CHRISTOPHE PETIT

Mail address: 16c Devonport Road, W12 8NY, London, UK.
Phone: 00447448817892 Email: christophe.f.petit@gmail.com.

Work experience

2014 - now **Research Associate / Invited Lecturer**
University College London, Computer Science Department, UK

2014 - now **Research Collaborator**
Université catholique de Louvain, Crypto Group, Belgium

2012 - now **Visiting Professor**
Université de Kinshasa, DRC

2013 - 2014 **Visiting Academic / Invited Lecturer**
University College London, Computer Science Department, UK

2013 - 2014 **F.R.S.-FNRS Research Collaborator**
Université catholique de Louvain, Crypto Group, Belgium

2009 - 2013 **F.R.S.-FNRS Postdoctoral Researcher**
Université catholique de Louvain, Crypto Group, Belgium

2005 - 2009 **F.R.S.-FNRS Research Fellow**
Université catholique de Louvain, Crypto Group, Belgium

Academic education

2005 - 2009 **PhD in Engineering Science**
Université catholique de Louvain, Crypto Group
PhD advisor: Jean-Jacques Quisquater
On graph-based cryptographic hash functions

2000 - 2005 **Ingénieur civil en Mathématiques Appliquées**
Université catholique de Louvain
La plus grande distinction
Master thesis advisor: Michel Verleysen
Anticipation des crises d'épilepsie par analyse dynamique des signaux électroencéphalographiques.

2003 - 2004 **Erasmus student**
Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística, Barcelona, Spain

Main research outcomes

- Found evidence that binary ECDLP can be solved in subexponential time.
- Provided a constructive version of Deuring's correspondence.
- Invented a new algorithm for finding roots of polynomials over $GF(p^n)$.
- Totally broke two group theory-based hash functions from CRYPTO'94 and Journal of Cryptology.
- Independent, long-term research on cryptographic assumptions and cryptanalysis since the beginning of my PhD.
- Collaborative research on cryptographic protocols and physical security.
- Author of 6 international peer-reviewed journal articles, 12 international peer-reviewed conference articles, 1 PhD thesis, 1 book chapter, 1 local conference paper, and 9 additional preprints.
- 243 citations since 2008; H-index 8 (source: Google Scholar 01/20/2014).
- Invited speaker at 11 international conferences or workshops and in 26 research centers.

Teaching and supervision experience

- Designing a new course at University College London: Cryptanalysis.
- Lecturer at University College London since 2013: Introduction to Cryptography.
- Teaching collaboration with University of Kinshasa. Yearly course on Cryptography and Information Security since 2012, supported by the International Mathematical Union.
- Lecturer at Université catholique de Louvain since 2011. Part of a Number Theory course dedicated to elliptic curves.
- Teaching assistant in Cryptography, Number Theory, Linear Algebra, Real and Complex Analysis at Université catholique de Louvain (2005-2013).
- Main PhD supervisor of one PhD thesis at AIMS-Senegal; examinator for one PhD thesis at University College London; mentoring of 4 PhD students at University College London and Kyushu University.
- Supervisor of 10 master theses and 3 research trainees at Université catholique de Louvain.

International research experience

- University College London, London, UK. Visit to Jens Groth (Oct 2013 - Sep 2014) .
- University of Oxford, Oxford, UK. Visit to Alan Lauder (Oct 2013 - Sep 2014) .
- Microsoft Research and University of California, San Diego, USA. Three visits to Kristin Lauter (Feb-May 2008, Feb-May 2010, Sep-Dec 2011, total 9 months).
- Université Pierre et Marie Curie, France. Two visits to Jean-Charles Faugère (Jan-Feb 2011, Jul-Aug 2011, total 4 months).
- Ecole polytechnique, France. One visit to Daniel Augot (Feb-Apr 2012, 3 months).
- Kyushu University, Japan. Two *invited* visits to Tsuyoshi Takagi (Feb-Mar 2013, Sep-Oct 2013, total 2 months).
- Université de Bordeaux, France. One *invited* visit to Gilles Zémor (Dec 2010).
- Florida Atlantic University, USA. One visit to Spyros Magliveras (Oct 2010).
- Université catholique de Louvain, Belgium. FRS-FNRS fellowships (2005-2014).

Competitive research grants

2013 - 2014	F.R.S.-FNRS research collaborator
2009 - 2013	F.R.S.-FNRS postdoctoral research fellow
2005 - 2009	F.R.S.-FNRS research fellow

Distinctions and awards

2005	CLUSTER Award.
2000 - 2002	Selection in the Belgian team for Euromath contest in 2000 (second) and 2002.
1997 - 2000	*Olympiade Mathématique Belge* : second prize in 2000, fourth price in 1997 and 1999, finalist in 1998. *Olympiade de Physique Belge* : finalist in 1999 and 2000. American International Mathematical Examination : ranked second for Belgium in 2000.
2000	Novel contest *Victor*, organized by *le Soir* in 2000 : second price.

Community services

- Running UCL Crypto Group seminars and of a research paper database at Université catholique de Louvain until 2014.
- Program committee member for the 2014 ACNS conference.
- Reviewer for the Designs, Codes and Cryptography journal, the Discrete Mathematics and Theoretical Computer Science journal, the transactions of IEICE, the Journal of Algebra and its Applications, the IET Information Security, the ANZIAM Journal and the Journal of Mathematical Cryptology.
- Reviewer for the Mathematical reviews/Mathscinet.
- Reviewer for the following conferences: CRYPTO 2008, CHES 2009, CECC 2009, Africacrypt 2010, CHES 2010, Asiacrypt 2010, ACNS 2010, CT-RSA 2011, CRYPTO 2011, ACNS 2012, ANTS 2012, CANS 2012, CRYPTO 2012, PKC 2013, FSE 2013, Asiacrypt 2013, Africacrypt 2014, ANTS 2014, PKC 2014, Eurocrypt 2014, CRYPTO 2014, ANTS XI (2014), Indocrypt 2014, Inscrypt 2014, Eurocrypt 2015, CT-RSA 2015.
- Session chair at the 13th Information Security Conference in Boca Raton, Florida.

References

Kristin Lauter, Principal Researcher at Microsoft Research, Redmond.
Olivier Pereira, Professor at Université catholique de Louvain.
Gilles Zémor, Professor at Institut de Mathématiques de Bordeaux.
Jean-Jacques Quisquater, Professor at Université catholique de Louvain.
Further references are available on request.

Languages

Mother language: **French**.
Fluent in **English** (USA) and **Spanish** (Spain).
Intermediary level in **Catalan**, **Dutch** (Belgium) and **Italian**.

Computer skills

General programming languages	C, C++, Java (basic knowledge).
Computing languages	Matlab (good knowledge).
Formal computing languages	Magma, Sage, Maple, Pari (good to advanced knowledge).
Office tools	LaTeX, Microsoft Word, Excell, PowerPoint.

Further training and education

2014	UCL Computer Science workshop on writing EPSRC grants.
2012	Entrepreneurship training "*From Research to Business*".
2010	Belgian cooperation agency information cycle.
2007	Participation to "*Start academy*" entrepreneurship contest.
2006	European First Aid training.
2006	Non-violent communication and conflict management.
2005	BEST summer course "*From Pythagoras to Wiles: Mathematics without the comma*". Uppsala, Sweden.
2003	Athens course "*Cryptographic Mechanisms for Security and Privacy in a Digital World*", *Teknische Universiteit van Delft*, Delft, Holland.
2000	European driving licence.

Social commitment and miscellaneous

2009 - now	Volunteer for the ASBL *Famisol*.
2003 - now	Foundation of the scout group of La Roche-en-Ardenne. Activity leader for the 8-12 year section from 2003 to 2006. Collaborator at the coordination staff from 2008.
2007	Creation of a social game "*SOS, Camp en Détresse!*" part of the final selection for the *Concours créateurs du Festival Ludique International de Parthenay.*
2004 - 2007	Co-responsability in the *kot-à-projet* Granzenfants (help to mentally disabled adults), 2004-2005 and 2006-2007.
2003	Participation at the ESA contest "*6th Parabolic Flight Campaign*".
1990 - 2000	Ten years practice of swimming and lifesaving, three Belgian records in *Cadet* and *Junior* categories.

Publication list

PhD thesis

1. *On graph-based cryptographic hash functions.* Christophe Petit. PhD thesis, Université catholique de Louvain (2009).

International peer-reviewed journals

2. *Degree of regularity of systems arising from a Weil descent.* Timothy Hodges, Christophe Petit and Jacob Schlather. Finite Fields and their Applications, Volume 30, November 2014, pp 155-177.
3. *Finding roots in $GF(p^n)$ with the successive resultants algorithm.* Christophe Petit. LMS Journal of Computation and Mathematics, Volume 17, Issue A, 2014, pp 203-217. Special issue for ANTS conference.
4. *On the quaternion ℓ-isogeny problem.* David Kohel, Kristin Lauter, Christophe Petit, Jean-Pierre Tignol. LMS Journal of Computation and Mathematics, Volume 17, Issue A, 2014, pp 418-432. Special issue for ANTS conference.
5. *On a particular case of the bisymetric equation for quasigroups.* Christophe Petit, Mathieu Renault, François-Xavier Standaert. Acta Mathematica Hungarica, Volume 143, Issue 2, July 2014, pp 330-336.
6. *Towards factoring in $SL(2, \mathbb{F}_{2^n})$.* Christophe Petit. Designs, codes and Cryptography, Volume 71, Issue 3, June 2014, pp 409-431.
7. *Rubik's for cryptographers.* Christophe Petit and Jean-Jacques Quisquater. Notices of the American Mathematical Society, June-July 2013 (60), pp 733-739. Chinese translation in Mathematical Advances in Translation, Volume 33, April 2014, Number 1, pp 5-13.

International peer-reviewed conference proceedings

8. *Improvement of Faugère et al.'s method to solve ECDLP.* Huang Yun-Ju, Christophe Petit, Naoyuki Shinohara, and Tsuyoshi Takagi. IWSEC2013 - the 8th International Workshop on Security, LNCS8231, pp 115-132.
9. *On polynomial systems arising from a Weil descent.* Christophe Petit and Jean-Jacques Quisquater. Asiacrypt 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, LNCS 7658, pp 451-466.
10. *Improving the complexity of index calculus algorithms in elliptic curves over binary fields.* Jean-Charles Faugère, Ludovic Perret, Christophe Petit, Guénaël Renault. Eurocrypt 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 7237, pp 27-44.
11. *Masking with Randomized Look Up Tables (Towards Preventing Side-Channel Attacks of All).* François-Xavier Standaert, Christophe Petit, Nicolas Veyrat-Charvillon. Cryptography and Security 2012, LNCS 6805, pp 283-299.
12. *Fresh Re-Keying II: Securing Multiple Parties against Side-Channel and Fault Attacks.* Marcel Medwed, Christophe Petit, Francesco Regazzoni, Mathieu Renauld, and François-Xavier Standaert. CARDIS 2011 - 10th Smart Card Research and Advanced Application Conference, LNCS7079, pp 115-132.

13. *One-time trapdoor one-way functions.* Julien Cathalo and Christophe Petit. Information security conference (ISC) 2010, LNCS6531, pp 182-195.
14. *Preimages for the Tillich-Zémor hash function.* Christophe Petit and Jean-Jacques Quisquater. Selected areas in cryptography (SAC) 2010, LNCS6544, pp282-301.
15. *Hard and Easy Components of Collision Search for the Zémor-Tillich Hash Function : new Attacks and reduced variants with equivalent security.* Christophe Petit, Jean-Jacques Quisquater, Jean-Pierre Tillich and Gilles Zémor. The Cryptographers' Track at the RSA Conference (CT-RSA) 2009, LNCS 5473, pp 182-194.
16. *Full Cryptanalysis of LPS and Morgenstern Hash Functions.* Christophe Petit, Kristin Lauter and Jean-Jacques Quisquater. Security and Cryptography for Networks (SCN) 2008, LNCS 5229, pp263-277.
17. *Efficiency and Pseudo-randomness of a Variant of Zémor-Tillich Hash Function.* Christophe Petit, Nicolas Veyrat-Charvillon and Jean-Jacques Quisquater. IEEE International Conference on Electronics, Circuits, and Systems (ICECS2008), pp 906-909.
18. *Fault Attacks on Public Key Elements: Application to DLP based Schemes.* Chong Hee Kim, Philippe Bulens, Christophe Petit and Jean-Jacques Quisquater. Public Key Infrastructure (Euro-PKI) 2008, LNCS 5057, pp 182-195.
19. *A Block Cipher based Pseudo Random Number Generator Secure Against Side-Channel Key Recovery.* Christophe Petit, François-Xavier Standaert, Olivier Pereira, Tal G. Malkin and Moti Yung. ACM Symposium on Information, Computer and Communications Security, (ASIACCS) 2008, pp 56-65.

Book chapter

20. *Cayley hash functions.* Christophe Petit, and Jean-Jacques Quisquater. Entry in the Encyclopedia of cryptography and security - 2nd edition.

Peer-reviewed local conference with proceedings

21. *Equitable Cake Cutting without Mediator.* Sophie Mawet, Olivier Pereira and Christophe Petit. IT Benelux 2010 - 5th Benelux Workshop on Information and System Security.

Preprints

22. *Traveling in supersingular elliptic curves isogeny graphs* Christophe Petit, Kristin Lauter.
23. *Application of the affine geometry of $GF(q^n)$ to root finding* Luca De Feo, Christophe Petit, and Michael Quisquater.
24. *On Generalized First Fall Degree Assumptions* Huang Yun-Ju, Christophe Petit, and Tsuyoshi Takagi.
25. *Short Accountable Ring Signatures from the DDH Assumption* Andrea Cerulli, Pyrros Chaidos, Jens Groth, Christophe Petit.
26. *Bounding HFE with SRA* Christophe Petit.

27. *Cryptographic Hash Functions and Expander Graphs: The End of the Story ?* Christophe Petit and Jean-Jacques Quisquater.
28. *New subexponential algorithms for factoring in $SL(2, 2^n)$* Jean-Charles Faugère, Ludovic Perret, Christophe Petit, Guénaël Renault.
29. *ZesT : an all-purpose hash function based on Zémor-Tillich* Christophe Petit, Giacomo de Meulenaer, Jean-Jacques Quisquater, Jean-Pierre Tillich, Nicolas Veyrat-Charvillon and Gilles Zémor
30. *Hardware Implementations of a Variant of the Zémor-Tillich Hash Function* Giacomo de Meulenaer, Christophe Petit and Jean-Jacques Quisquater

An updated list of publications can be found on my personal webpage:
`http://www0.cs.ucl.ac.uk/staff/C.Petit/`.

Invited talks and conference presentations

Invited talks at conferences and workshops

1. *Bounding HFE with SRA.*
DIMACS Workshop on the Mathematics of Post-Quantum Cryptography, South Plainfield, USA, January 2015.
2. *On the complexity of index calculus algorithms for ECDLP over composite fields.*
CryptoForma Workshop, London, UK, September 2014.
3. *The successive resultants algorithm and its connection to binary ECDLP*
DLP 2014 Conference, Ascona, Switzerland, May 2014.
4. *Rubik's for cryptographers*
Workshop on algebraic constructions for the foundations of a safe society, Fukuoka, Japan, August 2013.
5. *On polynomial systems arising from a Weil descent*
Workshop on solving multivariate polynomial systems and related topics, Fukuoka, Japan, March 2013.
6. *Complexity of index calculus algorithms for ECDLP over composite fields*
Elliptic Curve Cryptography Conference, Queretaro, Mexico, October 2012.
7. *On polynomial systems arising from a Weil descent*
CCA workshop, Institut Henri Pointcarré, Paris, April 2012.
8. *Computing paths in large Cayley graphs and cryptanalytic applications*
IWONT workshop, Brussels, July 2011.
9. *Hash functions and Cayley graphs: The end of the story ?*
Workshop on Computer Security and Cryptography, IRM, Montréal, April 2010.
10. *Hash functions and Cayley graphs: The end of the story ?*
ECRYPT II SHA-3 workshop, Tenerife, November 2009.
11. *Cryptographic hash functions from expander graphs.*
ECRYPT hash workshop, Leiden, June 2008.

Invited talks in other research groups

1. *On the complexity of index calculus algorithms for ECDLP over composite fields.*
University of Kent, March 2015.
2. *On the quaternion ℓ-isogeny problem.*
Uniervsité de Versailles-Saint-Quentin, November 2014.
3. *On the complexity of index calculus algorithms for ECDLP over composite fields.*
University College London, September 2014.
4. *Factorization problem in non-Abelian groups.*
Beijing University of Posts and Telecommunications, Beijing, China, August 2014.
5. *On the complexity of index calculus algorithms for ECDLP over composite fields.*
Shanghai Jiao Tong University, Shanghai, China, August 2014.

6. *On the complexity of index calculus algorithms for ECDLP over composite fields.*
   Oxford University, Oxford, UK, March 2014.
7. *On polynomial systems arising from a Weil descent*
   Center for Cryptology and Information Security (CCIS), Florida Atlantic University, Boca Raton, March 2013.
8. *On polynomial systems arising from a Weil descent*
   Institute of Mathematics for Industry, Kyushu University, February 2013, Fukuoka, Japan.
9. *On polynomial systems arising from a Weil descent*
   Ecole Normale Supérieure, Paris, France, February 2013.
10. *On polynomial systems arising from a Weil descent*
    Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, December 2012.
11. *On polynomial systems arising from a Weil descent*
    State Key Lab of Information Security, Chinese Academy of Science, Beijing, China, December 2012.
12. *From Rubik's to cryptography: a tour of mathematical challenges in the field*
    Control and systems seminars, ULG, Liège, Belgium, November 2012.
13. *On polynomial systems arising from a Weil descent*
    INRIA-LORIA research center, Nancy, November 2012.
14. *On polynomial systems arising from a Weil descent*
    Qualsec seminars, Brussels, October 2012.
15. *On polynomial systems arising from a Weil descent*
    Universitat Politècnica de Catalunya, Barcelona, Spain, May 2012.
16. *On polynomial systems arising from a Weil descent*
    Institut de Mathématiques de Luminy, Marseille, France, April 2012.
17. *On polynomial systems arising from a Weil descent*
    Ecole Polytechnique, Paris, France, March 2012.
18. *Rubik's for cryptographers: Towards factoring in* $SL(2,\mathbb{F}_{2^n})$
    Qualcomm Research, San Diego, USA, November 2011.
19. *Rubik's for cryptographers: Towards factoring in* $SL(2,\mathbb{F}_{2^n})$
    University of California, San Diego, USA, October 2011.
20. *Short factorizations in finite matrix groups and cryptographic hash functions*
    UCL Algebra seminars, Louvain-la-Neuve, Belgium, April 2011.
21. *Hash functions and Cayley graphs: The end of the story ?*
    Université Pierre et Marie Curie, Paris, France, November 2010.
22. *Hash functions and Cayley graphs: The end of the story ?*
    Center for Cryptology and Information Security (CCIS), Florida Atlantic University, Boca Raton, USA, November 2010.
23. *Hash functions and Cayley graphs: The end of the story ?*
    Microsoft Research, Seattle, USA, March 2010.
24. *Hash functions and Cayley graphs: The end of the story ?*
    Institut de Mathématiques de Bordeaux I, Bordeaux, France, December 2009.
25. *Cryptographic Hash Functions from Expander Graphs.*
    Large graph group, UCL, Louvain-la-Neuve, Belgium, February 2009.

26. *Security in a grey-box model.*
Microsoft Research, Seattle, USA, July 2007.

Paper presentations at international conferences

1. *On the quaternion ℓ-isogeny problem.* Algorithmic Number Theory Symposium (ANTS), GyeongJu, South Korea, August 2014.
2. *Finding roots in $GF(p^n)$ with the successive resultants algorithm.* Algorithmic Number Theory Symposium (ANTS), GyeongJu, South Korea, August 2014.
3. *On polynomial systems arising from a Weil descent*
Asiacrypt, Beijing, December 2012.
4. *One-time trapdoor one-way functions.*
Information security conference, Boca Raton, October 2010.
5. *Preimage algorithms for the Tillich-Zémor hash function.*
Selected areas in cryptography, Waterloo, August 2010.
6. *Hard and Easy Components of Collision Search for the Zémor-Tillich Hash Function: new Attacks and reduced variants with equivalent security.*
The Cryptographers' Track at the RSA Conference, San Francisco, April 2009.
7. *Full Cryptanalysis of LPS and Morgenstern Hash Functions.*
Conference on Security and Cryptography for Networks, Amalfi, September 2008.
8. *Fault Attacks on Public Key Elements: Application to DLP based Schemes.*
Public Key Infrastructure, Trondheim, June 2008
9. *A Block Cipher based Pseudo Random Number Generator Secure Against Side-Channel Key Recovery.*
ACM Symposium on Information, Computer and Communications Security, Tokyo, March 2008.