Sylvain Duquesne
Laboratoire IRMAR, UMR CNRS 6625
Université Rennes 1
Campus de Beaulieu
35042 Rennes cedex
tel : 02.23.23.60.14
courriel : `sylvain.duquesne@univ-rennes1.fr`
page web : `http://perso.univ-rennes1.fr/sylvain.duquesne`

Cursus

2008 Professeur à l'université de Rennes 1

2007 Habilitation à Diriger des Recherches, 27 novembre

Courbes algébriques : de l'inutile à l'indispensable

jury composé de J.C Bajard, H. Cohen, J.M. Couveignes (rapporteur), M. Girault (rapporteur), G. Frey (rapporteur), P. Michel et B. Vallée.

2007 Demi-délégation CNRS.

2004-12
2016-20 Bénéficiaire de la PEDR.

2003-08 Maître de conférences à l'université Montpellier II au sein de l'I3M (Institut de Mathématiques et de Modélisation de Montpellier) et chercheur associé au LIRMM (Laboratoire d'Informatique, de Robotique et de Microéléctronique de Montpellier) au sein de l'équipe ARITH.

2002-03 Post-doctorant à l'Université Bordeaux 1 dans le cadre du projet européen de cryptographie AREHCC.

1998-01 Thèse de Doctorat à l'Université Bordeaux 1, spécialité Mathématiques Pures, sous la direction d'Henri Cohen

Calculs effectifs des points entiers et rationnels sur les courbes

Soutenue le 7 décembre 2001 devant un jury composé de Y. Bilu, H. Cohen, V. Flynn (rapporteur), M. Matignon, J.F. Mestre (rapporteur) et F. Morain

1997-98 Agrégation de Mathématiques et DEA Méthodes algébriques de l'Université Paris VI.

1997-99 Élève de l'ENS de Cachan.

Liste de publications

1. *Efficient Scalar Multiplication for Ate Based Pairing over KSS Curve of Embedding Degree 18*, avec A. Khandaker, Y. Nogami et H. Seo, WISA, Lecture Notes in Computer Science, **10144** (2017), pp. 221–232.

2. *Arithmetic of Finite Fields, 6th International Workshop, WAIFI 2016, Ghent, Belgium, July 13-15, 2016, Revised Selected Papers,* éditeur avec Svetla Petkova-Nikova, Lecture Notes in Computer Science, **10064** (2017).

3. *An Improvement of Optimal Ate Pairing on KSS curve with Pseudo 12-sparse Multiplication,* avec A. Khandaker, H. Ono, Y. Nogami et M. Shirase, ICISC, Lecture Notes in Computer Science, **10157** (2017), pp. 1–12.

4. *Choosing and generating parameters for low level pairing implementation on BN curves,* avec N. El Mrabet, S. Haloui et F. Rondepierre, à paraître, Applicable Algebra in Engineering, Communication and Computing, (2017).

5. 2 Chapitres de *Guide to Pairing-Based Cryptography*, El Mrabet, Joye à paraître chez CRC Press (2016).
   — Chapitre 5 : *Arithmetic of Finite Fields* avec J.L. Beuchat, L. Fuentes-Castañeda, F. Rodríguez-Henríquez et F. Rondepierre
   — Chapitre 10 : *Choosing Parameters* avec N. ElMrabet, S. Haloui et F. Rondepierre

6. *Web-based Volunteer Computing for Solving an Elliptic Curve Discrete Logarithm Problem,* avec S. Kajitani, Y. Nogami, S. Miyoshi, T. Austin, K. Al-Amin et N. Begum, International Journal of Networking and Computing, **6 :2** (2016) pp 181–194.

7. *Memory-saving computation of the pairing final exponentiation on BN curves,* avec L. Ghammam, Groups, Complexity, Cryptology, **8 :1** (2016) pp 75–90.

8. *Efficient Pairing Computation on Jacobi Quartic Elliptic Curves,* avec N. El Mrabet et E. Fouotsa, Journal of Mathematical Cryptology, **8 :4** (2014) pp. 331–362.

9. *Combining leak-resistant arithmetic for elliptic curves defined over $\mathbb{F}_p$ and RNS representation*, avec J. C. Bajard et M. Ercegovac, Publications Mathématiques de Besancon, **1** (2013), pp. 67–87.

10. *Tate Pairing Computation on Jacobi's Elliptic Curves*, avec E. Fouotsa, Pairing, Lecture Notes in Computer Science, **7708** (2012), pp. 254–269 .

11. *FPGA Implementation of Pairings Using Residue Number System and Lazy Reduction* , avec R. Cheung, J. Fan, N. Guillermin, I. Verbauwhede et G. Yao, CHES, Lecture Notes in Computer Science, **6917** (2011), pp. 421–441.

12. *RNS arithmetic in $\mathbb{F}_{p^k}$ and application to fast pairing computation*, Journal of Mathematical Cryptology, **5 :1** (2011), pp. 51–88.

13. *Traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2*, Mathematics in Computer Science **3 :2** (2010), pp. 173-183.

14. *Montgomery Ladder for Genus 2 Curves in Characteristic 2*, WAIFI, Lecture Notes in Computer Sciences, **5130** (2008), pp. 174-188.

15. *Improving the Arithmetic of Elliptic Curves in the Jacobi Model*, Information Processing Letters **104 :3** (2007), pp. 101-105.

16. *Rational Points on Higher Genus Curves*, Chapitre 13 de "Number Theory, Volume II : Analytic and Modern Tools" de H. Cohen, Graduate Texts in Mathematics **240** (2007).

17. *Elliptic curves associated with simplest quartic fields*, Journ. Théor. Nombres Bordeaux, **19 :1** (2007), pp. 81-100.

18. *Residue systems efficiency for modular products summation : application to elliptic curves cryptography*, avec J. C. Bajard, M. Ercegovac, N. Meloni, SPIE **6313**, 631304 (2006) (Conférence internationale avec comité de lecture).

19. 4 Chapitres de *Handbook of elliptic and hyperelliptic curves in cryptography*, Cohen, Frey, Discrete Mathematics and Its Applications **34**, Chapman & Hall/CRC (2005)
    — Chapitre 6 : *Background on Pairings* avec G. Frey
    — Chapitre 14 : *Arithmetic of Hyperelliptic Curves*, avec T. Lange
    — Chapitre 16 : *Implementation of Pairings*, avec G. Frey
    — Chapitre 24 : *Pairing-Based Cryptography*, avec T. Lange

20. *Montgomery scalar multiplication for genus 2 curves*, ANTS VI, Lecture Notes in Comput. Sci. **3076** (2004), pp. 153-168.

21. *Classification of genus 2 curves over $\mathbb{F}_2^n$ and optimization of their arithmetic*, avec B. Byramjee, Cryptology ePrint Archive, no. 107 (2004)
    et dépôt de brevet international par Oberthur Card Systems.

22. *Hyperelliptic Curves Cryptosystems : a new solution to replace RSA*, avec B. Byramjee, e-smart 2003 (Conférence internationale avec comité de lecture).

23. *Numerical investigations related to the derivatives of the L-series of certain elliptic curves*, avec C. Delaunay, Experimental Mathematics **12 :3** (2003), pp. 311-317.

24. *Points rationnels et méthode de Chabauty elliptique*, Journ. Théor. Nombres Bordeaux **15 :1** (2003), pp. 99-113.

25. *Hauteurs et descente infinie sur les courbes hyperelliptiques*, Publications Mathématiques de Besançon en théorie des nombres (2002).

26. *Rational Points on Hyperelliptic Curves and an explicit Weierstrass Preparation Theorem*, Manuscripta Mathematica, **108** (2002), pp. 191-204.

27. *Integral Points on Elliptic Curves Defined by Simplest Cubic Fields*, Experimental Mathematics **10 :1** (2001), pp. 91-102.

Sélection d'interventions

1. Avril 2017 : *Index calculus on finite fields and applications to pairing based cryptography*, école de recherche CIMPA, Côte d'Ivoire, **invité**.

2. Février 2016 : *Cryptographie basée sur les courbes elliptiques*, école de recherche CIMPA, Mauritanie, **invité**.

3. Juillet 2015 : *Memory-saving computation of the pairing final exponentiation on BN curves*, 29ème JA, Hongrie.

4. Avril 2015 : *Pairings on elliptic curves and their computation*, Algebraic Structures, Cryptography, Number Theory and Applications, Cap vert, **invité**.

5. Juin 2014 : *Problème du logarithme discret et ses applications en cryptographie*, école de recherche CIMPA, Sénégal, **invité**.

6. Juillet 2013 : *Pairing Computation on Jacobi's Elliptic Curve*, EPSRC Warwick Number Theory Symposium, Royaume Uni, **invité**.

7. Juin 2012 : *Sécurité de l'information et cryptographie*, Journée MMS 2012, INSA Rennes, **invité**.
8. Mai 2009 : *RNS representation of numbers for pairings in elliptic curve cryptography*, Workshop on Pairings in Arithmetic Geometry and Cryptography, Allemagne, **invité**.
9. Juillet 2007 : *RNS representation applied to elliptic curve cryptography*, 25ème JA, Royaume Uni.
10. Juillet 2005 : *Elliptic curves associated with simplest quartic fields*, 24ème JA, Marseille.
11. Avril 2005 : *Cryptographie sur les courbes elliptiques*, École Jeunes Chercheurs algorithmique et calcul formel, Montpellier, **invité**.
12. Juillet 2004 : *Montgomery scalar multiplication for genus 2 curves*, ANTS VI, USA.
13. Juillet 2001 : *Méthodes de Chabauty Explicites*, 22ème JA, Lille.
14. Décembre 2000 : *Explicit Weierstrass Preparation Theorem in several variables and rational points on hyperelliptic curves*, Arithmetic geometry workshop, MSRI Berkeley, USA, **invité**.
15. Mai 2000 : *Integral Points on Elliptic Curves Defined by Simplest Cubic Fields*, Algorithmes en théorie des nombres, CIRM, Marseille.

Je suis également intervenu dans de nombreux séminaires de théorie des nombres ou de cryptographie régulièrement de 1999 à 2015 (Bordeaux, Caen, Clermont-Ferrand, Grenoble, Limoges, Lyon, Marseille, Montpellier, Nice, Paris, Rennes, Toulon, Toulouse).

Développement de Logiciels

1. Inclusion dans GP/Pari de l'algorithme SEA pour le comptage de points sur les courbes elliptiques avec Christophe Doche et Bill Allombert (2007-2008).
2. Bibliothèque C/C++ pour les courbes elliptiques en cryptographie (2002-2003).
3. Programmes GP/Pari de calcul des séries L et leurs dérivées associées aux courbes elliptiques (2002).
4. Programmes Magma de calcul des traces de la loi de groupe sur la variété de Kummer en genre 3 (2001).
5. Programmes Maple de la méthode de Chabauty elliptique et ses généralisations (2000).
6. Programmes GP/Pari de calcul des points entiers sur une courbe elliptique (1999).

Séjours scientifiques de longue durée (>1 mois)

— Université d'Okayama (Japon), Avril 2016, sur l'invitation de Yasuyuki Nogami.

— Université de Monastir (Tunisie), Octobre 2012 et Novembre 2013, sur l'invitation de Leila Ben Abdelghani.

— National Knowledge Center (Émirats Arabes Unis), Avril 2012 et Février 2013, sur l'invitation de Cédric Tavernier.

— Université de Yaoundé 1 (Cameroun), Mai 2010, Avril 2011 et Mars 2014 sur l'invitation de Marcel Tonga.

— University of Liverpool (Angleterre), Avril 2000 sur l'invitation de Victor Flynn.

Encadrements de thèses

— Türkü Özlüm Çelik (codirection avec C. Ritzenthaler) sur la cryptographie basée sur les courbes hyperelliptique pour les implémentations matérielles (2014-).

— Maxime Lebreton (CIFRE Orange) sur les infrastructures des crypto-systèmes basés sur courbes elliptiques (2014-).

— Loubna El Ghammam (cotutelle avec L. Abdelghani de l'université de Monastir, Tunisie) sur les couplages et leur implantation matérielle (2013-2016), pos-doc à Caen.

— Romain Basson (codirection avec R. Lercier) sur la reconstruction de courbes de genre 3 et 4 à partir de leurs invariants (2011-2015), Professeur en CPGE.

— Christophe Tran sur les applications des formules d'addition sur les jacobiennes de courbes hyperelliptiques à la cryptographie (2011-2014), Cryptographe au Crédit Mutuel.

— Emmanuel Fouotsa (codirection avec M. Tonga de l'université Yaoundé 1) sur l'utilisation de modèles alternatifs pour le calcul de couplages (2010-2013), Maître assistant à l'ENS de Bambili (Cameroun).

— Nicolas Guillermin sur l'implantation matérielle des systèmes de cryptographie basés sur les courbes elliptiques (2008-2011), Ingénieur de l'armement DGA à Paris.

— Nadia ElMrabet sur l'utilisation des couplages en cryptographie (2006-2009), Maître de conférences à Paris 8 détachée à l'école des mines de Saint-Etienne.

— Nicolas Méloni sur l'arithmétique pour la cryptographie basée sur les Courbes Elliptiques (2005-2008), Maître de conférences à Toulon.

Responsabilités administratives et scientifiques au niveau national et international

— Membre du jury du concours CR du CNRS (2017).

— Membre du conseil du GIS SARIMA (2015-2017).

— Expert SNSF, Swiss National Science Foundation (2015).

— Expert AAP Institut Mines-Telecom (2014).

— **Membre de l'équipe de direction du CIMPA en tant que Responsable Scientifique pour l'Afrique Subsaharienne** (2013-2017).

— Membre de la section 25 du CNU (2012-2016).

— Expert ANR (2011, 2012, 2015).

— Expert AERES (2011).

— Membre de jurys de thèse/HDR (en plus de mes étudiants) :

- Christophe Nègre (HDR 2016, rapporteur).
- Julien Eynard (2015, rapporteur).
- Kodjo Kpognon (2014, président).
- Jean-Christophe Zapalowicz (2014, président).
- Kissoon Yoon (2013).
- Davide Alessio (2011).
- Ana Charpentier (2011, président).
- Christophe Arène (2011, rapporteur).
- Safia Haloui (2011, rapporteur).
- Yoann Choyer (non soutenue, rapporteur).
- Moncef Amara (2011, rapporteur).

— Membre extérieur de la commission de spécialistes de Rennes (2005-2008) et de plusieurs comi-

tés de sélection.

— Membre du comité de rédaction de la revue africaine de la recherche en informatique et mathématiques appliquées (ARIMA)

— Rapporteur pour Math. Reviews. et plusieurs revues ("Journal de Théorie des nombres de Bordeaux", "Information Processing Letters", "Journal of Number Theory", "Publicationes Mathematicae Debrecen", "Designs Codes and Cryptography", "LMS Journal of Computation and Mathematics", "Discrete Applied Mathematics", "IEEE Transactions on Computers", "IEEE Communication letters", "International Journal of Computer Mathematics", "revue africaine de la recherche en informatique et mathématiques appliquées", "Mathematical Problems in Engineering", "Advances in Mathematics of Communications", "Informations Sciences", "Cryptography and Communications - Discrete Structures Boolean Functions and Sequences", "Groups, Complexity, Cryptology", "Applicable Algebra in Engineering, Communication and Computing") ou conférences (Eurocrypt, Indocrypt, Pairing, AGCT, CHES, IFIP SEC, PKC).

Responsabilités administratives et scientifiques au niveau local

— Directeur adjoint de l'IRMAR (2017).

— Responsable de domaine transverse pour l'IRMAR dans le pôle d'excellence Cybersécurité (2014-).

— Membre du conseil de l'IRMAR (2012-2016).

— Responsable à l'IRMAR des interactions avec l'informatique (2012-2017).

— Membre du conseil de l'UFR de mathématiques de Rennes (2011-2015).

— Responsable de l'équipe Géométrie algébrique réelle, Calcul formel et Cryptographie (2011-2015).

— Responsable du Colloquium Interactions Mathématiques & Informatique à Montpellier (2008).

— Membre du conseil du département de mathématiques de Montpellier (2007-2008).

— Responsable des relations avec le département informatique au département de mathématiques de Montpellier 2 (2006-2008).

— Membre local régulier de commissions de spécialistes et comité de sélections depuis 2005.

— Responsable scientifique des locaux du département de Mathématiques de Montpellier (2004-2008).

Responsabilités pédagogiques

— Président de la commission enseignement (en charge de l'organisation des enseignements, des maquettes, etc) de l'UFR de Mathématiques de Rennes (2010-2014).

— Membre de la commission enseignement de l'UFR de Mathématiques de Rennes (2009-).

— Responsable de la spécialité Mathématiques de l'information et cryptographie du Master de Mathématiques de Rennes depuis sa création : 61 étudiants formés en 6 promotions, 93% d'insertion professionnelle (2008-...).

— Responsable de la filière (L et M) Mathématiques et informatique de Montpellier (2006-2008).

— Membre du conseil du département enseignement de Mathématiques de Montpellier (2006-2008).

— Responsable de la préparation à l'option Calcul Formel de l'agrégation à Montpellier (2003-2007).

Animation de la recherche au niveau national et international

— Organisateur de WAIFI 2020 (International Workshop on the Arithmetic of Finite Fields) à Rennes.

— Membre du comité scientifique de CryptoPuce 2017 (France).

— Program Chair de WAIFI 2016 (International Workshop on the Arithmetic of Finite Fields) organisé en Belgique.

— Membre du comité scientifique de YACC 2016 (France).

— Membre du comité scientifique de l'école de Recherche CIMPA "Algorithmique en théorie des nombres et cryptographie" 2016 (Mauritanie).

— Organisateur des Rencontres de l'Arithmétique de l'Informatique Mathématique 2015 (Rennes).

— Membre du comité de programme de Pairing 2013 (Chine).

— Membre du comité scientifique de GeoCrypt 2013 (Tahiti).

— Membre du comité de programme de YACC 2012 (France).

— Organisateur de la conférence C2 à Dinard (2012).

— Membre du comité scientifique du séminaire de cryptographie de Rennes (2008-).

— Organisation du colloque jeunes chercheurs en théorie des nombres 2004 à Montpellier

Implication dans des projets de recherche

— Porteur pour l'IRMAR de l'ANR SafeTLS (2017-2020).

— Porteur pour l'IRMAR du projet interlabex Lebesgue/CominLabs H-A-H (2014-2017).

— Membre de l'équipe-projet MACISA (France, Afrique) d'INRIA (2013-2017).

— Membre de l'ANR SIMPATIC (2013-2016).

— Membre du projet PRMAIS (France, Allemagne, Afrique) de la fondation SIMONS (2013-2018).

— Membre de l'ANR PEACE (2012-2015).

— Membre de l'ANR CHIC (2011-2014).

— Membre de l'ANR Algol (2007-2011).

Collaborations industrielles

Dans le cadre de mes activités en cryptographie, j'ai eu des contacts avec de nombreux industriels et collaboré avec plusieurs d'entre eux. Je ne cite ici que les collaborations les plus significatives.

— INVIA (composants électroniques sécurisés).

— Orange.

— ARX-Arcéo (R&D sécurité de l'information).

— Voxaly (vote éléctronique).

— Amossys (Certification de sécurité).

— Paycool Developpement (Paiement par téléphone portable).

— Nethéos (Confidentialité et sûreté numérique).

— Mediscs (Authentification hautement sécurisée).

— Oberthur Card Systems (Fabricant de cartes à puces).

Enseignements

— Cours "Cryptographie basée sur les courbes elliptiques" en Mauritanie en 2016.

— Cours "Problème du logarithme discret et ses applications en cryptographie" au Sénégal en 2014.

— Cours de cryptographie en 5ème année de l'ESAIP à Angers en 2014.

— Cours de cryptographie de niveau M1 et M2 à l'université de Monastir en 2012 et 2013.

— Cours de cryptographie de niveau M1 et M2 à l'université de Yaoundé 1 en 2010, 2011 et 2014.

— Cours majoritairement en master et en préparation à l'agrégation à l'université de Rennes depuis 2008 (en moyenne 220 heqTD par an).

— Cours "Public Key Cryptography" dans le Master pro SISA (Security of Integrated Systems Applications) de l'école des Mines de Saint-Etienne en 2007.

— Cours de tous niveaux (L1, L2, M1, M2, agrégation) essentiellement en algèbre et en cryptographie mais également en mathématiques discrètes et en programmation à l'université Montpellier de 2003 à 2008.

— Encadrement de nombreux stages de L3, M1 et M2 en théorie des nombres et en cryptographie.

— TD et TP en DEUG MIAS à l'université de Bordeaux de 1999 à 2003

Vulgarisation scientifique

— Réalisation d'un modèle simplifié à but pédagogique de machine Enigma au LabFab de Cesson, en cours.

— Réalisation d'un reportage vidéo sur la cryptographie pour le CNED, juin 2105.

— Interview à la radio RCF sur la cryptographie, novembre 2014.

— Membre du conseil scientifique et technique du musée des Transmissions à Rennes (2013-).

— Participation à l'opération "A la découverte de la recherche" (interventions dans des lycées autour de Rennes) et au festival des sciences (exposés grand public dans des collectivités de l'agglomération de Rennes) tous les ans depuis 2009.

— Exposé devant les lauréats du Rallye Mathématique en 2013.

— Interview dans le journal Science Ouest en 2011.

— Intervention sur la recherche en cryptographie et son développement dans les pays sous développés sur Radio France International en 2011.

— Présentation des activités “sécurité numérique” à Montpellier lors d'un reportage de FR3 région à l'occasion de la visite de Vaughan Jones en juin 2007.

— Animation d'un “Bar des sciences” sur le thème de la sécurité de l'information en 2007.

— Exposés de Cryptographie grand public pour la fête de la science en 2006 et 2007 à Montpellier.

— Exposés de Cryptographie dans des lycées de l'agglomération montpellieraine en 2004, 2005, 2006 et 2007.