Olivier Blazy

Né le 20 mars 1986, à Décines Charpieu (Rhône)

Études

2012–* **Post-doctorat**, *à l'Université de Bochum*, sous la direction d'Eike Kiltz dans l'équipe Fondements de la Cryptographie au sein du département de mathématiques (RUB/HGI).
Travail sur les preuves à divulgations nulles de connaissance, les espaces semi-fonctionnels.

2008–2012 **Doctorat de l'Université Paris 7 spécialité Informatique**, sous la direction de David Pointcheval au sein de l'équipe Cryptographie de l'ENS (ENS / CNRS / INRIA).
Travail sur les protocoles à base de couplages et les Preuves de connaissance

2005–2009 **Prédoctorats d'Informatique (ENS)**, Paris.
- 2006-2009 **Master de Recherche en Informatique**, *MPRI / ENS.*
- 2005-2006 **Licence d'Informatique**, *Paris VII / ENS.*

2003–2005 **Classes préparatoires MPSI, MP* (Aux Lazaristes)**, Lyon.
- Juillet 2005 **Concours de l'Ecole Normale Supérieure**, *9ème.*

Thèse

Titre *Preuves de connaissance interactives et non-interactives*

Soutenance 27 septembre 2012, mention Très Honorable

Jury

Directeur	David Pointcheval	(CNRS, École Normale Supérieure)
Rapporteurs	Jean-Sébastien Coron	(Université du Luxembourg)
	Marc Fischlin	(Université de Darmstadt)
	Fabien Laguillaumie	(CNRS, LIP)
Examinateurs	Michel Abdalla	(CNRS, École Normale Supérieure)
	Antoine Joux	(DGA, Université de Versailles)
	Eike Kiltz	(Université de la Ruhr, Bochum)
	Damien Vergnaud	(École Normale Supérieure)

Manuscrit *http://www.blazy.eu/qualifications/these.pdf*

Expériences

2009–2011 **Monitorat**, *Université Paris Diderot (Paris VII)*, Paris.
- 2009–2011 TP d'Informatique Fondamentale en L1 : *Algorithmique, Programmation en Java.*
- 2010-2011 TD d'Éléments d'Algorithmique en L2 : *Algorithmique, Complexité, bases de Combinatoire.*

2008–2009 **Stage de Master**, *Équipe Crypto de l'ENS*, Paris.
- *Historique sur le traitor tracing* sous la direction de David Pointcheval.
- Thèmes: Recherche de traîtres, Couplage, Diffusion Chiffrée.

2005–2007 **Colleur**, *Aux Lazaristes*, Lyon, Interrogations Orales en MPSI, MP, MP*.

2007 **Stage de M1, 6 mois**, *Division Innovation de VeriSign*, Mountain View (Californie / USA).
- Intégration dans l'équipe d'intervention qui explore les nouvelles stratégies et concepts sans mettre en péril les services déjà fournis par VeriSign. Stage sous la direction de David M'Raihi.
- Le but principal de ce stage était de créer puis implémenter un moteur de recommandation pouvant être déployé sur de nombreux supports et gérant des mises à jour de donnés à la volée.
- Ce fut aussi l'occasion d'un contact avec le monde industriel et ses contraintes (Prototypes, NDA, ...)
- Thèmes : OpenID, Moteur de Recommandation, PKA, Ruby, Java, JDBC .

2006 **Stage de L3, 2 mois**, *Université Catholique de Louvain-la-Neuve (UCL)*, (Belgique).
- *Analyse automatique de procoles basés sur les exponentiations modulaires* sous la direction d'Olivier Pereira.
- Thèmes : Protocoles GDH, PKA, ...

2000–2004 **Beta-Tester**, *XoopS*, Web.
- Thèmes : CMS, PHP/MySQL, Sécurité Web, Travail en équipe en ligne.

Josephstrasse 3. – 44791 Bochum (Allemagne)
+33 6.46.18.71.80 • olivier.blazy@rub.de • http://www.blazy.eu

Autres Activités

2007–2009 Membre de l'équipe de l'annuaire des élèves

2006–2011 Président du Club Jeux de l'ENS

2006-2008 Co-Webmaster du Ciné-Club

2005–* Membre des Tuteurs / Wintuteurs / Modérateurs de l'ENS (Aide informatique multi-plateformes)

Divers

Informatique PHP/SQL, OCaML, Ruby on Rail, C, Java (JDBC), LaTeX, VBS

Langues Courant : Français, Anglais (TOEIC 985/990, OPC C2+)

Notions : Allemand (B1), Italien, Russe

Quelques Présentations

Déc 2012 **Signatures on Randomizable Ciphertext, some Probabilities for the Greater Good**, *Séminaire CITS*, Bochum (Allemagne).

Oct 2012 **Implicit proof of knowledge**, *Séminaire HGI*, Bochum (Allemagne).

Sept 2012 **Compact Round-Optimal Partially-Blind Signatures**, *SCN'12*, Amalfi (Italie).

Mars 2012 **Round-Optimal Privacy-Preserving Protocols with Smooth Projective Hash Functions**, *TCC'12*, Taormina (Italie).

Mars 2011 **Signatures on Randomizable Ciphertexts**, *PKC'11*, Taormina (Italie).

Sept 2010 **Randomizable signature on encrypted messages**, *ECrypt II Summer School*, Mikonos (Grêce).

Juin 2010 **Batch Groth Sahai**, *ACNS'10*, Beijing (Chine).

Jan 2010 **A Traceable Signature Scheme (reworked)**, *GREYC Crypto Seminar*, Caen (France).

Publications

[BCF+11] Olivier Blazy, Sébastien Canard, Georg Fuchsbauer, Aline Gouget, Hervé Sibert, and Jacques Traoré. Achieving optimal anonymity in transferable e-cash with a judge. In Abderrahmane Nitaj and David Pointcheval, editors, *AFRICACRYPT 11: 4th International Conference on Cryptology in Africa*, volume 6737 of *Lecture Notes in Computer Science*, pages 206–223. Springer, July 2011.

[BBCPV12] Fabrice Ben Hamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud. Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages. To appear in Kaoru Kurosawa edito, in International Workshop on Theory and Practice in Public Key Cryptography (PKC '13), in Lecture Notes in Computer Science, March 2013.

[BFI+10] Olivier Blazy, Georg Fuchsbauer, Malika Izabachène, Amandine Jambert, Hervé Sibert, and Damien Vergnaud. Batch Groth-Sahai. In Jianying Zhou and Moti Yung, editors, *ACNS 10: 8th International Conference on Applied Cryptography and Network Security*, volume 6123 of *Lecture Notes in Computer Science*, pages 218–235. Springer, June 2010.

[BFPV11] Olivier Blazy, Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Signatures on randomizable ciphertexts. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011: 14th International Workshop on Theory and Practice in Public Key Cryptography*, volume 6571 of *Lecture Notes in Computer Science*, pages 403–422. Springer, March 2011.

[BP12] Olivier Blazy and David Pointcheval. Traceable signature with stepping capabilities. In David Naccache, editor, *Quisquater Festschrift*, Lecture Notes in Computer Science. Springer, 2012.

[BPV12a] Olivier Blazy, David Pointcheval, and Damien Vergnaud. Round-optimal privacy-preserving protocols with smooth projective hash functions. In Ronald Cramer, editor, *Proceedings of TCC 2012*, Lecture Notes in Computer Science. Springer, 2012.

[BPV12b] Olivier Blazy, David Pointcheval, and Damien Vergnaud. Compact Round-Optimal Partially-Blind Signatures. In Roberto De Prisco and Ivan Visconti, editors, *The 8th Conference on Security in Communication Networks (SCN '12)*, volume 7485 of *Lecture Notes in Computer Science*, pages 95–113, Amalfi, Italy, 2012. Springer.