Nicolas ESTIBALS

LORIA — Équipe CARAMEL
Campus Scientifique, BP 239
54506 Vandœuvre-lès-Nancy Cedex FRANCE

Téléphone : +33(0)3 83 59 30 14
Adresse électronique : Nicolas.Estibals@loria.fr
Site web : http://www.loria.fr/~nestibal/

Né le 18 mars 1985 à Paris 17e.
Nationalité : Française.

Poste actuel

Étudiant en doctorat d'informatique avec un contrat doctoral à l'Université de Lorraine et une charge d'enseignement à l'ÉSIAL. Ma thèse est encadrée par Jérémie DETREY et Pierrick GAUDRY. Mon domaine de recherche concerne la **cryptographie** reposant sur les **courbes algébriques** et l'**arithmétique des ordinateurs** : j'étudie la conception d'**opérateurs matériels** pour la cryptographie à base de **couplages**.

Formations et diplômes

2009-____ Préparation d'un doctorat d'informatique dans l'équipe CARAMEL au LORIA, Nancy.

2007-2009 **Master d'Informatique Fondamentale** à l'ÉNS Lyon.
Mention très bien, classé 3ème sur 14.
Liste des cours suivis : Algorithmes arithmétiques, Algorithmes pour les réseaux et les télécommunications, Algorithmique des systèmes virgule flottante, Algorithmique parallèle, Arithmétique des corps finis, Compilation, Complexité de Kolmogorov, Complexité de Turing, Grilles, Images, Optimisations en compilation, Parallélisation automatique, Preuves, Probabilités en algorithmique, Sémantique du parallélisme, Systèmes distribués, Théorie de la démonstration.

2006-2007 **Licence d'Informatique Fondamentale** à l'ÉNS Lyon.
Mention assez bien.

2003-2006 **CPGE** : MPSI et MP* au Lycée Condorcet, Paris IX.

Séjours de recherche

2009 **Invitation** au CINVESTAV del IPN (Mexique) par Francisco RODRÍGUEZ-HENRÍQUEZ pour un séjour de 3 semaines.

2009 **Stage de Master 2** au LORIA, Nancy.
Génération automatique de circuits pour le calcul de l'exponentiation finale du couplage de Tate, sous la direction de Jérémie DETREY au sein de l'équipe CACAO.

2008 **Stage de Master 1** au LCIS, Université de Tsukuba, Japon.
Parallel multipliers over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{3^m}$ amenable for pairing computation, sous la direction de Jean-Luc BEUCHAT.

2007 **Stage de Licence**, IRISA, Rennes.
Génération de code GPU pour un langage intermédiaire data parallel, sous la direction de François BODIN dans l'équipe CAPS.

Publications et exposés [1]

Article de journal

[1] Jean-Luc Beuchat, Jérémie Detrey, Nicolas Estibals, Eiji Okamoto et Francisco Rodríguez-Henríquez. "Fast architectures for the η_T pairing over small-characteristic supersingular elliptic curves". Dans : *IEEE Transactions on Computers* 60.2 (fév. 2011), p. 266–281. doi : 10.1109/TC.2010.163. Extended version of the CHES 2009 article.

Conférences internationales avec actes

[2] Razvan Barbulescu, Jérémie Detrey, Nicolas Estibals et Paul Zimmermann. "Finding optimal formulae for bilinear map". Dans : *International Workshop on the Arithmetic of Finite Fields – WAIFI 2012*. Éd. : F. Özbudak et F. Rodríguez-Henríquez. Vol. 7369. Lecture Notes in Computer Science. Springer, juil. 2012, p. 168–186

[3] Diego F. Aranha, Jean-Luc Beuchat, Jérémie Detrey et Nicolas Estibals. "Optimal Eta pairing on supersingular genus-2 binary hyperelliptic curves". Dans : *Topics in Cryptology – CT-RSA 2012*. Éd. : O. Dunkelman. Vol. 7178. Lecture Notes in Computer Science. Springer, fév. 2012, p. 99–115. doi : 10.1007/978-3-642-27954-6_7

[4] Nicolas Estibals. "Compact hardware for computing the Tate pairing over 128-bit-security supersingular curves". Dans : *Pairing 2010 – 4th International Conference on Pairing-Based Cryptography*. Éd. : M. Joye, A. Miyaji et A. Otsuka. Vol. 6487. Lecture Notes in Computer Science. Springer, déc. 2010, p. 397–416. doi : 10.1007/978-3-642-17455-1_25

[5] Jean-Luc Beuchat, Jérémie Detrey, Nicolas Estibals, Eiji Okamoto et Francisco Rodríguez-Henríquez. "Hardware accelerator for the Tate pairing in characteristic three based on Karatsuba-Ofman multipliers". Dans : *Cryptographic Hardware and Embedded Systems – CHES 2009*. Éd. : C. Clavier et K. Gaj. Vol. 5747. Lecture Notes in Computer Science. Springer, août 2009, p. 225–239. doi : 10.1007/978-3-642-04138-9_17. Best Paper Award.

Séminaires

J'ai fait des présentations aux **journées C2** (Codage et Cryptographie) 2011 et aux **JNCF** (Journées Nationales du Calcul Formel) 2011. J'ai également été invité à donner des séminaires au CINVESTAV (Mexique), dans les équipes de cryptographie des universités de Rennes, Caen et Versailles ainsi que dans l'équipe Arénaire à l'ÉNS Lyon.

Expériences d'enseignement

2009-2012 **Monitorat à l'ÉSIAL** (École d'ingénieur en informatique), Nancy.
Contenu des enseignements :

- 90h de cours-TD de *Mathématiques pour l'Informatique* (algèbre de Boole, théorie des langages, automate, logique) en première année (équivalent L3) avec Francis Alexandre pour référent ;
- 24h de TD de *Mathématiques numériques* (nombres flottants, techniques algorithmiques d'interpolation et d'algèbre linéaire, etc.) en première année avec Bruno Pinçon ;

[1] Les publications sont téléchargeables à l'adresse www.loria.fr/~nestibal/?page=publications.

- 16h de TP-TD de *Spécification des circuits intégrés - VHDL* (spécification et implémentation d'opérateurs matériels) en deuxième année (équivalent M1) avec Alexandre Parodi ;
- 30h de TD de *Principes Fondamentaux des Systèmes Informatiques* (étude complète d'un microcontrôleur : de sa conception à sa programmation) en première année avec Alexandre Parodi ;
- 12h de TD d'*introduction à la cryptographie* en deuxième année avec Jérémie Detrey ;
- 12h de TP de *Programmation Shell* en première année avec Suzanne Collin.

2008-2009 **TP d'informatique en classe préparatoire PT et PTSI**, Lycée La Martinière, Lyon. 4 heures de TP hebdomadaires.

Charges collectives

Relectures pour les conférences **CHES** 2009, 2010, **Reconfig** 2009, **Pairing** 2010, **CANS** 2011, **EuroCrypt** 2011, **SympA** 2011 ainsi que pour les journaux IEEE **Transactions on Computers** et **Transactions on Very Large Scale Integration Systems**.

2012 Participation au comité pour l'évaluation du centre *Security, Reliability and Trust* au sein de l'Université de Luxembourg.

2011-___ Membre élu du conseil de laboratoire au LORIA.
