6 rue Waldeck-Rousseau
87000 Limoges (France)
+33 6.46.18.71.80
olivier@blazy.eu
http://www.blazy.eu
Born 20/03/1986 (Décines, France)

Olivier Blazy

Work Experiences

2014–* **Maître de Conférence (∼ Tenured Associate Professor)**, *University of Limoges*, Master level teaching in various areas of Security and Cryptography (Public Key, Private Key, Network Security and Administration, . . .).
- Young Researcher National Grant (ANR JCJC IDFIX): 2016 → 2020
- Internship Coordinator: Contact with our various partners to ensure each student finds a befitting long term internship
- Seminar Organizer: Organization of bi-monthly seminars with external researchers

April 2015 **Research Visitor (1 month)**, *Symphony*, Palo Alto (United States).
R&D Visit in the growing Secure Messaging Startup. Contact: David M'Raihi

2014-* **Program Commitees**, In charge of the selection of papers for various conferences.
Provsec, SCN, ISICS, IWSEC

2012–2014 **Postdoctoral Position**, *Ruhr-University Bochum*, with Eike Kiltz in the Foundation of Cryptography workgroup, Horst Görtz Institute for IT-Security.
Zero-Knowledge Proofs, Semi-Functional spaces, Tight Signatures

PhD

Title *Interactive and Non-Interactive Proofs of Knowledge*

Defense September 27th, 2012, with highest honor

Committee

Advisor	David Pointcheval	(CNRS, École Normale Supérieure)
Rapporteurs	Jean-Sébastien Coron	(University of Luxembourg)
	Marc Fischlin	(University of Darmstadt)
	Fabien Laguillaumie	(CNRS, LIP)
Examiners	Michel Abdalla	(CNRS, École Normale Supérieure)
	Antoine Joux	(DGA, University of Versailles)
	Eike Kiltz	(Ruhr-University, Bochum)
	Damien Vergnaud	(École Normale Supérieure)

Manuscript *http://www.blazy.eu/documents/these.pdf*

Education

2008–2012 **PhD in Computer Science**, *University Paris 7*, supervised by David Pointcheval (ENS, CNRS), Pairing-based cryptographic protocols and proofs of knowledge.

2005–2009 **Predoctoral Studies in Computer Science**, *ENS*, Paris.

2006-2009 **Research Master in Computer Science**, *MPRI, ENS*.

2007 **Master Internship (6 months)**, *VeriSign*, Mountain View (United States).
- Integration in the small swat team that is dedicated to explore new strategy and product concepts without disrupting VeriSign's existing businesses and committed execution. Supervised by David M'Raihi.
- The main purpose of this internship was to create and implement an efficient recommendation engine deployed on a variety of platforms, with live data updates.
- Topics: OpenID, Recommendation Engine, PKA, Ruby, Java, JDBC.

2005-2006 **Bachelor in Computer Science**, *Paris VII, ENS*.

2006 **Bachelor Internship (2 months)**, *Catholic University of Louvain-la-Neuve*, Belgium.
- *Automatic Analysis of cryptographic protocols based on modular exponentiation* Advisor Olivier Pereira.
- Topics: GDH Protocols, PKA, . . .

2003–2005 **Classes préparatoires MPSI, MP* (Aux Lazaristes)**, Lyon, France.

July 2005 **Admission to the École Normale Supérieure**, *National Rank 9th*.

Various

Computer	PHP/SQL, OCaML, Ruby on Rail, C, Java (JDBC), LaTeX, VBS
Languages	Fluent: French, English (TOEIC 985, OPC C2+)
	Notions: German (B2), Italian, Russian

Recent Presentations

Jun 2015 **Generic Construction of UC-Secure Oblivious Transfer**, *ACNS*, New York (United States).

Mar 2015 **Non-Interactive Zero-Knowledge Proofs of Non-Membership**, *CT-RSA*, San Francisco (United States).

Aug 2014 **(Hierarchical) Identity-Based Encryption from Affine Message Authentication**, *Crypto*, Santa Barbara (United States).

Feb 2014 **Blind Signatures with Flying Colors**, *Symposium on Numeric Trust*, Clermont-Ferrand (France).

Other Activities

2016–* Scientific Member of Maths en Jean (Mathematics vulgarization)

2007–2009 Student Directory team member

2006–2011 President of the ENS Games Club

2006–2008 Co-Webmaster for the AV-Club

2005–* Part of the ENS tutors, wintutors, moderators

Chosen Publications

[ABB+13] Michel Abdalla, Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, and David Pointcheval. SPHF-Friendly Non-Interactive Commitment Schemes. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - Proceedings of ASIACRYPT '13*, volume 8269 of *Lecture Notes in Computer Science*, pages 214–234, Bangalore, India, December 2013. Springer.

[BBC+13] Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud. New Techniques for SPHFs and Efficient One-Round PAKE Protocols. In Ran Canetti and Juan Garay, editors, *Advances in Cryptology - Proceedings of CRYPTO '13*, volume 8042 of *Lecture Notes in Computer Science*, pages 449–475, Santa Barbara, California, August 2013. Springer.

[BFPV13] Olivier Blazy, Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Short Blind Signatures. *Journal of Computer Security*, 21(5):627–661, November 2013.

[BKP14] Olivier Blazy, Eike Kiltz, and Jiaxin Pan. (Hierarchical) Identity-Based Encryption from Affine Message Authentication. In Ran Canetti and Juan Garay, editors, *Advances in Cryptology - Proceedings of CRYPTO '14*, volume 8616 of *Lecture Notes in Computer Science*, pages 408–426, Santa Barbara, California, August 2014. Springer.

[BPV12] Olivier Blazy, David Pointcheval, and Damien Vergnaud. Round-Optimal Privacy-Preserving Protocols with Smooth Projective Hash Functions. In Ronald Cramer, editor, *9th Theory of Cryptography Conference (TCC '12)*, volume 7194 of *Lecture Notes in Computer Science*, pages 94–111, Taormina, Italy, March 2012. Springer.

- Full list on: `http://blazy.eu/research.php`