Liste de publications P. Gaborit (2014)

profil google:

http://scholar.google.fr/citations?hl=fr&user=ClOD3r4AAAAJ&view_op=list_works&gmla=AJsN-F4guUJ39mDNk9h1xHM6zwYLd712xKJpYv0yGfYihwUuCfMF68QqCNPIVlkaXdui3flmSNK5e9KkJzNyGPQyrvdkaP4LtHLvQZPoAA2rJGe_NdulCry9bmqZ7JT_4fYxwIe5iP8D

- **Ouvrages individuels et collectifs** *:*

- Philippe Gaborit (Ed.): Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings, LNCS, 7932, springer 2013.

- Identity-based cryptography, chapitre 8 : « ***Identity-based Identification and Signature Schemes using Error Correcting Codes »*** *, P.L. Cayrel, P.Gaborit et M.Girault(2009)*

Articles dans des revues internationales a comité de lecture :

Auteur de 30 articles dans des publications internationales dont 11 IEEE Trans. On Inf. Theory, mais aussi Theoretical Computer Science, Discrete Math. ou J. Comb. Theory.

- 30. W. Abdul, P.Carré et P. Gaborit : Correcting Codes for Robust Color Wavelet Watermarking, EURASIP Journal of information security 1 (2013)

- 29. Claude Carlet, Philippe Gaborit, Jon-Lark Kim, Patrick Solé: A New Class of Codes for Boolean Masking of Cryptographic Computations. IEEE Transactions on Information Theory 58(9): 6000-6011 (2012)

- 28. Carlos Aguilar Melchor, Philippe Gaborit, Jon-Lark Kim, Lin Sok, Patrick Solé: Classification of Extremal and s-Extremal Binary Self-Dual Codes of Length 38. IEEE Transactions on Information Theory 58(4): 2253-2262 (2012)

- 27 Carlos Aguilar Melchor, Pierre-Louis Cayrel, Philippe Gaborit, Fabien Laguillaumie: A New Efficient Threshold Ring Signature Scheme Based on Coding Theory. IEEE Transactions on Information Theory 57(7): 4833-4842 (2011)

- 26. Carlos Aguilar, Christophe Chabot, Philippe Gaborit, There is no Euclidean self-dual quaternary [18,9,7] codes, Inter. Jour. Information and Coding Theory, Vol 1, Issue 2, 2010, p. 200-207.

- 25 Carlos Aguilar, Boussad Ait Salem, P. Gaborit et K. Tamine, Active Detection of Node Replication Attacks, International Journal on Computer Science and Network Security, Vol. 9 No. 2 pp. 13-21

- 24. Carlos Aguilar Melchor , Philippe Gaborit: On the Classification of Extremal [36, 18, 8] Binary Self-Dual Codes. IEEE Transactions on Information Theory 54IEEE Transactions on Information Theory 54 (10): 4743-4750 (2008)

- 23. Philippe Gaborit, Gilles ZémorGilles Zémor : Asymptotic Improvement of the Gilbert-Varshamov Bound for Linear Codes. IEEE Transactions on Information Theory 54IEEE Transactions

on Information Theory 54 (9): 3865-3872 (2008)

- 22. Oliver D. King Oliver D. King , Philippe Gaborit: Binary templates for comma-free DNA codes. Discrete Applied Mathematics 155Discrete Applied Mathematics 155 (6-7): 831-839 (2007)

- 21. Gaborit, Philippe A bound for certain s-extremal lattices and codes. Arch. Math. (Basel)Arch. Math. (Basel) 89 (2007), no. 2,89 (2007), no. 2, 143—151.

- 20. Gaborit, Philippe ; Zémor, GillesZémor, Gilles On the construction of dense lattices with a given automorphisms group. Ann. Inst. Fourier (Grenoble)Ann. Inst. Fourier (Grenoble) 57 (2007), no. 4,57 (2007), no. 4, 1051—1062.

- 19. Bautista, Evangeline P. ; Gaborit, PhilippeGaborit, Philippe ; Kim, Jon-LarkKim, Jon-Lark ; Walker, Judy L.Walker, Judy L. s-extremal additive ${F}_4$ codes. Adv. Math. Commun.Adv. Math. Commun. 1 (2007), no. 1,1 (2007), no. 1, 111—130.

-18 Claude Carlet , Philippe Gaborit: Hyper-bent functions and cyclic codes. J. Comb. Theory, Ser. A 113J. Comb. Theory, Ser. A 113 (3): 466-482 (2006)

-17. Hans Dobbertin , Gregor LeanderGregor Leander , Anne CanteautAnne Canteaut , Claude CarletClaude Carlet , Patrick FelkePatrick Felke , Philippe Gaborit: Construction of bent functions via Niho power functions. J. Comb. Theory, Ser. A 113J. Comb. Theory, Ser. A 113 (5): 779-798 (2006)

-16. Philippe Gaborit, Carmen-Simona NedeloaiaCarmen-Simona Nedeloaia , Alfred WassermannAlfred Wassermann : On the weight enumerators of duadic and quadratic residue codes. IEEE Transactions on Information Theory 51 (1): 402-407 (2005)

-15. Philippe Gaborit, Oliver D. KingOliver D. King : Linear constructions for DNA codes. Theor. Comput. Sci. 334Theor. Comput. Sci. 334 (1-3): 99-113 (2005)

-14 Christine Bachoc, Philippe Gaborit: Designs and self-dual codes with long shadows. J. Comb. Theory, Ser. A 105(1): 15-34 (2004)

- 13. Philippe Gaborit: Construction of new extremal unimodular lattices. Eur. J. Comb. 25(4): 549-564 (2004)

- 12. Philippe Gaborit, Jon-Lark Kim, Vera Pless: Decoding Binary ItR(25) by Hand. Discrete Mathematics 264(1-3): 55-74 (2003)

-11. Philippe Gaborit: Quadratic Double Circulant Codes over Fields. J. Comb. Theory, Ser. A 97(1): 85-107 (2002)

- 10 J. E. Fields, Philippe Gaborit, W. Cary Huffman, Vera Pless: On the classification of extremal even formally self-dual codes of lengths 20 and 22. Discrete Applied Mathematics 111(1-2): 75-86 (2001)

-9 Philippe Gaborit, Masaaki Harada: Construction of Extremal Type II Codes over Z. Des. Codes Cryptography 16(3): 257-269 (1999)

-8 Alexis Bonnecaze, Philippe Gaborit, Masaaki Harada, Masaaki Kitazume, Patrick Solé: Niemeier lattices and Type II codes over Z4. Discrete Mathematics 205(1-3): 1-21 (1999)

-7 J. E. Fields, Philippe Gaborit, W. Cary Huffman, Vera Pless: On the Classification of Extremal Even Formally Self-Dual Codes. Des. Codes Cryptography 18(1/3): 125-148 (1999)

- 6 Steven T. Dougherty, Philippe Gaborit, Masaaki Harada, Patrick Solé: Type II Codes Over F2 +

u F2. IEEE Transactions on Information Theory 45(1): 32-45 (1999)

- 5 Joe Fields, Philippe Gaborit: On the non Z4-linearity of certain good binary codes. IEEE Transactions on Information Theory 45(5): 1674-1677 (1999)

-4 Toru Aoki, Philippe Gaborit, Masaaki Harada, Michio Ozeki, Patrick Solé: On the covering radius of Z4-codes and their lattices. IEEE Transactions on Information Theory 45(6): 2162-2168 (1999)

-3 Steven T. Dougherty, Philippe Gaborit, Masaaki Harada, Akihiro Munemasa, Patrick Solé: Type IV self-dual codes over rings. IEEE Transactions on Information Theory 45(7): 2345-2360 (1999)

- 2 Joe Fields, Philippe Gaborit, Jeffrey S. Leon, Vera Pless: All Self-Dual Z4 Codes of Length 15 or Less Are Known. IEEE Transactions on Information Theory 44(1): 311-322 (1998)

- 1 Philippe Gaborit: Mass formulas for self-dual codes over Z4 and Fq+uFq rings. IEEE Transactions on Information Theory 42(4): 1222-1228 (1996)

- **<u>Articles dans des conférences:</u>**

- 27 A. Couvreur, Philippe Gaborit, V. Gauthier-Umana, A. Otmani, JP TIllich: Distinguisher-Based Attacks on Public-Key Cryptosystems Using Reed-Solomon Codes
proceedings of Workshop on codes and cryptography WCC 2013

- 26 Philippe Gaborit, Gaetan Murat, Oliver ruatta and G. zémor: LRPC codes and their applications to cryptography,
proceedings of Workshop on codes and cryptography WCC 2013

- 25 C. Aguilar, S. Bettaieb, Philippe Gaborit, J. Schrek: A Code-Based Undeniable Signature Scheme, IMA Int. Conf 2013. : 99-119

– 24 C. Aguilar, S. Bettaieb, X. Boyen Philippe Gaborit: Adapting Lyubashevsky's Signature Schemes to the Ring Signature Setting, AFRIcarypt 2013.: 1-25

- 23. Philippe Gaborit, Julien Schrek: Efficient code-based one-time signature from automorphism groups with syndrome compatibility. ISIT 2012: 1982-1986

- 22. Philippe Gaborit, Julien Schrek, Gilles Zémor: Full Cryptanalysis of the Chen Identification Protocol. PQCrypto 2011: 35-50

- 21. Carlos Aguilar Melchor, Philippe Gaborit, Julien Schrek: A new zero-knowledge code based identification scheme with reduced communication , ITW 2011.

- 20. P. Gaborit, Javier HerranzJavier Herranz : Additively Homomorphic Encryption with d-Operand Multiplications. CRYPTO 2010 : 138-154

- 19. Frederik ArmknechtFrederik Armknecht , Claude CarletClaude Carlet , Philippe Gaborit, Simon KünzliSimon Künzli , Willi MeierWilli Meier , Olivier RuattaOlivier Ruatta : Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks. EUROCRYPT 2006

: 147-164

- 18 . Delphine BoucherDelphine Boucher , Philippe Gaborit, Willi GeiselmannWilli Geiselmann , Olivier RuattaOlivier Ruatta , Felix UlmerFelix Ulmer : Key Exchange and Encryption Schemes Based on Non-commutative Skew Polynomials.PQCrypto 2010 : 126-141

- 17. Thierry P. BergerThierry P. Berger , Pierre-Louis CayrelPierre-Louis Cayrel , Philippe Gaborit, Ayoub OtmaniAyoub Otmani : Reducing Key Length of the McEliece Cryptosystem. AFRICACRYPT 2009: 77-97

-16 Carlos Aguilar MelchorCarlos Aguilar Melchor , Boussad Ait SalemBoussad Ait Salem , Philippe Gaborit: A Collusion-Resistant Distributed Scalar Product Protocol with Application to Privacy-Preserving Computation of Trust. NCA 2009NCA 2009 : 140-147

-15 - Wadood AbdulWadood Abdul , Philippe CarréPhilippe Carré , Philippe Gaborit: List decoding of Reed Solomon codes for wavelet based colour image watermarking scheme. IEEE ICIP 2009ICIP 2009 : 3637-3640

- 14 . Pierre-Louis CayrelPierre-Louis Cayrel , Philippe Gaborit, Emmanuel ProuffEmmanuel Prouff : Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices. CARDIS 2008CARDIS 2008 : 191-205

- 13. Carlos Aguilar MelchorCarlos Aguilar Melchor , Benoît CrespinBenoît Crespin , Philippe Gaborit, Vincent JolivetVincent Jolivet , Pierre RousseauPierre Rousseau : High-Speed Private Information Retrieval Computation on GPU. IEEE SECURWARE 2008 : 263-272

- 12 Carlos Aguilar, Guilhem Castagnos et Philippe Gaborit, Lattice-based homomorphic encryption of vector spaces, (IEEE ISIT'08) p.1858-1862

- 11. Carlos Aguilar et P. Gaborit A Fast Private Information Retrieval Protocol, The 2008 IEEE International Symposium on Information Theory (IEEE ISIT'08). p. 1848-1852

-10. Carlos Aguilar Melchor , Pierre-Louis CayrelPierre-Louis Cayrel , Philippe Gaborit: A New Efficient Threshold Ring Signature Scheme Based on Coding Theory. PQCrypto 2008PQCrypto 2008 : 1-16

- 9 Philippe Gaborit et Marc Girault, Lightweight code-based identification and signature ISIT 2007. IEEE ISIT 24-29 June 2007 Page(s):191 - 195

-8 Gaborit, Philippe; Lauradoux, Cedric; Sendrier, Nicolas; SYND: a Fast Code-Based Stream Cipher with a Security Reduction,Information Theory, 2007. ISIT 2007. IEEE International Symposium on Information Theory, 2007. ISIT 2007. IEEE International Symposium on 24-29 June 2007 Page(s):186 – 190

-7 -Gaborit, P.; Ruatta, O.;Efficient erasure list-decoding of Reed-Muller codes Information Theory, 2006 IEEE International Symposium on IT Information Theory, 2006 IEEE International Symposium on IT 9-14 July 2006 Page(s):148 - 152

-6 Gaborit, P.; Ruatta, O.;Improved Hermite multivariate polynomial interpolation Information Theory, 2006 IEEE International Symposium on Information Theory 9-14 July 2006 Page(s):143 - 147

- 5 . Wadood Abdul, Philippe Carré, Hakim Saadane, Philippe Gaborit: Watermarking using multiple visual channels for perceptual color spaces. ICIP 2010: 2597-2600

- 4 gaborit P, Pless, V, soléP, Atkin P, « Type II codes over GF(4) »
  proceedings International Symposium on Information Theory (ISIT) 2000

- 3 Gaborit P, Pless, V, soléP, Atkin P, « Decoding binary R(2,5) by hand and by machine »
  proceedings International Symposium on Information Theory (ISIT) 2001
- 2 Gaborit P, Otmani A, « Experimental constructions of self-dual codes over GF(3)and GF(4»proceedings International Symposium on Information Theory (ISIT) 2001

- 2 Carlet C., Gaborit, « Hyper bent finctions and cyclic codes», proceedings International Symposium on Information Theory (ISIT) 2004
- 1 Carlet C., Gaborit, « Weight enumertors of duaic and quadratic residue codes», proceedings International Symposium on Information Theory (ISIT) 2004

- 0 Carlet C., Gaborit, « On the construction of boolean functions with a good algebraic immunity», proceedings International Symposium on Information Theory (ISIT) 2005