Dr. Ludovic PERRET
Associate Professor, HDR
Computer Science Laboratory
Sorbonne University

Tel. : +33 6 95 51 66 81
Email : ludovic.perret@lip6.fr
Web : http://www-polsys.lip6.fr/~perret/
PolSys/LIP6
4, Place Jussieu
75005 Paris, France

Professional Experiences

2007 – current. Associate Professor, Sorbonne University
2019 – current. Co-founder of CryptoNext Security, post-quantum cryptography spin-off from Sorbonne University, INRIA and CNRS
2019 – 2021. CEO of CryptoNext Security
2022 – current. Chair of the Scientific Committee, Feynman Foundation
2015 – 2017. Scientific advisor, Kryptnostic (Californian startup)
2005 – 2007. Postdoctoral Researcher in the Crypto Group, Catholic University of Louvain–la–Neuve (Belgium)
2002 – 2005. Doctorate in Computer Science, Marne-la-Vallée University (France)

Diplomas

2016. Habilitation thesis, *"Gröbner Bases in Quantum-Safe Cryptography"*, Sorbonne University
- keywords : commutative algebra, Gröbner basis, algebraic cryptanalysis, post-quantum cryptography

2005. PhD thesis in Computer Science, *"Study of Algebraic and Combinatorial Tools for Public-Key Cryptography"*, Marne-la-Vallée University
- keywords : commutative algebra, Gröbner basis, cryptanalysis, post-quantum cryptography, word problem based cryptography

Awards and Recognition

2018. Atos-Fourier First Prize in the area of quantum technologies. Career award for my contributions to the design, analysis and technological transfer in post-quantum cryptography
2020. i-Lab Grand Prize for the start-up project CryptoNext Security
i-Lab is known as the most competitive innovation contest for science-driven startup. It is organized by French ministry of Research and Innovation. Grand prizes are awarded for exceptional projects addressing a major societal challenge
2020. Selection of a post-quantum signature scheme, G*e*MSS, for the third round of the NIST post-quantum standardization process
2020. Third prize, Chinese post-quantum design competition, design of the PKPDSS post-quantum signature scheme
2022. Top 100, most influential French innovators, magazine Le Point

Grants

2021 – 2023. ParisRegionQCI project, "*Quantum Communication Infrastructure for the Paris Region*", collaborative national project (funded by the Paris region)
— Task leader – Secure communication for ParisRegionQCI network

2021 - 2022. QSAFE project, "*Quantum Network System Architecture for Europe*", collaborative European project (funded by the European Commission (EC))
— Task leader – System-specific and security requirements of the EuroQCI Network

2020 – 2022. PI, NextHSM project, "*Next Generation of Hardware Security Module*", national project (funded by French Bank of Investment (BPI))

2017 - 2020. RISQ project, "*Gathering of French Industries for Post-Quantum Cryptography*", collaborative national project (funded BPI)
— Task leader : study and design of post-quantum schemes

2014 – 2018. Management committee member, CRYPTACUS project, "*Cryptanalysis of Ubiquitous Computing Systems*", collaborative European project (EU COST, founded by EC)

2014 – 2018. Management committee member (substitute), CryptoAction project,"*Cryptography for Secure Digital Interaction*", collaborative European project (EU COST, founded by EC)

2012 – 2016. Member, HPAC project, "*High Performance Algebraic Computing*", collaborative national project (founded by French National Research Agency (ANR))

2010 – 2014. PI ANR young researcher starting grant, CAC project, "*Cryptography and Computer Algebra*", national project (founded by ANR)

2010 – 2013. Member, EXACTA project, "*Exact/Certified Computation with Algebraic Systems*", International collaborative project (China and France, founded by Chinese National Science Foundation and ANR),

2010 – 2013. French PI, "*Statistical Techniques in Algebraic Cryptanalysis*", International project (France and UK, funded by Royal Society)

2008 – 2013. Associate member, ECRYPT II project, Cryptography Network of Excellence, collaborative European project (founded by EC)

2007 – 2010. Member, MAC project, "*Algebraic Methods in Cryptography*", collaborative national project (founded by ANR)

2005 – 2007. Member, ECRYPT project, Cryptography Network of Excellence, European collaborative project (founded by EC)

Technology Transfer

2019 – current. Co-founder CryptoNext Security

2015 – 2018. PI, HFEBoost project, maturation project, Sorbonne University innovation funding

- Co-author of a patent in multivariate cryptography [73]

Standardization

2022. Co-Chair Chair, IEEE P3172 Working Group, "*Quantum Security Working Group – Recommended Practice for Post-Quantum Cryptography Migration*"

2022 – 2024. Board member, *Crypto Review Panel*, (Internet Engineering Task Force, IETF)

2018. Member and contributor, US government think-tank on quantum technologies (*"Global Quantum Working Group"*), Advanced Technology Academic Research Center (ATARC)

2018. Co-chair, industrial think-tank on quantum-safe security (*"quantum-safe security working group"*), Cloud Security Alliance (CSA)

2016 – current. Member and contributor, European standardization group of post-quantum cryptography (*"Quantum-Safe Cryptography Specification Group"*) , ETSI (European Telecommunications Standards Institute)

2017 – current. Design of a post-quantum signature scheme submitted to the NIST post-quantum standardization process

*"G*e*MSS: A Great Multivariate Short Signature"*.
A. Casanova, J.-C. Faugère, G. Macario-Rat, J. Patarin, L. Perret and J. Ryckeghem.

2019 – 2020. Design of a post-quantum signature scheme for a Chinese post-quantum competition

*"*PKP-*Based Signature Scheme"*.
W. Beullens, J.-C. Faugère, E. Koussa, G. Macario-Rat, J. Patarin and L. Perret.

Research Activities

Research Interest

My research activity is in post-quantum cryptography with several facets going from the most theoretical aspects (91 publications summarized in the table below), technological transfer (in particular with the creation of a startup) and dissemination. My goal is to facilitate the large-scale deployment post-quantum cryptography. My specialities include the security analysis of post-quantum schemes with algebraic cryptanalysis and using tools from commutative algebra (notably, Gröbner bases), the design of new post-quantum primitives, the design of new hybrid protocols (using classical, post-quantum and possibly quantum cryptosystems) and the standardization of post-quantum protocols.

Guest editor of special issues in international journals	4
Book chapter	1
Papers in international journals	19
Rank A/A+ international conferences (very selective)	20
Rank B/C international conferences (selective)	16
Communication in international conferences with program committee (without acts)	12
Patent	1
Software	1
Standardization documents	5
Manuscripts	2
Preprints	3
Dissemination (large audience white papers)	7

Ph.D. Thesis Advisor and Postgraduate-Scholar Sponsor

post-doc	Rachel Player (currently lecturer at Royal Holloway University of London, RHUL)	2018
	Martin Albrecht (currently Professor at RHUL)	2010 – 2012
Phd	Sriram Gopalakrishnan	2022 – 2025
	Jocelyn Ryckeghem (formerly research engineer at CryptoNext)	2017 – 2020
	Olive Chakraborty (currently research engineer at CEA, France)	2017 – 2020
	Frédéric Urvoy de Portzamparc (currently senior pre-sales engineer at Sogeti, France)	2012 – 2015
	Luk Bettale (currently lead cryptographic engineer at IDEMIA, France)	2008 – 2011

Juries & Committees

- Referee for ANR (French National Research Agency) grants ($\times 2$), NSF grants ($\times 2$), NSA grant ($\times 1$) and Swiss NSF ($\times 2$)
- Steering committee of the "National Working Group in Coding and Cryptography",
- Evaluation committee, professor position, university of Bergen, Norway, 2016
- Hiring committee, associate professor position, "System, Security and Algorithms", Sorbonne University, 2016
- PhD committee, Frédéric Urvoy de Portzamparc, "Physical and Algebraic Analysis of Code-based Schemes", UPMC, 2015
- Hiring committee, Associate professor, "Computational Intelligence/Statistical Machine learning", Sorbonne University, 2015
- Phd committee, Luk Bettale, "Algebraic Cryptanalysis of Multivariate Schemes and Hash Functions", Sorbonne University, 2011
- PhD committee, Charles Bouillaguet,"Algorithms for some hard problems and cryptographic attacks against specific cryptographic primitives", ENS Paris, 2011

- PhD committee, Gilles Macario-Rat,"Cryptanalysis of Multivariate Schemes and Solving the Isomorphism of Polynomials", ENS Paris, 2010
- PhD committee, Anna Rimoldi, "On algebraic and statistical properties of AES-like ciphers", Univ. of Trento, 2009
- PhD committee, Ilaria Simonetti, "On some applications of commutative algebra to Boolean functions and their non-linearity", Univ. of Trento, 2009

Editorial Activities

2013 – 2019. Editorial board, *Design, Codes and Cryptography* (DCC)
2017 – 2019. Editorial board, *The Computer Journal*

- Guest Editor
  2013. Journal of Symbolic Computation, special issue on "*Mathematical and Computer Algebra Techniques in Cryptology*" with J.-C. Faugère, J. Gutierrez and D. Gómez-Pérez [1]
  2010. Mathematics in Computer Science, special issue "*Symbolic Computation and Cryptography*" with J.-C. Faugère [2]
  2009. Journal of Symbolic Computation, special issue on "*Gröbner Bases Techniques in Cryptography and Coding Theory*" with D. Augot [3]
  2009. RISC book series (Springer, Heidelberg), "*Gröbner Bases, Coding and Cryptography*" with M. Sala, T. Mora, S. Sakata and C. Traverso [4]

Program Committee (International Conferences)

- ACM Conference on Computer and Communications Security (CCS), 2022
- PKC, International Conference on Practice and Theory in Public-Key Cryptography (PKC'13, PKC'17 and PKC'19)
- ISSAC'16, 41th International Symposium on Symbolic and Algebraic Computation, Canada, 2016
- PASCO'15, 7th International Workshop on Parallel Symbolic Computation, UK, 2015
- EUROCRYPT'14, 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Danemark, 2014
- The Second International Workshop on Modern Cryptography and Security Engineering, MoCrySEn 2013, Germany, 2013
- International Conference on Symbolic Computation and Cryptography (SCC'2008, SCC'2010 and SCC'2012)
- Information Security and Cryptology, Inscrypt (2008, 2010, 2013), Chine
- Special Track on Symbolic Computation and Cryptology at Inscrypt'2008, Chine
- Special Track on Post-Quantum Cryptology at Inscrypt'2009, China
- Workshop on Tools for Cryptanalysis 2010, Angleterre, 2010
- Yet Another Conference on Cryptography 2010 (YACC'10), France, 2010
- Information and Network Security Track, Annual Summit and Conference of Asia-Pacific Signal and Information Processing Association 2010 (APSIPA ASC 2010), Singapour, 2010

Conference Organization

2024. Co-organizer (with J.-C. Faugère, D. Kahrobaei and V. Shpilrain), IHP Special Trimester "*Post-Quantum Algebraic Cryptography*", Paris, France
2018. Co-organizer (with M. Campagna, J.-C. Faugère, S. Gueron and R. Misoczki), one-day workshop, "*Quantum-Safe Cryptography for Industry (*`QsCI`*)*", Santa-Barbara, USA
2017. Co-organizer (with A. Facon, J.-C. Faugère and S. Guilley), one-day workshop, "*Quantum-Safe Cryptography for Industry (*`QsCI`*)*", Paris, France
2015. Co-organizer (with C. Eder, J.-C. Faugère and E. Tsigaridas), special session, "*Polynomial System Solving, Gröbner Basis, and Applications*", Kalamata, Greece
2012. Co-organizer (with C. Cid and J.-C. Faugère), summer school, "*Tools*", Mykonos, Greece
2009. Co-organizer (with L. Bettale, J.-C. Faugère and G. Renault), National days of cryptography and coding theory, Fréjus, France

2008. Co-organizer (with M. Abshoff, T. Daly, L. Fousse, C. Pernet and P. Zimmermann), Sage Days 10, France, Nancy

2007. Co-organizer (with C. Cid), summer school, "*Emerging Topics in Cryptographic Design and Analysis*", Samos, Greece

2007. Co-organizer (with M. Klin et M. Sala), workshop,"*Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics*", Linz, Austria

Invited Talks (selected)

- "Fast quantum algorithms for solving multivariate quadratic equations", Q-Workshop, CUNY Graduate Center, New-York, USA, May 16th, 2022
  - Vising professor at CUNY Graduate Center (3 weeks)
- " Post-quantum cryptography: From theory to practice", AMUSEC, Marseille, France, May 5th-6th, 2022
- " Panelist. Round-table on Impact of quantum technologies on blockchain", IQT Quantum Enterprise Event, San-Diego, USA, May 10th-12th, 2022
- "The Quantum-Safe Revolution", WISA 2016, Jeju Island, Korea, August 25-27, 2016
- "Gröbner Bases Techniques in Post-Quantum Cryptography", CiE 2016 : Pursuit of the Universal, special session on cryptography and information theory, June 27th 2016 - July 1st 2016, Paris, France
- "Gröbner Bases Techniques in Post-Quantum Cryptography", Winter School of PQC'16, February, 22 - 23, 2016, Fukuoka, Japan
- "Algebraic Algorithms for LWE", The Mathematics of Modern Cryptography, Jul. 6 - Jul. 10, 2015, Simons Institue, Berkeley, USA
- "Gröbner Bases in Public Key Cryptography" , Workshop on Cryptography and Computer Algebra, 7-8 November, 2008, Pisa, Italy
- "Gröbner Bases in Cryptography : An Overview," SAGE Days 6 on cryptology, number theory and arithmetic geometry, November 10-14, 2007, Bristol, UK
- "Gröbner Bases in Public Key Cryptography", ECRYPT PhD SUMMER SCHOOL on "Emerging Topics in Cryptographic Design and Cryptanalysis", 30 April - 4 May, 2007, Samos, Greece

List of publications

Guest editor of special issues

[1] J.-C. Faugère, J. Gutierrez, D. Gómez-Pérez and L. Perret. Mathematical and computer algebra techniques in cryptology. Guest editors for *Journal of Symbolic Computation*, volume 64, Elsevier, 2013.

[2] J.-C. Faugère and L. Perret. Symbolic computation and cryptography. Guest editors for *Mathematics in Computer Science*, volume 3, Birkhäuser and Springer, 2010.

[3] D. Augot, J.-C. Faugère and L. Perret. Gröbner Bases techniques in coding theory and cryptography. Guest editors for *Journal of Symbolic Computation*, volume 44, Academic Press, Inc., 2009.

[4] M. Sala, T. Mora, L. Perret, S. Sakata and C. Traverso. Gröbner Bases, coding and cryptography. Guest editors, Springer, 2009.

Book chapter

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

International journals

[6] O. Chakraborty, J.-C. Faugère and L. Perret. Cryptanalysis of the Extension Field Cancellation cryptosystem. *Des. Codes Cryptogr.*, 89(6) :1335–1364, 2021.

[7] M. R. Bender, J.-C. Faugère, L. Perret and E. P. Tsigaridas. A nearly optimal algorithm to decompose binary forms. *J. Symb. Comput.*, 105 :71–96, 2021.

[8] M. Conde Pena, R. Durán Díaz, J.-C. Faugère, L. Hernández Encinas and L. Perret. Non-quantum cryptanalysis of the noisy version of Aaronson-Christiano's quantum money scheme. *IET Inf. Secur.*, 13(4) :362–366, 2019.

[9] J.-C. Faugère, L. Perret and J. Ryckeghem. Software toolkit for HFE-based multivariate schemes. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2019(3) :257–304, 2019.

[10] J.-C. Faugère, A. Otmani, L. Perret, F. de Portzamparc and J.-P. Tillich. Structural cryptanalysis of McEliece schemes with compact keys. *Des. Codes Cryptogr.*, 79(1) :87–112, 2016.

[11] M. R. Albrecht, J.-C. Faugère, P. Farshim, G. Herold and L. Perret. Polly Cracker, revisited. *Des. Codes Cryptography*, 79(2) :261–302, 2016.

[12] J. Berthomieu, J.-C. Faugère and L. Perret. Polynomial-time algorithms for quadratic isomorphism of polynomials : The regular case. *Journal of Complexity*, (1–39) :39, 2015.

[13] J.-C. Faugère, A. Otmani, L. Perret, F. de Portzamparc and J.-P. Tillich. Folding alternant and Goppa codes with non-trivial automorphism groups. *IEEE Transactions on Information Theory*, 62(1) :184–198, 2016.

[14] N. Fazio, K. Iga, A. Nicolosi, L. Perret and W. E. Skeith III. Hardness of learning problems over Burnside groups of exponent 3. *Des. Codes Cryptography*, 75(1) :59–70, 2015.

[15] 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*, pages 87–112, January 2016.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] F. Levy-dit-Vehel and L. Perret. Security analysis of word problem-based cryptosystems. *Des. Codes Cryptography*, 54(1) :29–41, 2010.

[24] 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.

Publications in international conferences (Rank A+ or A)

[25] M. Bender, J.-C. Faugère, L. Perret and E. P. Tsigaridas. A superfast randomized algorithm to decompose binary forms. In Sergei A. Abramov, Eugene V. Zima, and Xiao-Shan Gao, editors, *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2016, Waterloo, ON, Canada, July 19-22, 2016*, pages 79–86. ACM, 2016.

[26] 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.

[27] 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.

[28] 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, TaÃ¯wan, September 2014.

[29] 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.

[30] 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.

[31] 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.

[32] L. 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] M. Sugita, M. Kawazoe, L. Perret and Hideki Imai. Algebraic cryptanalysis of 58-round SHA-1. In 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.

[42] 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.

[43] 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.

[44] L. Perret. A fast cryptanalysis of the isomorphism of polynomials with one secret problem. In 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.

Publications in international conferences (Rank B or C)

[45] W. Beullens, J.-C. Faugère, E. Koussa, G. Macario-Rat, J. Patarin and L. Perret. PKP-based signature scheme. In Feng Hao, Sushmita Ruj, and Sourav Sen Gupta, editors, *Progress in Cryptology - INDOCRYPT 2019 - 20th International Conference on Cryptology in India, Hyderabad, India, December 15-18, 2019, Proceedings*, volume 11898 of *Lecture Notes in Computer Science*, pages 3–22. Springer, 2019.

[46] J.-C. Faugère, E. Koussa, G. Macario-Rat, J. Patarin and L. Perret. Combinatorial digital signature scheme. In Marie-Rita Hojeij, Béatrice Finance, Yehia Taher, Karine Zeitouni, Rafiqul Haque, and Mohamed Dbouk, editors, *Proceedings of the 1st International Conference on Big Data and Cyber-Security Intelligence, BDCSIntell 2018, Hadath, Lebanon, December 13-15, 2018*, volume 2343 of *CEUR Workshop Proceedings*, pages 48–54. CEUR-WS.org, 2018.

[47] J.-C. Faugère and L. Perret. The quantum-safe revolution. In Dooho Choi and Sylvain Guilley, editors, *Information Security Applications - 17th International Workshop, WISA 2016, Jeju Island, Korea, August 25-27, 2016, Revised Selected Papers*, volume 10144 of *Lecture Notes in Computer Science*, pages 258–266, 2016.

[48] 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.

[49] 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.

[50] 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.

[51] F. Armknecht, D. Augot, L. Perret and A.-R. Sadeghi. On constructing homomorphic encryption schemes from coding theory. In 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.

[52] 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 6584, pages 1–18. Springer-Verlag, October 2010.

[53] 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.

[54] 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.

[55] 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.

[56] 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.

[57] 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.

[58] 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.

[59] F. Levy-dit-Vehel and L. Perret. Attacks on public key cryptosystems based on free partially commutative monoids and groups. In 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.

[60] F. Levy-dit-Vehel and L. Perret. Polynomial equivalence problems and applications to multivariate cryptosystems. In 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. Springer, 2003.

Communication in international conferences with programme commitees (whithout acts)

[61] M. Albrecht, C. Cid, J.-C. Faugère, R. Fitzpatrick 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.

[62] 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.

[63] 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.

[64] 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.

[65] 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.

[66] 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.

[67] 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.

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] 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.

Patent

[73] J.-C. Faugère and L. Perret. Mise en oeuvre optimisée du HFE. French patent, number WO2017001809A1, 2017.

Software

[74] J.-C. Faugère, L. Perret and J. Ryckeghem. `MQSoft`, A fast multivariate cryptography library. Available from `https://www-polsys.lip6.fr/Links/NIST/MQsoft.html`.

Standardisation documents

[75] L. Perret (rapporteur). Quantum-safe signatures. `ETSI` Technical Report (TR 103 616), 2021.

[76] O. Chakraborty, J.-C. Faugère and L. Perret. CFPKM : A Key encapsulation mechanism based on solving system of non-linear multivariate polynomials. A submission to the `NIST` round-1 post-quantum standardization process, 2017.

[77] J.-C. Faugère, L. Perret and J. Ryckeghem. `DualModeMS` : A dual mode for multivariate-based signature. A submission to the `NIST` round-1 post-quantum standardization process, 2017.

[78] A. Casanova, J.-C. Faugère, G. Macario-Rat, J. Patarin, L. Perret and J. Ryckeghem. G*e*MSS : A Great Multivariate Short Signature. A submission to the `NIST` post-quantum submission process. Selected for the `NIST` round-3 (alternate), 2017 – 2022.

[79] W. Beullens, J.-C. Faugère, X. Han, D. Lin, E. Koussa, G. Macario-Rat, J. Patarin and L. Perret. `PKPDSS` : A submission to the Chinese post-quantum competition, 2019. Available from `https://sfjs.cacrnet.org.cn/upload/5db973084bc8b.zip`.

Manuscrits

[80] L. Perret. Gröbner bases in quantum-safe cryptography. Habilitation thesis, Sorbonne University, 2016. Available from `https://tel.archives-ouvertes.fr/tel-01417808/document`.

[81] L. Perret. Algebraic and combinatorial tools for public-key cryptography. PhD thesis, Marne-la-Vallée University, 2005. Available from `https://www.iacr.org/phds/index.php?p=detail&entry=1185`

Preprints

[82] J.-C. Faugère, K. Horan, D. Kahrobaei, M. Kaplan, E. Kashefi and L. Perret. Fast quantum algorithm for solving multivariate quadratic equations. IACR *Cryptol. ePrint Arch.*, 2017 :1236 (Citations : 29, Google Scholar).

[83] M. R. Albrecht, C. Cid, J.-C Faugère, R. Fitzpatrick and L. Perret. Algebraic algorithms for LWE problems. IACR *Cryptology ePrint Archive*, 2014 :1018, 2014 (Citations : 82, Google Scholar).

[84] J.-C. Faugère, L. Perret, C. Petit and G. Renault. New subexponential algorithms for factoring in $\mathrm{SL}(2, \mathbb{F}_q)$. IACR *Cryptology ePrint Archive*, 2011 :598, 2011 (Citations : 10, Google Scholar).

Dissemination

[85] R. Grimes, E. Chiu, J. Gable, B. Huttner and L. Perret. Practical preparations for the post-quantum world. Cloud Security Alliance, QSS WG white paper, 2021.

[86] R. Faux and L. Perret. Confidence in post-quantum algorithms. Cloud Security Alliance, QSS WG white paper, 2021.

[87] ATARC Quantum Working Group. White Paper : Quantum-safe framework. An intra and inter-agency guide to being quantum ready. ATARC white paper, 2021

[88] ATARC Quantum Working Group. Applied quantum computing for today's military. ATARC white paper, 2021

[89] R. Faux and L. Perret. Mitigating the quantum threat with hybrid cryptography. Cloud Security Alliance, QSS WG white paper, 2018.

[90] B. Huttner, J. Melia, L. Perret and L. Wilson. Applied quantum-safe security quantum-resistant algorithms and quantum-key distribution. Cloud Security Alliance, QSS WG white paper, 2017.

[91] B. Huttner, J. Melia, L. Perret and L. Wilson. Quantum-safe security glossary. Cloud Security Alliance, QSS WG white paper, 2017.