Dr. Ludovic Perret
Associate Professor

LIP6 – UPMC Univ. Paris 6
INRIA Paris-Rocquencourt
`PolSys` team
4, Place Jussieu
75015 Paris, France
Tel. : +33 01 44 27 87 59
Email : `ludovic.Perret@lip6.fr`
Web :
`http://www-polsys.lip6.fr/~perret/`

Professional Experience

Fev. 2007	Associate Professor at UPMC Univ. Paris 6
Oct. 2005 – January 2007	Postdoctoral Researcher in the Crypto Group Univ. Catholique of Louvain–la–Neuve (Belgique)
Oct. 2005	Doctorate in Computer Science University of Marne–la–Vallée **Study of Algebraic and Combinatorial Tools for Public-Key Cryptography.**

Grants

2012 – 2016	Member of ANR project High Performance Algebraic Computing (HPAC)
2010 – 2014	PI (with G. Renault) of the ANR grant Jeunes Chercheurs "Cryptography and Computer Algebra" *Members:* J.-C. Faugère, L. Perret, G. Renault
2008 – 2013	Associate member of the NoE FP7 project ECRYPT II
2007 – 2010	Member of the ANR project Algebraic Methods in Cryptography (MAC)
Oct. 2005 – January 2007	Members of the FP6 EU project INSPIRED
Oct. 2005 – January 2007	Members of the NoE FP6 project ECRYPT

Scientific Activities

Supervision

PhD Luk Bettale (2008 – 2011) on "Algebraic Cryptanalysis of Multivariate Schemes and Hash Functions"

PhD Frédéric Urvoy de Portzamparc (2012 – 2015) on "Physical and Algebraic Analysis of Code-based Schemes"

Editorial Activity

- Editorial board of *Design, Codes and Cryptography* (DCC).
- Guest Editor [S1] (with J.-C. Faugère, J. Gutierrez, D. Gómez-Pérez), *Journal of Symbolic Computation*, special issue "Mathematical and Computer Algebra Techniques in Cryptology".
- Guest Editor [S2] (with J.-C. Faugère), *Mathematics in Computer Science*, special issue "Symbolic Computation and Cryptography".
- Guest Editor [S3] (with D. Augot, and J.-C. Faugère), *Journal of Symbolic Computation*, special issue "Gröbner Bases Techniques in Cryptography and Coding Theory".
- Guest Editor [B4] (with M. Sala, T. Mora, S. Sakata, and C. Traverso), RISC book series (Springer, Heidelberg), "Gröbner Bases, Coding, and Cryptography".

Conference Organization

- Co-organizer (with C. Eder, J.-C. Faugère, E. Tsigaridas) of a special session on "Polynomial System Solving, Groebner Basis, and Applications" at ACA'2015, July 20 - 23 (2015), Kalamata, Greece.
- Co-organizer (with C. Cid and J.-C. Faugère), Summer School on "Tools", Mykonos (Greece), 28 May – 1 June 2012.
- Co-organizer (with L. Bettale, J.-C. Faugère, G. Renault), National Days in Coding and Cryptography, Fréjus, France, October 2009.
- Co-organizer (with M. Abshoff, T. Daly, L. Fousse, C. Pernet and P. Zimmermann), Sage Days 10, Nancy, October 2008.
- Co-organizer (with C. Cid), Summer School "Emerging Topics in Cryptographic Design and Analysis", Samos, Greece, 30 Avr.–4 May, 2007.
- Co-organizer of the workshop (with M. Klin, and M. Sala) "Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics", Linz, Austria, 1–6 May, 2006.

Program Committee

- EUROCRYPT'14, 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, 11 – 15 May 2014, Copenhagen, Denmark.
- PKC'2013, 16th International Conference on Practice and Theory in Public-Key Cryptography, February 26 - March 1, Nara, Japan.
- The Second International Workshop on Modern Cryptography and Security Engineering, MoCrySEn 2013, September 2nd – 6th (2013), University of Regensburg, Germany.

- International Conference on Symbolic Computation and Cryptography(SCC'2008, SCC'2010, and SCC'2012).
- Information Security and Cryptology, Inscrypt (2008, 2010, and 2013).
- Special Track on Symbolic Computation and Cryptology at Inscrypt'2008.
- Special Track on Post-Quantum Cryptology at Inscrypt'2009.
- Workshop on Tools for Cryptanalysis 2010.
- Yet Another Conference on Cryptography 2010 (YACC'10).
- Information and Network Security Track of the Annual Summit and Conference of Asia-Pacific Signal and Information Processing Association 2010 (APSIPA ASC 2010).

List of Publications

Guest Editors

[S1] J.-C. Faugère, J. Gutierrez, D. Gómez-Pérez, and L. Perret. *Mathematical and Computer Algebra Techniques in Cryptology*, volume 64. Elsevier, Journal of Symbolic Computation, November 2013.

[S2] J.-C. Faugère and L. Perret. *Symbolic Computation and Cryptography*, volume 3. Birkhäuser and Springer, Mathematics in Computer Science, 2010.

[S3] D. Augot, J.-C. Faugère, and L. Perret. *Gröbner Bases Techniques in Coding Theory and Cryptography*, volume 44. Academic Press, Inc., Journal of Symbolic Computation, 2009.

[B4] M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso. *Gröbner Bases, Coding, and Cryptography*. Springer, 2009.

Book Chapter

[CB5] F. Levy-dit Vehel, M.G. Marinari, L. Perret, and C. Traverso. *Gröbner Bases, Coding, and Cryptography*, chapter A Survey on Polly Cracker Systems, pages 143–155. Springer, 2009.

Journal

[J6] J.-C. Faugère, A. Otmani, L. Perret, F. De Portzamparc, and J.-P. Tillich. Structural Cryptanalysis of McEliece Schemes with Compact Keys. *Designs, Codes and Cryptography*, page 26,

[J7] M. Albrecht, C. Cid, J.-C. Faugère, R. Fitzpatrick, and L. Perret. On the Complexity of the BKW Algorithm on LWE. *Designs, Codes and Cryptography*, 74(2):325–354, July 2015.

[J8] L. Bettale, J.-C. Faugère, and L. Perret. Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic. *Designs, Codes and Cryptography*, 69(1):1 – 52, 2013.

[J9] J.-C. Faugère, V. Gauthier-Umana, A. Otmani, L. Perret, and J.-P. Tillich. A Distinguisher for High Rate McEliece Cryptosystems. *IEEE Transactions on Information Theory*, 59(10):6830–6844, June 2013.

[J10] J.-C. Faugère, D. Lin, L. Perret, and T. Wang. On Enumeration of Polynomial Equivalence Classes and Their Application to MPKC. *Finite Fields and Their Applications*, 18(2):283 – 302, 2012.

[J11] M. Albrecht, C. Cid, J.-C. Faugère, and L. Perret. On the Relation Between the MXL Family of Algorithms and Gröbner Basis Algorithms. *Journal of Symbolic Computation*, 47(8):926–941, 2012.

[J12] F. Levy-dit Vehel and L. Perret. Security Analysis of Word Problem-Based Cryptosystems. *Des. Codes Cryptography*, 54(1):29–41, 2010.

[J13] L. Bettale, J.-C. Faugère, and L. Perret. Hybrid Approach for Solving Multivariate Systems over Finite Fields. *Journal of Mathematical Cryptology*, 3(3):177–197, 2010.

[J14] J.-C. Faugère and L. Perret. An Efficient Algorithm for Decomposing Multivariate Polynomials and its Applications to Cryptography. *Journal of Symbolic Computation*, 44(12):1676–1689, 2009.

[J15] F. Levy-dit Vehel and L. Perret. A Polly Cracker System Based on Satisfiability. *Progress in Computer Science and Applied Logic*, 23:177–192, 2004.

Fully Refereed International Conferences Papers with Proceedings (Rank A+ or A)

[A16] M. Conde Pena, J.-C. Faugère, and L. Perret. Algebraic Cryptanalysis of a Quantum Money Scheme The Noise-Free Case. In *IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'15)*, Maryland, United States, March 2015.

[A17] J.-C. Faugère, D. Gligoroski, L. Perret, S. Samardjiska, and E. Thomae. A Polynomial-Time Key-Recovery Attack on MQQ Cryptosystems. In *IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'15)*, Maryland, United States, March 2015.

[A18] J.-C. Faugère, L. Perret, and F. De Portzamparc. Algebraic Attack against Variants of McEliece with Goppa Polynomial of a Special Form. In *Advances in Cryptology Asiacrypt 2014*, Kaohsiung, Tawan, September 2014.

[A19] M. Albrecht, J.-C. Faugère, R. Fitzpatrick, and L. Perret. Lazy Modulus Switching for the BKW Algorithm on LWE. In Hugo Krawczyk, editor, *Public-Key Cryptography PKC 2014*, volume 8383 of *Lecture Notes in Computer Science*, pages 429–445, Buenos Aires, Argentina, March 2014. Springer Berlin Heidelberg.

[A20] M. Albrecht, J.-C. Faugère, R. Fitzpatrick, L. Perret, Y. Todo, and K. Xagawa. Practical Cryptanalysis of a Public-Key Encryption Scheme Based on New Multivariate Quadratic Assumptions. In Hugo Krawczyk, editor, *Public-Key Cryptography PKC 2014*, volume 8383 of *Lecture Notes in Computer Science*, pages 446–464, Buenos Aires, Argentina, March 2014. Springer Berlin Heidelberg.

[A21] Luk Bettale, J.-C. Faugère, and L. Perret. Solving Polynomial Systems over Finite Fields: Improved Analysis of the Hybrid Approach. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 67–74, New York, NY, USA, 2012. ACM.

[A22] J.-C. Faugère, L. Perret, C. Petit, and G. Renault. Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 27–44. Springer Berlin/Heidelberg, 2012.

[A23] M. Albrecht, J.-C. Faugère, P. Farshim, and L. Perret. Polly Cracker, Revisited. In D.H. Lee and X. Wang, editors, *Advances in Cryptology Asiacrypt 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 179–196. Springer Berlin/Heidelberg, 2011.

[A24] L. Bettale, J.-C. Faugère, and L. Perret. Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants. In D. Catalano et al., editor, *Public Key Cryptography - PKC 2011*, volume 6571 of *Lecture Notes in Computer Science*, pages 441–458. Springer-Verlag, 2011.

[A25] C. Bouillaguet, J.-C. Faugère, P.-A. Fouque, and L. Perret. Practical Cryptanalysis of the Identification Scheme Based on the Isomorphism of Polynomial with One Secret Problem. In D. Catalano et al., editor, *Public Key Cryptography - PKC 2011*, volume 6571 of *Lecture Notes in Computer Science*, pages 1–12. Springer-Verlag, 2011.

[A26] J.-C. Faugère, J. von zur Gathen, and L. Perret. Decomposition of Generic Multivariate Polynomials. In *ISSAC '10: Proceedings of the 2010 international symposium on Symbolic and algebraic computation*, ISSAC '10, pages 131–137, New York, NY, USA, 2010. ACM.

[A27] J.-C. Faugère, A. Otmani, L. Perret, and J.-P. Tillich. Algebraic Cryptanalysis of McEliece variants with compact keys. In *Proceedings of Eurocrypt 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 279–298. Springer Verlag, 2010.

[A28] J.-C. Faugère and L. Perret. High Order Derivatives and Decomposition of Multivariate Polynomials. In *ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, ISSAC '09, pages 207–214, New York, NY, USA, 2009. ACM.

[A29] J.-C. Faugère, F. Levy-dit Vehel, and L. Perret. Cryptanalysis of Minrank. In David Wagner, editor, *Advances in Cryptology CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 280–296, Berlin, Heidelberg, August 2008. Springer-Verlag.

[A30] P.-A. Fouque, G. Macariorat, L. Perret, and J. Stern. On the Security of the l-IC Signature Scheme. In *Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2008*, volume 4939 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2008.

[A31] M. Sugita, M. Kawazoe, L. Perret, and H. Imai. Algebraic Cryptanalysis of 58-Round SHA-1. Alex Biryukov, editor, *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*, pages 349–365. Springer, 2007

[A32] J.-C. Faugère and L. Perret. Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 30–47. Springer Berlin/Heidelberg, 2006.

[A33] Jean-Charles Faugère and L. Perret. Cryptanalysis of 2R– Schemes. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 357–372. Springer Berlin/Heidelberg, August 2006.

[A34] L. Perret. A Fast Cryptanalysis of the Isomorphism of Polynomials with One Secret Problem. Ronald Cramer, editor *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*, pages 354–370, Springer, 2005.

Fully Refereed International Conferences Papers with Proceedings (Rank B or C)

[B35] J.-C. Faugère, L. Perret, F. De Portzamparc, A. Otmani, and J.-P. Tillich. Structural Weakness of Compact Variants of the McEliece Cryptosystem. In *IEEE International Symposium on Information Theory - ISIT 2014*, pages 1717–1721, Honolulu, United States, June 2014.

[B36] J.-C. Faugère, D. Gligoroski, E. Jensen, R. Odegard, L. Perret, S. Johan Knapskog, and S. Markovski. MQQ-SIG. In Liqun Chen, Moti Yung, and Liehuang Zhu, editors, *Trusted Systems - The Third International Conference on Trusted Systems - INTRUST 2011*, volume 7222 of *Lecture Notes in Computer Science*, pages 184–203. Springer Verlag, 2012.

[B37] F. Armknecht, D. Augot, L. Perret, and A.-R. Sadeghi. On Constructing Homomorphic Encryption Schemes from Coding Theory. Liqun Chen, editor *Cryptography and Coding - 13th IMA International Conference, IMACC 2011, Oxford, UK, December 12-15, 2011. Proceedings*, volume 7089 of *Lecture Notes in Computer Science*, pages 23–40. Springer, 2011.

[B38] J.-C. Faugère, V. Gauthier-Umana, A. Otmani, L. Perret, and J.-P. Tillich. A Distinguisher for High Rate McEliece Cryptosystems. In *Information Theory Workshop (ITW), 2011 IEEE*, pages 282–286, October 2011.

[B39] J.-C. Faugère, R. Odegard, L. Perret, and D. Gligoroski. Analysis of the MQQ Public Key Cryptosystem. In Swee-Huay Heng, Rebecca N. Wright, and Bok-Min Goi, editors, *Ninth International Conference on Cryptology And Network Security (CANS 2010)*, volume 6467 of *Security and Cryptology*, pages 1–14. Springer-Verlag, December 2010.

[B40] J.-C. Faugère, A. Joux, L. Perret, and J. Treger. Cryptanalysis of the Hidden Matrix Cryptosystem. In Michel Abdalla and Paulo Barreto, editors, *Progress in Cryptology, LATINCRYPT 2010*, volume 6212 of *Lecture Notes in Computer Science*, pages 241–254. Springer Berlin/Heidelberg, 2010.

[B41] M. Albrecht, C. Cid, T. Dulien, J.-C. Faugère, and L. Perret. Algebraic Precomputations in Differential Cryptanalysis. In M. Yung and X. Lai, editors, *Information Security and Cryptology: 6th International Conference, Inscrypt 2010, Revised Selected Papers*, volume To appear, pages 1–18. Springer-Verlag, October 2010.

[B42] J.-C. Faugère and L. Perret. Algebraic Cryptanalysis of Curry and Flurry using Correlated Messages. In M. Yung and F. Bao, editors, *Information Security and Cryptology: 5th International Conference, Inscrypt 2009, Beijing, China, December, 2009, Revised Selected Papers*, volume 6151, pages 266–277, Berlin, Heidelberg, 2010. Springer-Verlag.

[B43] L. Bettale, J.-C. Faugère, and L. Perret. Security Analysis of Multivariate Polynomials for Hashing. In Moti Yung, Dongdai Lin, and Peng Liu, editors, *Information Security and Cryptology: 4th International Conference, Inscrypt 2008, Revised Selected Papers*, volume 5487, pages 115–124, Berlin, Heidelberg, December 2009. Springer-Verlag.

[B44] L. Bettale, J.-C. Faugère, and L Perret. Cryptanalysis of the TRMS Cryptosystem of PKC'05. In Serge Vaudenay, editor, *AfricaCrypt 2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 143–155, Casablanca, Morocco, 2008. Springer.

[B45] F. Levy dit Vehel and L. Perret. On the Wagner-Magyarik Cryptosystem. In *Selected papers of WCC 2005 Conference*, volume 3969, pages 316–329. Springer-Verlag, 2005.

[B46] F. Levy dit Vehel and L. Perret. Attacks on Public Key Cryptosystems Based on Free Partially Commutative Monoids and Groups. Anne Canteaut and Kapalee Viswanathan, editors, *Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings*, volume 3348 of *Lecture Notes in Computer Science*, pages 275–289. Springer, 2004.

[B47] F. Levy dit Vehel and L. Perret. Polynomial Equivalence Problems and Applications to Multivariate Cryptosystems. Thomas Johansson and Subhamoy Maitra, editors, *Progress in Cryptology - INDOCRYPT 2003, 4th International Conference on Cryptology in India, New Delhi, India, December 8-10, 2003, Proceedings*, volume 2904 of *Lecture Notes in Computer Science*, pages 235–251, 2003.

Fully Refereed International Conferences Papers (no Proceeding)

[O48] M. Albrecht, C. Cid, J.-C. Faugère, Robert F., and L. Perret. On the Complexity of the Arora-Ge algorithm against LWE. In *SCC '12: Proceedings of the 3nd International*

Conference on Symbolic Computation and Cryptography, pages 93–99, Castro-Urdiales, July 2012.

[O49] M. Albrecht, Carlos Cid, J.-C. Faugère, R. Fitzpatrick, and L. Perret. On the Complexity of BKW Algorithm against LWE. In *SCC'12: Proceedings of the 3nd International Conference on Symbolic Computation and Cryptography*, pages 100–107, Castro-Urdiales, July 2012.

[O50] J.-C. Faugère, A Otmani, L. Perret, and J.-P. Tillich. A Distinguisher for High Rate McEliece Cryptosystem – Extended Abstract. In P. Véron, editor, *Yet Another Conference on Cryptography, YACC 2010*, pages 1–4, Toulon, 2010.

[O51] J.-C. Faugère, A Otmani, L. Perret, and J.-P. Tillich. Algebraic Cryptanalysis of McEliece variants with compact keys – toward a complexity analysis. In P. Véron, editor, *Yet Another Conference on Cryptography, YACC 2010*, pages 1–4, Toulon, 2010.

[O52] M. Albrecht, C. Cid, T. Dulien, J.-C. Faugère, and L. Perret. Algebraic Precomputations in Differential Cryptanalysis. In *Tools'10: Proceedings of the Workshop on Tools for Cryptanalysis 2010*, pages 1–14, RHUL, June 2010. Ecrypt II.

[O53] L. Bettale, J.-C. Faugère, and L. Perret. Hybrid Approach : a Tool for Multivariate Cryptography. In *Tools'10: Proceedings of the Workshop on Tools for Cryptanalysis 2010*, pages 1–2, RHUL, June 2010. Ecrypt II.

[O54] J.-C. Faugère, A Otmani, L. Perret, and J.-P. Tillich. Algebraic Cryptanalysis of McEliece variants with compact keys – toward a complexity analysis. In *SCC '10: Proceedings of the 2nd International Conference on Symbolic Computation and Cryptography*, pages 45–55, RHUL, June 2010.

[O55] J.-C. Faugère, R. Odegard, L. Perret, and D. Gligoroski. Analysis of the MQQ Public Key Cryptosystem. In *SCC'10: Proceedings of the 2nd International Conference on Symbolic Computation and Cryptography*, pages 101–116, RHUL, June 2010.

[O56] J.-C. Faugère, L. Perret, and P.-J. Spaenlehauer. Algebraic-Differential Cryptanalysis of DES. In *Western European Workshop on Research in Cryptology - WEWoRC 2009*, pages 1–5, July 2009.

[O57] J.-C. Faugère and L. Perret. High Order Derivatives and Decomposition of Multivariate Polynomials. In *Second Workshop on Mathematical Cryptology*, pages 15–19, Santander (Spain), October 2008.

[O58] J.-C. Faugère and L. Perret. On the Security of UOV. In *First International Conference on Symbolic Computation and Cryptography, SCC 08*, LMIB, pages 103–109, Beijing, China, April 2008.

[O59] I. Simonetti, J.-C. Faugère, and L. Perret. Algebraic Attack Against Trivium. In *First International Conference on Symbolic Computation and Cryptography, SCC 08*, LMIB, pages 95–102, Beijing, China, April 2008.

[O60] L. Perret. A Geometrical Approach to a Polynomial Equivalence Problem. In Proceedings of International Conference on Polynomial System Solving (ICPSS), in honor of Daniel Lazard, pp. 30–33, 2004.