Publications

Journals

[1] N di Pietro, G. Zémor and J. J. Boutros, LDA Latices Without Dithering Achieve Capacity on the Gaussian Channel, *IEEE Trans. on Information Theory*, to appear.

[2] C. Bachoc, O. Serra and G. Zémor, An analogue of Vosper's Theorem for Extension Fields, *Math. Proc. Cambridge Philos. Soc.*, Vol. 163, No 3 (2017) pp. 423–452.

[3] D. P. Gaborit and G. Zémor, On the hardness of the decoding and the minimum distance problems for rank codes, *IEEE Trans. on Information Theory*, IT-62, No 12 (2016) pp. 7245–7252.

[4] C. Bachoc, O. Serra and G. Zémor, Revisiting Kneser's Theorem for Field Extensions, *Combinatorica,* to appear.

[5] N. Delfosse and G. Zémor, A homological upper bound on critical probabilities for hyperbolic percolation, *Annales de l'Institut Henri Poincaré D*, Vol. 3, No 2 (2016) pp. 139–161.

[6] D. Mirandola and G. Zémor, Critical pairs for the Product Singleton Bound, *IEEE Trans. on Information Theory*, IT-61, No 9 (2015) pp. 4928–4937.

[7] I. Cascudo, R. Cramer, D. Mirandola, and G. Zémor, Squares of random linear codes, *IEEE Trans. on Information Theory*, IT-61, No 3 (2015) pp. 1159–1173.

[8] N. Kashyap and G. Zémor, Upper bounds on the size of grain-correcting codes, *IEEE Trans. on Information Theory*, IT-60, No 8 (2014) pp. 4699–4709.

[9] J.P. Tillich and G. Zémor, Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength, *IEEE Trans. on Information Theory*, IT-60, No 2 (2014) pp. 1193–1202.

[10] A. Couvreur, N. Delfosse and G. Zémor, A Construction of Quantum LDPC Codes from Cayley Graphs, *IEEE Trans. on Information Theory*, IT-59, No 9 (2013) pp. 6087–6098.

[11] N. Delfosse and G. Zémor, Upper Bounds on the Rate of Low Density Stabilizer Codes for the Quantum Erasure Channel, *Quantum Information & Computation*, Vol. 13, No 9&10 (2013) pp. 0793-0826.

[12] O. Serra and G. Zémor, A Structure Theorem for Small Sumsets in Non-abelian Groups, *European Journal of Combinatorics*, Vol. 34, No 8 (2013) pp. 1436–1453.

[13] A. Mazumdar, A. Barg and G. Zémor, Constructions of Rank Modulation Codes, *IEEE Trans. on Information Theory*, IT-59, No 2 (2013) pp. 1018–1029.

[14] C. Bachoc and G. Zémor, Bounds for binary codes relative to pseudo-distances of k points, *Advances in Mathematics of Communications*, Vol. 4, No. 4 (2010) pp. 547–565.

[15] J. Boutros, A. Guillen i Fabregas, E. Biblieri and G. Zémor, Low-Density Parity-Check Codes for Nonergodic Block-Fading Channels, *IEEE Trans. on Information Theory*, IT-56, No 9 (2010) pp. 4286 - 4300.

[16] O. Serra and G. Zémor, Large sets with small doubling modulo p are well covered by an arithmetic progression, *Annales de l'Institut Fourier*, 59 no. 5 (2009), pp. 2043–2060.

[17] A. Barg, A. Mazumdar and G. Zémor, Weight distribution and decoding of codes on hypergraphs, *Advances in Mathematics of Communications*, Vol. 2, No 4 (2008) pp. 433–450.

[18] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji and G. Zémor, Theoretical and Practical Boundaries of Binary Secure Sketches, *IEEE Transactions on Information Forensics & Security*, Vol. 3, No. 4. (2008), pp. 673–683.

[19] P. Gaborit and G. Zémor, Asymptotic improvement of the Gilbert-Varshamov bound for linear codes, *IEEE Trans. on Information Theory*, IT-54, No 9 (2008) pp. 3865–3872.

[20] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor et P. Grangier, Multidimensional reconciliation for continuous-variable quantum key distribution, *Physical Review A*, vol. 77, 042325 (2008).

[21] Y. O. Hamidoune, O. Serra et G. Zémor, On Some Subgroup Chains Related to Kneser's Theorem, *Journal de Théorie des nombres de Bordeaux*, vol. 20 (2008), pp. 125–130.

[22] Y. O. Hamidoune, O. Serra et G. Zémor, On the critical pair theory in abelian groups : Beyond Chowla's Theorem, *Combinatorica*, vol. 28 No 4 (2008) pp. 441-467.

[23] P. Gaborit and G. Zémor, On the construction of dense lattices with a given automorphism group, *Annales de l'Institut Fourier*, vol. 57 No. 4 (2007), pp. 1051–1062.

[24] J. Boutros and G. Zémor, On quasi-cyclic interleavers for parallel turbo codes, *IEEE Trans. on Information Theory*, IT-52, No 4 (2006) pp. 1732–1739.

[25] A. Barg and G. Zémor, Distance properties of expander codes, *IEEE Trans. on Information Theory*, IT-52, No 1 (2006) pp. 78–90.

[26] Y. O. Hamidoune, O. Serra et G. Zémor, On the critical pair theory in $\mathbb{Z}/p\mathbb{Z}$, *Acta Arithmetica*, Vol. 121, No 2, (2006) pp. 99–115.

[27] A. Barg, and G. Zémor, Concatenated codes : serial and parallel, *IEEE Trans. on Information theory*, IT-51, No 5 (2005) pp. 1625–1634.

[28] A. Barg, and G. Zémor, Error exponents of expander codes under linear-complexity decoding, *SIAM J. on Discrete Mathematics*, vol. 17, No 3, (2004) pp. 426–445.

[29] J-P. Tillich and G. Zémor, The Gaussian isoperimetric inequality and error probabilities for the Gaussian channel, *IEEE Trans. on Information theory*, IT-50 No 2 (2004) pp. 328–331.

[30] A. Barg, and G. Zémor, Error exponents of expander codes, *IEEE Trans. on Information theory*, IT-48 No 6, (2002) pp. 1725–1729.

[31] A. Barg, G. Cohen, S. Encheva, G. Kabatianski and G. Zémor, A hypergraph approach to the identifying parent property: the case of multiple parents, *SIAM J. on Discrete Math.*, vol. 14, No 3, (2001) pp. 423–431.

[32] G. Zémor, On Expander Codes, *IEEE Trans. on Information theory*, IT-47 No 2, (2001) pp. 835–837.

[33] G. Cohen, S. Litsyn, and G. Zémor, Binary B_2-Sequences : a new upper bound, *JCT-A*, vol. 94, No 1 (2001) pp 152–155.

[34] G. Cohen, I. Honkala, A. Lobstein and G. Zémor, On codes identifying vertices in the two-dimensional square lattice with diagonals, *IEEE Trans. on Computers* vol. 50 (2001) pp. 174–176.

[35] O. Serra and G. Zémor, On a generalisation of a theorem by Vosper, *INTEGERS* Electronic J. Combinatorial Number Theory 0 (2000) #*A*10.

[36] G. Cohen, I. Honkala, A. Lobstein and G. Zémor, Bounds for codes identifying vertices in the hexagonal grid, *Siam Journal on Discrete Math.*, vol. 13, No 4, (2000) pp. 492–504.

[37] J-P Tillich and G. Zémor, Isoperimetric inequalities and the probability of a decoding error, *Combinatorics, Probability & Computing*, vol. 9, (2000) pp. 465–479.

[38] G. Cohen, S. Encheva and G. Zémor, Copyright protection for digital data, *IEEE Communications letters*, 4, (2000) pp. 158–160.

[39] L. Bassalygo, G. Cohen and G. Zémor, Codes with forbidden distances, *Discrete Math.* 213, (2000) pp. 3–11.

[40] G. Cohen, S. Encheva and G. Zémor, Antichain codes, *Designs, Codes and Cryptography*, vol. 18 (1999) pp. 71–80.

[41] G. Cohen, J. Rifá, J. Tena and G. Zémor, On the Characterization of Linear Uniquely Decodable Codes, *Designs, Codes and Cryptography*, vol. 17, No 1/2/3, (1999) pp. 87–96.

[42] G. Cohen and G. Zémor, Subset sums and coding theory, *Astérisque*, 258, (1999) pp. 327–339.

[43] G. Cohen, I. Honkala, A. Lobstein and G. Zémor, New Bounds for Codes Identifying Vertices in Graphs, *The Electronic Journal of Combinatorics*, vol. 6(1) (1999) R19.

[44] G. Zémor, An upper bound on the size of the Snake-in-the-box, *Combinatorica*, 17 (2) (1997) pp. 287–298.

[45] J-P. Tillich and G. Zémor, Optimal cycle codes constructed from Ramanujan graphs, *Siam Journal on Discrete Math.*, vol. 10, No 3, (1997) pp. 447–459.

[46] L. Decreusefond and G. Zémor, On the error-correcting capabilities of cycle codes of graphs, *Combinatorics, Probability & Computing*, vol. 6 (1997) pp. 27–38.

[47] Y. O. Hamidoune and G. Zémor, On zero-free subset sums, *Acta Arithmetica*, LXXVIII (1996) pp. 143–153.

[48] G. Cohen, S. Litsyn, and G. Zémor, On greedy algorithms in coding theory, *IEEE Trans. on Information theory*, IT-42 (1996) pp. 2053–2057.

[49] G. Cohen, S. Litsyn, and G. Zémor, On the traveling salesman problem in Hamming spaces, *IEEE Trans. on Information theory*, IT-42 (1996) pp. 1274–1276.

[50] G. Cohen, S. Litsyn, A. Vardy and G. Zémor, Tilings of binary Spaces, *Siam Journal on Discrete Math.*, vol. 9 No 3, (1996) pp. 393–412.

[51] G. Zémor and G. Cohen, The threshold probability of a code, *IEEE Trans. on Information theory*, IT-41 (1995) pp. 469–477.

[52] G. Cohen, S. Litsyn and G. Zémor, Upperbounds on generalized distances *IEEE Trans. on Information theory*, IT-40 (1994) pp. 2090–2092.

[53] G. Cohen and G. Zémor, Intersecting codes and independent families *IEEE Trans. on Information theory*, IT-40 (1994) pp. 1872–1881.

[54] G. Zémor, Hash functions and Cayley Graphs, *Designs, Codes and Cryptography*, 4 (1994) pp. 381-394.

[55] G. Zémor, A generalisation to non-commutative groups of a theorem of Mann, *Discrete Math.* 126 (1994) pp. 365–372.

[56] G. Cohen and G. Zémor, Write-Isolated Memories, *Discrete Math.* vol. 114 (1993).

[57] G. Zémor, Subset sums in binary spaces, *European Journal of Combinatorics*, 13 (1992) pp. 221-230.

[58] G. Zémor and G. Cohen, Applications of coding theory to interconnection networks *Discrete Applied Math.* 37/38 (1992) pp. 553-562.

[59] G. Zémor and G. Cohen, Error-correcting WOM-codes, *IEEE Trans. on Information theory*, IT-37 (1991) pp. 730-735.

[60] G. Zémor, On positive and negative atoms of Cayley digraphs, *Discrete Appl. Math.* 23 (1989) pp. 193-195.

[61] G. Cohen and G. Zémor, An application of combinatorial group theory to coding, *ARS COMBINATORIA* 23 A (1987) pp. 81–89.

Conference proceedings

[62] G. Spini and G. Zémor, Perfectly Secure Message Transmission in Two Rounds, *Theory of Cryptography Conference (TCC)* 2016-B, Beijing, LNCS 9985, pp. 286–304.

[63] G. Spini and G. Zémor, Secure Network Coding with Feedback, *IEEE Symposium on Information Theory, ISIT 2016*, July 10-15, Barcelona, pp. 2339–2343.

[64] A. Leverrier, J-P. Tillich and G. Zémor, Quantum Expander Codes, *56th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 810–824, 2015.

[65] P. Gaborit, O. Ruatta, J. Schrek and G. Zémor, RankSign: An Efficient Signature Algorithm Based on the Rank Metric, *PQCrypto 2014*, LNCS 8772, Springer.

[66] P. Gaborit, O. Ruatta, J. Schrek and G. Zémor, New Results for Rank-Based Cryptography, *AfricaCrypt 2014*, LNCS 8469, Springer, pp. 1–12.

[67] G. Castagnos, S. Renner and G. Zémor, High-order masking by using coding theory and its application to AES, *14th IMA International Conference on Cryptography and Coding, IMACC 2013, LNCS 8308, pp. 193-212, 2013.*

[68] N. Kashyap and G. Zémor, Upper Bounds on the Size of Grain-Correcting Codes, *IEEE Symposium on Information Theory, ISIT 2013*, July 7-12, Istanbul.

[69] N. di Pietro, G. Zémor and J. Boutros, New results on Construction A Lattices based on Very Sparse Parity-Check Matrices, *IEEE Symposium on Information Theory, ISIT 2013*, July 7-12, Istanbul.

[70] N. di Pietro, J. Boutros, G. Zémor and L. Brunel, Integer Low-Density Lattices based on Construction A. *2012 IEEE Information Theory Workshop, ITW 2012*, September 3–7, Lausanne.

[71] P. Gaborit, J. Schrek and G. Zémor, Full Cryptanalysis of the Chen Identification Protocol. *Post-Quantum Cryptography 4th International Workshop*, PQCrypto 2011, Taipei. LNCS 7071, pp. 35–50.

[72] A. Couvreur, N. Delfosse and G. Zémor, A Construction of Quantum LDPC Codes from Cayley Graphs, Proceedings of the *IEEE Symposium on Information Theory, ISIT 2011*, July 31 - August 5, St-Petersburg.

[73] A. Barg and G. Zémor, List Decoding of Product Codes by the MinSum Algorithm, Proceedings of the *IEEE Symposium on Information Theory, ISIT 2011*, July 31 - August 5, St-Petersburg.

[74] A. Barg, A. Mazumdar and G. Zémor, Constructions of Rank Modulation Codes, Proceedings of the *IEEE Symposium on Information Theory, ISIT 2011*, July 31 - August 5, St-Petersburg.

[75] N. Delfosse and G. Zémor, Quantum erasure-correcting codes and percolation on regular tilings of the hyperbolic plane, Proc. of *IEEE Information Theory Workshop* (ITW) 2010, Dublin.

[76] O. Serra and G. Zémor, Cycle codes of graphs and MDS array codes, proceedings of *Eurocomb 2009*, Electronic Notes in Discrete Math. Vol 34, pp. 95–99.

[77] J.P. Tillich and G. Zémor Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$, Proceedings of the *IEEE Symposium on Information Theory, ISIT 2009*, Seoul, pp.799-804.

[78] G. Zémor, On Cayley Graphs, Surface Codes, and the Limits of Homological Coding for Quantum Error Correction, in *Coding and Cryptology, second international workshop IWCC 2009*, LNCS 5557, Springer pp. 259-273.

[79] C. Petit, J-J. Quisquater, J-P. Tillich and G. Zémor, Hard and easy Components of Collision Search in the Zemor-Tillich Hash Function: new Attacks and Reduced Variants with Equivalent Security, *RSA Conference 2009, Cryptographers' Track*, LNCS 5473, Springer pp. 182-194.

[80] G. Cohen, H. Randriam and G. Zémor, Witness sets, *Coding Theory and Applications*, 2nd International Castle Meeting, ISMCTA 2008, Spain, LNCS 5228, Springer, pp. 37-45.

[81] J. Boutros, G. Zémor, A. Guillén y Fàbregas and E. Biglieri, Full-Diversity Product Codes for Block Erasure and Block Fading Channels, *IEEE Information Theory Workshop* (ITW), Porto, Portugal, May 2008.

[82] J-P. Tillich and G. Zémor, Collisions for the LPS Expander Graph Hash Function, *Eurocrypt 2008*, Istanbul, LNCS 4965, Springer, pp. 254–269.

[83] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji and G. Zémor, Optimal Iris Fuzzy Sketches, *First IEEE International Conference on Biometrics: Theory, Applications, and Systems*, 2007. BTAS 2007, Washington.

[84] J. Boutros, A. Guillén y Fàbregas, E. Biglieri and G. Zémor, Design and analysis of low-density parity-check codes for block-fading channels, *Information Theory and Applications Workshop*, janvier-février 2007, Information Theory and Applications Center (ITA), UCSD.

[85] G. Cohen and G. Zémor, Syndrome coding for the wire-tap channel revisited, *IEEE Information Theory Workshop* (ITW'06) Chengdu, Chine, 2006, pp. 33–36.

[86] P. Gaborit and G. Zémor, Asymptotic improvement of the Gilbert-Varshamov bound for binary linear codes, in proc. of *IEEE International Symposium on Information Theory*, juillet 2006, pp. 287–291.

[87] J-P. Tillich and G. Zémor, On the minimum distance of structured LDPC codes with 2 variable nodes of degree 2 per parity-check equation, in proc. of *IEEE International Symposium on Information Theory*, juillet 2006, pp. 1549–1553.

[88] A. Barg and G. Zémor, Multilevel generalizations of expander codes, in *Algebraic coding theory and information theory*, A. Ashikhmin and A. Barg (Eds), Amer. Math. Soc., DIMACS series in Discrete Math. and Theoretical Computer Science, Vol. 68, pp. 69–84, 2005.

[89] G. Cohen and G. Zémor, The wire-tap channel applied to biometrics, *International Symposium on Information Theory and Applications*, Parma, Italie, octobre 2004.

[90] S. Léveiller, G. Zémor, J. Boutros, and P. Guillot, A new cryptanalytic attack for PN-generators filtered by a Boolean function, *Selected areas in Cryptography*, 9th Annual workshop, St. John's, Lecture notes in Comput. Sci. 2595, Springer-Verlag, 2003, pp. 232–249.

[91] G. Cohen, S. Litsyn et G. Zémor, Binary codes for collusion-secure fingerprinting, in *ICISC 2001*, 4th International Conference Seoul, Lecture Notes in Comput. Sci. 2288, Springer-Verlag, 2002, pp. 178–185.

[92] S. Léveiller, J. Boutros, P. Guillot, and G. Zémor, Cryptanalysis of Nonlinear Filter Generators with $\{0,1\}$-Metric Viterbi Decoding, in *Cryptography and Coding*, 8th IMA International Conference Cirencester, Lecture notes in Comput. Sci. 2260, Springer-Verlag, 2001, pp. 402–414.

[93] G. Cohen, I. Honkala, A. Lobstein and G. Zémor, On identifying codes, in *Codes and Association Schemes*, A. Barg and S. Litsyn Eds., Vol. 54 of DIMACS Series in discrete math. and theoretical computer science, AMS 2001, pp. 97–109.

[94] G. Zémor, On iterative decoding of cycle codes of graphs, in *Codes, Systems, and Graphical Models*, Vol. 123 of IMA Volumes in Math. and its Applications, Springer-Verlag, 2001, pp. 311–326.

[95] H. Sawaya, S. Vialle, J. Boutros and G. Zémor, Performance Limits of Compound Codes with Symbol-Based Iterative Decoding, in *WCC2001, International Workshop on Coding and Cryptography*, Electronic Notes in Discrete Math., Vol. 6, April 2001, pp 433-443.

[96] J-P Tillich and G. Zémor, An Overview of the Isoperimetric Method in Coding Theory, (invited paper) in *Cryptography and Coding*, Cirencester, december 1999, Lecture notes in Comput. Sci. 1746, Springer-Verlag, pp 129–134.

[97] J. Boutros, O. Pothier and G. Zémor, Generalized low density (Tanner) codes, in *IEEE International Conference on Communications, ICC'99*, june 1999, pp. 441–445 vol. 1.

[98] G. Cohen, A. Lobstein, D. Naccache and G. Zémor, How to improve an exponentiation black-box, in *Eurocrypt'98* Lecture notes in Comput. Sci. 1403, Springer-Verlag, pp. 211–220.

[99] J-P Tillich and G. Zémor, Hashing with SL_2, in CRYPTO'94, Lecture notes in Comput. Sci. 839, Springer-Verlag, pp. 40–49.

[100] G. Cohen, Ll Huguet and G. Zémor, Bounds on generalized weights, in *First French-Israeli workshop on algebraic coding*, Paris, july 1993 Lecture notes in Comput. Sci. 781, Springer-Verlag, pp. 270–277.

[101] J-P Tillich and G. Zémor, Group-theoretic hash functions, in *First French-Israeli workshop on algebraic coding*, Paris, july 1993 Lecture notes in Comput. Sci. 781, Springer-Verlag, pp. 90–110.

[102] G. Zémor, Threshold effects in codes, in *First French-Israeli workshop on algebraic coding*, Paris, july 1993 Lecture notes in Comput. Sci. 781, Springer-Verlag, pp. 278–286.

[103] G. Cohen, C. Van Eijl, G. Zémor, Error-correcting for WIMs and WUMs, *AAECC9* New Orleans, oct. 1991, Lecture notes in Comput. Sci. 539, Springer-Verlag, pp. 159–170.

[104] G. Zémor, An extremal problem related to the covering radius of binary codes, *First French-Soviet workshop on algebraic coding* Paris, july 1991, Lecture notes in Comput. Sci. 573 Springer-Verlag, pp. 42–51.

[105] G. Zémor, Hash functions and graphs with large girths, *Eurocrypt'91*, Lecture notes in Comput. Sci. 547, Springer-Verlag, pp. 508–511.

Biography

[106] A. Plagne, O. Serra and G. Zémor, Yahya Ould Hamidoune's mathematical journey: A critical review of his work, *European Journal of Combinatorics*, Vol. 34 (2013) 1207–1222.

Book

[107] G. Zémor, *Cours de cryptographie*, Cassini, 2000.

Patent

[108] (WO/2010/000965) Method and device for protecting the integrity of data transmitted over a network (EN) / Procédé et dispositif de protection de l'intégrité de données transmises sur un réseau (FR).
Inventors : J. Lopez, J-M. Camus, J-M. Couveignes, G. Zémor, M. Perret.
http://www.wipo.int/pctdb/fr/wo.jsp?WO=2010000965