Bibliography on Authentication Codes

D. R. Stinson and R. Wei
Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada

October 29, 1998

We felt it would be useful to create an up-to-date bibliography on authentication codes and make it available on the WWW. This is the postscript version of the bibliography. The html version can be found at `http://cacr.math.uwaterloo.ca/~dstinson/acbib.html`. By "authentication codes" we mean Simmons-type codes that provide unconditional security against substitution and impersonation frauds. Thus, we do not consider related concepts such as MACs, MDCs or signature schemes.

The current version of this bibliography has 127 entries.

In general, we are including papers that are published or accepted for publication in conference proceedings and journals (but not unpublished technical reports or dissertations). We would appreciate knowing of any errors in this list, as well as any papers that should be added, updates to unpublished papers, etc.

1. M. H. G. Anthony, K. M. Martin, J. Seberry and P. Wild, Some remarks on authentication systems. in "Advances in Cryptology – AUSCRYPT '90", J. Seberry and J. Pieprzyk, eds., *Lecture Notes in Computer Science* **453** (1990), 122-139.

2. M. Atici and D. R. Stinson, Universal hashing and multiple authentication, in "Advances in Cryptology – CRYPTO '96", N. Koblitz, ed., *Lecture Notes in Computer Science* **1109** (1996), 16-30.

3. S. Bakhtiari, R. Safavi-Naini and J. Pieprzyk, A message authentication code based on latin squares, in "Information Security and Privacy – ACISP '97", V. Varadharajan, J. Pieprzyk and Y. Mu, eds., *Lecture Notes in Computer Science* **1270** (1997), 194-203.

4. L. A. Bassalygo, Lower bounds for the probability of successful message deception, *Probl. Inf. Trans.* **29** (1993), 104-108.

5. A. Beutelspacher, Enciphered geometry, some applications of geometry to cryptography, in "Combinatorics '86", A. Barlotti, M. Marchi and G. Tallini, eds., *Annals of Discrete Mathematics* **37** (1988), 59-68.

6. A. Beutelspacher, Perfect and essentially perfect authentication schemes, in "Advances in Cryptology – EUROCRYPT '87", D. Chaum and W. L. Price, eds., *Lecture Notes in Computer Science* **304** (1988), 167-170.

7. A. Beutelspacher, Applications of finite geometry to cryptography, in "Geometries, Codes and Cryptography", G. Longo, M. Marchi and A. Sgarro, eds., *CISM Courses and Lectures No. 313*, Springer-Verlag, 1990, 161-186.

8. A. Beutelspacher and U. Rosenbaum, Essentially l-fold secure authentication systems, in "Advances in Cryptology – EUROCRYPT '90", I. B. Damgard, ed., *Lecture Notes in Computer Science* **473** (1991), 294-305.

9. A. Beutelspacher, G. Tallini and C. Zanella, Examples of essentially s-fold secure geometric authentication systems with large s, *Rend. Mat. Appl.* **10** (1990), 321-326.

10. J. Bierbrauer, Monotypical uniformly homogeneous sets of permutations, *Arch. Math.* **58** (1992), 375-406.

11. J. Bierbrauer, A^2 codes from universal hash classes, in "Advances in Cryptology – EUROCRYPT '95", L. C. Guillou and J.-J. Quisquater, eds., *Lecture Notes in Computer Science* **921** (1995), 311-318.

12. J. Bierbrauer, Universal hashing and geometric codes, *Designs, Codes and Cryptography.* **11** (1997), 207-221.

13. J. Bierbrauer, Authentication via algebraic-geometric codes, *Rend. Circ. Mat. Palermo (2) Suppl.* **51** (1998), 139-152.

14. J. Bierbrauer and Y. Edel, Theory of perpendicular arrays, *Journal of Combinatorial Designs* **2** (1994), 338-344.

15. J. Bierbrauer, T. Johansson, G. Kabatianskii and B. Smeets, On families of hash functions via geometric codes and concatenation, in "Advances in Cryptology – CRYPTO '93", D. R. Stinson, ed., *Lecture Notes in Computer Science* **773** (1994), 331-342.

16. J. Bierbrauer and T. v. Tran, Halving $\mathrm{PGL}(2, 2^f), f$ odd: a series of cryptocodes, *Designs, Codes and Cryptography* **1** (1991), 141-148.

17. J. Bierbrauer and T. v. Tran, Some highly symmetric authentication perpendicular arrays, *Designs, Codes and Cryptography* **1** (1992), 307-319.

18. C. Blundo, A. De Santis, K. Kurosawa and W. Ogata, A note on authentication codes, to appear in *Journal of Cryptology.*

19. E. F. Brickell, A few results in message authentication, *Congressus Numerantium* **43** (1984), 141-154.

20. E. F. Brickell and D. R. Stinson, Authentication codes with multiple arbiters, in "Advances in Cryptology – EUROCRYPT '88", C. G. Gunther, ed., *Lecture Notes in Computer Science* **330** (1988), 51-55.

21. L. R. A. Casse K. M. Martin and P.R. Wild, Bounds and characterisations of authentication/secrecy schemes, *Designs, Codes and Cryptography* **13**(1998), 107-129.

22. G. Castagnoli, Comments on Massey's concepts of perfect secrecy and perfect authenticity, *Alta Frequenza* **56** (1987), 227-228.

23. B. den Boer, A simple and key-economical unconditional authentication scheme, *Journal of Computer Security* **2** (1993), 65-71.

24. M. De Soete, Some constructions for authentication - secrecy codes, in "Advances in Cryptology – EUROCRYPT '88", C. G. Gunther, ed., *Lecture Notes in Computer Science* **330** (1988), 57-75.

25. M. De Soete. Authentication/secrecy codes, in "Geometries, Codes and Cryptography", G. Longo, M. Marchi and A. Sgarro, eds., *CISM Courses and Lectures No. 313*, Springer-Verlag, 1990, 187-199.

26. M. De Soete, Bounds and constructions for authentication - secrecy codes with splitting, in "Advances in Cryptology – CRYPTO '88", S. Goldwasser, ed., *Lecture Notes in Computer Science* **403** (1989), 311-317.

27. M. De Soete, New bounds and constructions for authentication/secrecy codes with splitting, *Journal of Cryptology* **3** (1991), 173-186.

28. M. De Soete, K. Vedder and M. Walker, Cartesian authentication schemes, in "Advances in Cryptology – EUROCRYPT '89", J.-J. Quisquater and J. Vandewalle, eds., *Lecture Notes in Computer Science* **434** (1990), 476-490.

29. Y. Desmedt, Unconditionally secure authentication schemes and practical and theoretical consequences, in "Advances in Cryptology – CRYPTO '85", H. C. Williams, ed., *Lecture Notes in Computer Science* **218** (1986), 42-55.

30. Y. Desmedt, Y. Frankel and M. Yung Multi-receiver/multi-sender network security: efficient authenticated multicast/feedback, in "IEEE Infocom '92" (1992), 2045-2054.

31. Y. Desmedt and M. Yung, Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks, in "Advances in Cryptology – CRYPTO '90", A. J. Menezes and S. A. Vanstone, eds., *Lecture Notes in Computer Science* **537** (1991), 177-188.

32. M. van Dijk, C. Gehrmann and B. Smeets, Unconditionally secure group authentication, *Des. Codes, Cryptogr.* **14** (1998), 281-296.

33. V. Fak, Repeated use of codes which detect deception, *IEEE Transactions on Information Theory* **25** (1979), 233-234.

34. R.-Q. Feng and Z.-X. Wan, A construction of Cartesian authentication codes from geometry of finite groups, to appear in *Journal of Combinatorics, Information and System Sciences.*

35. R. Feng and Z. Wan, A construction of Cartesian authentication codes from vector space and dual authentication codes, *Northeast. Math. J.***13**(1997), 63-72.

36. H. Fujii, W. Kachen and K. Kurosawa, Combinatorial bounds and design of broadcast authentication, *IEICE Transactions Fundamentals* **E79-A** (1996).

37. Y. Gao and Y. D. Wang, Some constructions of Cartesian authentication codes from pseudo-symplectic geometry, *Northeastern Math. Journal* **11** (1995), 47-55.

38. Y. Gao and Z. Zou, Two new constructions of Cartesian authentication codes from symplectic geometry, *Appl. Math. J. Chinese Univ. Ser. B* **10** (1995), 345-356.

39. G. Ge and L. Zhu, Authentication perpendicular arrays $\mathrm{APA}_1(2,5,v)$, *J. Combin. Des.* **4** (1996), 365-375.

40. G. Ge and L. Zhu, Authentication perpendicular arrays $\mathrm{APA}_1(2,7,v)$, *J. Combin. Des.* **5** (1997), 111-124.

41. C. Gehrmann, Cryptanalysis of the Gemmell and Naor multiround authentication protocol, in "Advances in Cryptology – CRYPTO '94", Y. G. Desmedt, ed., *Lecture Notes in Computer Science* **839** (1994), 121-128.

42. C. Gehrmann, Secure multiround authentication protocols, in "Advances in Cryptology – EUROCRYPT '95", L. C. Guillou and J.-J. Quisquater, eds., *Lecture Notes in Computer Science* **921** (1995), 158-167.

43. P. Gemmell and M. Naor, Codes for interactive authentication, in "Advances in Cryptology – CRYPTO '93", D. R. Stinson, ed., *Lecture Notes in Computer Science* **773** (1994), 355-367.

44. E. N. Gilbert, F. J. MacWilliams and N. J. A. Sloane, Codes which detect deception, *Bell System Technical Journal* **53** (1974), 405-424.

45. S. Halevi and H. Krawczyk, MMH: Message authentication in software in the Gbit/sec rates, In "Proceedings of the 4th Workshop on Fast Software Encryption", *Lecture Notes in Computer Science* **1267** (1997), 172-188.

46. T. Helleseth and T. Johansson, Universal hash functions from exponential sums over finite fields, in "Advances in Cryptology – CRYPTO '96", N. Koblitz, ed., *Lecture Notes in Computer Science* **1109** (1996), 31-44.

47. T. Hwang and C-H. Wang, Arbitrated unconditionally secure authentication scheme with multi-senders, *Inform. Process. Lett.* **65**(1998), 189-193.

48. M. Jimbo and R. Fuji-Hara, Optimal authentication systems and combinatorial designs, *IEEE Transactions on Information Theory* **36** (1990), 54-62.

49. R. Johannesson and A. Sgarro, Strengthening Simmon's bound on impersonation, *IEEE Transactions on Information Theory* **37** (1991), 1182-1185.

50. T. Johansson, A shift register construction of unconditionally secure authentication codes, *Designs, Codes and Cryptography* **4** (1994), 69-82.

51. T. Johansson, On the construction of perfect authentication codes that permit arbitration, in "Advances in Cryptology – CRYPTO '93", D. R. Stinson, ed., *Lecture Notes in Computer Science* **773** (1994), 343-354.

52. T. Johansson, Lower bounds on the probability of deception in authentication with arbitration, *IEEE Transactions on Information Theory* **40** (1994), 1573-1585.

53. T. Johansson, Authentication codes for nontrusting parties obtained from rank metric codes, *Designs, Codes and Cryptography* **6** (1995), 205-218.

54. T. Johansson, Bucket hashing with a small key size, in "Advances in Cryptology – EUROCRYPT '97", *Lecture Notes in Computer Science* **1233** (1997).

55. T. Johansson, G. Kabatianskii and B. Smeets, On the relation between A-codes and codes correcting independent errors, in "Advances in Cryptology – EUROCRYPT '93", T. Helleseth, ed., *Lecture Notes in Computer Science* **765** (1994), 1-11.

56. T. Johansson and B. Smeets, On A^2 codes including arbiter's attacks, in "Advances in Cryptology – EUROCRYPT '94", A. De Santis, ed., *Lecture Notes in Computer Science* **950** (1995), 456-460.

57. T. Johansson, B. Smeets and G. Kabatianskii, On the cardinality of systematic authentication codes via error correcting codes, *IEEE Transactions on Information Theory* **42** (1996), 566-578.

58. H. Krawczyk, LFSR-based hashing and authentication, in "Advances in Cryptology – CRYPTO '94", Y. G. Desmedt, ed., *Lecture Notes in Computer Science* **839** (1994), 129-139.

59. H. Krawczyk, New hash functions for message authentication, in "Advances in Cryptology – EUROCRYPT '95", L. C. Guillou and J.-J. Quisquater, eds., *Lecture Notes in Computer Science* **921** (1995), 301-310.

60. K. Kurosawa, New bound on authentication code with arbitration, in "Advances in Cryptology – CRYPTO '94", Y. G. Desmedt, ed., *Lecture Notes in Computer Science* **839** (1994), 140-149.

61. K. Kurosawa, T. Johansson and D. R. Stinson, Almost k-wise independent sample spaces and their cryptologic applications, in “Advances in Cryptology – EUROCRYPT '97”, *Lecture Notes in Computer Science* **1233** (1997), 409-421.

62. K. Kurosawa and S. Kageyama, New bound for affine resolvable designs and its application to authentication codes, in “COCOON '95”, *Lecture Notes in Computer Science* **959** (1995), 292-302.

63. K. Kurosawa and S. Obana, Combinatorial bounds for authentication codes with arbitration, in “Advances in Cryptology – EUROCRYPT '95”, L. C. Guillou and J.-J. Quisquater, eds., *Lecture Notes in Computer Science* **921** (1995), 289-300.

64. K. Kurosawa and S. Obana, Characterization of (k, n)-multireceiver authentication, in “Information Security and Privacy – ACISP '97”, V. Varadharajan, J. Pieprzyk and Y. Mu, eds., *Lecture Notes in Computer Science* **1270** (1997), 204-215.

65. K. Kurosawa, K. Okada, H. Saido, and D. R. Stinson. New combinatorial bounds for authentication codes and key predistribution schemes, *Designs, Codes and Cryptography,* **15** (1998), 87-100.

66. K. M. Martin and R. Safavi-Naini, Multisender authentication schemes with unconditional security, in “Information and Communications Security” *Lecture Notes in Computer Seience* **1334**, (1997) 130-143.

67. K. M. Martin, J. Seberry and P. Wild, Resolvable designs applicable to cryptographic authentication schemes, *Journal of Combinatorial Mathematics and Combinatorial Computing* **12** (1992), 153-160.

68. J. L. Massey, Cryptography – a selective survey, in “Digital Communications”, E. Biglieri and G. Prati, eds., North-Holland, 1986, 3-21. [Also published in *Alta Frequenza* **55** (1986), 4-11.]

69. J. L. Massey, Contemporary cryptology: an introduction, in “Contemporary Cryptology, The Science of Information Integrity”, G. J. Simmons, ed., IEEE Press, 1992, 1-39. [Preliminary version appeared in *Proceedings of the IEEE* **76** (1988), 533-549.]

70. U. Maurer, A unified and generalized treatment of authentication theory, in “Proceedings of the 13th Symposium on Theoretical Aspects of Computer Science”, *Lecture Notes in Computer Science* **1046** (1996), 387-398.

71. C. J. Mitchell, F. C. Piper, M. Walker and P. Wild, Authentication schemes, perfect local randomizers, perfect secrecy and secret sharing schemes, *Designs, Codes and Cryptography* **7** (1996), 101-110.

72. C. Mitchell, M. Walker and P. Wild, The combinatorics of perfect authentication schemes, *SIAM J. Discrete Math.* **7** (1994), 102-107.

73. S. Obana and K. Korusawa, A^2-code = Affine resolvable + BIBD, in "Proc. of ICICS'97", *Lecture Notes in Computer Science,* **1334**(1997), 118-129.

74. D. Pei, Information-theoretic bounds for authentication codes and block designs, *Journal of Cryptology* **8** (1995), 177-188.

75. R. S. Rees and D. R. Stinson, Combinatorial characterizations of authentication codes II, *Designs, Codes and Cryptography* **7** (1996), 239-259.

76. P. Rogaway, Bucket hashing and its application to fast message authentication, in "Advances in Cryptology – CRYPTO '95", D. Coppersmith, ed., *Lecture Notes in Computer Science* **963** (1995), 29-42.

77. U. Rosenbaum, A lower bound on authentication after having observed a sequence of messages, *Journal of Cryptology* **6** (1993), 135-156.

78. R. Safavi-Naini and L. Tombak, Authentication codes under impersonation attack, in "Advances in Cryptology – AUSCRYPT '92", J. Seberry and Y. Zheng, eds., *Lecture Notes in Computer Science* **718** (1993), 35-47.

79. R. Safavi-Naini and L. Tombak, Optimal authentication systems, in "Advances in Cryptology – EUROCRYPT '93", T. Helleseth, ed., *Lecture Notes in Computer Science* **765** (1994), 12-27.

80. R. Safavi-Naini and L. Tombak, Authentication codes in plaintext and chosen-content attacks, *Designs, Codes and Cryptography* **7** (1996), 83-99. [Preliminary version appeared in "Advances in Cryptology – EUROCRYPT '94", A. De Santis, ed., *Lecture Notes in Computer Science* **950** (1995), 254-265.]

81. R. Safavi-Naini and L. Tombak, Near-perfect protection and key strategies in authentication codes under spoofing attack of order r, *Ars Combinatoria* **44** (1996), 149-160.

82. R. Safavi-Naini and L. Tombak, Combinatorial structure of A-codes with r-fold security, in "Advances in Cryptology – ASIACRYPT '94", J. Pieprzyk and R. Safavi-Naini, eds., *Lecture Notes in Computer Science* **917** (1995), 211-223.

83. P. Schobi. Perfect authentication systems for data sources with arbitrary statistics, unpublished (presented at EUROCRYPT '86).

84. A. Sgarro, Informational divergence bounds for authentication codes, in "Advances in Cryptology – EUROCRYPT '89", J.-J. Quisquater and J. Vandewalle, eds., *Lecture Notes in Computer Science* **434** (1990), 93-101.

85. A. Sgarro, An introduction to the theory of unconditional secrecy and authentication, in "Geometries, Codes and Cryptography", G. Longo, M. Marchi and A. Sgarro, eds., *CISM Courses and Lectures No. 313*, Springer-Verlag, 1990, 131-160.

86. A. Sgarro. Three types of perfection in Shannon-theoretic cryptography, In in "Sequences, Combinatorics, Compression, Security and Transmission", R. M. Capocelli, ed., Springer-Verlag, 1990, 420-425.

87. A. Sgarro, Lower bounds for authentication codes with splitting, in "Advances in Cryptology – EUROCRYPT '90", I. B. Damgard, ed., *Lecture Notes in Computer Science* **473** (1991), 283-293.

88. A. Sgarro, Information-theoretic bounds for authentication frauds, *Journal of Computer Security* **2** (1993), 53-63. [Preliminary version appeared in "Advances in Cryptology – EUROCRYPT '92", R. A. Rueppel, ed., *Lecture Notes in Computer Science* **658** (1993), 467-471.]

89. V. Shoup, On fast and provably secure message authentication based on universal hashing, in "Advances in Cryptology – CRYPTO '96", N. Koblitz, ed., *Lecture Notes in Computer Science* **1109** (1996), 313-328.

90. G. J. Simmons, Message authentication without secrecy, in "Secure Communications and Asymmetric Cryptosystems", G. J. Simmons, ed., Westview Press, 1982, 105-139.

91. G. J. Simmons, A game theory model of digital message authentication, *Congressus Numerantium* **34** (1982), 413-424.

92. G. J. Simmons, Verification of treaty compliance — revisited, in "Proceedings of the 1983 Symposium on Security and Privacy", IEEE Press, 1983, 61-66.

93. G. J. Simmons, Message authentication: a game on hypergraphs, *Congressus Numerantium* **45** (1984), 161-192.

94. G. J. Simmons, The prisoner's problem and the subliminal channel, in "Advances in Cryptology – CRYPTO '83", D. Chaum, ed., Plenum Press, 1984, 51-67.

95. G. J. Simmons, Authentication theory/coding theory, in "Advances in Cryptology – CRYPTO '84", G. R. Blakley and D. Chaum, eds., *Lecture Notes in Computer Science* **196** (1985), 411-432.

96. G. J. Simmons, The practice of authentication, in "Advances in Cryptology – EUROCRYPT '85", F. Pilcher, ed., *Lecture Notes in Computer Science* **219** (1986), 261-272.

97. G. J. Simmons, Authentication codes that permit arbitration, *Congressus Numerantium* **59** (1988), 275-290.

98. G. J. Simmons, Message authentication with arbitration of transmitter/receiver disputes, in "Advances in Cryptology – EUROCRYPT '87", D. Chaum and W. L. Price, eds., *Lecture Notes in Computer Science* **304** (1988), 151-165.

99. G. J. Simmons, A natural taxonomy for digital information authentication schemes, "Advances in Cryptology – CRYPTO '87", C. Pomerance, ed., *Lecture Notes in Computer Science* **293** (1988), 269-288.

100. G. J. Simmons, A Cartesian product construction for unconditionally secure authentication codes that permit arbitration, *Journal of Cryptology* **2** (1990), 77-104.

101. G. J. Simmons, Weakly resolvable designs and unconditionally secure authentication codes, *Congressus Numerantium* **79** (1990), 89-100.

102. G. J. Simmons, A survey of information authentication, in "Contemporary Cryptology, The Science of Information Integrity", G. J. Simmons, ed., IEEE Press, 1992, 379-419. [Preliminary version appeared in *Proceedings of the IEEE* **76** (1988), 603-620.]

103. G. J. Simmons amd B. Smeets, A paradoxical result in unconditionally secure authentication codes – and an explanation, in "Cryptography and Coding", H. J. Beker and F. C. Piper, eds., Oxford University Press, 1989, 231-258.

104. N. J. A. Sloane, Error-correcting codes and cryptography, in "The Mathematical Gardner", D. A. Klarner, ed., Prindle, Weber and Schmidt, 1981, 346–382.

105. B. Smeets, Bounds on the probability of deception in multiple authentication, *IEEE Transactions on Information Theory* **40** (1994), 1586-1591.

106. B. Smeets, P. Vanroose and Z.-X. Wan, On the construction of authentication codes with secrecy and codes which stand spoofing attacks of order L at least 2, in "Advances in Cryptology – EUROCRYPT '90", I. B. Damgard, ed., *Lecture Notes in Computer Science* **473** (1991), 306-312.

107. D. R. Stinson, Some constructions and bounds for authentication codes. *Journal of Cryptology* **1** (1988), 37–51. [Preliminary version appeared in "Advances in Cryptology – CRYPTO '86", A. M. Odlyzko, ed., *Lecture Notes in Computer Science* **263** (1987), 418-425.]

108. D. R. Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, *Journal of Cryptology* **1** (1988), 119-127. [Preliminary version appeared in "Advances in Cryptology – CRYPTO 87", C. Pomerance, ed., *Lecture Notes in Computer Science* **293** (1988), 355-366.]

109. D. R. Stinson, The combinatorics of authentication and secrecy codes, *Journal of Cryptology* **2** (1990), 23-49.

110. D. R. Stinson and L. Teirlinck, A construction for authentication/secrecy codes from 3-homogeneous permutation groups, *European Journal of Combinatorics* **11** (1990), 73-79.

111. D. R. Stinson, Combinatorial characterizations of authentication codes, *Designs, Codes and Cryptography* **2** (1992), 175-187. [Preliminary version appeared in "Advances in Cryptology – CRYPTO '91", J. Feigenbaum, ed., *Lecture Notes in Computer Science* **576** (1992), 62-73.]

112. D. R. Stinson, Combinatorial designs and cryptography, in "Surveys in Combinatorics, 1993", K. Walker, ed., Cambridge University Press, 1993, 257-287.

113. D. R. Stinson, Universal hashing and authentication codes, *Designs, Codes and Cryptography* **4** (1994), 369-380. [Preliminary version appeared in "Advances in Cryptology – CRYPTO '91", J. Feigenbaum, ed., *Lecture Notes in Computer Science* **576** (1992), 74–85.]

114. R. Taylor, Nearly optimal unconditionally secure authentication, in "Advances in Cryptology – EUROCRYPT '94", A. De Santis, ed., *Lecture Notes in Computer Science* **950** (1995), 244-253.

115. H. C. A. van Tilborg, Authentication codes: an area where coding and cryptology meet, in "Cryptography and Coding V", C. Boyd, ed., *Lecture Notes in Computer Science* **1025** (1996), 169-183.

116. L. Tombak and R. Safavi-Naini, Authentication codes with perfect protection, in "Advances in Cryptology – AUSCRYPT '92", J. Seberry and Y. Zheng, eds., *Lecture Notes in Computer Science* **718** (1993), 15-26.

117. L. Tombak and R. Safavi-Naini, Authentication codes that are r-fold secure against spoofing, *Utilitas Mathematica* **48** (1995), 215-224. [Also appears in "Proceedings of the Second ACM Conference on Computer and Communications Security".]

118. T. v. Tran, On the construction of authentication and secrecy codes, *Designs, Codes and Cryptography* **5** (1995), 269-280.

119. S. G. Vluaduct, A note on authentication codes from algebraic geometry, *IEEE trans. Inform. Theory* **44**(1998), 1342-1345.

120. M. Walker, Information-theoretic bounds for authentication systems, *Journal of Cryptology* **2** (1990), 131-143.

121. Z.-X. Wan, Construction of Cartesian authentication codes from unitary geometry, *Designs, Codes and Cryptography* **2** (1992), 333-356.

122. Z.-X. Wan, Further construction of Cartesian authentication codes from symplectic geometry, *Northeastern Mathematics Journal (China)* **8** (1992), 4-20.

123. Z.-X. Wan, B. Smeets and P. Vanroose On the construction of Cartesian authentication codes over symplectic spaces, *IEEE Transactions on Information Theory* **40** (1994), 920-929.

124. M. N. Wegman and J. L. Carter, New hash functions and their use in authentication and set equality, *Journal of Computer and System Sciences* **22** (1981), 265-279.

125. H. You and Y. Gao, Some new constructions of Cartesian authentication codes from symplectic geometry, *Systems Sci. Math. Sci.* **7** (1994), 317-327.

126. H. You and F. Zhou, Construction of Cartesian authentication codes from pseudo symplectic geometry, *J. Inform. Optim. Sci.* **16** (1995), 113-125.

127. C. Zanella, Linear sections of the finite Veronese varieties and authentication systems defined using geometry, *Designs, codes and Crytography* **13** (1998), 199-212.