Curriculum Vitæ

Paris, July 2017

-**Surname** : MESNAGER
-**Name** : Sihem
-**Date of birth** : [redacted]
-**Family situation** : [redacted]
-**Nationality** : [redacted]
-**Position** : Professor with Telecom ParisTech and associate professor in Mathematics at University of Paris VIII.
-**Professional address** : Telecom ParisTech, department INFRES, 46 rue Barrault F-75634 Paris Cedex 13 and University of Paris VIII, department of Mathematics, 2 place de la Liberté 93526 Saint Denis Cedex, France.
E-mail : smesnager@univ-paris8.fr
-**Laboratory** : LAGA (Analysis, Geometry and Applications), UMR 7539, University of Paris XIII, CNRS.
-**Research group** : Mathematics for information and image processing (MTII) and Research group MIC2 in Mathematics of the department INFRES, Telecom Paris-Tech (ex. National High School of telecommunication)
-**Personal address** : [redacted]
-**Personal telephone** [redacted]

Research areas and topics

- Discrete mathematics and its applications for symmetric cryptography and coding theory ;
- Commutative algebra and computational algebraic geometry.

Disciplines

- Discrete mathematics (finite fields, exponential sums, bent functions, Boolean functions etc) ;
- Algorithms and computational mathematics ;
- Symmetric cryptography ;
- Coding theory ;
- Theoretical computer science, information security ;
- Combinatorics ;
- Commutative algebra ;
- Algebraic geometry.

Education

-M.A. in Mathematics : Algebraic methods at University of Pierre and Marie Curie (Paris VI).

-PhD thesis in Mathematics of University of Pierre and Marie Curie (Paris VI) entitled "Contribution to the study of morphisms of affine schemes." defended on 21 November 2002.

-HDR (Habilitation to Direct Research) thesis in Mathematics (University of Paris VIII) entitled "Contributions on Boolean Functions for Symmetric Cryptography and Error Correcting Codes." defended on 10 December 2012.

Qualification

— Qualified for a full professor in Mathematics at the universities (qualification's number : 13125129518).
— Qualified for a full professor in Computer science at the universities (qualification's number : 13127129518).

Publications

• *Full papers in international journals :*

1. S. Mesnager, On resultant criteria and formulas for the inversion of a polynomial map. **Communications in Algebra** n°29 (8), pages 3327-3339, 2001.
2. S. Mesnager, Construction of the integral closure of an affine domain in a finite field extension of its quotient field. **Journal of Pure and Applied Algebra**, volume n°194, pages 311-327, 2004.
3. S. Mesnager, Test of epimorphism for finitely generated morphisms between affine algebras over Computational rings. **Journal of Algebra and Applications**, volume n°4 (4), pages 1-15, 2005.
4. C. Carlet et S. Mesnager, Improving the upper bounds on the covering radii of binary Reed-Muller codes. **IEEE Transactions on Information Theory-IT**, volume n°53 (1), pages 162-173, 2007.
5. S. Mesnager, On the number of resilient Boolean functions. **Number Theory and its Applications**, volume 5, pages 139-153, 2008.
6. S. Mesnager, Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity. **IEEE Transactions on Information Theory-IT**, volume n°54 (8), pages 3656-3662, 2008.
7. C. Carlet and S. Mesnager, On the construction of bent vectorial functions. **Journal of Information and Coding Theory : Algebraic and Combinatorial Coding Theory**. volume 1, No. 2, pages 133-148, 2010.
8. S. Mesnager, A New Class of Bent and Hyper-Bent Boolean Functions in Polynomial Forms. **Journal Designs, Codes and Cryptography**, volume 59, Numbers 1-3, pages 265-279, 2011.
9. S. Mesnager, Bent and Hyper-bent Functions in polynomial form and Their Link With Some Exponential Sums and Dickson Polynomials. **IEEE Transactions on Information Theory-IT.** Vol 57, No 9, pages 5996-6009, 2011.
10. S. Mesnager, Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. **IEEE Transactions on Information Theory-IT.** Vol 57, No 11, pages 7443–7458, 2011.
11. C. Carlet and S. Mesnager, On Dillon's class H of bent functions, Niho bent functions and o-polynomials. **Journal of Combinatorial Theory-JCT-serie A. 118**, pages 2392–2410, 2011.
12. C. Carlet and S. Mesnager, On Semi-bent Boolean Functions. **IEEE Transactions on Information Theory-IT.** Vol 58, No 5, pages 3287-3292, 2012.
13. L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha and S. Mesnager, Further Results on Niho Bent Functions. **IEEE Transactions on Information Theory-IT.** Vol. 58, No. 11, pages 6979-6985, 2012.

14. S. Mesnager and J.P Flori, Bent and hyper-bent functions via Dillon-like exponents. **IEEE Transactions on Information Theory-IT.** Vol. 59 No. 5, pages 3215-3232, 2013.
15. J.P Flori and S. Mesnager, An efficient characterization of a family of hyper-bent functions with multiple trace terms. **Journal of Mathematical Cryptology.** Vol 7, No 1, pages 43-68, 2013.
16. D. Auger, G. Cohen and S. Mesnager, Sphere coverings and Identifying Codes. Publié dans la revue **Journal Designs, Codes and Cryptography, Volume 70, Issue 1-2, pages 3-7, 2014.**
17. G. Cohen and S. Mesnager, On constructions of semi-bent functions form bent functions. **Journal Contemporary Mathematics 625, Discrete Geometry and Algebraic Combinatorics, Americain Mathematical Society, pages 141-154 (2014).**
18. S. Mesnager, Bent vectorial functions and linear codes from o-polynomials. To appear in **Journal Designs, Codes and Cryptography (DCC).**
19. S. Mesnager, Bent functions from spreads. **Journal of the American Mathematical Society (AMS), Contemporary Mathematics,** Volume 632, page 295-316, 2015.
20. S. Mesnager, Several new infinite families of bent functions and their duals. **IEEE Transactions on Information Theory-IT. Vol. 60, No. 7, Pages 4397-4407, 2014.**
21. S. Mesnager, Bent functions from spreads. **Journal of the American Mathematical Society (AMS), Contemporary Mathematics,** Volume 632, pages 295-316, 2015.
22. S. Mesnager, Bent vectorial functions and linear codes from o-polynomials. **Journal Designs, Codes and Cryptography (DCC)** 77(1), pages 99-116, 2015.
23. S. Mesnager, Further constructions of infinite families of bent functions from new permutations and their duals. **journal Cryptography and Communications (CCDS), Springer,** 8(2), pages 229-246, 2016.
24. C. Xiang, C. Ding and S. Mesnager, Optimal codebooks from binary codes meeting the Levenshtein bound. **Journal IEEE Transactions on Information Theory-IT.** 61(12) : pages 6526-6535, 2015.
25. C. Carlet et S. Mesnager, Four decades of research on bent functions. **Journal Designs, Codes and Cryptography (DCC), Springer,** Vol. 78, No. 1, pages 5-50, 2016.
26. G. Cohen, S. Mesnager et H. Randriam, Yet another variation on minimal linear codes. **Journal Advances in Mathematics of Communications (AMC),** Vol. 10, No. 1, pages 53-61, 2016.
27. S. Mesnager, Further constructions of infinite families of bent functions from new permutations and their duals. **journal Cryptography and Communications (CCDS), Springer,** 8(2), pages 229-246, 2016.
28. X. Cao, H. Chen et S. Mesnager, Further results on semi-bent functions in polynomial form. **Journal Advances in Mathematics of Communications (AMC),** 10(4) pages 725-741, 2016.
29. J. Liu, S. Mesnager et L. Chen, Variation on correlation immune Boolean and vectorial functions. **Journal Advances in Mathematics of Communications (AMC),** 10(4) pages 895-919, 2016.
30. P. Charpin, S. Mesnager et S. Sarkar, Involutions over the Galois field F_2^n. **Journal IEEE Transactions on Information Theory-IT.** 62(4) pages 2266-2276, 2016.
31. P. Charpin, S. Mesnager et S. Sarkar, Dickson polynomials that are Involutions. **Contemporary Developments in Finite Fields and Their Applications, World Scientific Press** , pages 22-45, World Scientific Press, 2016.
32. K. Abdukhalikov et S. Mesnager, Bent functions linear on elements of some classical spreads and presemifields spreads.**International Journal Cryptography and Communications (CCDS),** 9(1) pages 3-21, 2017, Springer.

33. J. Liu, S. Mesnager et L. Chen, On the nonlinearity of S-boxes and linear codes. **Journal Cryptography and Communications- Discrete Structures, Boolean Functions and Sequences (CCDS)**, 9(3) pages 345-361, 2017, Springer.
34. N. Bennenni, K. Guenda et S. Mesnager, DNA cyclic codes over rings. **Journal Advances in Mathematics of Communications (AMC)**, Vol 11, No. 1, pages 83-98, 2017.
35. S. Mesnager, Linear codes with few weights from weakly regular bent functions based on a generic construction.**Journal Cryptography and Communications- Discrete Structures, Boolean Functions and Sequences (CCDS)**, 9(1) pages 71-84, 2017, Springer.
36. S. Mesnager, G. McGrew, J. Davis, D. Steele et K. Marsten. A comparison of Carlet's second order nonlinearity bounds. **International Journal of Computer Mathematics** 94(3), pages 427-436, 2017.
37. K. Abdukhalikov et S. Mesnager Explicit constructions of bent functions from pseudo-planar functions. **Journal Advances in Mathematics of Communications (AMC)**, Vol 11, No. 2, pages 293-299, 2017.
38. S. Mesnager et G. Cohen, Fast algebraic immunity of Boolean functions. **Journal Advances in Mathematics of Communications (AMC)**, Vol 11, No. 2, pages 373-377, 2017.
39. F. Zhang, S. Mesnager et Y. Zhou, On construction of bent functions involving symmetric functions and their duals. **Journal Advances in Mathematics of Communications (AMC)**, Vol 11, No. 2, pages 347-352, 2017.
40. S. Mesnager et F. Zhang, On constructions of bent, semi-bent and five valued spectrum functions from old bent functions. **Journal Advances in Mathematics of Communications (AMC)**, Vol 11, No. 2, pages 339-345, 2017.
41. J. Liu, S. Mesnager et L. Chen, New constructions of optimal locally recoverable codes via good polynomials. **IEEE Transactions on Information Theory**. To appear.
42. S.Mesnager, C. Tang et Y. Qi Generalized plateaued functions and admissible (plateaued) functions. **IEEE Transactions on Information Theory**. To appear.

• *Full papers in proceedings of international conferences, published by journals or Lecture Notes in Computer Science :*

43. S. Mesnager, Test of monomorphism for finitely generated morphisms between affine schemes. **Proceedings of the sixth workshop on Computer Algebra in Scientific Computing, CASC'04**, Euler International Mathematical Institute, Saint-Pétersbourg, pages 348-357, 2004.
44. C. Carlet and S. Mesnager, On the Walsh support of Boolean functions. **Proceedings of the first workshop on Boolean functions : Cryptography and Applications, BFCA'05**, pages 65-82, 2005. *Cryptology ePrint archive : 2004/256*
45. C. Carlet, P. Guillot and S. Mesnager, On immunity profile of Boolean functions. **Proceedings of SEquences and Their Applications, SETA 2006**. LNCS, Springer, pages 364-375, 2006.
46. S. Mesnager, A new class of Bent Boolean functions in polynomial forms. **Proceedings of international Workshop on Coding and Cryptography, WCC 2009**, pages 5-18, Ullensvang, Norvège, 2009.
47. S. Mesnager, A new family of hyper-bent Boolean functions in polynomial form. **Proceedings of Twelfth International Conference on Cryptography and Coding**. IMACC 2009, LNCS 5921, pages 402-417, Springer, 2009.
48. S. Mesnager, Hyper-bent Boolean Functions with Multiple Trace Terms. **Proceedings of International Workshop on the Arithmetic of Finite Fields**, WAIFI 2010, LNCS 6087, pages 97-113. Springer, 2010.

49. J-P. Flori, H. Randriambololona, G. Cohen and S. Mesnager, On a conjecture about binary strings distribution. **Proceedings of 6-th International conference SEquences and Their Applications, SETA 2010**, LNCS 6338, pages 346-358. Springer, 2010.
50. S. Mesnager and G. Cohen, On the link of some semi-bent functions with Kloosterman sums. **Proceeding of International Workshop on Coding and Cryptology"**, IWCC 2011, LNCS 6639, Springer pages 263–272, Springer, 2011.
51. J.P. Flori, S. Mesnager and G. Cohen Binary Kloosterman sums with value 4. **Proceedings of Thirteenth International Conference on Cryptography and Coding**, IMACC 2011, LNCS 7089, pages 61-78, Springer, 2011.
52. S. Mesnager, Semi-bent functions with multiple trace terms and hyperelliptic curves. **Proceeding of International Conference IACR on Cryptology and Information Security in Latin America, Latincrypt 2012**, LNCS 7533, pages 18-36, Springer, 2012.
53. J.P. Flori and S. Mesnager, Dickson polynomials, hyperelliptic curves and hyper-bent functions. **Proceedings of 7-th International conference SEquences and Their Applications, SETA 2012**, LNCS 7280, pages 40-52, Springer, 2012.
54. T. Helleseth, A. Kholosha and S. Mesnager, Niho Bent Functions and Subiaco/Adelaide Hyperovals. **Proceedings of the 10-th International Conference on Finite Fields and Their Applications** Fq'10, Contemporary Mathematics, AMS, 2012. Vol 579, pages 91-101, 2012.
55. G. Cohen, S. Mesnager and A. Patey, On Minimal and Quasi-Minimal Linear Codes. **Proceedings of 14th International Conference on Cryptography and Coding, IMACC 2013** Oxford, United Kingdom, LNCS 8308, pages 85-98. Springer, Heidelberg, 2013.
56. S. Mesnager, Semi-bent functions from oval polynomials. **Proceedings of 14th International Conference on Cryptography and Coding, IMACC 2013** Oxford, United Kingdom, LNCS 8308, pages 1-15. Springer, Heidelberg, 2013.
57. S. Mesnager, On semi-bent functions and related plateaued functions over the Galois field $\mathbb{F}_{2^n}$. Proceedings **Open Problems in Mathematics and Computational Science**, LNCS, Springer, pages 243-273, 2014.
58. S. Mesnager, Characterizations of plateaued and bent functions in characteristic p. **Proceedings of 8-th International conference SEquences and Their Applications, SETA 2014**, Melbourne, Australie, LNCS, Springer, pages 72-82, 2014.
59. S. Mesnager, F. Özbudak et A. Sınak, Results on Characterizations of Plateaued Functions in Arbitrary Characteristic. **Proceedings of BalkanCryptSec 2015**, LNCS 9540, Springer, pages 17-30, 2015.
60. N. Koçak, S. Mesnager and F. Özbudak, Bent and semi-bent functions via linear translators. **Proceedings of International Conference on Cryptography and Coding, Oxford, United Kingdom (IMACC 2015)** pages 205-224, Springer, Heidelberg, 2015.
61. J. Liu, S. Mesnager and L. Chen, On the diffusion property of iterated functions. **Proceedings of International Conference on Cryptography and Coding, Oxford, United Kingdom (IMACC 2015)**, pages 239-253, Springer, Heidelberg, 2015.
62. S. Mesnager, G. Cohen and D. Madore, On existence (based on an arithmetical problem) and constructions of bent functions. **Proceedings of International Conference on Cryptography and Coding, Oxford, United Kingdom, (IMACC 2015)**, pages 3-19, Springer, Heidelberg, 2015.
63. J. Liu, S. Mesnager and L. Chen, Secret Sharing Schemes with General Access Structures. **Proceedings of the "11th International Conference on Information Security and Cryptology" (Inscrypt 2015)** (IACR),Volume 9589, Springer, 2016.
64. A. Mrabet, N. El-Mrabet, R. Lashermes, J-B. Rigaud, B. Bouallegue, S. Mesnager and M. Machhout High-performance Elliptic Curve Cryptography by Using the CIOS Method for Modular Multiplication. **Proceedings of "The 11th International Conference on Risks and Security of Internet and Systems" (CRISIS 2016)**, Springer, 2016.

65. A. Mrabet, N. El-Mrabet, R. Lashermes, J-B. Rigaud, B. Bouallegue, S. Mesnager and M. Machhout A Scalable and Systolic Architectures of Montgomery Modular Multiplication for Public Key Cryptosystems Based on DSPs. **Proceedings of "The Sixth International Conference on Security, Privacy and Applied Cryptographic Engineering " (Space 2016)**, Springer, 2016.
66. J. Liu, S. Mesnager and L. Chen Partially homomorphic encryption schemes over finite fields. **Proceedings of "The Sixth International Conference on Security, Privacy and Applied Cryptographic Engineering " (Space 2016)**, Springer, 2016.
67. C. Carlet, S. Mesnager, F. Özbudak, et A. Sınak, Explicit Characterizations for Plateauedness of p-ary (Vectorial) Functions. **Proceedings of the international Conference on Codes, Cryptology and Information Security (C2SI-2017)** pages 328-345, Springer 2017.
68. S. Mesnager, P. Ongan et F. Özbudak, New Bent Functions from Permutations and Linear Translators. **Proceedings of the international Conference on Codes, Cryptology and Information Security (C2SI-2017)** pages 282-297, Springer 2017.
69. A. Aloui, M. Msahli, T. Abdessalem, S. Bressan et S. Mesnager, Protocol for Preserving Privacy in Distributed System (PPDS). **Proceedings of the 13th International Wireless Communications and Mobile Computing Conference (IWCMC 2017)**, 2017. To appear.
70. S. Mesnager, F. Özbudak et A. Sınak, A new class of three-weight linear codes from weakly regular plateaued functions. **Proceedings of The Tenth International Workshop on Coding and Cryptography** (WCC 2017). Saint-Petersburg, Russie.

- *Other full papers in proceedings of international conferences :*

71. C. Carlet and S. Mesnager, Improving the upper bounds on the covering radii of Reed-Muller codes. **IEEE International Symposium on Information Theory, ISIT 2005**, Australie, Septembre 2005.
72. P. Guillot and S. Mesnager, Non-Linearity and Security of Self Synchronizing Stream Ciphers. **International Symposium on Nonlinear Theory and its Applications, NOLTA 2005**, Bruges, Belgique, Octobre 2005.
73. S.T. Dougherty, S. Mesnager and P. Solé Secret Sharing Schemes Based on Self-dual Codes. **IEEE Information Theory Workshop (ITW 2008)**, Porto, Portugal 5-9 Mai 2008.
74. S. Mesnager, Recent Results on Bent and Hyper-bent Functions and Their Link With Some Exponential Sums. **IEEE Information Theory Workshop (ITW 2010)**, Dublin, August-September 2010.
75. G. Cohen and S. Mesnager, Constrained memories, coverings, identification. **Congres 26-th convention IEEEI 2010**, Eilat, Israel, Novembre 2010.
76. G. Cohen and S. Mesnager, Generalized witness sets. **Proceeding 1st International Conference on Data Compression, Communication and Processing CCP 2011**, Italie, juin 2011.
77. C. Carlet, T. Helleseth, A. Kholosha and S. Mesnager, On the Dual of Bent Functions with 2^r Niho Exponents. **IEEE International Symposium on Information Theory, ISIT 2011**, pages 703-707, Saint-Petersturg, Russie, Juillet-aout 2011.
78. D. Auger, G. Cohen and S. Mesnager, Sphere coverings and Identifying Codes. **Proceeding of 3rd International Castle Meeting on coding theory and Application (3 ICMT)**, pages 31-36, Barcelone, Espagne, septembre 2011.
79. C. Carlet and S. Mesnager, On Dillon's class H of Niho bent functions and o-polynomials. **International Symposium on Artificial Intelligence and Mathematics, ISAIM 2012**, Fort Lauderdale, Floride, USA, Janvier 2012.

80. S. Mesnager and J.P. Flori On hyper-bent functions via Dillon-like exponents. **ISIT 2012. IEEE International Symopsium on Infomation Theory**. IMT, Cambridge, Boston, USA, Juillet 2012.
81. A. Mrabet , B. Bouallegue, M. Machhout, N. EL Mrabet and S. Mesnager, Implementation of Faster Miller over Barreto-Naehrig Curves in Jacobian Cordinates **Proceedings of GSCT, IEEE, Sousse, Tunisie, juin 2014.**
82. G. Cohen and S. Mesnager, On Minimal and Almost-Minimal Linear Codes. **Proceedings of the 21st International Symposium on Mathematical Theory of Networks and Systems (MTNS 2014)**, pages 928-931, Groningen, Netherlands.
83. S. Mesnager, A note on linear codes and algebraic immunity of Boolean functions. **Proceedings of the 21st International Symposium on Mathematical Theory of Networks and Systems (MTNS 2014)**, pages 923-927, Groningen, Netherlands.
84. G. Cohen and S. Mesnager, Variations on Minimal Linear Codes. **Proceedings of 4th International Castle Meeting on Coding Theory and Applications**. To appear.
85. S. Mesnager and G. Cohen, Cyclic codes and algebraic immunity of Boolean functions. **Proceedings IEEE Information Theory Workshop (ITW) 2015, Jerusalem, Israel.**
86. P. Charpin, S. Mesnager and S. Sarkar, On involutions of finite fields. **Proceedings of 2015 IEEE International Symposium on Information Theory, ISIT 2015, Hong-Kong, 2015.**
87. S. Mesnager, F. Özbudak and A. Sınak, Characterizations of plateaued functions in arbitrary characteristic. **Proceedings of The International Conference on Coding theory and Cryptography** (ICCC 2015), Algeria.
88. S. Mesnager On constructions of bent functions from involutions. **Proceedings of 2016 IEEE International Symposium on Information Theory** (ISIT 2016), Barcelone, Spain.

• Books :

1. S. Mesnager, "Bent functions : fundamentals and result", Springer Verlag (544 pages), 2016.
2. S. Mesnager, "Finite fields and error correcting codes", Pearson Education, 2007 (in French).

Talks

• *International conferences :*

1. [March 2005] **International conference, BFCA Cryptography and Applications**, at Rouen (France) *"On the Walsh support of Boolean functions".*
2. [September 2006] **International conference, SETA (The fourth international conference on SEquences and Their Applications)** at Beijing (China) *"On immunity profile of Boolean functions".*
3. [May 2007] **International conference, SAGA (Symposium on Algebraic Geometry and its Applications)** at Papeande (Tahiti) *"On the number of resilient Boolean functions".*
4. [May 2009] **International conference Workshop on Coding and Cryptography (WCC)** at Ullensvang (Norwey) *"A new class of Bent Boolean functions in polynomial forms".*
5. [December 2009] **International conference,Twelfth International Conference on Cryptography and Coding (IMACC)** at Cirencester (United Kingdom) *"A new family of hyper-bent Boolean functions in polynomial form".*

6. [June 2010] **International conference, Workshop on the Arithmetic of Finite Fields (WAIFI)** at Istanbul (Turkey) *"Hyper-bent Boolean Functions with Multiple Trace Terms"*.
7. [September 2010] **International conference, IEEE Information Theory Workshop (ITW)** at Dublin (Ireland) *"Recent Results on Bent and Hyper-bent Functions and Their Link With Some Exponential Sums"*.
8. [February 2011] **International conference (sur invitation), Workshop Information Theory and Applications (ITA)** at San Diego (USA) *"On the link of some semi-bent functions in polynomial forms with exponential sums"*.
9. [May-June 2011] **International conference (sur invitation), Workshop of International Workshop on Coding and Cryptology (IWCC 2011)** at Qingdao (China) *"On the link of some semi-bent functions with Kloosterman sums"*.
10. [September 2011] **International conference Castle Meeting on coding theory and Application (3ICMTA)**, Cardona (Spain) *"Sphere coverings and Identifying Codes."*.
11. [October 2011] **Twenty-Fifth Midwest Conference on Combinatorics, Cryptography, and Computing (MCCC)**, Las Vegas (USA) *"Identifying codes and Covering by Spheres"*.
12. [February 2012] **Workshop Information Theory and Applications (ITA 2012), San Diego (USA)**, *"New semi-bent functions with multiple trace terms"*.
13. [June 2012] **International conference SETA (The 7th international conference on SEquences and Their Applications)** at Waterloo (Canada) *"Dickson polynomials, hyperelliptic curves and hyper-bent functions"*.
14. [July 2012] **International conference, ISIT 2012, IEEE International Symposium on Information Theory** at MIT, Boston (USA) *"Hyper-bent functions via Dillon-like exponents"*.
15. [September 2012] **International conference, Yet Another Conference on Cryptography (YACC) 2012** at l'iles of Porquerolles (France) *"Bent and hyper-bent functions via Dillon-like exponents"*.
16. [October 2012] **International conference, Cryptology and Information Security in Latin America (Latincrypt) 2012** at Santiago (Chili) *"Semi-bent functions with multiple trace terms and hyperelliptic curves"*.
17. [July 2013] **International conference Finite Fields and their Applications, Fq11** at Magdeburg, (Germany) *"Bent functions from spreads"*.
18. [December 2013] **International conference on Cryptography and Coding IMACC 2013** at Oxford (United Kingdom) *"Semi-bent functions from oval polynomials"*.
19. [November 2014] **International conference SETA (The 8th international conference on SEquences and Their Applications)** at Melbourne (Australia) *"Characterizations of plateaued and bent functions in characteristic p"*.
20. [April 2015] **International conference ITW 2015 (the Information Theory Workshop)** at Jerusalem (Israel) *"Cyclic codes and algebraic immunity of Boolean functions"*.
21. [June 2015] **International conference ISIT 2015 International Symposium on Information Theory** at Hong-Kong (China) *"On involutions of finite fields"*.
22. [July 2015] **International conference Finite field and their Applications Fq12 à New York** *"On p-ary bent functions from (maximal) partial spreads"*.
23. [July 2015] **International conference Finite field and their Applications Fq12 at New York** *" Dickson Polynomials that are Involutions"*.
24. [July 2015] **International conference "Workshop on Mathematics in Communications (WMC 2016) à Santander, Espagne.** *"On construction of bent functions involving symmetric functions and their duals"*.

25. [July 2015] **International conference "Workshop on Mathematics in Communications (WMC 2016) à Santander, Espagne.** *"Fast algebraic immunity of Boolean functions".*
26. [July 2015] **International conference "Workshop on Mathematics in Communications (WMC 2016) à Santander, Espagne.** *"Explicit constructions of bent functions from pseudo-planar functions".*
27. [July 2015] **International conference "Workshop on Mathematics in Communications (WMC 2016) à Santander, Espagne.** *"On constructions of bent, semi-bent and five valued spectrum functions from old bent functions".*
28. [July 2015] **IEEE International Symposium on Information Theory (ISIT 2016) à Barcelone, Espagne.** *"On constructions of bent functions from involutions".*
29. [December 2015] **International conference Fiftennth IMA International conference on cryptography and coding** at Oxford, England. ***"On the diffusion property of iterated functions".***
30. [June 2017] **International conference "Finite field and their Applications" Fq13 at Gaeta, Italy** *"On the nonlinearity of Boolean functions with restricted input".*
31. [July 2017] **International conference "Workshop on Boolean Functions and Their Applications" (BFA 2017) at Solstrand, Norway** *"Generalized plateaued functions and admissible (plateaued) functions".*

- *Invited talks in international conferences and international meeting/seminar :*

32. [September 2010] International Information Theory Workshop (ITW 2010) at Dublin (Ireland). Invitation of Marcus Greferath.
33. [February 2011] International Workshop Information Theory and Applications (ITA 2011) at San Diego (USA). Invitation of Alexander Vardy.
34. [May 2011] International Workshop on Coding and Cryptology (IWCC 2011) at Qingdao (China). Invitation of Xian Hequn.
35. [November 2011] International seminar in Coding Theory at Dagsthul (Germany). Invitation of Joachim Rosenthal and Amin Shokrollahi.
36. [February 2012] International Workshop Information Theory and Applications (ITA 2012) at San Diego (USA). Invitation of Alexander Vardy.
37. [May 2012] International Workshop on coding based crypto (Ecrypt 2012), Lyngby (Denmark). Invitation of Tom Høholdt.
38. [September 2012] International Workshop on finite fields character sums end polynomials, Strobl (Austria). Invitation of the organizers of the Workshop.
39. [October 2012] International Conference Trends in coding theory, Monté Verita (Switzerland). Invitation of Elisa Gorla, Joachim Rosenthal and Amin Shokrollahi.
40. [Ausgust 2013] International seminar in Coding Theory at Dagsthul (Germany). Invitation of Hans-Andrea Loeliger, Emina Soljanin and Judy L. Walker.
41. [December 2013] Emerging applications of finite fields, Linz (Australia). Invitation of Alina Ostafe, Daniel Panario and Igor Shparlinski.
42. [Mai 2014] Conférence internationale "Workshop on Polynomials over Finite Fields : Functional and Algebraic Properties" à Barcelone (Espagne). Invitation of the organizers : Joachim von zur Gathen, Jaime Gutierrez, Alina Ostafe, Daniel Panario and Alev Topuzoglu.
43. [Juillet 2014] International conference in coding MTNS2014 (The 21th international symposium on Mathematical Theory of Networks and Systems) at Groningen (netherlands). Invitation of Heide Gluesing-Luerssen, Joachim Rosenthal and Margreta Kuijper.

44. [September 2014] International Workshop on Boolean Functions and Their Applications" at Rosendal (Norway). Invitation of Lilya Budaghyan, Tor Helleseth and Alexander Kholosha.
45. [November 2015] International conference "International Conference on Coding and Cryptography" ICCC 2015, Alger, Algeria. Invitation of Kamel Bettina and Kenza Guenda.
46. [December 2015] International conference "Fiftennth IMA International conference on cryptography and coding" à L'université d'Oxford, Angleterre. Invitation of Jens Groth, (University "College London").
47. [June 2016] International Conference "Yet Another Conference on Cryptography" (YACC 2016)
Porquerolles Island, France.
48. [February 2017] International conference "number theory in the low countries" at l'university of Gant, Belgium. Invitation of Léo Storm.
49. [July 2017] International Workshop on Boolean Functions and Their Applications" at Solstrand (Norway). Invitation of Lilya Budaghyan, Claude Carlet and Tor Helleseth.

• *Other conferences and seminars :*

50. Seminar Workshop of Mathematics, Institute Henri Poincaré, Paris, France, March 2002.
51. Seminar Algebraic geometry, University of Rennes I, Rennes, France, April 2002.
52. Seminar Information theory and security, University of Paris VIII, France, June 2003.
53. Seminar of Cryptography, University of Rennes, Rennes, France, April 2005.
54. Seminar Algebraic combinatorics, University of Paris 13, France, April 2005.
55. Seminar Codes and Cryptography ENSTA, Paris, October 2005.
56. Seminar I3S, Sophia-Antipolis, Nice, France, April 2009.
57. Seminar MTII, University of Paris VIII, France, June 2009
58. Seminar project Boole, Institut Henri Poincaré, Paris, France, May 2010.
59. Seminar MTII, University of Paris VIII, France, January 2011.
60. Seminar Arithmetic and information theory (ATI) institute of Mathematics of Luminy, Marseille, France, February 2011.
61. Invited talk at "Coding and Cryptography" (C2), Saint Pierre d'Oléron, France, April 2011.
62. Seminar Information Theory, Telecom Paris-Tech, France, December 2011.
63. Seminar project Boole, Institut Henri Poincaré, Paris, France, January 2012.
64. Séminaire UCD School of Mathematical Sciences, Dublin, Ireland, February 2012.
65. Seminar project Boole, University of Paris VI, France, June 2013.
66. Seminar LIP 6, University of Paris VI, France, April 2014.
67. Seminar University of Paris 13, Team "combinatorics", May 2014.
68. Seminar Algebra at department of mathematics of El Ain's University, October 2014.
69. Seminar Mathematics at the Department of Mathematical Sciences UAE University, UAE, October 2014.
70. Seminar "Cryptography" at University of Xuzhou China, December 2014. Invitation of Fengrong Zhang.
71. Seminar "Discrete Mathematics" at University of Nanjing, China, December 2014. Invitation of Xiwang Cao.
72. Seminar "Cryptography" University Cergy, France, April 2015. Invitation of Valerie Nachef and Emmanuel Volte.
73. Seminar "Algebra and Geometry" at University of Versailles, France, April 2015.

74. Seminar "Algebra, coding and cryptography" at university de Hong-Kong, China, June 2015. Invitation de Cunsheng Ding.
75. Seminar Combinatorics and algorithms at university of Rouen, France, February 2016.
76. Seminar " Discrète mathematics" at university of Paul Sabatier, Toulouse, France, May 2016.
77. Seminar "mathematics" at university of Southwest Jiaotong, Chungdu, China, July 2016.
78. Seminar "mathematics" at university of Nanchong, China, July 2016.
79. Seminar in mathematics for cryptography and coding theory at Chinese Academy of Sciences, Bejiin, China, September 2016.
80. Seminar in mathematics for cryptography and coding theory at Tianjin and Nankai Universities, China, September 2016.
81. Seminar " protection de l'information" at University of Paris 8, France, November 2016.
82. Seminar " Algebra and number theory" at Aalto University School of Science, Finlande, February 2017.

President of program committees

1. Co-chair (with Erkay Savas) of program comitties WAIFI 2014 (Workshop on the Arithmetic of Finite Fields), Gebze, Turkey, September 2014.
2. Chair of program comitties of International Conference in Cryptography and Coding theory, Algeria, November 2015.
3. Co-chair of session's program "Computational aspects and mathematical methods for finite field and their applications in information theory" in the conference ACA 2015 , International Conference on Applications of Computer Algebra, Kalamata, Greece, 20-23 July 2015.

Participations in program committees

1. Member of program comitties of the 2sd African International Conference on Cryptology Africacrypt 2009,Tunisia, 21-25 june 2009.
2. Member of program comitties of the 6th International Conference on SEquences and Their Applications SETA 2010, Paris, France, 12-17 september 2010.
3. Member of program comitties of the 7th International Workshop on Coding and Cryptography WCC 2011, Paris, France, 11-15 April 2011.
4. Member of program comitties of the 8th International Workshop on Coding and Cryptography WCC 2013, Begen, Norwey, 15-19 April 2013.
5. Member of program comitties of the 4th International Workshop 4ICMCTA "4th International Castle Meeting on Coding Theory and Applications", Tomar, Portugal 15-18 September 2014.
6. Member of program comitties of the 8th International Conference on SEquences and Their Applications SETA 2014, "8th International Conference on SEquences and Their Applications" Melbourne, Australia, 24-28 november 2014.
7. Member of program comitties of Workshop on the Arithmetic of Finite Fields (WAIFI 2014), Gebze, Turkey, 26-28 September 2014.
8. Member of program comitties of the 9th International Workshop on Coding and Cryptography WCC 2015, "9th International Workshop on Coding and Cryptography" Paris, France 13-17 April 2015.

9. Member of program comitties international conference ICCA 2016, "International Conference on Cryptography and its Applications", Oran, Algeria, 26-27 April 2016.
10. Member of program comitties international conference WAIFI 2016 "International Workshop on the Arithmetic of Finite Fields", Ghent, Belgique, 13-16 July 2016.
11. Member of program comitties international conference SETA 2016, "9th International Conference on SEquences and Their Applications ", Chungdu, China, 9-14 October 2016.
12. Member of program comitties of the international conference "Codes, Cryptology and Information Security" Rabat, Maroco, 10-12, April 2017.
13. Member of program comitties of the international conference 5ICMCTA 2017 "4th International Castle Meeting on Coding Theory and Applications, Estonia, August-September 2017.
14. Member of program comitties of the international conference "10th International Workshop on Coding and Cryptography " (WCC 2017), St Petersburg, Russia, 18-22 September, 2017.

Editorial responsibility

1. Editor in Chief of the international journal "International Journal of Information and Coding Theory" (IJOCT).
2. Editor in International journal IEEE Transactions on Information Theory (IEEE-IT).
3. Editor in the Journal Advances in Mathematics of Communications (AMC), published by AIMS (American Institute of Mathematical Sciences).
4. Editor in International journal "Cryptography and Communications-Discrete Structures, Boolean Functions and Sequences" (CCDS) (les articles acceptés sont publiés dans SPRINGER).
5. Editor in the international journal RAIRO ITA (Theoretical Informatics and Applications) -Published by Cambridge University Press.

Visiting Positions

1. Invitation in September 2010 by professor Marcus Greferath, University College Dublin, Irland.
2. Invitation in November 2010 by professor Simon Litsyn, University Tel Aviv, Israel.
3. Invitation in October 2013 by professor Janos Korner, University Roma, Italy.
4. Invitation in September 2014 by professor Ferruh Ozbudak, Université of Ankara, Turkey.
5. Invitation in October 2014 by professor Kanat Abdukhalikov, department of mathematics, El Ain, UAE.
6. Invitation in June 2015 by professeur Cunsheng Ding, department of mathematics, and computer science, Hong-Kong, China.
7. Invitation i, July 2016 par professeur Zhengchun Zhou , department dof mathematics, university of Southwest Jiaotong, Chungdu, China.
8. Invitation in September 2016 of Professors Dongdai Lin, Keqin Feng and Baofeng Wu at the Chinese Academy of Sciences, China.
9. Invitation in September 2016 of Professors Francoise Soulier, Fangwei Fu and Jian Liu at Tianjin and Nankai Universities, China.
10. Invitation in February 2017 of Professors Marcus Greferath and Camilla Hollanti at department of mathematics of University Aalto, Finland.

Other scientific activities

1. I am Vice-president of the french chapter of IEEE in information theory : Transactions on Information Theory.
2. Supervisor of PhD students :
   — Co-supervisor (with Gérard Cohen and Hugues Randriambololona) of Jean-Pierre Flori at Telecom Paris-Tech (doctor since January 2012 and researcher at ANSSI (National Agency security of information system, Paris) ;
   — Supervisor of Aloui Achref at university of Paris VIII ;
   — Co-supervisor (with N. Mrabet) of Amine Mrabet (joint thesis with University of Tunis, Tunisia and university of Paris VIII, Paris, France).
   — Co-supervisor (with Lusheng Chen) of Jian Liu with the China Scholarship Council (doctor since May 2015).
   — Co-supervisor (with Ferruh Ozbudak) of Ahmet Sinak (joint thesis with Institute of Applied Mathematics, METU, Ankara, Turquie and university of Paris VIII, Paris, France).
   — Co-supervisor (with Kenza Guenda) of Bennenni Nabil (University of Sciences and Technology Houari Boumedienne USTHB, Algeria).
   — Co-supervisor (with Matthieu Rivain and Pascal Paillier) of Junwei Wang at University of Paris VIII.
3. I was in charge of the seminar protection of information for 6 years (from 2006 to 2012).
4. Participation to Research Projects :
   — I was in the project ANR "BOOLE" (Boolean functions) from January 2009 to August 2013 with UVSQ, ENS, INRIA, University of Aix-Marseille II, University of Paris XI, University of Caen (and University Paris VIII), University of Nantes, University of Provence and University Paris Diderot (Paris VII) ;
   — I am member of Office of Research and Sponsored Project "Special Functions for Cryptography" in UAE University with Claude Carlet and Kanat Abdukhalikov (from January 2014 to December 2016) ;
   — I am involved in the ANR "MANTA" from September 2015 to August 2018. The main topics are : Algebraic Geometry and Coding Theory. The partners are : INRIA, IMT (Institut de Mathématiques de Toulouse) et Télécom Paris-tech.
   — I am involved in the Eurpean project SECODE for three years in which the partners are l'INRIA (France), Télécom Paristech (France), Université Catholique de Louvain UCL (Belgium) and the Sabancı University (Turkey).
   —
5. Participation to the expertise of national and international projects (ex. Research Foundation etc.).
6. I was referee for various international journals amongst them IEEE Transactions on Information Theory, journal Cryptography and Communication - Discrete Structures, Boolean Functions and Sequences (CCDS), Journal of Information and Coding Theory, journal Designs, Codes and Cryptography (DCC), Journal of Finite Fields and their Applications (FFA), Journal Advances in Mathematics of Communications (AMC), International Journal of Computer Mathematics (CM), Journal Discrete Mathematics and Applications, SIAM journal on Discrete Mathematics, Journal Discrete Applied Mathematics (DMA), Journal of Fourier Analysis and Applications (JFAA), journal Information Sciences, journal Information Processing Letters (IPL), International Journal of Information and Coding theory (IJIcoT), etc
7. I was referee for various international conferences and workshops amongst them the Workshop on Coding and Cryptography (WCC), International Symposium on Information Theory

(ISIT), International Conference on Sequences and their Applications (SETA), Africacrypt (an IACR conference), Applied algebra, Algebraic algorithms, and Error Correcting Codes (AAECC), International Conference on Cryptology in India (Indocrypt).

8. Participation to jury PhD thesis :
   - PdD thesis of Rafael Fourquet "Décodage par liste des codes de Reed-Muller et application à la cryptanalyse",2011, Paris VIII, France (examiner) ;
   - PhD thesis of Jean-Pierre Flori "Fonctions booléennes, courbes algébriques et multiplication complexe", 2012, Telecom ParisTech, France (examiner) ;
   - PhD thesis of Chérif Mihoubi "Codes cycliques ternaires de rendement 1/2", 2012, Telecom ParisTech, France (examiner) ;
   - PhD thesis of Lin Sok "Code, Lattices et fonctions booléennes", 2013, Telecom ParisTech, France (referee).
   - PhD thesis of Ding Tang "Fonctions Boolennes pour les Schemas Cryptographiques par Flots et par Blocs", 2014, University of Paris VIII, France (examiner) ;
   - PhD thesis of Valentin Suder "Propriétés différentielles des permutations et application en cryptographie symmetrique", 2014 INRIA Paris-Rocquencourt, SECRET project-team, France (examiner) ;
   - PhD thesis of Brahim Merabet "Critères de sécurité des fonctions booléennes vis à vis des attaques algébriques sur les schémas par flots et par blocs", January 2015, University of Boumediene, Algeria (referee) ;
   - PhD thesis of Soukayna Qarboua. June 2016, Télécom Bretagne, France (referee) ;
   - PhD thesis of Nabil Bennenni "Construction des codes cycliques sur les anneaux finis pour computation d' ADN", October 2016, department of mathematics of University USTHB, Algeria (examiner) ;
   - PhD thesis of Samir Hodzic "Characterisation of generalized bent functions and some other topics related to cryptography", August 2017, Koper, Slovenia (referee).

Administration activities

1. I am co-heading of the research team MTII at the laboratory LAGA.
2. I am heading the Master degree of mathematics (Master MACC : Mathematics and Applications to Coding theory and Cryptography) at the University of Paris VIII since 2013.
3. I was in charge (with C. Carlet) of the Master degree of mathematics from 2006 to 2009.
4. I was Member of the council of Unity of formation and research at the University of Paris VIII from 2006 to 2010.
5. I was in charge of the budget of the department of Mathematics at the University of Paris VIII from 2006 to 2009.
6. I was in charge of teaching and administrative training in cryptology between Thales and University Paris VIII form 2008 to 2009.
7. I am member of the Recruitment Commission : I'm member (and Vice-president) of the Recruitment Commission for Mathematics at university of Paris VIII since 2008. This commission is in charge of the recruitments of Assistant Professors.
8. I am member of the french research coordination comitiee (Codes and Cryptography), gathering more than 250 researchers.

Educational activities

1. Author of book : Joint author of the book Mathematics L2 Pearson Education, 2007 (Chapter "Quotients rings and finite fields" and Chapter complement "From finite fields to error-correcting codes").

2. Jury member of a national competition : competition Mathematics A (Algebra and Analysis) from 2005 to 2013.
3. Corrective books : book "oral competitions Central School / Supelec School/ Mine School/ Polytechnic School" ; collection Ellipses and book "Mathematics L1" ; collection Pearson Education.
4. Scientific document examiner : "An analysis of scientific papers" in Mathematics for Polytechnic competitions in 2011.
5. Framing of training courses : framing of almost 50 training courses Master in Mathematics and information theory from 2006 to 2009.
6. Oral examinations in preparatory classes : preparation for the oral competition in Mathematics (1st and 2nd year of preparatory classes for high school) for more than 19 years.

Teaching

I have taught courses (in more than 19 years) for Undergraduate's and Master's students at 7 universities and hight schools :

1. Mathematics : Algebra, Analysis and Geometry.
2. Applied Mathematics : Cryptology and Coding theory.
3. Mathematical Programming : Computational Number Theory in C, Arithmetic in C, Cryptography in C etc.