europass **Curriculum vitae**

Informaţii personale

Prenume /Nume	**ROBERT ROLLAND**
Titlul științific	Professor Information Theory - Research
Afiliere instituțională	ERISCS Research Lab and Institut de Mathématiques de Luminy Université de la Méditerranée Aix-Marseille II
Email	robert.rolland@acrypta.fr
Pagina web	http://robert.rolland.acrypta.com/
Țara de proveniență	France

Prestigiul științific

Educaţie şi formare	• 1965 – 1968, Ecole Normale Supérieure de Cachan, Agrégation de Mathématiques, Mathématiques • HDR, Université de la Méditerranée
Experienţa profesională	• Directeur de Recherche Associé ERISCS; ancien MdC HDR; Aix-Marseille Université • Université de la Méditerranée Aix-Marseille II, France • Chercheur, Institut de Mathématiques de Luminy • 2006-present ACrypta Expert
Domenii de cercetare	information security, cryptographye, navigation.
Lucrări publicate (selecţii)	Cărţi: • **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 • **Kohel** David, **Rolland Robert** (Editors). *Arithmetic, Geometry, Cryptography and Coding Theory 2009,* Contemporary Mathematics, AMS, Vol. 521 (2010). Publicaţii în jurnale: • **Ballet** Stéphane, **Rolland Robert**, *Lower bounds on the class number of algebraic function fields defined over any finite field*, accepted in Journal de Théorie des nombres de Bordeaux, 2012 • **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. • **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 • **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. • **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. • **Poulakis** Dimitrios, **Rolland** Robert., *A digital Signature Scheme for Long-Term Security*., Cryptology ePrint Archive 2012/134 • **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. • **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 • **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

- **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.
- **Robert Rolland***: The Number of MDS[7, 3] Codes on Finite Fields of Characteristic*. Appl. Algebra Eng. Commun. Comput. 3: 301-310 (1992)

Publicaţii în Proc.:

- **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
- **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
- **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.
- **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.
- **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
- **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
- **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.
- B**allet 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

Experienţa anterioară în organizarea de evenimente similare

- president of ACrypta (Association de Cryptographie Théorique et Appliquée)
- member of IACR (International Association for Cryptologic Research)
- honorary member of ERISCS Research Lab and Institut de Mathématiques de Luminy.
- project director: Arcana-ECDB database of elliptic curves