

LISTE DE PUBLICATIONS THEMATIQUES
de Philippe GABORIT - avril 2007

• **SECURITE ET CRYPTOGRAPHIE**

- **Revue internationale**

References

[1] **Hyper-bent functions and cyclic codes**, C. Carlet and P. Gaborit, *J. Combin. Theory Ser. A* 113 (2006), no. 3, 466-482.

[2] **Construction of bent functions via Niho power functions**, H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke and P. Gaborit, *à paraître dans J. Combin. Theory Ser. A*, (2006).

- **Proceedings avec comité de lecture**

[3] **Shorter keys for code-based cryptography**, P. Gaborit, *Proceedings of Workshop on Codes and Cryptography*, Bergen, (2005), p. 81-90.

[4] **On the construction of Boolean functions with a good algebraic immunity**, C. Carlet et P. Gaborit, *Proceedings of the first International Workshop on Boolean Function and Applications*, (2005).

[5] **Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks**, F. Armknecht, C. Carlet, P. Gaborit, S. Kunzli, W. Meier et O. Ruatta, *EuroCrypt 2006*, St Petersburg, (2006).

[6] **SYND: a Fast Code-Based Stream Cipher with a Security Reduction** P. Gaborit, C. Lauradoux et N. Sendrier, *à paraître dans ISIT 2007*.

[7] **Lightweight code-based authentication and signature**, P. Gaborit et M. Girault, *à paraître dans ISIT 2007*.

[8] **Identity-based identification and signature schemes using correcting codes**, P.-L. Cayrel, P. Gaborit et M. Girault, *à paraître dans WCC 2007*.

[9] **Projet Européen SWAN: Services WI-FI appliqués aux NTIC**, D. Chiron, P. Gaborit, M. Giry, B. Jecko et T. Colombeau, *Journées Réseaux 2005* (2005).

- **Autres (Préprints, rapports de recherche...)**

- [10] **Improved Fast Syndrome Based Cryptographic Hash Function**, M. Finiasz, P. Gaborit et N. Sendrier, soumis.
- [11] **Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks**, F. Armknecht, C. Carlet, P. Gaborit, S. Kunzli, W. Meier et O. Ruatta, soumis a Journal of Cryptography.
- [12] **Single-Database Private Information Retrieval Protocols : Overview, Usability and Trends**, C. Aguilar et P. Gaborit, soumis.
- [13] **Fast Single-Database Private Information Retrieval With Lattices**, C. Aguilar et P. Gaborit, soumis.
- [14] **CTRU, a coding analog of NTRU**, P. Gaborit, J. Ohler et P. Solé, *rapport de recherche INRIA RR-4621* (2002).

• **CODES CORRECTEURS D'ERREURS**

- **Revue internationale**

- [15] **Mass formula for self-dual codes over \mathbb{Z}_4 and $\mathbb{F}_q + u\mathbb{F}_q$ rings**, P. Gaborit, *IEEE Trans. Inform. Theory*, **42**, (1996), pp. 1222-1228.
- [16] **All self-dual \mathbb{Z}_4 codes of length 15 or less are known**, J. Fields, P. Gaborit, J. Leon and V. Pless, *IEEE Trans. Inform. Theory*, **44**, (1998), pp. 311 - 322.
- [17] **Construction of extremal Type II codes over \mathbb{Z}_4** , P. Gaborit and M. Harada, *Designs, Codes and Cryptogr*, **16**, (1999), pp. 257-269.
- [18] **Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$** , S. Dougherty, P. Gaborit, M. Harada and P. Solé, *IEEE Trans. Inform. Theory* **45**, (1999), pp. 32-45.
- [19] **On the non \mathbb{Z}_4 -linearity of certain good binary codes**, J. E. Fields and P. Gaborit, *IEEE Trans. Inform. Theory*, **45**, (1999), pp. 1674 - 1677.
- [20] **On the covering radius of \mathbb{Z}_4 -codes and their lattices**, T. Aoki, P. Gaborit, M. Harada, M. Ozeki and Patrick Solé, *IEEE Trans. Inform. Theory*, **45**, (1999), pp. 2162-2168.
- [21] **Type IV self-dual codes over rings**, S. Dougherty, P. Gaborit, M. Harada, A. Munemasa and P. Solé, *IEEE Trans. Inform. Theory*, **45**, (1999), pp. 2345-2360.
- [22] **On the classification of extremal even formally self-dual codes**, J. E. Fields, P. Gaborit, W. C. Huffman and V. Pless, *Designs, Codes and Cryptography*, **18**, No. 1/2/3,(1999), pp. 125-148.

- [23] **On extremal additive $\text{GF}(4)$ codes of lengths 10 to 18**, C. Bachoc and P. Gaborit, *J. Theorie des Nomb. Bordeaux*, **12**(2), (2000), pp. 255-272.
- [24] **On the classification of extremal even formally self-dual codes of lengths 20 and 22**, J. E. Fields, P. Gaborit, W. C. Huffman and V. Pless, *J. Discrete Applied Math.*,111,(2001),pp. 75-86.
- [25] **On additive $\text{GF}(4)$ codes** P. Gaborit, J.L. Kim, W. C. Huffman and V. Pless, DIMACS Workshop on Codes and Association Schemes, DIMACS Series in Discrete Math. and Theo. Computer Science, A.M.S., Vol. 56 (2001), 135-149.
- [26] **Quadratic Double Circulant Codes over Fields**, P. Gaborit, *J. Comb. Theory (A)*, **97**, (2002), 1, pp. 85-107.
- [27] **On Type II Codes over $\text{GF}(4)$** , P. Gaborit, V. Pless, P. Solé and A. O. L. Atkin, *Finite Fields and Appl.*, **8**, (2002), pp. 171-183.
- [28] **Decoding binary $\text{R}(2,5)$ by hand**, P. Gaborit, J.L. Kim, and V. P less, *Discrete Math.*, **264** (2003), pp. 55-73.
- [29] **Experimental construction of self-dual codes**, P. Gaborit and A. Otmani, *Finite Fields and Appl.*, **9**, (2003), pp. 372-394.
- [30] **Designs and self-dual codes with long shadows**, C. Bachoc and P. Gaborit, *J. Comb. Theory (A)*, **105**, (2004), p. 15-34.
- [31] **On the weight enumerators of duadic and quadratic residue codes**, P. Gaborit, C. Nedeloaia A. Wassermann, *IEEE Transactions on Information Theory* 51(1): 402-407 (2005)
- **Proceedings avec comité de lecture (sans compter les versions courtes des papiers parus dans des revues)**
- [32] **Self-dual codes over \mathbb{Z}_4 and unimodular lattices: a survey**, M. Harada, P. Solé and P. Gaborit, *the Proc. of ICAC (International Congr ess in Algebras and Combinatorics 1997 19-23 August, Hong Kong published by Springer-Verlag* , (1999), pp. 255-275.
- [33] **Experimental constructions of codes over rings and construction of an optimal unimodular lattice in dimension 43**, P. Gaborit and A. Otmani, *Proceedings of the eight Algebraic and Combinatorial Coding Theory (ACCT VIII)*, Tsarkoe Selo, Russia, (20 02), pp. 128-131.
- [34] **Asymptotic improvement of the Gilbert-Varshamov bound for linear codes**, P. Gaborit et G. Zemor, ISIT 2006, Seattle, p.287-291.
- [35] **Improved Hermite multivariable polynomial interpolation**, P. Gaborit et O. Ruatta, ISIT 2006, Seattle, p.143-147.

[36] **Efficient list-decoding for erasure of Reed-Muller codes**, P. Gaborit et O. Ruatta, ISIT 2006, Seattle, p.148-152.

- **Autres (preprints, rapport de recherche...)**

[37] **Codes auto-duaux et applications des codes**, P. Gaborit, Habilitation à diriger des recherches, Université de Limoges, (2004)

• **THEORIE DES NOMBRES: RESEAUX**

- **Reuves internationales**

[38] **Niemeier lattices and Type II codes over \mathbf{Z}_4** , A. Bonnecaze, P. Gaborit, M. Harada, M. Kitazume and P. Solé, *Discrete Math.* **205**, (1999), pp. 1-21.

[39] **2-modular lattices from ternary codes**, R. chapman, S. T. dougherty, P. Gaborit and P. Solé, *J. Theorie des Nomb. Bordeaux*, **14** (2002), pp. 73-85.

[40] **Constructions of new extremal unimodular lattices**, P. Gaborit, *Eur. Jour. of Comb*, **25** (2004), p. 549-564.

[41] **Eisenstein Lattices, Galois Rings and Quaternary Codes**, P. Gaborit, A. M. Natividad, Patrick Solé, à paraître dans *Int. Jour. Numb Theory*.

[42] **Bounds for s-extremal codes and lattices**, P. Gaborit, à paraître dans *Archiv der Math.*

[43] **Construction of dense lattices with a given automorphism group**, P. Gaborit et G. Zémor, à paraître aux *Annales de l'institut Fourier*.

[44] **Linear constructions for DNA codes**, P. Gaborit, O. D. King, *Theoret. Compu t. Sci.* **334** (2005), no. 1-3, 99–113.

[45] **Binary templates for comma-free DNA codes**, O.D. King and P. Gaborit, à paraître dans *Discrete Applied Mathematics*, (2005).

- **AUTRES (préprint, rapport de recherche..)**

[46] **Experimental constructions of codes over rings and construction of an optimal unimodular lattice in dimension 43**, P. Gaborit and A. Otmani, *Proceedings of the eight Algebraic and Combinatorial Coding Theory (ACCT VIII)*, Tsarkoe Selo, Russia, (20 02), pp. 128-131.