

# Publications

## Journals

- [1] C. LIN AND G. ZÉMOR, **Kneser’s Theorem for Codes and  $\ell$ -divisible set families**, *Finite Fields and Their Applications*, to appear.
- [2] F. ARNAULT, P. GABORIT, W. ROZENDAAL, N. SAUSSAY AND G. ZÉMOR, **A Variant of the Bravyi-Terhal Bound for Arbitrary Boundary Conditions**, *IEEE Trans. on Information Theory*, to appear.
- [3] C. AGUILAR-MELCHOR, N. ARAGON, J-C. DENEUVILLE, P. GABORIT, J. LACAN, G. ZÉMOR, **Efficient error-correcting codes for the HQC post-quantum cryptosystem**, *Designs, Codes and Cryptography*, Vol. 92, (2024) pp. 4511–4530.
- [4] W. ROZENDAAL AND G. ZÉMOR, **Analysis of the Error-Correcting Radius of a Renormalisation Decoder for Kitaev’s Toric Code**, *IEEE Trans. on Information Theory*, IT-70 No 10 (2024) pp. 7036–7048.
- [5] A. LEVERRIER AND G. ZÉMOR, **Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes**, *ACM Transactions on Algorithms*, on-line 2024.
- [6] A. LEVERRIER AND G. ZÉMOR, **Decoding Quantum Tanner Codes**, *IEEE Trans. on Information Theory*, IT-69 No 8 (2023) pp. 5100–5115.
- [7] A. BARG AND G. ZÉMOR, **High-rate storage codes on triangle-free graphs**, *IEEE Trans. on Information Theory*, IT-68 No 12 (2022) pp. 7787–7797.
- [8] N. ARAGON, O. BLAZY, J-C. DENEUVILLE, P. GABORIT AND G. ZÉMOR, **Ouroboros: An efficient and provably secure KEM family**, *IEEE Trans. on Information Theory*, IT-68 No 9 (2022) pp. 6233–6244.
- [9] S. EVRAI, T. KAUFMAN AND G. ZÉMOR, **Decodable quantum LDPC codes beyond the  $\sqrt{n}$  distance barrier using high dimensional expanders**, *SIAM J. on Computing*, special section FOCS 2020 <https://doi.org/10.1137/20M1383689>.
- [10] A. LEVERRIER, V. LONDE AND G. ZÉMOR, **Towards local testability for quantum coding**, *Quantum*, 6, 661 (2022).
- [11] F. OGGIER AND G. ZÉMOR, **Coding Constructions for Efficient Oblivious transfer from Noisy Channels**, *IEEE Trans. on Information Theory*, IT-68 No 4 (2022) pp. 2719–2734.
- [12] N. RON-ZEWI, M. WOOTTERS AND G. ZÉMOR, **Linear-time Erasure List Decoding of Expander Codes**, *IEEE Trans. on Information Theory*, IT-67 No 9 (2021) pp. 5827–5839.

- [13] N. DELFOSSE AND G. ZÉMOR, [Linear-time maximum likelihood decoding of surface codes over the quantum erasure channel](#), *Physical Review Research*, **2** 033042, July 2020.
- [14] G. SPINI AND G. ZÉMOR, [Efficient protocols for Perfectly Secure Message Transmission with applications to secure network coding](#), *IEEE Trans. on Information Theory*, IT-66 No 10 (2020) pp. 6340–6353.
- [15] N. ARAGON, P. GABORIT, A. HAUTEVILLE, O. RUATTA AND G. ZÉMOR, [Low Rank Parity Check Codes: New Decoding Algorithms and Applications to Cryptography](#), *IEEE Trans. on Information Theory*, IT-65 No 12 (2019) pp. 7697–7717.
- [16] C. BACHOC, A. COUVREUR AND G. ZÉMOR, [Towards a function field version of Freiman’s Theorem](#), *Algebraic Combinatorics*, Vol. 1 No 4 (2018) pp. 501–521.
- [17] C. AGUILAR, O. BLAZY, J-C. DENEUVILLE, P. GABORIT AND G. ZÉMOR, [Efficient Encryption from Random Quasi-Cyclic Codes](#), *IEEE Trans. on Information Theory*, IT-64 No 5 (2018) pp. 3927–3943.
- [18] N. DI PIETRO, G. ZÉMOR AND J. J. BOUTROS, [LDA Lattices Without Dithering Achieve Capacity on the Gaussian Channel](#), *IEEE Trans. on Information Theory*, IT-64 No 3 (2018) pp. 1561–1594.
- [19] C. BACHOC, O. SERRA AND G. ZÉMOR, [Revisiting Kneser’s Theorem for Field Extensions](#), *Combinatorica*, Vol. 39 No 4 (2018) pp. 759–777.
- [20] 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.
- [21] 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.
- [22] 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.
- [23] 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.
- [24] 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.

- [25] 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.
- [26] 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.
- [27] 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.
- [28] 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.
- [29] 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.
- [30] 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.
- [31] 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.
- [32] 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.
- [33] 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.
- [34] 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.
- [35] 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.

- [36] 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.
- [37] 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).
- [38] 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.
- [39] 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.
- [40] 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.
- [41] 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.
- [42] A. BARG AND G. ZÉMOR, [Distance properties of expander codes](#), *IEEE Trans. on Information Theory*, IT-52, No 1 (2006) pp. 78–90.
- [43] 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.
- [44] A. BARG, AND G. ZÉMOR, [Concatenated codes : serial and parallel](#), *IEEE Trans. on Information theory*, IT-51, No 5 (2005) pp. 1625–1634.
- [45] 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.
- [46] J-P. TILICH 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.
- [47] A. BARG, AND G. ZÉMOR, [Error exponents of expander codes](#), *IEEE Trans. on Information theory*, IT-48 No 6, (2002) pp. 1725–1729.
- [48] 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.

- [49] G. ZÉMOR, **On Expander Codes**, *IEEE Trans. on Information theory*, IT-47 No 2, (2001) pp. 835–837.
- [50] 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.
- [51] 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.
- [52] O. SERRA AND G. ZÉMOR, On a generalisation of a theorem by Vosper, ***INTEGERS Electronic J. Combinatorial Number Theory* 0 (2000) #A10.**
- [53] 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.
- [54] J-P TILlich AND G. ZÉMOR, Isoperimetric inequalities and the probability of a decoding error, *Combinatorics, Probability & Computing*, vol. 9, (2000) pp. 465–479.
- [55] G. COHEN, S. ENCHEVA AND G. ZÉMOR, Copyright protection for digital data, *IEEE Communications letters*, 4, (2000) pp. 158–160.
- [56] L. BASSALYGO, G. COHEN AND G. ZÉMOR, Codes with forbidden distances, *Discrete Math.* 213, (2000) pp. 3–11.
- [57] G. COHEN, S. ENCHEVA AND G. ZÉMOR, Antichain codes, *Designs, Codes and Cryptography*, vol. 18 (1999) pp. 71–80.
- [58] 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.
- [59] G. COHEN AND G. ZÉMOR, Subset sums and coding theory, *Astérisque*, 258, (1999) pp. 327–339.
- [60] 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.
- [61] G. ZÉMOR, An upper bound on the size of the Snake-in-the-box, *Combinatorica*, 17 (2) (1997) pp. 287–298.
- [62] 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.

- [63] L. DECREUSEFOND AND G. ZÉMOR, On the error-correcting capabilities of cycle codes of graphs, *Combinatorics, Probability & Computing*, vol. 6 (1997) pp. 27–38.
- [64] Y. O. HAMIDOUNE AND G. ZÉMOR, On zero-free subset sums, *Acta Arithmetica*, LXXVIII (1996) pp. 143–153.
- [65] G. COHEN, S. LITSYN, AND G. ZÉMOR, On greedy algorithms in coding theory, *IEEE Trans. on Information theory*, IT-42 (1996) pp. 2053–2057.
- [66] 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.
- [67] 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.
- [68] G. ZÉMOR AND G. COHEN, The threshold probability of a code, *IEEE Trans. on Information theory*, IT-41 (1995) pp. 469–477.
- [69] G. COHEN, S. LITSYN AND G. ZÉMOR, Upperbounds on generalized distances *IEEE Trans. on Information theory*, IT-40 (1994) pp. 2090–2092.
- [70] G. COHEN AND G. ZÉMOR, Intersecting codes and independent families *IEEE Trans. on Information theory*, IT-40 (1994) pp. 1872–1881.
- [71] G. ZÉMOR, Hash functions and Cayley Graphs, *Designs, Codes and Cryptography*, 4 (1994) pp. 381–394.
- [72] G. ZÉMOR, A generalisation to non-commutative groups of a theorem of Mann, *Discrete Math.* 126 (1994) pp. 365–372.
- [73] G. COHEN AND G. ZÉMOR, Write-Isolated Memories, *Discrete Math.* vol. 114 (1993).
- [74] G. ZÉMOR, Subset sums in binary spaces, *European Journal of Combinatorics*, 13 (1992) pp. 221–230.
- [75] G. ZÉMOR AND G. COHEN, Applications of coding theory to interconnection networks *Discrete Applied Math.* 37/38 (1992) pp. 553–562.
- [76] G. ZÉMOR AND G. COHEN, Error-correcting WOM-codes, *IEEE Trans. on Information theory*, IT-37 (1991) pp. 730–735.
- [77] G. ZÉMOR, On positive and negative atoms of Cayley digraphs, *Discrete Appl. Math.* 23 (1989) pp. 193–195.

- [78] G. COHEN AND G. ZÉMOR, An application of combinatorial group theory to coding, *ARS COMBINATORIA* 23 A (1987) pp. 81–89.

### Conference proceedings

- [79] WOUTER ROZENDAAL AND G. ZÉMOR, A worst-case analysis of a renormalisation decoder for Kitaev’s toric code, *IEEE Symposium on Information Theory, ISIT 2023*, pp. 625–629.
- [80] A. LEVERRIER AND G. ZÉMOR, **Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes**, *ACM-SIAM Symposium on Discrete Algorithms (SODA23)*, pp. 1216–1244.
- [81] A. LEVERRIER AND G. ZÉMOR, **Quantum Tanner Codes**, *63rd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 872–883, 2022.
- [82] C. AGUILAR-MELCHOR, N. ARAGON, V. DYSERYN, P. GABORIT AND G. ZÉMOR, **LRPC Codes with Multiple Syndromes: Near Ideal-Size KEMs Without Ideals** *Post-Quantum Cryptography - PQCrypto 2022*, Springer LNCS 13512, pp. 45–68.
- [83] A. LEVERRIER, V. LONDE AND G. ZÉMOR, Towards Local Testability for Quantum Coding **Towards Local Testability for Quantum Coding**, *12th Innovations in Theoretical Computer Science Conference (ITCS)*, 2021.
- [84] S. EVRAI, T. KAUFMAN AND G. ZÉMOR, **Decodable quantum LDPC codes beyond the square root distance barrier using high dimensional expanders**, *IEEE 61st Annual Symposium on Foundations of Computer Science FOCS*, pp. 218–227, 2020.
- [85] N. RON-ZWI, M. WOOTTERS AND G. ZÉMOR, **Linear-time erasure list-decoding of expander codes**, *IEEE Symposium on Information Theory, ISIT 2020*, pp. 379–383.
- [86] C. GAVOILLE, G. KACHIGAR AND G. ZÉMOR, **Localisation-Resistant Random Words with Small Alphabets**, in *Combinatorics on Words, Proceedings*, 2019, Springer LCNS 11682, pp. 193–206.
- [87] N. ARAGON, O. BLAZY, P. GABORIT, A. HAUTEVILLE AND G. ZÉMOR, **Durandal: a rank metric based signature scheme**, *Eurocrypt 2019*, Springer LNCS 11478, pp. 728–758.

- [88] J. BOUTROS, U. EREZ, J. VAN WONTERGHEM, G. SHAMIR AND G. ZÉMOR, **Geometric shaping: low-density coding of Gaussian-like constellations**, *2018 IEEE Information Theory Workshop (ITW)*, 25-29 Nov. 2018, publisher IEEE.
- [89] J-C. DENEUVILLE, P. GABORIT AND G. ZÉMOR, **Ourobouros: A simple, secure and efficient key exchange protocol based on Coding Theory**, *Post-Quantum Cryptography - PQCrypto 2017* Utrecht, Springer LNCS 10346, pp. 18–34.
- [90] G. SPINI AND G. ZÉMOR, **Perfectly Secure Message Transmission in Two Rounds**, *Theory of Cryptography Conference (TCC) 2016-B*, Beijing, Springer LNCS 9985, pp. 286–304.
- [91] G. SPINI AND G. ZÉMOR, **Secure Network Coding with Feedback**, *IEEE Symposium on Information Theory, ISIT 2016*, July 10-15, Barcelona, pp. 2339–2343.
- [92] A. LEVERRIER, J-P. TILICH AND G. ZÉMOR, **Quantum Expander Codes**, *56th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 810–824, 2015.
- [93] P. GABORIT, O. RUATTA, J. SCHREK AND G. ZÉMOR, **RankSign: An Efficient Signature Algorithm Based on the Rank Metric**, *PQCrypto 2014*, LNCS 8772, Springer.
- [94] P. GABORIT, O. RUATTA, J. SCHREK AND G. ZÉMOR, **New Results for Rank-Based Cryptography**, *AfricaCrypt 2014*, LNCS 8469, Springer, pp. 1–12.
- [95] 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*, Springer LNCS 8308, pp. 193–212, 2013.
- [96] 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.
- [97] 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.
- [98] 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.

- [99] P. GABORIT, J. SCHREK AND G. ZÉMOR, Full Cryptanalysis of the Chen Identification Protocol. *Post-Quantum Cryptography 4th International Workshop*, PQCrypto 2011, Taipei. Springer LNCS 7071, pp. 35–50.
- [100] 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.
- [101] 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.
- [102] 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.
- [103] 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.
- [104] 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.
- [105] 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.
- [106] 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.
- [107] 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.
- [108] 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.
- [109] 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.

- [110] J-P. TILlich AND G. ZÉMOR, [Collisions for the LPS Expander Graph Hash Function](#), *Eurocrypt 2008*, Istanbul, LNCS 4965, Springer, pp. 254–269.
- [111] 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.
- [112] 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.
- [113] 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.
- [114] 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.
- [115] 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.
- [116] 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.
- [117] G. COHEN AND G. ZÉMOR, The wire-tap channel applied to biometrics, *International Symposium on Information Theory and Applications*, Parma, Italie, octobre 2004.
- [118] 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.
- [119] 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.
- [120] 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.
- [121] 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.
- [122] 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.
- [123] 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.
- [124] 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.
- [125] 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.
- [126] 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.
- [127] J-P TILlich AND G. ZÉMOR, Hashing with  $SL_2$ , in CRYPTO'94, Lecture notes in Comput. Sci. 839, Springer-Verlag, pp. 40–49.
- [128] 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.
- [129] 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.
- [130] 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.

- [131] 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.
- [132] 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.
- [133] G. ZÉMOR, Hash functions and graphs with large girths, *Eurocrypt'91*, Lecture notes in Comput. Sci. 547, Springer-Verlag, pp. 508–511.

### Biography

- [134] 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

- [135] G. ZÉMOR, *Cours de cryptographie*, Cassini, 2000.

### Patent

- [136] (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>