CURRICULUM VITÆ (23 février 2018)

Nom : THOMÉ
Prénom : Emmanuel
Date et lieu de naissance : 30/08/1976, Rennes (35)
3 enfants (2005, 2007, 2011)
Nationalité : Français
Sexe : M
Adresse électronique : Emmanuel.Thome@inria.fr
Page Web personnelle : http://www.loria.fr/~thome/
Centre de recherche Inria : Nancy
Équipe-projet de recherche : Caramba

1.1 Diplômes

Doctorat(s)
Intitulé : Algorithmes de calcul de logarithmes discrets dans les corps finis.
Date de soutenance : 12/05/2003.
Établissement ayant délivré la thèse : École polytechnique.
Organisme d'accueil (laboratoire, équipe, etc.) pour la préparation de la thèse : Laboratoire LIX, École polytechnique.

Habilitation à diriger des recherches (HDR)
Intitulé : Théorie algorithmique des nombres et applications à la cryptanalyse de primitives cryptographiques.
Date de soutenance : 13/12/2012.
Établissement ayant délivré le diplôme : Université de Lorraine.

Autres diplômes (à partir du niveau Master) :

- Agrégation de mathématiques, 1997 (rang : 30).
- DEA Algorithmique, 1997 (rang : 1).

1.2 Parcours Professionnel

1.2.1 Situation professionnelle actuelle

Statut et fonction : Directeur de recherche (DR2 depuis le 01/10/2015)
Établissement : INRIA Nancy
Date d'entrée en fonction : 01/10/2003

1.2.2 Expériences professionnelles antérieures

Dates début	Dates fin	Établissements	Fonctions et statuts
01/01/2006	01/10/2015	INRIA, Nancy	Chargé de recherches (CR1)
01/10/2003	01/01/2006	INRIA, Nancy	Chargé de recherches (CR2)
01/09/2000	01/09/2003	École polytechnique	Doctorant
01/09/1999	01/07/2000	University of Illinois, Chicago	Visiteur (pré-doc)
01/09/1995	01/07/1999	École normale supérieure, Paris	Élève fonctionnaire

1.3 Prix et distinctions

- Best Paper Award, ACM CCS 2015, pour l'article *Imperfect Forward Secrecy : How Diffie-Hellman Fails in Practice*, correspondant notamment à l'attaque LOGJAM.
- Prime d'encadrement doctoral et de recherche (PEDR) INRIA, 2015-2018.
- Grand prix du chercheur de la Région Lorraine 2014.
- Best Paper Award, Eurocrypt 2014, pour l'algorithme quasi-polynomial de calcul de logarithmes discrets dans les corps finis de petite caractéristique.

- Prix La Recherche, 2012 (P. Gaudry, A. Kruppa, moi-même, et P. Zimmermann), catégorie «Sciences de l'information», pour la factorisation de RSA-768.
- Prime d'excellence scientifique (PES) INRIA, 2011-2014.
- Grid'5000 award, 2010.
- IACR distinguished paper, 2007 (Enge-Gaudry-Thomé, *An $L(1/3)$ discrete logarithm algorithm for low degree curves*).
- Prix de thèse de l'École polytechnique, 2003.

1.4 Invitations à des conférences internationales

J'ai été orateur invité aux conférences internationales ECC 2002, Waifi 2012, ECC 2014, WCC 2015, ECC 2017, ANTS 2018.

1.5 Encadrement de thèses de doctorat

- Romain Cosset (2008-2011). «Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques». Co-encadrement avec Guillaume Hanrot. R. Cosset occupe maintenant un poste en classes préparatoires, ce qui correspond à son souhait initial.
- Hamza Jeljeli (2011-2015). Utilisation d'accélérateurs logiciels et matériels pour l'algèbre linéaire creuse sur les corps finis. H. Jeljeli travaille maintenant pour la société Gemalto.
- Hugo Labrande (2013-2016). Calcul explicite d'isogénies entre variétés abéliennes, cotutelle avec l'université de Calgary (Canada).
- Svyatoslav Covanov (2014-2018). Calculs de complexité minimale pour les opérations bilinéaires.
- Simon Masson (2018-). Algorithmique des courbes destinées aux contextes de la cryptographie bilinéaire et post-quantique. (thèse Cifre).

1.6 Responsabilités collectives

1.6.1 Conférences

Je suis ou j'ai été membre des comités de programme des conférences Eurocrypt 2016, ECC 2015, LatinCrypt 2014, SAC 2014, ECC 2012, ECC 2011, WCC 2011, Journées C2 2007.

J'ai organisé ou co-organisé les conférences ECC 2011, ANTS 2010, JNCF 2008, JNCF 2007, Workshop Cado 2008, RNC7.

Je suis membre du comité de pilotage de la conférence internationale biennale ANTS (Algorithmic Number Theory Symposium).

Au niveau national, je suis membre du comité scientifique des journées nationales de calcul formel, et j'ai été membre du comité de programme des journées du groupe de travail «C2» (Codage et Cryptographie) du GDR IM en 2007 et en 2015.

1.6.2 Jurys de thèse et HDR

Outre les soutenances de mes doctorants, j'ai été membres des jurys de thèse et HDR suivants :

- rapporteur de la thèse de Kisoon Yoon (Université de Caen–Basse-Normandie), septembre 2013.
- rapporteur de la thèse de Bastien Vialla (Université de Montpellier), décembre 2015.
- rapporteur, et président du jury, de l'HDR de Guénaël Renault (Université Paris 6), novembre 2016, président du jury.
- président du jury de thèse de Ludovic Robin (Université de Lorraine), février 2018.

1.6.3 Commisions

J'ai été de septembre 2011 à septembre 2014 membre élu de la Commission d'évaluation de l'INRIA. À ce titre j'ai participé aux instances suivantes :

- commission nationale de suivi des ADT (à compter de 2013).
- groupe de travail «vie des logiciels».
- concours CR (2012, 2013(2), 2014(2)).

J'ai également participé aux concours CR suivants :

- Inria Bordeaux, 2017.
- Inria Nancy, 2018 (président).

J'ai été membre, de janvier 2013 à janvier 2015, du bureau de la «commission de mention informatique», émanation de l'école doctorale lorraine IAEM pour ce qui concerne l'informatique. Cette commission instruit les dossiers de demande d'inscription en thèse et en habilitation, les demandes de coencadrement et cotutelle, ainsi que les procédures de soutenance.

Je suis membre, depuis janvier 2014, de la «Comipers-chercheurs» à l'INRIA Nancy.

J'ai été membre, de 2008 à 2011, de la CDT (commission des développements technologiques) à Nancy.

J'ai été membre de comités de sélection pour des postes de maître de conférences (Grenoble, UJF, 2012, sections CNU 25 et 27 ; Nancy, ESIAL, 2013, section 27).

Je suis correspondant local des groupes de travail C2 et Calcul Formel du GDR IM du CNRS.

Je participe, ou j'ai participé, à deux commissions non scientifiques à l'INRIA Nancy :

- commission de développement durable de 2011 à 2014.
- comité local hygiène, sécurité, et conditions de travail (CLHSCT), depuis 2013.
- comité local hygiène, sécurité, et conditions de travail (CLHSCT) du laboratoire LORIA, depuis la création de cette instance en 2016.

1.7 Management

Depuis sa création au 01/09/2016, je suis le responsable de l'équipe-projet Caramba, commune avec l'Inria, le CNRS, et l'Université de Lorraine.

Je suis porteur du sous-programme «Cyber-Entreprises», au sein du programme «sciences du numérique» pour le CPER 2015-2020 avec l'État et la Région (initialement Lorraine, puis Grand Est). (enveloppe totale environ 4.5 M€)

J'ai été le coordinateur du projet ANR CATREL (programme Blanc, 2013-2016, 670k€).

J'ai été responsable scientifique de la partie nancéienne du projet ANR CHIC (programme Blanc, 2009-2012, 450k€).

1.8 Enseignement

Environ 50 heures par an depuis 2009 (Télécom Nancy, École des Mines de Nancy, Université de Lorraine, Université Paris 7, École Normale Supérieure), sur les thèmes de la cryptologie et de la théorie des nombres.

1.9 Publications

Mes publications personnelles peuvent être téléchargées à l'adresse :
https://members.loria.fr/EThome/publis.html