Curriculum Vitae

Gilles Zémor

Date of birth: January 5, 1963, Paris, France. **Citizenship:** French.

Current position: Professor, classe exceptionnelle 1, université de Bordeaux, Institut de mathématiques (IMB) UMR 5251. From October 2023 : senior member of Institut Universitaire de France.

Education and Diplomas: École normale supérieure de Fontenay-aux-Roses 1982-1986. Agrégation de mathématiques 1984. PhD from École nationale supérieure des télécommunications, 1989, under the supervision of Gerard Cohen. Thesis title: *Problèmes combinatoires liés à l'écriture sur des mémoires*. Habilitation in mathematics 2002 from university of Paris 6.

Positions held. Associate professor at École nationale supérieure des télécommunications (ENST, Telecom Paris) from September 1990 to August 2006. Professor at Mathematics Institute of Bordeaux University since September 2006. Promoted by the national council of universities (CNU) "première classe" in 2010, "classe exceptionnelle" in 2017.

Fields of Research: Information Theory, Coding Theory, Additive Combinatorics, Combinatorics, Cryptography, Quantumm error correction.

Former Ph. D. students.
Walid Benameur (2000), Sabine Leveiller (2004), Anthony Leverrier (2009, prize for best thesis ParisTech 2010), Bruno Kindarji (2010), Amandine Jambert (2010), Nicolas Delfosse (2012), Nicola di Pietro (2014), Soline Renner (2014), Diego Mirandola (2017), Gabriele Spini (2017), Ghazal Kachigar (2019), Nicolas Aragon (2020).

Current Ph. D. student. Wouter Rozendaal (2022-), *Quantum LDPC codes.*

Editorial Activities:
In 2020 guest editor for the special issue of the journal *IEEE Transactions on Information Theory* in memory of V. I. Levenshtein.
Guest Editor of Special Issue of European Journal of Combinatorics "In Memory of Yahya Ould Hamidoune", 2013.
Associate Editor for journals *IEEE Transactions on Information Theory* (2003–2006), and *Advances in mathematics of communications* (2007–2013).

Organising or Program committee of international conferences:
- Eurocrypt 2020
– IEEE International Symposium on Information Theory (ISIT) 2022 (Aalto, Finland), 2021 (Melbourne, on-line) 2020 (Los Angeles, on-line) 2019 (Paris) 2018 (Vail, Colorado), 2016 (Barcelone), 2015 (Hong-Kong). In 2019 co-chair of program committee (over 1000 attendees).
– 5th International Castle Meeting on Coding Theory and Applications, Estonia, 2017.
– International Workshop on coding and cryptography (WCC), Saint-Petersburg, 2017 (also Paris 2015, Bergen 2005, Paris 2003).

– Discrete Mathematics Days, Barcelona, 2016.
– IEEE Information Theory Workshop (ITW), Dublin 2010 (chair).
– Selected Areas in Cryptography (SAC) 2010, Waterloo.
– Twelfth IMA International Conference on Cryptography and Coding, Cirencester, 2009, 2007, 2005.

Organisation of events and conferences:
- Coorganiser of semester "Error-Correcting codes : theory and practice" at the Simons Institute, Berkeley, in 2024.
- Coorganiser with J. Boutros of IEEE Information Theory Workshop 2023 in Saint-Malo.
- Coorganiser with S. Mesnager and H. Randriam of the conference CohenFest 2016 in Paris
- Coorganiser with C. Bachoc, F. Hennecart and A. Plagne of the conference Additive Combinatorics in Bordeaux in 2016.
- Coorganiser with C. Bachoc of the conference Algebra, Codes and Networks (ACN) in 2014.
- Coorganiser with A. Shokrollahi and R. Urbanke of the semester programme Combinatorial, Algebraic and Algorithmic Aspects of Coding Theory, at the Bernoulli Center of EPFL, Lausanne, in 2011.

Grants and contracts:
- I have been awarded the PEDR and PES grants every year since 2007.
- in charge for Bordeaux of the project "NISQ2LSQ" (From NISQ to LSQ : bosonic and LDPC quantum codes), part of the national plan (PEPR) on quantum technology.
- member of the ANR projet "Barracuda" (Algebra and coding theory) 2022–2025.
- was in charge at IMB of the ANR project Code-based Cryptography (CBCRYPT) 2017–2021.
- I have been a member of the ANR project Manta (Algebraic Geometry and Coding Theory) 2016–2020.
- I was the coordinator of the PEPS (CNRS) project "Topology and quantum codes" in 2013.
- I was in charge at IMB of the ANR project COCQ Quantum error correcting codes 2009-2012.
- I was in charge of the Cifre contract with Mitsubishi Electric for the PhD thesis of N. di Pietro (2011-2013). I also obtained a DGA grant in 2009 for the thesis of N. Delfosse.

Administrative Duties:
- I was deputy director of the Mathematics Institute (IMB) in 2011 and 2012.
- I was deputy director of the doctoral school in Mathematics and Computer Science from 2014 to 2017.
- I was a member of the CNU (section 25, mathematics) from 2012 to 2015.

Recent highlight: I am involved in two proposals, BIKE and HQC, that have reached the fourth round of the standardisation process for post-quantum cryptography, organised by NIST. According to NIST, one of those proposals, using code-based cryptography, will be chosen as a standard for post-quantum cryptography.

Teaching: In charge since 2007 of the Master Course "Cryptology and Information Security" of Bordeaux University.

Publications

Journals

[1] A. Leverrier and G. Zémor, Decoding Quantum Tanner Codes, *IEEE Trans. on Information Theory*, IT-69 No 8 (2023) pp. 5100–5115.

[2] 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.

[3] 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.

[4] 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,* to appear.

[5] A. Leverrier, V. Londe and G. Zémor, Towards local testability for quantum coding, *Quantum*, 6, 661 (2022).

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] C. Bachoc, O. Serra and G. Zémor, Revisiting Kneser's Theorem for Field Extensions, *Combinatorica,* Vol. 39 No 4 (2018) pp. 759–777.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

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

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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).

[33] 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.

[34] 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.

[35] 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.

[36] 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.

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

[38] 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.

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

[40] 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.

[41] 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.

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

[43] 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.

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

[45] 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.

[46] 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.

[47] O. Serra and G. Zémor, On a generalisation of a theorem by Vosper, *INTEGERS* Electronic J. Combinatorial Number Theory 0 (2000) $\#A10$.

[48] 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.

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

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

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

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

[53] 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.

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

[55] 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.

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

[57] 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.

[58] L. DECREUSEFOND AND G. ZÉMOR, On the error-correcting capabilities of cycle codes of graphs, *Combinatorics, Probability & Computing*, vol. 6 (1997) pp. 27–38.

[59] Y. O. HAMIDOUNE AND G. ZÉMOR, On zero-free subset sums, *Acta Arithmetica*, LXXVIII (1996) pp. 143–153.

[60] G. COHEN, S. LITSYN, AND G. ZÉMOR, On greedy algorithms in coding theory, *IEEE Trans. on Information theory*, IT-42 (1996) pp. 2053–2057.

[61] 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.

[62] 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.

[63] G. ZÉMOR AND G. COHEN, The threshold probability of a code, *IEEE Trans. on Information theory*, IT-41 (1995) pp. 469–477.

[64] G. COHEN, S. LITSYN AND G. ZÉMOR, Upperbounds on generalized distances *IEEE Trans. on Information theory*, IT-40 (1994) pp. 2090–2092.

[65] G. COHEN AND G. ZÉMOR, Intersecting codes and independent families *IEEE Trans. on Information theory*, IT-40 (1994) pp. 1872–1881.

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

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

[68] G. COHEN AND G. ZÉMOR, Write-Isolated Memories, *Discrete Math.* vol. 114 (1993).

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

[70] G. ZÉMOR AND G. COHEN, Applications of coding theory to interconnection networks *Discrete Applied Math.* 37/38 (1992) pp. 553-562.

[71] G. ZÉMOR AND G. COHEN, Error-correcting WOM-codes, *IEEE Trans. on Information theory*, IT-37 (1991) pp. 730-735.

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

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

Conference proceedings

[74] 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.

[75] A. Leverrier and G. Zémor, Quantum Tanner Codes, *63rd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, to appear, 2022.

[76] 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.

[77] 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.

[78] 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.

[79] 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.

[80] 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.

[81] 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.

[82] 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.

[83] 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.

[84] 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.

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

[86] 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.

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

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

[89] 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.*

[90] 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.

[91] 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.

[92] 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.

[93] 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.

[94] 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.

[95] 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.

[96] 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.

[97] 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.

[98] 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.

[99] 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.

[100] 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.

[101] 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.

[102] 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.

[103] 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.

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

[105] 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.

[106] 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.

[107] 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.

[108] 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.

[109] 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.

[110] 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.

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

[112] 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.

[113] 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.

[114] 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.

[115] 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.

[116] 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.

[117] 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.

[118] 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.

[119] 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.

[120] 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.

[121] J-P TILLICH AND G. ZÉMOR, Hashing with SL_2, in CRYPTO'94, Lecture notes in Comput. Sci. 839, Springer-Verlag, pp. 40–49.

[122] 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.

[123] 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.

[124] 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.

[125] 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.

[126] 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.

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

Biography

[128] 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

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

Patent

[130] (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