List of Publications

Mise à jour du 4 Novembre 2017

Publications In International Journals

2017
Kevin Atighehchi, Robert Rolland
Optimization of Tree Modes for Parallel Hash Functions : A Case Study
Transactions on Computers, IEEE, Volume 66 Issue 9, September 1, 2017, 1585 - 1598
doi : 10.1109/TC.2017.2693185

2017
Kevin Atighehchi, Stéphane Ballet, Alexis Bonnecaze, Robert Rolland
Arithmetic in Finite Fields based on Chudnovsky's multiplication algorithm
Mathematics of computation, Volume 86, Number 308, November 2017, 2975-3000
doi: https://doi.org/10.1090/mcom/3230

2017
Miriam Abdon, Robert Rolland
Hamming distances from a function to all codewords of a Generalized Reed-Muller code of order one
Applicable Algebra in Engineering, Communication and computing, Volume 28, Number 5, pp 387–408, November 2017
doi 10.1007/s00200-016-0311-x

2016
Kevin Atighehchi, Stéphane Ballet, Alexis Bonnecaze, Robert Rolland
Effective arithmetic in finite fields based on Chudnovsky's multiplication algorithm.
Comptes Rendus Mathématique, Volume 354, Number 2, pp 137-141, February 2016

2015
Ballet Stéphane, Rolland Robert, Tutdere Seher
Effective bounds on class number and estimation for any step of towers of algebraic function fields over finite fields. Moscow Mathematical Journal, Volume 15, Number 4, pp. 653–677, October-December 2015.

2015
Ballet Stéphane, Rolland Robert, Tutdere Seher.
Lower Bounds on the number of rational points of Jacobians over finite fields and application to algebraic function fields in towers. Moscow Mathematical Journal, Volume 15, Number 3, pp 425-433, July – September 2015.

2015
Lachaud Gilles, Rolland Robert.
On the Number of Points of Algebraic Sets over Finite Fields, Journal of Pure and Applied Algebra 219 (2015) pp 5117–5136.

2014
Ballet Stéphane, Rolland Robert.
On low weight codewords of generalized affine and projective Reed-Muller codes.
Designs, Codes and Cryptography, Volume 73, Issue 2, pp 271-297, November 2014
DOI : 10.1007/s10623-013-9911-7, 2014.

2012
Ballet Stéphane, Rolland Robert.
Lower bounds on the class number of algebraic function fields defined over any finite field.
Journal de Théorie des nombres de Bordeaux, T. 24, N. 3 (2012), p. 505-540.

2011
Ballet Stéphane, Rolland Robert.
Minoration du nombre de classes des corps de fonctions algébriques définis sur un corps fini.
C.R. Acad. Sci. Paris, Ser. I, 349, 709--712, 2011, doi:10.1016/j.crma.2011.06.016, 2011.

2011
Ballet Stéphane, Rolland Robert.
A note on a Yao's theorem about pseudo-random generators.
Cryptography and Communications, Vol. 3 N. 4 (2011), Page 189-206 doi: 10.1007/s12095-011-0047-1, Springer, 2011.

2011
Ballet Stéphane, Rolland Robert.
Families of curves over any finite field attaining the generalized Drinfeld-Vladut bound.
Publ. Math. Univ. Franche-Comté Besançon Algèbr. Theor. 5-18, 2011.

2010
Rolland Robert. The second weight of generalized Reed-Muller codes in most cases. Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences, Vol. 2, N. 1, April 2010

2009
Ballet Stéphane, Ritzenthaler Christophe, Rolland Robert. On the existence of dimension zero divisors in algebraic function fields defined over F_q. Acta Arithmetica, 143, N°4, 377--392, 2010

2004
Ballet Stéphane, Rolland Robert, Multiplication algorithm in a finite field and tensor rank of the multiplication.
Journal of Algebra, Vol 272/1, 173--185, 2004.

2000
Lachaud Gilles, Lucien Isabelle, Mercier Dany-Jack and Rolland Robert, Group structure on projective spaces and cyclic codes over finite fields, Finite Fields and Their Applications 6, no.2, pp.119-129 (available on Ideal), 2000

1998
Mercier Dany-Jack and Rolland Robert, Polynômes homogènes qui s'annulent sur l'espace projectif Pm (Fq) [Homogeneous polynomials that vanish on the projective space Pm (Fq)],
J. Pure Appl. Algebra 124, no. 1-3, 227--240, 1998

1996
Cherdieu Jean Pierre and Rolland Robert,
On the number of points of some hypersurfaces in Fnq,
Finite Fields Appl. 2, no. 2, 214--224, 1996

1992
Rolland Robert
The number of MDS [7,3] codes on finite fields of characteristic 2,
Appl. Algebra Engrg. Comm. Comput. 3, no. 4, 301--310, 1992

1988
Dumas P, Humbert A, Mathieu G, Mathiez P, Mouttet C, Rolland R, Salvan F, Thibaudau F.
Scanning Tunneling Microscopy Studies on AU/SI(111) interfaces
Journal of Vacuum Science & Technologie A-vacuum surfaces and films Vol. 6, Issue 2, p. 517-518
interfaces
Mars-April 1988

1988
Dumas P, Humbert A, Mathieu G, Mathiez P, Mouttet C, Rolland R, Salvan F, Thibaudau F, Tosh S .
Structure of the AU/SI(111) surface by scanning tunneling microscopy
Physica Scripta Vol. 38 N. 2 1988

1971
Rolland Robert
Sur l'existence et l'unicité de bases complémentairement universelles pour quelques classes de bases d'espaces de Banach,
C. R. Acad. Sci. Paris Sér. A-B 272, A1567--A1569, 1971

Refereed Publications In Proceedings of International Conferences

2015
Poulakis Dimitrios, Rolland Robert
A Digital Signature Scheme Based on Two Hard Problems
In Computation, Cryptography, and Network Security
Conference held in April 2013 at the Hellenic Military Academy
Athens, Greece, p. 441-450 Springer 2015

2015
Rolland Robert
Randomnes in Cryptography
In Computation, Cryptography, and Network Security
Conference held in April 2013 at the Hellenic Military Academy
Athens, Greece, p. 451-459 Springer 2015

2013
Ballet Stéphane, Rolland Robert.
On low weight codewords of generalized affine and projective Reed-Muller codes (Extended abstract).
Pre-proceedings of International Workshop on Coding and Cryptography. (WCC2013)
http://www.selmer.uib.no/WCC2013/PreProceedings.pdf

2010
Atighehchi Kévin, Muntean Traian, Parlanti Sylvain, Rolland Robert, Vallet Laurent. A Key Forwarding Protocol for Secure Communicating Systems, Proceedings of SYNASC 2010, 12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing. Timisoara, Romania, p. 339-346 IEEE 2010

2010
Ivey-Law Hamish, Rolland Robert. Constructing a database of cryptographically strong elliptic curves. Proceedings of SAR-SSI 2010: Fifth Conference on Network and Information Systems Security (SAR/SSI 2010), Rocquebrune Cap-Martin, France.

2009
Ballet Stéphane, Le Brigand Dominique, Rolland Robert. On an application of the definition field descent of a tower of function fields. Proceedings of the Conference "Arithmetic, Geometry and Coding Theory" (AGCT 2005), Société Mathématique de France, sér. Séminaires et Congrès 21, 187--203, 2009.

2008
Robert Rolland, Number of points of non-alsolutely irreducible hypersurfaces, In Proceedings of the First SAGA Conference, Series on Number Theory and Its Applications, World Scientific, Vol. 5, p. 481-487, 2008

2005
Ballet Stéphane, Rolland Robert, On the bilinear complexity of the multiplication in finite fields. Proceedings of the Conference "Arithmetic, Geometry and Coding Theory" (AGCT 2003), Société Mathématique de France, sér. Séminaires et Congrès 11, 179--188, 2005.

1996
Cherdieu Jean Pierre and Rolland Robert,
On hypersurfaces defined by a separated variables polynomial over a finite field,
Arithmetic, geometry and coding theory (Luminy, 1993), 35--43, de Gruyter, Berlin, 1996

1996
Rolland Robert and Skorobogatov Alexei N.,
Dénombrement des configurations dans le plan projectif [Enumeration of configurations in the projective plane],
Arithmetic, geometry and coding theory (Luminy, 1993), 199--207, de Gruyter, Berlin, 1996

Editor of Proceedings

2014
Muntean Traian, Rolland Robert, Mugwaneza Léon (Editors).
13th International Symposium on Parallel and Distributed Computing
ISPDC 2014, IEEE Computer Society, 2014

2013
Muntean, Traian, Poulakis, Dimitrios, Rolland Robert (Editors).
Algebraic Informatics, 5th International Conference on Algebraic Informatics, CAI 2013, Lecture Notes in Computer Science Vol. 8080, 2013.

2010
Kohel David, Rolland Robert (Editors). Arithmetic, Geometry, Cryptography and Coding Theory 2009, Contemporary Mathematics, AMS, Vol. 521 (2010).

2008
Jean Chaumine, James Hirschfeld & Robert Rolland, (Editors) Algebraic Geometry and Its Applications, Dedicated to Gilles Lachaud on His 60th Birthday, Proceedings of the First SAGA Conference, Series on Number Theory and Its Applications, World Scientific, Vol. 5, 2008

National Journals

2011
Barthélemy Pierre, Rolland Robert.
L'emploi de la cryptographie pour la sécurisation des données sur clés USB.
Sécurité de l'Information, N. 11, Mars 2011, CNRS.

2007
Rolland Robert, Sécurité des systèmes de chiffrements à clé publique basés sur le problème du logarithme discret..
In : Journée annuelle de la Société Mathématique de France: Nouvelles Méthodes Mathématiques en Cryptographie, 23 Juin 2007.

Books

2017
Robert Rolland,
Théorie de la mesure et de l'intégration
Cours et exercices corrigés
Collection Références Sciences, Éditions Ellipses, 2017
ISBN : 9782340017467

2015
Robert Rolland,
Géométrie Projective
Collection Références Sciences, Éditions Ellipses, 23 juin 2015
ISBN : 9782340005051

2012
Barthélemy Pierre, Rolland Robert, Véron Pascal. Cryptographie : principes et mises en oeuvre, 2e édition revue et augmentée
Ouvrage, Edition Hermès Science, collection informatique, 2012.
Librairie Lavoisier ISBN-10: 2746238160
ISBN-13: 978-2746238169

2005
Barthélemy Pierre, Rolland Robert, Véron Pascal, Cryptographie : principes et mises en oeuvre.
Ouvrage, Edition Hermès Science, collection informatique, 2005.
Librairie Lavoisier ISBN-10: 2746211505
ISBN-13: 978-2746211506

1994
Maltret J.L. and Rolland Robert,
Mathématiques Algorithmique et Informatique,
Ellipses, ISBN 2-7298-9410-1, 1994

1979
Rolland Robert
Théorie des séries. 2 [Theory of series. 2] Séries entières [Power series] With the collaboration of Y. Chevallard,
CEDIC, Paris. 139 pp. ISBN: 2-7124-0713-X, 1979

1979
Chevallard Y, With the collaboration of Robert Rolland.
Théorie des séries. 1 [Theory of series. 1] Séries numériques. [Numerical series],
CEDIC, Paris. 234 pp. ISBN: 2-7124-0712-1, 1979

Chapters in Books

2011
Lectures sur les Mathématiques, l'Enseignement et les concours, Volume 4, sous la direction de Dany-Jack Mercier.
Robert Rolland : Problèmes choisis, p. 69-144

2010
Lectures sur les Mathématiques, l'Enseignement et les concours, Volume 2, sous la direction de Dany-Jack Mercier.
Robert Rolland : Fonctions d'une variable complexe, p. 57-137

2009
Lectures sur les Mathématiques, l'Enseignement et les concours, Volume 1, sous la direction de Dany-Jack Mercier.
Robert Rolland : Outils élémentaires de l'Analyse, p. 163-223

1997
Rolland Robert, Convexité,
Encyclopaedia Universalis, article repris dans Encyclopaedia Universalis, Dictionnaire des Mathématiques, Albin Michel, ISBN 2-226-09423-7, 1997

1997
Rolland Robert and Verley Jean-Luc., Normés (Espaces Vectoriels),
Encyclopaedia Universalis, article repris dans Encyclopaedia Universalis, Dictionnaire des Mathématiques Albin Michel, ISBN 2-226-09423-7,1997

1993
Barthelemy Pierre and Rolland Robert, WAIS, Wide Area Information Server,
L'Internet Professionnel, CNRS Editions, ISBN 2-271-05256 and also in Revue Tribunix, vol.9, n.51 (sept.-oct.1993), pp.11-21. Ed.AFUU, 1993

Participation in a book

1995
A. Poli with participation from L. Bénéteau, F. Cortial, M.C. Gennero, Ll. Huguet, H. Imai, R. Kohno, J.P. Rocher, R. Rolland. Exercices sur les Codes Correcteurs : 600 exercices corrigés. MASSON ed., (220 pages).

ArXiv, HAL et Researchgate

2015
Robert Rolland
fonctions maximalement non-linéaires sur un corps fini
Researchgate 287207746

2015
Kevin Atighehechi, Robert Rolland
Optimization of Tree Modes for Parallel Hash Functions
ArXiv:1512.05864

2015
Miriam Abdon, Robert Rolland
Hamming distances from a function to all codewords of a Generalized Reed-Muller code of order one
ArXiv:1512.04788

2015
Kevin Atighehchi, Stéphane Ballet, Alexis Bonnecaze, Robert Rolland
On Chudnovsky-Based Arithmetic Algorithms in Finite Fields
ArXiv:1510.00090

2014
Lachaud Gilles, Rolland Robert.
On the Number of Points of Algebraic Sets over Finite Fields.
ArXiv: 1405.3027

2013
Ballet Stéphane, Rolland Robert, Tutdere Seher.
Lower Bounds on the number of rational points of Jacobians over finite fields and application to algebraic function fields in towers.
arXiv:1303.5822

2013
Ballet Stéphane, Rolland Robert.
Remarks on low weight codewords of generalized affine and projective Reed-Muller codes (full paper). arXiv:1203.5244

2012
Bonnecaze Alexis, Rolland Robert.
Collecting Data while Preserving Individual's Privacy: a case study.

Cryptology ePrint Archive, 2012/603

2012
Poulakis Dimitrios, Rolland Robert.
A digital Signature Scheme for Long-Term Security.
Cryptology ePrint Archive 2012/134

2011
Ballet Stéphane, Chaumine Jean, Pieltant Julia, Rolland Robert.
On the tensor rank of multiplication in finite extensions of finite fields. arXiv:1107.1184

2009
Ballet Stéphane, Rolland Robert.Families of curves over any finite field with a class number greater than the Lachaud - Martin-Deschamps bounds. arXiv:0906.5432v1

2009
Robert Rolland. The second weight of generalized Reed-Muller codes in most cases.
ArXiv:0902.0058

2009
Ballet Stéphane, Ritzenthaler Christophe, Rolland Robert. On the existence of dimension zero divisors in algebraic function fields defined over F_q. ArXiv:0906.5216

2009
Robert Rolland. L'organisation de la cryptologie moderne. HAL Id : cel-00420483, version 1

2004
Ballet Stéphane, Le Brigand Dominique, Rolland Robert. Descent of the definition field of a tower of function fields and applications. ArXiv:math/0409173