List of Publications: Professor Cunsheng Ding

Research Monographs

1. C. Ding, **Codes from Difference Sets**, World Scientific, 2015. [Cover page here] [Corrections are here]
2. T. Cusick, C. Ding, and A. Renvall, **Stream Ciphers and Number Theory**, North-Holland Mathematical Library 55, Elsevier/North-Holland, 1998. Revised edition, The North-Holland Mathematical Library, Vol. 66, 2004. [Cover page here]
3. C. Ding, D. Pei and A. Salomaa, **Chinese Remainder Theorem: Applications in Computing, Coding and Cryptography,** Singapore: World Scientific, 1996. [Cover page here]
4. C. Ding and G. Xiao, **Stream Ciphers and Their Applications** (In Chinese), Beijing: National Defense Press, 1994. [Cover page here]
5. C. Ding, G. Xiao, and W. Shan, **The Stability Theory of Stream Ciphers,** LNCS 561, Heidelberg: Springer-Verlag, 1991. [Cover page here]

Edited Books

1. C. P. Rangan and C. Ding, *Progress in Cryptography – INDOCRYPT 2001,* Lecture Notes in Computer Science 2247, Springer Verlag, 2001.
2. C. Ding, T. Helleseth, and H. Niederreiter, *Sequences and Their Applications - Proceedings of SETA'98,* London: Springer-Verlag, 1999.

Edited Journal Special Issues

1. Special Issue on Special Functions and Codes, *Cryptography and Communications*, Vol. 9, No. 1, Jan. 2017, Springer, Heidelberg, Co-edited with Z. Zhou.
2. Special Issue on Cryptology, *Internal Journal on Foundations of Computer Science*, Vol. 22, No. 6, September 2011, World Scientific, Singapore, Co-edited with Q. Wang.
3. Special Issue on Coding Theory and Cryptography, *Designs, Codes and Cryptography,* Vol. 48, No. 2, Springer-Verlag, 2008, co-edited with T. Helleseth and O. Ytrehus.
4. Special Issue in Coding Theory and Cryptography, *Journal of Complexity,* Vol. 20, Nos. 2–3, Academic Press, 2004, Co-edited with C. Xing.
5. Special Issue on Cryptography, *Theoretical Computer Science*, Vol. 226, No. 1, Elsevier, September 1999. Guest Editor.
6. Special Issue on Cryptology, *Information and Computation*, Vol. 151, No. 1, June 1999, Academic Press, USA. Guest Editor.

Refereed Journal Papers

1. C. Ding, Infinite families of 3-designs from a type of five-weight code, **Designs, Codes and Cryptography,** to appear. PDF file
2. C. Ding, H. Liu and V. D. Tonchev, All binary linear codes that are invariant under $\mathrm{PSL}_2(n)$, **IEEE Trans. Information Theory,** to appear. PDF file
3. C. Ding, A sequence construction of cyclic codes over $\mathrm{GF}(q)$, **Cryptography and Communications**, to appear. PDF file
4. C. Ding, An infinite family of Steiner systems $S(2, 4, 2^m)$ from cyclic codes, **J. Combinatorial Designs,** to appear. PDF file
5. S. Li, C. Ding, M. Xiong and G. Ge, Narrow-sense projective BCH codes of length $(q^m - 1)/(q - 1)$, **IEEE Trans. Information Theory,** Vol. 63, No. 11, pp. 7219–36, Nov. 2017. PDF file
6. C. Ding and C. Li, Infinite families of 2-designs and 3-designs from linear codes, **Discrete Math.**, Vol. 340, No. 10, pp. 2415-2431, Oct. 2017. PDF file
7. Z. Heng, C. Ding and Q. Yue, New constructions of asymptotically optimal codebooks with multiplicative characters, **IEEE Trans. Information Theory,** Vol. 63, No. 10, pp. 6179–6187, Oct. 2017. PDF file
8. S. Li, C. Li, C. Ding and H. Liu, Two families of LCD BCH codes, **IEEE Trans. Information Theory,** Vol. 63, No. 9, pp. 5699–5717, Sept. 2017. PDF file
9. H. Liu, C. Ding, and C. Li, Dimensions of three types of BCH codes over $\mathrm{GF}(q)$, **Discrete Math.**, Vol. 340, No. 8, pp. 1910–1927, August 2017. PDF file
10. D. Wu, P. Yuan, C. Ding, and Y. Ma, Permutation trinomials over $\mathbb{F}_{2^m}$, **Finite Fields and Their Applications,** Vol. 46, pp. 38–56, July 2017. PDF file
11. C. Li, C. Ding, and S. Li, LCD cyclic codes over finite fields, **IEEE Trans. Information Theory,** Vol. 63, No. 7, pp. 4344–4356, July 2017. PDF file
12. C. Ding, C. Fan and Z. Zhou, The dimension and minimum distance of two classes of primitive BCH codes, **Finite Fields and Their Applications,** Vol. 45, pp. 237-263, May 2017. PDF file
13. C. Ding, A construction of binary linear codes from Boolean functions, **Discrete Mathematics**, Vol. 339, No. 9, pp. 2288–2303, 2016. PDF file
14. M. Xiong, N. Li, Z. Zhou and C. Ding, Weight distribution of cyclic codes with arbitrary number of generalized Niho type zeroes, **Designs, Codes and Cryptography,** Vol. 78, No. 3, pp. 713–730, March 2016. PDF file
15. C. Ding, C. Li, N. Li and Z. Zhou, Three-weight cyclic codes and their weight distributions, **Discrete Mathematics,** Vol. 339, no. 2, pp.415–427, Feb. 2016. PDF file
16. C. Xiang, C. Ding and S. Mesnager, Optimal codebooks from binary codes meeting the Levenshtein bound, **IEEE Trans. Information Theory,** Vol. 61, No. 12, pp. 6526–6535, Dec. 2015. PDF file
17. K. Ding and C. Ding, A class of two-weight and three-weight codes and their applications in secret sharing, **IEEE Trans. Information Theory,** Vol. 61, No. 11, pp. 5835–5842, Nov. 2015. PDF file
18. C. Ding, Parameters of several classes of BCH codes, **IEEE Trans. Information Theory,** Vol. 61, No. 10, pp. 5322–5330, Oct. 2015. PDF file

19. C. Ding, A. Pott, and Q. Wang, Skew Hadamard difference sets from the Dickson polynomials of order 7, **J. Combinatorial Designs**, Vol. 23, No. 10, pp. 436–461, Oct. 2015. PDF file
20. C. Ding, Linear codes from some 2-designs, **IEEE Trans. Information Theory**, Vol. 60, No. 6, pp. 3265–3275, June 2015. PDF file
21. C. Ding, X. Du and Z. Zhou, The Bose and minimum distance of a class of BCH codes, **IEEE Trans. Information Theory,** Vol. 61, No. 5., pp. 2351–2356, May 2015. PDF file
22. C. Ding, L. Qu, Q. Wang, J. Yuan and P. Yuan, Permutation trinomials over finite fields with even characteristic, **SIAM J. Discrete Mathematics,** Vol. 29, No. 1, pp. 79–92, 2015. PDF file
23. K. Ding and C. Ding, Binary linear codes with three weights, **IEEE Communication Letters,** Vol. 18, No. 11, pp. 1879–1882, November 2014. PDF file
24. Z. Zhou, C. Ding and N. Li, New families of codebooks achieving the Levenstein bound, **IEEE Trans. Information Theory,** Vol. 60, No. 11, pp. 7382–7386, November 2014. PDF file
25. 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, November 2014. PDF file
26. C. Ding, A. Pott and Q. Wang, Constructions of almost difference sets, **Designs, Codes and Cryptography,** Vol. 72, No. 3, pp. 581–592, September 2014. PDF file
27. P. Yuan and C. Ding, Permutation polynomials of the form $L(x) + S_{2k}^a + S_{2k}^b$ over $\mathbb{F}_{q^{3k}}$, **Finite Fields and Their Applications,** Vol. 29, pp. 106–117, September, 2014. PDF file Correction here
28. 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, August 2014. PDF file
29. L. Qu and C. Ding, Dickson polynomials of the second kind that permutes Z_m, **SIAM J. Discrete Mathematics,** Vol. 28, No. 2, pp. 722–735, June 2014. PDF file
30. C. Ding, Q. Wang, and M. Xiong, Three new families of zero-difference balanced functions with applications, **IEEE Trans. Information Theory**, Vol. 60, No. 4, pp. 2407–2413, April 2014. PDF file
31. P. Yuan and C. Ding, Further results on permutation polynomials over finite fields, **Finite Fields and Their Applications**, Vol. 27, pp. 88–103, 2014. PDF file Correction here
32. C. Ding and Z. Zhou, Binary cyclic codes from explicit polynomials over GF(2^m), **Discrete Mathematics**, Vol. 321, pp. 76–89, April 2014. PDF file
33. Z. Zhou and C. Ding, A class of three-weight cyclic codes, **Finite Fields and Their Applications,** Vol. 25, pp. 79–93, Jan. 2014. PDF file
34. C. Ding, Cyclic codes from some monomials and trinomials, **SIAM J. Discrete Mathematics**, Vol. 27, No. 4, pp. 1977–1994, December 2013. PDF file
35. C. Ding, Y. Gao, Z. Zhou, Five families of three-weight cyclic codes and their duals, **IEEE Trans. Information Theory,** Vol. 59, No. 12, pp. 7940–7946, December 2013. PDF file
36. Z. Zhou, C. Ding, Seven families of three-weight cyclic codes, **IEEE Trans. Communications,** Vol. 61, No. 10, pp. 4120–4126, November 2013. PDF file
37. Z. Zhou, C. Ding, J. Luo and A. Zhang, A family of five-weight cyclic codes and their weight distributions, **IEEE Trans. Information Theory,** Vol. 59, No. 10, pp. 6674–6682, Oct. 2013. PDF file
38. J. Yang, M. Xiong, C. Ding, J. Luo, Weight distribution of a class of cyclic codes with arbitrary number of zeros, **IEEE Trans. Information Theory**, Vol. 59, No. 9, pp. 5985–5993, Sept. 2013. PDF file

39. Z. Zhou, A. Zhang, C. Ding, M. Xiong, The weight enumerator of three families of cyclic codes, **IEEE Trans. Information Theory,** Vol. 59, No. 9, pp. 6002–6009, Sept. 2013. PDF file
40. C. Ding, T. Helleseth, Optimal ternary cyclic codes from monomials, **IEEE Trans. Information Theory**, Vol. 59, No. 9, pp. 5898–5904, Sept. 2013. PDF file
41. C. Ding, K. Feng, R. Feng, M. Xiong and A. Zhang, Unit time-phase signal sets: bounds and constructions **Cryptography and Communications**, Vol. 5, No. 3, pp. 209-227, 2013. PDF file
42. C. Ding, Cyclic codes from cyclotomic sequences of order four, **Finite Fields and Their Applications**, Vol. 23, pp. 8–34, 2013. PDF file
43. C. Ding and S. Ling, A q-polynomial approach to cyclic codes, **Finite Fields and Their Applications**, Vol. 20, pp. 1–14, 2013. PDF file
44. C. Ding and J. Yang, Hamming weights in irreducible cyclic codes, **Discrete Mathematics,** Vol. 313, pp. 434–446, 2013. PDF file
45. C. Ding, Cyclic codes from the two-prime sequences, **IEEE Trans. Information Theory,** Vol. 58, No. 6, pp. 3881–3890, June 2012. PDF file
46. W. Si and C. Ding, A binary additive stream cipher based on permutations, **Cryptography and Communications,** Vol. 4, No. 2, pp. 79–104, June 2012. PDF file
47. C. Ding, Cyclotomic constructions of cyclic codes with length being the product of two primes, **IEEE Trans. Information Theory,** Vol. 58, No. 4, pp. 2231–2236, April 2012. PDF file
48. C. Ding and Y. Tan, Zero-difference balanced functions with applications, **J. Statistical Theory and Practice**, Vol. 6, pp. 3–19, 2012. PDF file
49. C. Ding, Y. Liu, C. Ma, L. Zeng, The weight distributions of the duals of cyclic codes with two zeros, **IEEE Trans. Information Theory,** Vol. 57, No. 12, pp. 8000–8006, Dec. 2011. PDF file
50. P. Yuan and C. Ding, Permutation polynomials over finite fields from a powerful lemma, **Finite Fields and Their Applications,** Vol. 17, pp. 560–574, 2011. PDF file Correction here
51. C. Ma, L. Zeng, Y. Liu, D. Feng, and C. Ding, The weight enumerator of a class of cyclic codes, **IEEE Trans. Information Theory,** Vol. 57, No. 1, pp. 397–402, Jan. 2011. PDF file
52. X. Tang and C. Ding, New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value, **IEEE Trans. Information Theory,** Vol. 56, No. 12, pp. 6398–6405, Dec. 2010. PDF file
53. C. Ding, Y. Yang, and X. Tang, Optimal sets of frequency hopping sequences from linear cyclic codes, **IEEE Trans. Information Theory,** Vol. 56, No. 7, pp. 3605–3612, July 2010. PDF file
54. C. Ding and X. Tang, The crosscorrelation of binary sequences with optimal autocorrelation, **IEEE Trans. Information Theory,** Vol. 56, No. 4, pp. 1694–1701, April 2010. PDF file
55. C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo, and M. Mishima, Sets of frequency hopping sequences: bounds and optimal constructions, **IEEE Trans. Information Theory,** Vol. 55, No. 7, pp. 3297–3304, July 2009. PDF file
56. Y. Cai and C. Ding, Binary sequences with optimal autocorrelation, **Theoretical Computer Science,** Vol. 410, pp. 2316–2322, May 2009. PDF file
57. C. Ding, Q. Xiang, J. Yuan, and P. Yuan, Explicit classes of permutation polynomials over GF(3^{3m}), **Sciences in China Ser. A**, Vol. 53, No. 4, pp. 639–647, April 2009. PDF file

58. C. Ding, The weight distribution of some irreducible cyclic codes, **IEEE Trans. Information Theory,** Vol. 55, No. 3, pp. 955–960, March 2009. PDF file

59. C. Ding, Optimal and perfect difference systems of sets, **J. Combinatorial Theory Ser. A**, Vol. 116, No. 1, pp. 109–119, January 2009. PDF file

60. C. Ding, Optimal constant composition codes from zero-difference balanced functions, **IEEE Trans. Information Theory,** Vol. 54, No. 12, pp. 5766–5770, December 2008. PDF file

61. C. Ding and J. Yin, Constructions of almost difference families, **Discrete Mathematics,** Vol. 308, pp. 4941–4954, 2008. PDF file

62. C. Ding and J. Yin, Sets of optimal frequency hopping sequences, **IEEE Trans. Information Theory,** Vol. 54, No. 8, pp. 3741–3745, August 2008. PDF file

63. J. Yuan, C. Ding, H. Wang and J. Pieprzyk, Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$, **Finite Fields and Their Applications**, Vol. 14, No. 2, pp. 482–493, April 2008. PDF file

64. C. Ding, Two constructions of $\left(v, \frac{v-1}{2}, \frac{v-3}{2}\right)$ difference families, **J. Combinatorial Designs,** Vol. 16, No. 2, pp. 164–171, March 2008. PDF file

65. C. Ding and T. Feng, Codebooks from cyclic almost difference sets, **Designs, Codes and Cryptography,** Vol. 46, pp. 113–126, Jan. 2008. PDF file

66. C. Ding and T. Feng, A generic construction of complex codebooks meeting the Welch bound, **IEEE Trans. Information Theory,** Vol. 53, No. 11, pp. 4245–4250, Nov. 2007. PDF file

67. J. Yuan and C. Ding, Four classes of permutation polynomials of F_{2^m}, **Finite Fields and Their Applications,** Vol. 13, No. 4, Pages 869–876, November 2007. PDF file

68. C. Ding, M. Miosio and J. Yuan, Algebraic constructions of optimal frequency hopping sequences, **IEEE Trans. Information Theory,** Vol. 53, No. 7, pp. 2606–2610, July 2007. PDF file

69. C. Ding, Z. Wang and Q. Xiang, Skew Hadamard difference sets from the Ree-Tifts slice sympletic spreads in PG$(3, 3^{2h+1})$, **J. Combinatorial Theory Ser. A**, Vol. 114, No. 5, pp. 867–887, July 2007. PDF file

70. C. Ding and H. Niederreiter, Cyclotomic linear codes of order 3, **IEEE Trans. Information Theory**, Vol. 53, No. 6, pp. 2274–2277, June 2007. PDF file

71. C. Ding, T. Helleseth, T. Kløve and X. Wang, A general construction of authentication codes, **IEEE Trans. Information Theory**, Vol. 53, No. 6, pp. 2229–2235, June 2007. PDF file

72. C. Ding and J. Yin, Signal sets from functions with optimum nonlinearity, **IEEE Trans. Communications**, Vol. 55, No. 5, pp. 936–940, June 2007. PDF file

73. C. Carlet and C. Ding, Nonlinearities of S-boxes, **Finite Fields and Their Applications,** Vol. 13, pp. 121–135, Jan. 2007. PDF file

74. C. Ding, Complex codebooks from combinatorial designs, **IEEE Trans. Information Theory,** Vol. 52, No. 9, pp. 4229–4235, September 2006. PDF file

75. C. Ding and J. Yin, Direct constructions for cyclically relative difference matrices with five rows, **J. Combinatorial Designs,** Vol. 14, No. 5, pp. 391–399, September 2006. PDF file

76. C. Ding and J. Yuan, A family of skew Hadamard difference sets, **J. Combinatorial Theory Ser. A**, Vol. 113, No. 7, pp. 1526–1535, October 2006. PDF file

77. C. Ding and J. Yin, A construction of optimal constant composition codes, **Designs, Codes and Cryptography**, Vol. 40, No. 2, pp. 157–165, 2006. PDF file

78. Y. Chang and C. Ding, Constructions of external difference families and disjoint difference families, **Designs, Codes and Cryptography,** Vol. 40, No. 2, pp. 167–185, 2006. PDF file

79. C. Ding and A. Salomaa, On some problems of Mateescu concerning subword occurrences, **Fundamenta Informaticae**, Vol. 71, Nos. 1–2, pp. 51–63, 2006. PDF file

80. C. Ding and A. Salomaa, Secret sharing schemes with nice access structures, **Fundamenta Informaticae**, Vol. 71, Nos. 1–2, pp. 65–79, 2006. PDF file

81. C. Carlet, C. Ding and H. Niederreiter, Authentication schemes from highly nonlinear functions, **Designs, Codes and Cryptography,** Vol. 40, No. 1, pp. 71–79, 2006. PDF file

82. J. Yuan, C. Carlet and C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, **IEEE Trans. Information Theory**, Vol. 52, No. 2, pp. 712–717, Feb. 2006. PDF file

83. J. Yuan and C. Ding, Secret sharing schemes from three classes of linear codes, **IEEE Trans. Information Theory,** Vol. 52, No. 1, pp. 206–212, 2006. PDF file

84. C. Ding and J. Yin, Combinatorial constructions of constant composition codes, **IEEE Trans. Information Theory,** Vol. 51, No. 10, pp. 3671–3674, 2005. PDF file

85. C. Ding and J. Yuan, A family of optimal constant composition codes, **IEEE Trans. Information Theory,** Vol. 51, No. 10, pp. 3668–3671, 2005. PDF file

86. C. Carlet, C. Ding and J. Yuan, Linear codes from highly nonlinear functions and their secret sharing schemes, **IEEE Trans. Information Theory**, Vol. 51, No. 6, pp. 2089–2102, 2005. PDF file

87. C. Ding and J. Yin, Algebraic constructions of constant composition codes, **IEEE Trans. Information Theory**, Vol. 51, No. 4, pp. 1585–1589, 2005. PDF file

88. C. Ding, A. Salomaa, P. Sole and X. Tian, Three constructions of authentication/secrecy codes, **J. Pure and Applied Algebra,** Vol. 196, Nos. 2–3, pp. 149–168, 2005. PDF file

89. C. Ding and X. Wang, A coding theory construction of new systematic authentication codes, **Theoretical Computer Science**, Vol. 330, No. 1, pp. 81–99, 2005. PDF file

90. C. Ding and H. Niederreiter, Systematic authentication codes from highly nonlinear functions, **IEEE Trans. Information Theory,** Vol. 50, No. 10, pp. 2421–2428, 2004. PDF file

91. C. Ding and X. Tian, Three constructions of authentication codes with perfect secrecy, **Designs, Codes and Cryptography,** Vol. 33, pp. 227–239, 2004. PDF file

92. C. P. Lai and C. Ding, Several generalizations of Shamir's secret sharing scheme, **International Journal of Foundations of Computer Science,** Vol. 15, No. 2, pp. 445–458, 2004. PDF file

93. C. Carlet and C. Ding, Highly nonlinear mappings, **J. Complexity**, Vol. 20, No. 2, pp. 205–244, 2004. PDF file

94. C. Ding and C. Xing, Cyclotomic optical orthogonal codes of composite lengths, **IEEE Trans. Communications,** Vol. 52, No. 2, pp. 263–268, Feb. 2004. PDF file

95. T. W. Sze, S. Chanson, C. Ding, T. Helleseth and M. G. Parker, Logarithm authentication codes, **Information and Computation**, Vol. 184, No. 1, 93–108, July 2003. PDF file

96. C. Ding, M. Golin and T. Kløve, Meeting the Welch and Karytinos-Pados bounds on DS-CDMA binary signature sets, **Designs, Codes and Cryptography**, Vol. 30, pp. 73–84, July 2003. PDF file

97. C. Ding and C. Xing, Several classes of $(2^m - 1, w, 2)$ optical orthogonal codes, **Discrete Applied Mathematics**, Vol. 128, No. 1, pp. 103–120, 2003. PDF file

98. C. Xing, P. V. Kumar and C. Ding, Low correlation, large linear span sequences from function fields, **IEEE Trans. Information Theory,** Vol. 49, No. 6, pp. 1439–1446, 2003. PDF file

99. S. Chanson, C. Ding and A. Salomaa, Cartesian authentication codes from functions with optimal nonlinearity, **Theoretical Computer Science**, Vol. 290, No. 3, pp. 1737–1752, 2003. PDF file

100. 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, 2002. PDF file

101. C. Ding, F. W. Fu, T. Kløve and V. Wei, Construction of permutation arrays, **IEEE Trans. Information Theory**, Vol. 48, No. 4, pp. 977–980, 2002. PDF file

102. K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar and H. Martinsen, Almost difference sets and their sequences with optimal autocorrelation, **IEEE Trans. Information Theory,** Vol. 47, No. 7, pp. 2834–2943, 2001. PDF file

103. C. Ding, T. Kløve and F. Sica, Two classes of ternary codes and their weight distributions, **Discrete Applied Mathematics**, Vol. 111, No. 1–2, pp. 37–53, 2001. PDF file

104. C. Ding, T. Helleseth and H. Martinsen, New families of binary sequences with optimal three-level autocorrelation, **IEEE Trans. Information Theory**, Vol. 47, No. 1, pp. 428–433, January 2001. PDF file

105. C. Ding, H. Niederreiter and C. Xing, Some new codes from algebraic curves, **IEEE Trans. Information Theory**, Vol. 46, No. 7, pp. 2638–2642, 2000. PDF file

106. C. Ding, D. Kohel and S. Ling, Secret sharing with a class of ternary codes, **Theoretical Computer Science**, Vol. 246, pp. 285–298, 2000. PDF file

107. C. Ding, T. Helleseth and K. Y. Lam, Duadic sequences of prime lengths, **Discrete Mathematics**, Vol. 218, No. 1-3, pp. 33–49, 2000. PDF file

108. C. Ding, D. Kohel and S. Ling, Split group codes, **IEEE Trans. Information Theory**, Vol. 46, No. 2, pp. 485–495, March 2000. PDF file

109. C. Ding, D. Kohel and S. Ling, Elementary 2-group character codes, **IEEE Trans. Information Theory**, Vol. 46, No. 1, pp. 280–284, Jan. 2000. PDF file

110. D. Ye, C. Ding and K. Y. Lam, Properties and construction of antisymmetric matrices, **International Journal of Applied Mathematics**, Vol. 2, No. 2, pp. 185–198, 2000.

111. 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, November 1999. PDF file

112. C. Xing, H. Niederreiter, K. Y. Lam and C. Ding, Construction of sequences with almost perfect linear complexity profile from curves over finite fields, **Finite Fields and Their Applications**, Vol. 5, pp. 301–313, 1999. PDF file

113. C. Ding, K. Y. Lam and C. Xing, Enumeration and construction of all duadic codes of length p^m, **Fundamenta Informaticae**, Vol. 38, No. 1, pp. 149–161, 1999. PDF file

114. 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, 467–474, 1999. PDF file

115. C. Ding and V. Pless, Cyclotomy and duadic codes of prime lengths, **IEEE Trans. Information Theory**, Vol. 45, No. 2, 453–466, 1999. PDF file

116. C. Ding and T. Helleseth, New generalized cyclotomy and its applications, **Finite Fields and Their Applications,** Vol. 4, pp. 140–166, 1998. PDF file

117. C. Ding and T. Helleseth, On cyclotomic Generator of order r, **Information Processing Letters**, Vol. 66, No. 1, pp. 21–25, 1998. PDF file

118. R. Anderson, C. Ding, T. Helleseth and T. Kløve, How to build robust shared control systems, **Designs, Codes and Cryptography**, Vol. 15, No. 2, pp. 111–124, 1998. PDF file

119. C. Ding, Autocorrelation values of generalized cyclotomic sequences of order two, **IEEE Trans. Information Theory**, Vol. 44, No. 4, pp. 1698–1702, July 1998. PDF file

120. C. Ding, Pattern distribution of Legendre sequences, **IEEE Trans. Information Theory**, Vol. 44, No. 4, pp. 1693–1698, 1998. PDF file

121. C. Ding, Linear complexity of some generalized cyclotomic sequences, **International Journal of Algebra and Computation**, Vol. 8, No. 4, pp. 431–442, 1998.

122. 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 file

123. C. Ding, T. Laihonen and A. Renvall, Linear multi-secret sharing schemes and error-correcting codes, **J. Universal Computer Science**, Vol. 3, No. 9, pp. 1023–1036, 1997. PDF file

124. C. Ding, Linear complexity of generalized cyclotomic sequences of order 2, **Finite Fields and Their Applications**, Vol. 3, No. 1, pp. 159–174, 1997. PDF file

125. C. Ding and A. Salomaa, Cooperative hashing and ciphering, **Computers and Artificial Intelligence,** Vol. 15, pp. 233–245, 1996. PDF file

Book Chapters and Refereed Conference Papers

1. C. Ding and Z. Zhou, Parameters of 2-designs from some BCH codes, In: S. El Hajji, A. Nitaj and E. M. Souidi (Eds.), *Codes, Cryptography and Information Security*, Lecture Notes in Computer Science, Vol. 10194, pp. 110–127, Springer, 2017. PDF file

2. C. Ding and W. Si, Binary additive stream ciphers, in: *Number Theory and Related Area*, Advanced Lectures in Mathematics, Vol. 27, pp. 1–23, March 2013. PDF file

3. C. Ding, A class of three-weight and four-weight codes, in: Xing C. et al. (Eds.) *Proc. of the Second International Workshop on Coding Theory and Cryptography*, Lecture Notes in Computer Science 5557, pp. 34–42, Springer Verlag, 2009. PDF file

4. C. Ding, J. Luo and H. Niederreiter, Two weight codes punctured from irreducible cyclic codes, in: Li Y., Ling S., Niederreiter H., Wang H., Xing C., Zhang S. (Eds.) *Proc. of the First International Workshop on Coding Theory and Cryptography*, pp. 119 – 124. Singapore, World Scientific, 2008. PDF file

5. X. Tian and C. Ding, A construction of authentication codes with secrecy, in: *Coding, Cryptography, and Combinatorics, Progress in Computer Science and Logic, vol. 23, K. Feng, H. Niederreiter and C. Xing Eds.,* Birhäuser Verlag, 2004, pp. 319–330.

6. C. Ding, X. Tian and X. Wang, Simple and efficient symmetric A-codes from error correcting codes, in: *Progress on Cryptography: the last 25 years of cryptography in China,* Kluwer Academic Publisher, 2004, pp. 33–44.

7. C. Ding and J. Yuan, Covering and secret sharing with linear codes, in: *Discrete Mathematics and Theoretical Computer Science*, Lecture Notes in Computer Science 2731, 2003, Springer Verlag, pp. 11–25. PDF file

8. C. Ding, A. Salomaa, P. Sole and X. Tian, Three constructions of authentication/secrecy codes, in: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes,* Lecture Notes in Computer Science, vol. 2643, Springer Verlag, 2003, pp. 24–33. [This paper has a journal version]
9. J. Yuan and C. Ding, Secret sharing schemes from two-weight codes, in: *R. C. Bose Centenary Symposium on Discrete Mathematics and Applications*, December 20-23, 2002, Indian Statistical Institute, Kolkata, India.
10. C. Ding and C. Xing, A cyclotomic construction of some constant weight cyclically permutable codes, in: *Proceedings of the 2002 International Symposium on Information Theory and Its Applications,* October 7–11, 2002, pp. 407–410.
11. C. Ding and C. Xing, Several classes of optimal binary cyclic self-complementary codes, in: *Proceedings of the IEEE Symposium on Information Theory*, June 2001, pp. 67–67.
12. C. Ding and C. Xing, $(2^m - 1, w, 2)$ optical orthogonal codes with $w = 11$ and 13, in: *Proceedings of the International Workshop on Coding and Cryptography*, Paris, France, Jan. 8–12, 2001, pp. 167–176. [This paper has a journal version]
13. C. Ding, Optical orthogonal codes with parameters $(2^m - 1, 19, 2)$, in: *Proceedings of the 2000 International Symposium on Information Theory and Its Applications*, Hawaii, USA, 2000, pp. 553–556.
14. C. Ding, D. Kohel and S. Ling, Counting the number of points on affine diagonal curves, in: *Cryptography and Computational Number Theory,* Progress in Computer Science and Logic 20, Birhäuse, 2001, pp. 15–24,.
15. C. Ding and V. Pless, Cyclotomy and duadic codes of prime lengths, in: *Proc. of the 1998 IEEE International Symposium on Information Theory*, 1998, p. 234. [This paper has a journal version]
16. C. Ding, V. Niemi, A. Renvall and A. Salomaa, TWOPRIME: a fast stream ciphering algorithm, in: *Fast Software Encryption, LNCS 1267*, Springer-Verlag, 1997, 88–102.
17. A. Renvall and C. Ding, The access structure of some secret sharing schemes, in: *Information Security and Privacy, LNCS 1172*, Springer-Verlag, 1996, 67–78.
18. A. Renvall and C. Ding, A nonlinear secret sharing scheme, in: *Information Security and Privacy, LNCS 1172*, Springer-Verlag, 1996, 56–65.
19. C. Ding, Binary cyclotomic generators, in: *Fast Software Encryption, LNCS 1008*, Springer-Verlag, 1995, 29–61.
20. C. Ding, The differential cryptanalysis and design of natural stream ciphers, in: *Fast Software Encryption, LNCS 809*, Springer-Verlag, 1994, 101–115.
21. T. Beth and C. Ding, On almost perfect nonlinear permutations, in: *Advances in Cryptology–Eurocrypt'93*, LNCS 765, Springer-Verlag, 1994, 65–76. PDF file
22. C. Ding, Lower bounds on the weight complexity of cascaded binary sequences, in: *Proc. of Auscrypt' 90, Advances in Cryptology, LNCS 453*, Springer-Verlag, 1990, 39–43.
23. C. Ding, G. Xiao and W. Shan, New measure indexes on the security of stream ciphers, in: *Proc. of the Third National Workshop on Cryptography*, Xian, 1988, 5–15.
24. C. Ding, Proof of Massey's conjectured algorithm, in: *Advances in Cryptology: Eurocrypt '88, LNCS 330*, Springer-Verlag, 1988, 345–349. PDF file
25. G. Xiao, B. Shen, C. Ding and C. K. Wu, Some applications of spectral techniques to coding, in: *Proc. of the Second International Workshop on Spectral Techniques*, Canada, 1986.