended version)," *Corr*, vol. abs/0810.4015, 2008. [Online]. Available: http://arxiv.org/abs/0810.4015.

[21] T. Helleseth, A. Kholosha, and A. Johansen, "M-sequences of different lengths with four-valued cross correlation," *Corr*, vol. abs/0712.3757, 2007. [Online]. Available: http://arxiv.org/abs/0712.3757.

[22] T. Helleseth, A. Kholosha, and G. J. Ness, "Characterization of m-sequences of lengths $2^{2k}-1$ and 2^k-1 with three-valued crosscorrelation," *Corr*, vol. abs/cs/0702139, 2007. [Online]. Available: http://arxiv.org/abs/cs/0702139.

4 Conference Papers (145)

IEEE International Symposium on Information Theory (53)

[1] L. Budaghyan, C. Carlet, T. Helleseth, and N. Li, "On the (non-)existence of APN (n, n)-functions of algebraic degree n," in *IEEE International Symposium on Information Theory, ISIT 2016, barcelona, spain, july 10-15, 2016*, PDF, 2016, pp. 480–484.

[2] T. Helleseth and A. Kholosha, "New ternary binomial bent functions," in *IEEE International Symposium on Information Theory, ISIT 2016, barcelona, spain, july 10-15, 2016*, PDF, 2016, pp. 101–104.

[3] L. Budaghyan, A. Kholosha, C. Carlet, and T. Helleseth, "Niho bent functions from quadratic o-monomials," in *Proceedings of the 2014 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2014, pp. 1827–1831.

[4] H. Hu, S. Shao, G. Gong, and T. Helleseth, "On the proof of Lin's conjecture," in *Proceedings of the 2014 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2014, pp. 1822–1826.

[5] L. Budaghyan, C. Carlet, T. Helleseth, and A. Kholosha, "Generalized bent functions and their relation to Maiorana-McFarland class," in *Proceedings of the 2012 IEEE International Symposium on Information Theory*, PDF, IEEE, Jul. 2012, pp. 1217–1220.

[6] C. Li and T. Helleseth, "New nonbinary sequence families with low correlation and large linear span," in *Proceedings of the 2012 IEEE International Symposium on Information Theory*, PDF, IEEE, Jul. 2012, pp. 1416–1420.

[7] N. Li, X. Tang, and T. Helleseth, "New classes of generalized boolean bent functions over $\mathbb{Z}_4$," in *Proceedings of the 2012 IEEE International Symposium on Information Theory*, PDF, IEEE, Jul. 2012, pp. 841–845.

[8] J. Luo and T. Helleseth, "Binary Niho sequences with four-valued cross correlations," in *Proceedings of the 2012 IEEE International Symposium on Information Theory*, PDF, IEEE, Jul. 2012, pp. 1221–1225.

[9] C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, "On the dual of bent functions with 2^r Niho exponents," in *Proceedings of the 2011 IEEE International Symposium on Information Theory*, PDF, IEEE, Jul. 2011, pp. 657–661.

[10] M. M. Hassanzadeh and T. Helleseth, "Algebraic attack on the alternating step (r, s) generator," in *Proceedings of the 2010 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2010, pp. 2493–2497.

[11] T. Helleseth and A. Kholosha, "New binomial bent functions over the finite fields of odd characteristic," in *Proceedings of the 2010 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2010, pp. 1277–1281.

[12] C. Bracken and T. Helleseth, "Triple-error-correcting BCH-like codes," in *Proceedings of the 2009 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2009, pp. 1723–1725.

[13] P. Charpin, T. Helleseth, and V. A. Zinoviev, "Divisibility properties of Kloosterman sums over finite fields of characteristic two," in *Proceedings of the 2008 IEEE International Symposium on Information Theory*, PDF, IEEE, Jul. 2008, pp. 2608–2612.

[14] T. Helleseth, A. Kholosha, and A. Johansen, "m- sequences of different lengths with four-valued cross correlation," in *Proceedings of the 2008 IEEE International Symposium on Information Theory*, PDF, IEEE, Jul. 2008, pp. 2598–2602.

[15] P. Charpin, T. Helleseth, and V. A. Zinoviev, "On binary primitive BCH codes with minimum distance 8 and exponential sums," in *Proceedings of the 2007 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2007, pp. 1976–1980.

[16] T. Helleseth, T. Kløve, and V. I. Levenshtein, "A bound for codes with given minimum and maximum distances," in *Proceedings of the 2006 IEEE International Symposium on Information Theory*, PDF, IEEE, Jul. 2006, pp. 292–296.

[17] G. J. Ness and T. Helleseth, "Three-valued crosscorrelation between m- sequences of different lengths," in *Proceedings of the 2006 IEEE International Symposium on Information Theory*, PDF, IEEE, Jul. 2006, pp. 1653–1657.

[18] P. Charpin, T. Helleseth, and V. A. Zinoviev, "Coset distribution of triple-error-correcting binary primitive BCH codes," in *Proceedings of the 2005 IEEE International Symposium on Information Theory*, PDF, IEEE, Sep. 2005, pp. 1972–1976.

[19] H. Molland and T. Helleseth, "A linear weakness in the Klimov-Shamir T-function," in *Proceedings of the 2005 IEEE International Symposium on Information Theory*, PDF, IEEE, Sep. 2005, pp. 1106–1110.

[20] S. M. Dodunekov, T. Helleseth, and V. A. Zinoviev, "On q- ary Grey-Rankin bound and codes meeting this bound," in *Proceedings of the 2004 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2004, p. 528.

[21] T. Helleseth, J. E. Mathiassen, M. Maas, and T. Segers, "Linear complexity over $\mathbb{F}_p$ of Sidel'nikov sequences," in *Proceedings of the 2004 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2004, p. 122.

[22] Y.-S. Kim, J.-W. Jang, J.-S. No, and T. Helleseth, "New p- ary bent sequences," in *Proceedings of the 2004 IEEE International Symposium on Information Theory*, IEEE, Jun. 2004, p. 498.

[23] T. Helleseth, T. Kløve, and V. I. Levenshtein, "Error-correction capability of binary linear codes," in *Proceedings of the 2003 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2003, p. 463.

[24] ——, "The simplex codes are not optimal for binary symmetric channels," in *Proceedings of the 2003 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2003, p. 161.

[25] J.-W. Jang, Y.-S. Kim, J.-S. No, and T. Helleseth, "New family of p- ary sequences with optimal correlation property and large linear span," in *Proceedings of the 2003 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2003, p. 405.

[26] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation function," in *Proceedings of the 2002 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2002, p. 182.

[27] T. Helleseth, S.-H. Kim, and J.-S. No, "Linear complexity over $\mathbb{F}_p$ and trace representation of Lempel-Cohn-Eastman sequences," in *Proceedings of the 2002 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2002, p. 180.

[28] J.-S. No, D.-J. Shin, and T. Helleseth, "On the p- ranks and characteristic polynomials of cyclic difference sets," in *Proceedings of the 2002 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2002, p. 96.

[29] T. Helleseth, T. Kløve, and V. I. Levenshtein, "Ordered orthogonal arrays of strength 4 and 5 from double-error-correcting BCH codes," in *Proceedings of the 2001 IEEE International Symposium on Information Theory*, IEEE, Jun. 2001, p. 201.

[30] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. M. Martinsen, "Ternary m- sequences with three-valued crosscorrelation function: Two new decimations," in *Proceedings of the 2000 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2000, p. 329.

[31] T. Helleseth, P. V. Kumar, and H. M. Martinsen, "A new family of ternary sequences with ideal two-level autocorrelation function," in *Proceedings of the 2000 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2000, p. 328.

[32] J.-S. No, H. Chung, H.-Y. Song, K. Yang, J.-D. Lee, and T. Helleseth, "Balanced and almost balanced binary sequences of period $p^m - 1$ with optimal autocorrelation using the polynomial $(z+1)^d + az^d + b$ over $GF(p^m)$," in *Proceedings of the 2000 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 2000, p. 299.

[33] T. Helleseth and V. A. Zinoviev, "On the coset weight distributions of the $\mathbb{Z}_4$- linear Goethals codes," in *Proceedings of the 1998 IEEE International Symposium on Information Theory*, PDF, IEEE, Aug. 1998, p. 400.

[34] K. Yang and T. Helleseth, "Kerdock codes over $\mathbb{Z}_4$ and their application to designs," in *Proceedings of the 1998 IEEE International Symposium on Information Theory*, PDF, IEEE, Aug. 1998, p. 399.

[35] T. Helleseth, T. Kløve, and V. I. Levenshtein, "On the information function of an error correcting code," in *Proceedings of the 1997 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 1997, p. 362.

[36] C. Rong and T. Helleseth, "The algebraic decoding of the $\mathbb{Z}_4$- linear Calderbank-McGuire code," in *Proceedings of the 1997 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 1997, p. 328.

[37] K. Yang and T. Helleseth, "On the generalized Hamming weights for Preparata codes over $\mathbb{Z}_4$," in *Proceedings of the 1997 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 1997, p. 205.

[38] ——, "On the minimum support weights of Goethals codes over $\mathbb{Z}_4$," in *Proceedings of the 1997 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 1997, p. 204.

[39] X. Chen, I. S. Reed, and T. Helleseth, "On Gröbner bases of the error-locator ideal of Hermitian codes," in *Proceedings of the 1995 IEEE International Symposium on Information Theory*, PDF, IEEE, Sep. 1995, p. 94.

[40] T. Helleseth and P. V. Kumar, "The algebraic decoding of the $\mathbb{Z}_4$- linear Goethals code," in *Proceedings of the 1995 IEEE International Symposium on Information Theory*, PDF, IEEE, Sep. 1995, p. 408.

[41] T. Helleseth, P. V. Kumar, O. Moreno, and A. G. Shanbhag, "Improved estimates for the minimum distance of weighted degree $\mathbb{Z}_4$ trace codes," in *Proceedings of the 1995 IEEE International Symposium on Information Theory*, PDF, IEEE, Sep. 1995, p. 283.

[42] T. Helleseth, P. V. Kumar, and A. G. Shanbhag, "New codes with the same weight distributions as the Goethals codes and the Delsarte-Goethals codes," in *Proceedings of the 1995 IEEE International Symposium on Information Theory*, PDF, IEEE, Sep. 1995, p. 274.

[43] T. Helleseth and E. Winjum, "The generalized Hamming weight of some BCH codes and related codes," in *Proceedings of the 1995 IEEE International Symposium on Information Theory*, PDF, IEEE, Sep. 1995, p. 281.

[44] A. G. Shanbhag, P. V. Kumar, and T. Helleseth, "An upper bound for extended Kloosterman sums over Galois rings," in *Proceedings of the 1995 IEEE International Symposium on Information Theory*, PDF, IEEE, Sep. 1995, p. 88.

[45] ——, "An upper bound for the aperiodic correlation of weighted-degree CDMA sequences," in *Proceedings of the 1995 IEEE International Symposium on Information Theory*, PDF, IEEE, Sep. 1995, p. 92.

[46] T. Helleseth and P. V. Kumar, "The weight hierarchy of the Kasami codes," in *Proceedings of the 1994 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 1994, p. 308.

[47] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "An upper bound for some exponential sums over Galois rings and applications," in *Proceedings of the 1994 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 1994, p. 70.

[48] P. V. Kumar, T. Helleseth, A. R. Calderbank, and J. A. Roger Hammons, "Large families of quaternary sequences with low correlation," in *Proceedings of the 1994 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 1994, p. 71.

[49] E. R. Hauge and T. Helleseth, "DeBruijn sequences, irreducible codes and cyclotomy," in *Proceedings of the 1993 IEEE International Symposium on Information Theory*, PDF, IEEE, Jan. 1993, p. 361.

[50] N. Hamada, T. Helleseth, and Ø. Ytrehus, "A new class of nonbinary codes meeting the Griesmer bound," in *Proceedings of the 1991 IEEE International Symposium on Information Theory*, PDF, IEEE, Jun. 1991, p. 9.

[51] T. Helleseth, "Legendre sums and weights of QR codes," in *Abstracts of papers of the 1990 IEEE International Symposium on Information Theory*, IEEE, Jan. 1990, p. 148.

[52] ——, "On the covering radius of cyclic linear codes and arithmetic codes," in *Abstracts of papers of the 1985 IEEE International Symposium on Information Theory*, IEEE, Jun. 1985, p. 69.

[53] ——, "Codes meeting the Griesmer bound," in *Abstracts of papers of the 1982 IEEE International Symposium on Information Theory*, IEEE, Jun. 1982, p. 52.

IEEE Information Theory Workshop (6)

[1] L. Budaghyan, C. Carlet, and T. Helleseth, "On bent functions associated to AB functions," in *Proceedings of the 2011 IEEE Information Theory Workshop*, PDF, IEEE, Oct. 2011, pp. 150–154.

[2] L. A. Bassalygo, S. M. Dodunekov, T. Helleseth, and V. A. Zinoviev, "On a new q-ary combinatorial analog of the binary Grey-Rankin bound and codes meeting this bound," in *Proceedings of the 2006 IEEE Information Theory Workshop*, PDF, IEEE, Mar. 2006, pp. 278–282.

[3] T. Helleseth and A. Kholosha, "New monomial bent functions over the finite fields of odd characteristic," in *Proceedings of the 2005 IEEE Information Theory Workshop*, PDF, IEEE, Aug. 2005, pp. 72–76.

[4] T. Helleseth, T. Kløve, and V. I. Levenshtein, "A coset weight count that proves that the simplex codes are not optimal for error correction," in *Proceedings of the 2003 IEEE Information Theory Workshop*, PDF, IEEE, Mar. 2003, pp. 234–237.

[5] T. Helleseth, P. V. Kumar, A. G. Shanbhag, and K. Yang, "On the weight hierarchy of some codes over $\mathbb{Z}_4$," in *Proceedings of the 1997 IEEE Information Theory Workshop*, IEEE, Jul. 1997, pp. 7–8.

[6] P. V. Kumar and T. Helleseth, "An expansion for the coordinates of the trace function over Galois rings," in *Proceedings of the 1997 IEEE Information Theory Workshop*, IEEE, Jul. 1997, pp. 5–6.

International Symposium on Information Theory and Its Applications (4)

[1] A. Johansen and T. Helleseth, "Crosscorrelation of m- sequences with decimation $d = (p^l+1)/(p^k+1)$," in *Proceedings of the 2008 International Symposium on Information Theory and Its Applications*, PDF, IEEE, Dec. 2008, pp. 1570–1575.

[2] T. Helleseth, T. Kløve, and V. I. Levenshtein, "The Newton radius of equidistant codes," in *Proceedings of the 1996 IEEE International Symposium on Information Theory and its applications*, vol. II, IEEE, Sep. 1996, pp. 721–722.

[3] K. Yang, T. Helleseth, P. V. Kumar, and A. G. Shanbhag, "On the generalized Hamming weights for Kerdock codes over $\mathbb{Z}_4$," in *Proceedings of the 1996 IEEE International Symposium on Information Theory and its applications*, vol. I, IEEE, Sep. 1996, pp. 39–42.

[4] T. Helleseth and Ø. Ytrehus, "Hunting for optimal codes of small dimensions," in *Proceedings of the 1990 International Symposium on Information Theory and Its Applications*, vol. 1, IEEE, Nov. 1990, pp. 29–30.

Other IEEE conferences/workshops (9)

[1] T. Helleseth, C. J. Jansen, O. Kazymyrov, and A. Kholosha, "State space cryptanalysis of the MICKEY cipher," in *Proceedings of the 2013 IEEE information theory and applications workshop (ita)*, PDF, IEEE, Feb. 2013, pp. 1–10.

[2] T. Helleseth and S. Rønjom, "Simplifying algebraic attacks with univariate analysis," in *Proceedings of the 2011 IEEE information theory and applications workshop (ita)*, PDF, IEEE, Feb. 2011, pp. 1–7.

[3] J. Luo, T. Helleseth, and A. Kholosha, "Two nonbinary sequences with six-valued cross correlation," in *Fifth international workshop on signal design and its applications in communications, iwsda '11*, PDF, IEEE, Oct. 2011, pp. 44–47.

[4] M. M. Hassanzadeh and T. Helleseth, "Algebraic attack on the more generalized clock-controlled alternating step generator," in *Proceedings of the 2010 IEEE international conference on signal processing and communications (spcom)*, PDF, IEEE, Jul. 2010, pp. 1–5.

[5] T. Helleseth and A. Kholosha, "On generalized bent functions," in *Proceedings of the 2010 IEEE information theory and applications workshop (ita)*, PDF, IEEE, Jan. 2010, pp. 1–6.

[6] T. Helleseth, "Cross-correlation of m-sequences, exponential sums and Dickson polynomials," in *Fourth international workshop on signal design and its applications in communications, iwsda '09*, PDF, IEEE, Oct. 2009, p. 2.

[7] M. M. Hassanzadeh, M. G. Parker, T. Helleseth, Y. E. Salehani, and M. R. S. Abyaneh, "Differential distinguishing attack on the Shannon stream cipher based on fault analysis," in *Proceedings of the 2008 IEEE international symposium on telecommunications*, PDF, IEEE, Aug. 2008, pp. 671–676.

[8] P. V. Kumar, H. F. F. Lu, T. Helleseth, and D.-J. Shin, "On the large family of low correlation quaternary sequences $S(2)$," in *Proceedings of the 2000 IEEE international conference on personal wireless communications*, PDF, IEEE, Dec. 2000, pp. 33–37.

[9] T. Helleseth, T. Kløve, and Ø. Ytrehus, "Codes, weight hierarchies, and chains," in *Proceedings of the iccs/isita '92 communications on the move*, PDF, vol. 2, IEEE, Nov. 1992, pp. 608–612.

Finite Fields and Related Topics (5)

[1] T. Helleseth, P. V. Kumar, and A. G. Shanbhag, "Exponential sums over Galois rings and their applications," in *Finite fields and applications*, S. D. Cohen and H. Niederreiter, Eds., ser. London Mathematical Society Lecture Note Series, PDF, vol. 233, New York: Cambridge University Press, 1996, pp. 109–128.

[2] C. Rong and T. Helleseth, "Use characteristic sets to decode cyclic codes up to actual minimum distance," in *Finite fields and applications*, S. D. Cohen and H. Niederreiter, Eds., ser. London Mathematical Society Lecture Note Series, PDF, vol. 233, New York: Cambridge University Press, 1996, pp. 297–312.

[3] X. Chen, I. S. Reed, T. Helleseth, and T.-K. Truong, "Algebraic decoding of cyclic codes: A polynomial ideal point of view," in *Finite fields: Theory, applications, and algorithms*, G. L. Mullen and P. J.-S. Shiue, Eds., ser. Contemporary Mathematics, PDF, vol. 168, Providence, Rhode Island: American Mathematical Society, 1994, pp. 15–22.

[4] N. Hamada and T. Helleseth, "A characterization of some ternary codes meeting the Griesmer bound," in *Finite fields: Theory, applications, and algorithms*, G. L. Mullen and P. J.-S. Shiue, Eds., ser. Contemporary Mathematics, PDF, vol. 168, Providence, Rhode Island: American Mathematical Society, 1994, pp. 139–150.

[5] ——, "A characterization of some minihypers and codes meeting the Griesmer bound over GF(q), $q > 9$," in *Finite fields, coding theory, and advances in communications and computing*, G. L. Mullen and P. J.-S. Shiue, Eds., ser. Lecture Notes in Pure and Applied Mathematics, PDF, vol. 141, New York: Marcel Dekker, Inc., 1993, pp. 105–122.

Springer Lecture Notes in Computer Science/Mathematics (14)

[1] T. Helleseth and A. Kholosha, "m- sequences of lengths $2^{2k} - 1$ and $2^k - 1$ with at most four-valued cross correlation," in *Sequences and their applications - seta 2008*, S. W. Golomb, M. G. Parker, A. Pott, and A. Winterhof, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 5203, Berlin: Springer-Verlag, 2008, pp. 106–120.

[2] C. J. A. Jansen, T. Helleseth, and A. Kholosha, "Cascade jump controlled sequence generator and Pomaranch stream cipher," in *New stream cipher designs - the estream finalists*, M. Robshaw and O. Billet, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 4986, Berlin: Springer-Verlag, 2008, pp. 224–243.

[3] T. Helleseth and A. Kholosha, "On the dual of monomial quadratic p- ary bent functions," in *Sequences, subsequences, and consequences*, S. Golomb, G. Gong, T. Helleseth, and H.-Y. Song, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 4893, Berlin: Springer-Verlag, 2007, pp. 50–61.

[4] S. Rønjom, G. Gong, and T. Helleseth, "A survey of recent attacks on the filter generator," in *Applied algebra, algebraic algorithms and error-correcting codes*, S. Boztas and H.-F. Lu, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 4851, Berlin: Springer-Verlag, 2007, pp. 7–17.

[5] ——, "On attacks on filtering generators using linear subspace structures," in *Sequences, subsequences, and consequences*, S. Golomb, G. Gong, T. Helleseth, and H.-Y. Song, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 4893, Berlin: Springer-Verlag, 2007, pp. 204–217.

[6] S. Rønjom and T. Helleseth, "Attacking the filter generator over $GF(2^m)$," in *Arithmetic of finite fields*, C. Carlet and B. Sunar, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 4547, Berlin: Springer-Verlag, 2007, pp. 264–275.

[7] ——, "The linear vector space spanned by the nonlinear filter generator," in *Sequences, subsequences, and consequences*, S. Golomb, G. Gong, T. Helleseth, and H.-Y. Song, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 4893, Berlin: Springer-Verlag, 2007, pp. 169–183.

[8] X. Tang, T. Helleseth, L. Hu, and W. Jiang, "A new family of Gold-like sequences," in *Sequences, subsequences, and consequences*, S. Golomb, G. Gong, T. Helleseth, and H.-Y. Song, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 4893, Berlin: Springer-Verlag, 2007, pp. 62–69.

[9] H. Molland, J. E. Mathiassen, and T. Helleseth, "Improved fast correlation attack using low rate codes," in *Cryptography and coding*, K. G. Paterson, Ed., ser. Lecture Notes in Computer Science, PDF, vol. 2898, Berlin: Springer-Verlag, 2003, pp. 67–81.

[10] H. G. Schaathun and T. Helleseth, "Separating and intersecting properties of BCH and Kasami codes," in *Cryptography and coding*, K. G. Paterson, Ed., ser. Lecture Notes in Computer Science, PDF, vol. 2898, Berlin: Springer-Verlag, 2003, pp. 52–65.

[11] T. Helleseth, "Codes over $\mathbb{Z}_4$," in *Computational discrete mathematics: Advanced lectures*, H. Alt, Ed., ser. Lecture Notes in Computer Science, PDF, vol. 2122, Berlin: Springer-Verlag, 2001, pp. 47–55.

[12] ——, "Correlation of m- sequences and related topics," in *Sequences and their applications*, C. Ding, T. Helleseth, and H. Niederreiter, Eds., ser. Discrete Mathematics and Theoretical Computer Science, Berlin: Springer-Verlag, 1999, pp. 49–66.

[13] T. Helleseth, T. Kløve, and Ø. Ytrehus, "Generalizations of the Griesmer bound," in *Error control, cryptology, and speech compression*, A. Chmora and S. B. Wicker, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 829, Berlin: Springer-Verlag, 1994, pp. 41–52.

[14] N. Hamada and T. Helleseth, "On a characterization of some minihypers in PG(t, q) ($q = 3$ or 4) and its applications to error-correcting codes," in *Coding theory and algebraic geometry*, H. Stichtenoth and M. A. Tsfasman, Eds., ser. Lecture Notes in Mathematics, PDF, vol. 1518, Berlin: Springer-Verlag, 1992, pp. 43–62.

SEquence and Their Applications - SETA (9)

[1] Y. Xia, T. Helleseth, and G. Wu, "A note on cross-correlation distribution between a ternary m- sequence and its decimated sequence," in *Sequences and their applications - seta 2014*, K.-U. Schmidt and A. Winterhof, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 8865, Berlin: Springer-Verlag, 2014, pp. 249–259.

[2] G. Gong, T. Helleseth, H. Hu, and C. Li, "New three-valued Walsh transforms from decimations of Helleseth-Gong sequences," in *Sequences and their applications - seta 2012*, T. Helleseth and J. Jedwab, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 7280, Berlin: Springer-Verlag, 2012, pp. 327–337.

[3] T. Helleseth and A. Kholosha, "Sequences, bent functions and jacobsthal sums," in *Sequences and their applications - seta 2010*, C. Carlet and A. Pott, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 6338, Berlin: Springer-Verlag, 2010, pp. 416–429.

[4] L. Budaghyan and T. Helleseth, "New perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p," in *Sequences and their applications - seta 2008*, S. W. Golomb, M. G. Parker, A. Pott, and A. Winterhof, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 5203, Berlin: Springer-Verlag, 2008, pp. 403–414.

[5] X. Tang, T. Helleseth, and A. Johansen, "On the correlation distribution of Kerdock sequences," in *Sequences and their applications - seta 2008*, S. W. Golomb, M. G. Parker, A. Pott, and A. Winterhof, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 5203, Berlin: Springer-Verlag, 2008, pp. 121–129.

[6] T. Helleseth, C. J. A. Jansen, S. Khazaei, and A. Kholosha, "Security of jump controlled sequence generators for stream ciphers," in *Sequences and their applications - seta 2006*, G. Gong, T. Helleseth, H.-Y. Song, and K. Yang, Eds., ser. Lecture Notes in Computer Science, PDF, vol. 4086, Berlin: Springer-Verlag, 2006, pp. 141–152.

[7] T. Helleseth, "On the crosscorrelation of m- sequences and related sequences with ideal autocorrelation," in *Sequences and their applications - seta '01*, T. Helleseth, P. V. Kumar, and K. Yang, Eds., ser. Discrete Mathematics and Theoretical Computer Science, Berlin: Springer-Verlag, 2002, pp. 34–45.

[8] T. Helleseth and K. Yang, "On binary sequences of period $n = p^m - 1$ with optimal autocorrelation," in *Sequences and their applications - seta '01*, T. Helleseth, P. V. Kumar, and K. Yang, Eds., ser. Discrete Mathematics and Theoretical Computer Science, Berlin: Springer-Verlag, 2002, pp. 209–217.

[9] T. Helleseth, P. V. Kumar, H. M. Martinsen, and O. N. Vassbakk, "Correlation distribution of the quaternary Kasami sequences," in *Sequences and Their Applications*, C. Ding, T. Helleseth, and H. Niederreiter, Eds., ser. Discrete Mathematics and Theoretical Computer Science, Berlin: Springer-Verlag, 1999, pp. 240–253.

CRYPTO/EUROCRYPT/ASIACRYPT (3)

[1] S. Rønjom, N. G. Bardeh, and T. Helleseth, "Yoyo tricks with AES," in *Advances in cryptology - ASIACRYPT 2017 - 23rd international conference on the theory and applications of cryptology and information security, hong kong, china, december 3-7, 2017, proceedings, part I*, PDF, 2017, pp. 217–243.

[2] H. Molland and T. Helleseth, "An improved correlation attack against irregular clocked and filtered keystream generators," in *Advances in cryptology - CRYPTO 2004*, M. Franklin, Ed., ser. Lecture Notes in Computer Science, PDF, vol. 3152, Berlin: Springer-Verlag, 2004, pp. 373–389.

[3] T. Helleseth and T. Johansson, "Universal hash functions from exponential sums over finite fields and Galois rings," in *Advances in cryptology - CRYPTO '96*, N. Koblitz, Ed., ser. Lecture Notes in Computer Science, PDF, vol. 1109, Berlin: Springer-Verlag, 1996, pp. 31–44.

International Workshop on Algebraic and Combinatorial Coding Theory (8)

[1] P. Charpin, T. Helleseth, and V. A. Zinoviev, "On binary BCH codes with minimal distance 8 and Kloosterman sums," in *Ninth International Workshop on Algebraic and Combinatorial Coding Theory*, PDF, Sofia: Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 2004, pp. 90–94.

[2] T. Helleseth, "On some ternary m- sequences with good autocorrelation and crosscorrelation," in *Seventh International Workshop on Algebraic and Combinatorial Coding Theory*, Sofia: Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 2000, pp. 168–171.

[3] T. Helleseth and V. A. Zinoviev, "On $\mathbb{Z}_4$- linear Goethals codes, Kloosterman sums and Dickson polynomials," in *Seventh International Workshop on Algebraic and Combinatorial Coding Theory*, PDF, Sofia: Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 2000, pp. 172–176.

[4] ——, "On coset weight distribution of the $\mathbb{Z}_4$- linear Goethals codes," in *Sixth International Workshop on Algebraic and Combinatorial Coding Theory*, PDF, Moskva: Mezhdunarodnyj Tsentr Nauchnoj i Tekhnicheskoj Informatsii, 1998, pp. 130–134.

[5] I. Boukliev, S. M. Dodunekov, T. Helleseth, and Ø. Ytrehus, "Two new binary optimal 8-dimensional codes," in *Fifth International Workshop on Algebraic and Combinatorial Coding Theory*, Shumen: Unicorn, 1996, pp. 66–67.

[6] T. Helleseth and P. V. Kumar, "The weight hierarchy of semiprimitive codes," in *Fourth International Workshop on Algebraic and Combinatorial Coding Theory*, 1994, pp. 94–97.

[7] N. Hamada and T. Helleseth, "On the construction of $[q^3 - q^2 + 1, 4, q^3 - 2q^2 + q;\ q]$- codes meeting the Griesmer bound," in *International Workshop on Algebraic and Combinatorial Coding Theory*, Shumen: Hermes & Hermes, 1992, pp. 80–83.

[8] T. Helleseth, T. Kløve, and Ø. Ytrehus, "Codes and the chain condition," in *International Workshop on Algebraic and Combinatorial Coding Theory*, Shumen: Hermes & Hermes, 1992, pp. 88–91.

International Workshop on Optimal Codes and Related Topics (8)

[1] A. Johansen, T. Helleseth, and X. Tang, "The correlation distribution of sequences of period $2(2^n - 1)$," in *Optimal codes and related topics, fifth international workshop*, PDF, Sofia: Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 2007, pp. 93–99.

[2] T. Helleseth, A. Kholosha, and G. J. Ness, "On the correlation distribution of the Coulter-Matthews decimation," in *Optimal codes and related topics, fourth international workshop*, PDF, Sofia: Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 2005, pp. 190–195.

[3] N. Hamada and T. Helleseth, "Codes and minihypers," in *Third euroworkshop on optimal codes and related topics*, PDF, Sofia: Institute of Mathematics and Informatics, 2001, pp. 79–84.

[4] T. Helleseth, "Sequences with ideal autocorrelation," in *Third euroworkshop on optimal codes and related topics*, PDF, Sofia: Institute of Mathematics and Informatics, 2001, pp. 91–95.

[5] T. Helleseth, C. Rong, and K. Yang, "Some 3-designs from Goethals codes over $\mathbb{Z}_4$," in *Optimal codes and related topics, second international workshop*, PDF, Sofia: Institute of Mathematics and Informatics, 1998, pp. 84–89.

[6] N. Hamada and T. Helleseth, "A characterization of $\{3v_1 + v_4, 3v_0 + v_3;\ 4, 3\}$- minihypers and projective ternary $[78, 5, 51]$ codes," in *International workshop on optimal codes and related topics*, PDF, Shumen: Panorama, 1995, pp. 61–64.

[7] ——, "The nonexistence of ternary $[270, 6, 179]$ codes and $[309, 6, 205]$ codes," in *International workshop on optimal codes and related topics*, PDF, Shumen: Panorama, 1995, pp. 65–68.

[8] T. Helleseth and P. V. Kumar, "A new proof of the minimum distance of the quaternary Preparata code and Goethals code," in *International workshop on optimal codes and related topics*, PDF, Shumen: Panorama, 1995, pp. 69–73.

Annual Allerton Conference on Communication, Control, and Computing (5)

[1] A. Chang, T. Helleseth, and P. V. Kumar, "Further results on a conjectured 2- level autocorrelation sequence," in *Proceedings of the thirty-sixth annual allerton conference on communication, control, and computing*, Monticello, Illinois, Sep. 1998, pp. 598–599.

[2] T. Helleseth and V. A. Zinoviev, "On the coset weight distributions of $\mathbb{Z}_4$- linear Goethals codes and some relations to Kloosterman sums," in *Proceedings of the thirty-sixth annual allerton conference on communication, control, and computing*, Monticello, Illinois, Sep. 1998, pp. 593–597.

[3] T. Helleseth, P. V. Kumar, C. Rong, and K. Yang, "On infinite families of 3- designs from Preparata codes and related codes over $\mathbb{Z}_4$," in *Proceedings of the thirty-fifth annual allerton conference on communication, control, and computing*, Monticello, Illinois, Sep. 1997, pp. 395–403.

[4] T. Helleseth, P. V. Kumar, A. G. Shanbhag, and K. Yang, "On Galois rings: A Hasse-Davenport-type relation for $\mathbb{Z}_4$ Kerdock code and applications," in *Proceedings of the thirty-third annual allerton conference on communication, control, and computing*, Monticello, Illinois, Oct. 1995, pp. 480–482.

[5] A. G. Shanbhag, P. V. Kumar, and T. Helleseth, "Improved binary codes and sequence families from $\mathbb{Z}_4$- linear codes," in *Proceedings of the thirty-second annual allerton conference on communication, control, and computing*, Monticello, Illinois, Sep. 1994.

Other Collections and Proceedings (21)

[1] L. Budaghyan, T. Helleseth, N. Li, and B. Sun, "Some results on the known classes of quadratic APN functions," in *Codes, cryptology and information security - second international conference, C2SI 2017, rabat, morocco, april 10-12, 2017, proceedings - in honor of claude carlet*, PDF, 2017, pp. 3–16.

[2] A. Alahmadi, T. Helleseth, N. M. Muthana, A. Almuzaini, and P. Solé, "Irreducible cyclic $\mathbb{Z}_4$ - codes and allied sequences," in *Seventh international workshop on signal design and its applications in communications, IWSDA 2015, bengaluru, india, september 14-18, 2015*, PDF, 2015, pp. 160–164.

[3] N. Li, Z. Zhou, and T. Helleseth, "On a conjecture about a class of optimal ternary cyclic codes," in *Seventh international workshop on signal design and its applications in communications, IWSDA 2015, bengaluru, india, september 14-18, 2015*, PDF, 2015, pp. 62–65.

[4] T. Helleseth, A. Kholosha, and S. Mesnager, "Niho bent functions and Subiaco hyperovals," in *Theory and applications of finite fields*, M. Lavrauw, G. L. Mullen, S. Nikova, D. Panario, and L. Storme, Eds., ser. Contemporary Mathematics, PDF, vol. 579, Providence, Rhode Island: American Mathematical Society, 2012, pp. 91–101.

[5] L. Budaghyan and T. Helleseth, "Planar functions and commutative semifields," in *Nilcrypt'10*, O. Grošek, T. Helleseth, A. Kholosha, and K. Nemoga, Eds., ser. Tatra Mountains Mathematical Publications, PDF, vol. 45, Bratislava: Mathematical Institute, Slovak Academy of Sciences, 2010, pp. 15–25.

[6] M. M. Hassanzadeh and T. Helleseth, "Algebraic attack on the second class of modified alternating k- generators," in *Norwegian information security conference nisk 2010*, P. Bours, Ed., PDF, Trondheim: Tapir Akademisk Forlag, 2010, pp. 12–20.

[7] T. Helleseth, "Linear and nonlinear sequences and applications to stream ciphers," in *Recent trends in cryptography*, ser. Contemporary Mathematics, I. Luengo, Ed., vol. 477, PDF, Providence, Rhode Island: American Mathematical Society, 2009, pp. 21–46.

[8] T. Helleseth, M. Hojsık, and S. Rønjom, "Algebraic attacks on filter and combiner generators," in *Enhancing cryptographic primitives with techniques from error correcting codes*, ser. NATO Science for Peace and Security Series, Sub-Series D: Information and Communication Security, B. Preneel, S. Dodunekov, V. Rijmen, and S. Nikova, Eds., vol. 23, PDF, Amsterdam: IOS Press, 2009, pp. 39–48.

[9] T. Helleseth, G. Kyureghyan, G. J. Ness, and A. Pott, "On a family of perfect nonlinear binomials," in *Boolean functions in cryptology and information security*, ser. NATO Science for Peace and Security Series, Sub-Series D: Information and Communication Security, B. Preenel and O. A. Logachev, Eds., vol. 18, PDF, Amsterdam: IOS Press, 2008, pp. 126–138.

[10] C. Jansen, T. Helleseth, and A. Kholosha, "Cascade jump controlled sequence generator and pomaranch stream cipher," in *New stream cipher designs - the eSTREAM finalists*, 2008, pp. 224–243. DOI: 10.1007/978-3-540-68351-3_17.

[11] T. Helleseth and A. Kholosha, "Monomial bent functions over the finite fields of odd characteristic," in *Coding theory and cryptography*, S. Nikova, B. Preneel, L. Storme, and J. A. Thas, Eds., PDF, Brussels: Koninklijke Vlaamse Academie van Belgie voor Wetenschappen en Kunsten, 2006, pp. 43–48.

[12] T. Helleseth, J. Lahtonen, and P. Rosendahl, "On certain equations over finite fields and cross-correlations of m- sequences," in *Coding, cryptography and combinatorics*, K. Feng, H. Niederreiter, and C. Xing, Eds., ser. Progress in Computer Science and Applied Logic, PDF, vol. 23, Berlin: Springer-Verlag, 2004, pp. 169–176.

[13] T. Helleseth, "Pairs of m- sequences with a six-valued crosscorrelation," in *Mathematical properties of sequences and other combinatorial structures*, ser. The Kluwer International Series in Engineering and Computer Science, J.-S. No, H.-Y. Song, T. Helleseth, and P. V. Kumar, Eds., PDF, Dordrecht: Kluwer Academic Publishers, 2003, pp. 1–6.

[14] T. Helleseth, T. Kløve, and V. I. Levenshtein, "Binary even-weight codes for error correction," in *International conference on software, telecommunications and computer networks - softcom 2003*, PDF, University of Split, Croatia, Oct. 2003, pp. 822–826.

[15] Y.-S. Kim, J.-W. Jang, J.-S. No, and T. Helleseth, "On p- ary bent functions defined on finite fields," in *Mathematical properties of sequences and other combinatorial structures*, ser. The Kluwer International Series in Engineering and Computer Science, J.-S. No, H.-Y. Song, T. Helleseth, and P. V. Kumar, Eds., Dordrecht: Kluwer Academic Publishers, 2003, pp. 65–76.

[16] K. Shum, P. V. Kumar, and T. Helleseth, "The L-function of Gold exponential sum," in *Finite fields and applications*, D. Jungnickel and H. Niederreiter, Eds., Berlin: Springer-Verlag, 2001, pp. 418–427.

[17] T. Helleseth and P. V. Kumar, "Codes and sequences over $\mathbb{Z}_4$ - a tutorial overview," in *Difference sets, sequences and their correlation properties*, ser. NATO Science Series, Series C: Mathematical and Physical Sciences, A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, Eds., vol. 542, Dordrecht: Kluwer Academic Publishers, 1999, pp. 195–225.

[18] T. Helleseth and T. Kløve, "The weight hierarchies of some product codes," in *Arithmétique, géométrie, et algorithmique dans la théorie des codes correcteurs d'erreurs*, Pointe-á-Pitre, Guadeloupe, Apr. 1996.

[19] T. Helleseth, in *A collection of contributions in honour of jack van lint*, ser. Topics in Discrete Mathematics, P. J. Cameron and H. C. van Tilborg, Eds., vol. 7, Reprint of [15], Amsterdam: North-Holland, 1992, pp. 265–271.

[20] ——, "Legendre sums and codes related to QR codes," in *Fourth joint swedish-soviet international workshop on information theory*, Lund: Studentlitteratur, 1989, pp. 218–222.

[21] ——, "On the covering radius of cyclic linear codes and arithmetic codes," in *Kiberneticheskiy sbornik, novaya seriya*, O. Lupanov and O. Kasim-Zade, Eds., vol. 25, Russian translation of [3], PDF, Moscow: Mir, 1988, pp. 64–84.

5 List of Co-authors (129)

The indices of co-authors in the following list is available at this link.

1. Adel Alahmadi
2. Hussain Alhazmi
3. Shakir Ali
4. Atiqah Almuzaini
5. Ross J. Anderson
6. K. T. Arasu
7. Navid Ghaedi Bar
8. Leonid A. Bassaly
9. Iliya Boukliev
10. Carl Bracken
11. Lilya Budaghyan
12. Han Cai
13. A. Robert Calderb
14. Claude Carlet
15. Anchung Chang
16. Samuel T. Chanso
17. Pascale Charpin
18. Shaoping Chen
19. Xuemin Chen
20. Habong Chung
21. Cunsheng Ding
22. Hans Dobbertin
23. Stefan M. Dodune
24. Iwan M. Duursma
25. Cuiling Fan
26. Pingzhi Fan
27. Patrick Felke
28. Peter Gaal
29. Solomon W. Golo
30. Guang Gong
31. Noboru Hamada
32. A. Roger Hammon Jr.
33. M. Anwar Hasan
34. Mehdi M. Hassanzadeh
35. Erik R. Hauge
36. Rola Hijazi
37. Michal Hojsík
38. Henk D. L. Hollma
39. Seokbeom Hong
40. Bo Hove
41. Honggang Hu
42. Lei Hu
43. Ji-Woong Jang
44. Cees J. A. Jansen
45. Jonathan Jedwab
46. Wenjie Jia
47. Wenfeng Jiang
48. Aina Johansen
49. Thomas Johansson
50. Oleksandr Kazymyrov
51. Shahram Khazaei
52. Alexander Kholos
53. Sang-Hyo Kim
54. Young-Sik Kim
55. Torleiv Kløve
56. P. Vijay Kumar
57. Jyrki T. Lahtonen
58. Kwok-Yan Lam
59. Jung-Do Lee
60. Vladimir I. Levenshtein
61. Chaoyun Li
62. Chunlei Li
63. Ming Li
64. Nian Li
65. Jinquan Luo
66. M. Maas
67. Nikolai L. Manev

68. H. M. Martinsen
69. Halvard Martinsen
70. John Erik Mathias
71. H. F. Mattson
72. Gary McGuire
73. Sihem Mesnager
74. Håvard Molland
75. Oscar Moreno
76. Najat M. Muthana
77. Johannes Mykkelt
78. Geir Jarle Ness
79. Harald Niederreite
80. Jong-Seon No
81. Hosung Park
82. Matthew G. Parke
83. Bart Preneel
84. Yanfeng Qi
85. Kalle Ranto
86. Irving S. Reed
87. Chunming Rong
88. Sondre Rønjom
89. Petri Rosendahl
90. Daniel Sandberg
91. Dilip V. Sarwate
92. Hans Georg Schaathun
93. T. Segers
94. Weijuan Shan
95. Abhijit G. Shanbh
96. Shuai Shao
97. Dong-Joon Shin
98. Patrick Solé
99. Hong-Yeop Song
100. Bo Sun
101. Zhimin Sun
102. T. W. Sze
103. Pan Tan
104. Chunming Tang
105. Deng Tang
106. Xiaohu Tang
107. Henk C. A. van Tilborg
108. Trieu-Kien Truong
109. Ziran Tu
110. Parampalli Udaya
111. José Felipe Voloc
112. X. Wang
113. Zeying Wang
114. Jinming Wen
115. Gaofei Wu
116. Yongbo Xia
117. Qing Xiang
118. Zibi Xiao
119. Chaoping Xing
120. Xiaofang Xu
121. Kyeongcheol Yan
122. Yang Yang
123. Øyvind Ytrehus
124. Xiangyong Zeng
125. Dan Zhang
126. Xiaosong Zhang
127. Yuqing Zhang
128. Zhengchun Zhou
129. Victor A. Zinoviev