CURRICULUM VITÆ (3 novembre 2015)

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 : Caramel

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 [9].
- 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 [10].

- Prix La Recherche, 2012 (P. Gaudry, A. Kruppa, moi-même, et P. Zimmermann), catégorie «Sciences de l'information», pour la factorisation de RSA-768 [15].
- Prime d'excellence scientifique (PES) INRIA, 2011-2014.
- Grid'5000 award, 2010.
- IACR distinguished paper, 2007 [5].
- Prix de thèse de l'École polytechnique, 2003.

1.4 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-). S. Covanov Calculs de complexité minimale pour les opérations bilinéaires.

1.5 Responsabilités collectives

1.5.1 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.

1.5.2 Rapporteur de thèses

J'ai été rapporteur des thèses suivantes :

- Kisoon Yoon (Université de Caen–Basse-Normandie), septembre 2013.
- Bastien Vialla (Université de Montpellier), décembre 2015.

1.5.3 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 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.

1.6 Management

Je suis porteur de la proposition en cours de montage de l'équipe-projet Caramba, appelée à prendre la suite de l'équipe-projet Caramel.

Je suis porteur de l'une des deux propositions sur le thème «sciences du numérique» pour le prochain CPER 2015-2020 avec la Région Lorraine (enveloppe prévisionnelle octroyée de 2.9 M€)

Je suis 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€).

1.7 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.

1.8 Publications

Mes publications personnelles peuvent être téléchargées à l'adresse :
http://www.loria.fr/~thome/publis.html

Revues internationales avec comité de lecture

[1] S. Bai, R. P. Brent, and E. Thomé, *Root optimization of polynomials in the number field sieve*, Math. Comp. **84**(295) (2015), 2447–2457. Available at http://dx.doi.org/10.1090/S0025-5718-2015-02926-3.

[2] A. Enge and E. Thomé, *Computing class polynomials for abelian surfaces*, Experiment. Math. **23** (2014), 129–145. Available at http://dx.doi.org/10.1080/10586458.2013.878675.

[3] S. Burckel, E. Gioan, and E. Thomé, *Computation with No Memory, and Rearrangeable Multicast Networks*, Discrete Math. Theor. Comput. Sci. **16**(1) (2014), 121-142.

[4] T. Kleinjung, J. Bos, A. K. Lenstra, D. A. Osvik, K. Aoki, S. Contini, J. Franke, E. Thomé, P. Jermini, M. Thiémard, P. Leyland, P. Montgomery, A. Timofeev, and H. Stockinger, *A Heterogeneous Computing Environment to Solve the 768-bit RSA Challenge*, Cluster Comput. **15**(1) (2012), 53–68. Available at http://dx.doi.org/10.1007/s10586-010-0149-0.

[5] A. Enge, P. Gaudry, and E. Thomé, *An $L(1/3)$ discrete logarithm algorithm for low degree curves*, J. Cryptology **24**(1) (2011), 24–41. Available at http://dx.doi.org/10.1007/s00145-010-9057-y. **IACR Distinguished paper**.

[6] C. Diem and E. Thomé, *Index calculus in class groups of non-hyperelliptic curves of genus three*, J. Cryptology **21**(4) (2008), 593–611. Available at http://dx.doi.org/10.1007/s00145-007-9014-6.

[7] P. Gaudry, E. Thomé, N. Thériault, and C. Diem, *A double large prime variation for small genus hyperelliptic index calculus*, Math. Comp. **76**(257) (2007), 475–492. Available at http://dx.doi.org/10.1090/S0025-5718-06-01900-4.

[8] E. Thomé, *Subquadratic computation of vector generating polynomials and improvement of the block Wiedemann algorithm*, J. Symbolic Comput. **33**(5) (2002), 757–775. Available at http://dx.doi.org/10.1006/jsco.2002.0533.

Conférences internationales avec comité de lecture

À l'exception de [21], tous les articles ci-dessous ont été présentés dans des conférences avec actes.

[9] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. Alex Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Béguelin, and P. Zimmermann, *Imperfect Forward Secrecy: How Diffie-Hellman fails in practice*, CCS'15. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 5–17. ACM, 2015. Available at http://dx.doi.org/10.1145/2810103.2813707. **Best Paper Award**.

[10] R. Bărbulescu, P. Gaudry, A. Joux, and E. Thomé, *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*. In P. Q. Nguyen and E. Oswald (eds.), EUROCRYPT 2014, vol. 8441 of *Lecture Notes in Comput. Sci.*, 1–16. Springer–Verlag, 2014. Available at http://dx.doi.org/10.1007/978-3-642-55220-5_1. **Best Paper Award**.

[11] R. Bărbulescu, C. Bouvier, J. Detrey, P. Gaudry, H. Jeljeli, E. Thomé, M. Videau, and P. Zimmermann, *Discrete logarithms in* $\mathrm{GF}(2^{809})$ *with FFS*. In H. Krawczyk (ed.), Public Key Cryptography - PKC 2014, vol. 8383 of *Lecture Notes in Comput. Sci.*, 221–238. Springer–Verlag, 2014. Available at http://dx.doi.org/10.1007/978-3-642-54631-0_13.

[12] E. Thomé, *Square Root Algorithms for the Number Field Sieve*. In F. Özbudak and F. Rodríguez-Henríquez (eds.), WAIFI 2012, vol. 7369 of *Lecture Notes in Comput. Sci.*, 208–224. Springer–Verlag, 2012. Available at http://dx.doi.org/10.1007/978-3-642-31662-3_15. Article invité.

[13] V. Cortier, J. Detrey, P. Gaudry, F. Sur, E. Thomé, M. Turuani, and P. Zimmermann, *Ballot stuffing in a postal voting system*. In IEEE (ed.), Revote 2011 - International Workshop on Requirements Engineering for Electronic Voting Systems, 27–36. IEEE, 2011. Available at http://dx.doi.org/10.1109/REVOTE.2011.6045913.

[14] T. Kleinjung, L. Nussbaum, and E. Thomé, *Using a grid platform for solving large sparse linear systems over GF(2)*, 11th ACM/IEEE International Conference on Grid Computing (Grid 2010), 161–168, 2010. Available at http://dx.doi.org/10.1109/GRID.2010.5697952.

[15] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann, *Factorization of a 768-bit RSA modulus*. In T. Rabin (ed.), CRYPTO 2010, vol. 6223 of *Lecture Notes in Comput. Sci.*, 333–350. Springer–Verlag, 2010. Available at http://dx.doi.org/10.1007/978-3-642-14623-7_18.

[16] A. Joux, R. Lercier, D. Naccache, and E. Thomé, *Oracle-assisted static Diffie-Hellman is easier than discrete logarithms*. In M. G. Parker (ed.), Cryptography and Coding 2009, vol. 5921 of *Lecture Notes in Comput. Sci.*, 351–367. Springer–Verlag, 2009. Available at http://dx.doi.org/10.1007/978-3-642-10868-6_21.

[17] S. Burckel, E. Gioan, and E. Thomé, *Mapping Computation with No Memory*, 8th International Conference on Unconventional Computation - UC09, vol. 5715 of *Lecture Notes in Comput. Sci.*, 85–97. Springer–Verlag, 2009. Available at http://dx.doi.org/10.1007/978-3-642-03745-0_15.

[18] R. Brent, P. Gaudry, E. Thomé, and P. Zimmermann, *Faster Multiplication in GF(2)[x]*. In A. van der Poorten and A. Stein (eds.), ANTS-VIII, vol. 5011 of *Lecture Notes in Comput. Sci.*, 153–166. Springer–Verlag, 2008. Available at http://dx.doi.org/10.1007/978-3-540-79456-1.

[19] A. Joux, D. Naccache, and E. Thomé, *When e-th roots become easier than factoring*. In K. Kurosawa (ed.), ASIACRYPT 2007, vol. 4833 of *Lecture Notes in Comput. Sci.*, 13–28. Springer–Verlag, 2008. Available at http://dx.doi.org/10.1007/978-3-540-76900-2_2.

[20] H. Cheng, G. Hanrot, E. Thomé, E. Zima, and P. Zimmermann, *Time- and Space-Efficient Evaluation of Some Hypergeometric Constants*. In C. W. Brown (ed.), ISSAC 2007, 85–91. ACM Press, 2007. Available at http://dx.doi.org/10.1145/1277548.1277561.

[21] P. Gaudry and E. Thomé, *The mpFq library and implementing curve-based key exchanges*, SPEED: Software Performance Enhancement for Encryption and Decryption, 49–64, 2007. Available at http://hal.inria.fr/inria-00168429. Conférence sans actes formellement publiés.

[22] E. Thomé, *Computation of discrete logarithms in* $\mathbb{F}_{2^{607}}$. In C. Boyd and E. Dawson (eds.), ASIACRYPT 2001, vol. 2248 of *Lecture Notes in Comput. Sci.*, 107–124. Springer–Verlag, 2001. Available at http://dx.doi.org/10.1007/3-540-45682-1_7.

[23] E. Thomé, *Fast computation of linear generators for matrix sequences and application to the block Wiedemann algorithm*. In B. Mourrain (ed.), ISSAC 2001, 323–331. ACM Press, 2001. Available at http://dx.doi.org/10.1145/384101.384145.

Thèses

[24] E. Thomé, *Théorie algorithmique des nombres et applications à la cryptanalyse de primitives cryptographiques*, Habilitation thesis, Université de Lorraine, 2012, http://hal.inria.fr/tel-00765982.

[25] E. Thomé, *Algorithmes de calcul de logarithme discret dans les corps finis*, Thèse, École polytechnique, 2003, http://hal.inria.fr/tel-00007532.

Édition d'ouvrages

[26] G. Hanrot, F. Morain, and E. Thomé (eds.), *ANTS-IX*, Lecture Notes in Comput. Sci., vol. 6197, Springer–Verlag, 2010. Available at http://dx.doi.org/10.1007/978-3-642-14518-6.

Revues nationales

[27] P. Gaudry, E. Thomé, and P. Zimmermann, *RSA: la fin des clés de 768 bits*, Techniques de l'ingénieur Innovations en technologies de l'information (2011). Vulgarisation (en français).

Autres publications

[28] A. K. Lenstra, T. Kleinjung, and E. Thomé, *Universal Security; From bits and mips to pools, lakes — and beyond*. In M. Fischlin and S. Katzenbeisser (eds.), Number Theory and Cryptography. *Lecture Notes in Comput. Sci.*, 121–124. Springer–Verlag, 2013. Available at http://dx.doi.org/10.1007/978-3-642-42001-6_9. Humoristic.

[29] E. Thomé, *Function Field Sieve*. In H. C. A. van Tilborg and S. Jajodia (eds.), Encyclopedia of Cryptography and Security, 501–502. Springer–Verlag, 2011. Available at http://dx.doi.org/10.1007/978-1-4419-5906-5_450. Short entry in a dictionary-style work.

[30] E. Thomé, *Sieving in Function Fields*. In H. C. A. van Tilborg and S. Jajodia (eds.), Encyclopedia of Cryptography and Security, 1205–1206. Springer–Verlag, 2011. Available at http://dx.doi.org/10.1007/978-1-4419-5906-5_476. Short entry in a dictionary-style work.

Records de calcul

L'importance des calculs records dans mon travail, visant à établir l'état de l'art, m'amène à ajouter ici une liste de mes réalisations de ce type, qui pour certaines ont uniquement fait l'objet d'une annonce sur une liste de diffusion.

[31] C. Bouvier, P. Gaudry, L. Imbert, H. Jeljeli, and E. Thomé, *Discrete logarithms in* GF(p) *— 180 decimal digits*, 2014/6/11. Email to the NMBRTHRY mailing-list, short computation report.

[32] A. Enge and E. Thomé, *Genus 2 CM construction for class number 20,016*, 2014/03/29. Email to the NMBRTHRY mailing-list, short computation report, described in [2].

[33] R. Bărbulescu, C. Bouvier, J. Detrey, P. Gaudry, H. Jeljeli, E. Thomé, M. Videau, and P. Zimmermann, *Discrete logarithms in* GF(2^{809}) *with FFS*, 2013/10/04. Email to the NMBRTHRY mailing-list, short computation report, described in [11].

[34] R. Bărbulescu, C. Bouvier, J. Detrey, P. Gaudry, H. Jeljeli, E. Thomé, M. Videau, and P. Zimmermann, *The relationship between some guy and cryptography*, 2012. Available at http://ecc.2012.rump.cr.yp.to/. ECC2012 rump session talk (humoristic), short computation report.

[35] S. Bai, E. Thomé, and P. Zimmermann, *Factorisation of RSA-704 with CADO-NFS*, 2012. Available at http://eprint.iacr.org/2012/369. Extended computation report.

[36] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann, *Factorization of a 768-bit RSA modulus*, 2010/01/07. Email to the NMBRTHRY mailing-list, short computation report, described in [15].

[37] E. Thomé, *Discrete logarithms on a genus-3 curve — 93 bits*, 2007. Record computation, described in [6].

[38] E. Thomé, *Discrete logarithms on a genus-3 curve — 81 bits*, 2006. Record computation, described in [7].

[39] E. Thomé, *Discrete logarithms in* GF(2^{607}), 2002/02/23. Email to the NMBRTHRY mailing-list, short computation report, described in [22].

Rapports de recherche et articles soumis

[40] S. Covanov and E. Thomé, *Fast arithmetic for faster integer multiplication*, 2015. Available at http://hal.inria.fr/hal-01108166. Submitted.

[41] S. Ionica and E. Thomé, *Isogeny graphs with maximal real multiplication*, 2015. Available at http://hal.inria.fr/hal-00967742. Submitted.