Conseil Scientifique de l'institut INS2I
Collège A1
Pierrick Gaudry

Curriculum Vitae

Éléments biographiques

Coordonnées et situation présente

Nom :	**Gaudry**
Prénom :	**Pierrick**
Date de naissance :	Né le 17 mai 1973 à Pithiviers (45)
Statut :	Directeur de recherche CNRS
Adresse :	LORIA – UMR 7503 Campus Scientifique 54500 Vandœuvre-lès-Nancy
Email :	Pierrick.Gaudry@loria.fr
Www :	http://members.loria.fr/PGaudry/
Téléphone :	03 83 59 20 62

Parcours

2010-	DR CNRS au LORIA (DR1 en 2018)
2008	HdR, Université Nancy 1
2005-2010	CR CNRS au LORIA (CR1 en 2006)
2001-2005	CR CNRS au LIX, École polytechnique
1998-2001	Thèse de doctorat en informatique, dirigée par F. Morain, LIX, École polytechnique
1997-1998	4ème année à l'ENS Cachan, début officieux de la thèse
1996-1997	Service national
1995-1996	Agrégation de maths, option info
1994-1995	DEA maths-informatique

Thèmatiques de recherche passées et présentes

- Algorithmiques des courbes algébriques pour la cryptographie
  - Problème du logarithme discret
  - Arithmétique efficace
  - Comptage de points
- Algorithme du crible algébrique et consorts
  - Factorisation d'entiers.
  - Logarithme discret dans les corps finis
- Vote électronique

Responsabilités collectives

- Directeur adjoint du LORIA de janvier 2011 à décembre 2012.
- Direction d'équipe de 2010 à 2015.
- Comité de visite HCERES (CRIStAL 2019, LITIS 2015).
- Vice-responsable de la partie Informatique de l'Écolde Doctorale de 2015 à 2020.
- Membre du Conseil Scientifique du GDR Informatique Mathématique depuis 2019.

Encadrement

Encadrements de 8 doctorants et doctorantes, au devenirs variés : CNRS, université, industrie.

Production scientifique

Auteur d'environ 20 articles dans des revues internationales à comité de lecture et 40 articles dans des conférences internationales à comité de lecture. La liste complète est disponible en ligne à l'adresse `https://members.loria.fr/PGaudry/publications/` avec la version preprint de presque toutes les publications.

Sélection de publications

[1] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin Vandersloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. Imperfect Forward Secrecy : How Diffie-Hellman Fails in Practice. In *ACM CCS 2015*, page 14, 2015.

[2] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *Eurocrypt 2014*, volume 8441 of *LNCS*, pages 1–16. Springer, 2014.

[3] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann. Comparing the difficulty of factorization and discrete logarithm : a 240-digit experiment. In *CRYPTO 2020*, volume 12171 of *LNCS*, pages 62–91. Springer, 2020.

[4] Véronique Cortier and Pierrick Gaudry. *Le vote électronique - les défis du secret et de la transparence*. Odile Jacob, May 2022. Préface de Gérard Berry.

[5] Véronique Cortier, Pierrick Gaudry, and Stephane Glondu. Belenios : a simple private and verifiable electronic voting system. In *Foundations of Security, Protocols, and Equational Reasoning*, volume 11565 of *LNCS*, pages 214–238. Springer, 2019.

[6] Gabrielle de Micheli, Pierrick Gaudry, and Cécile Pierrot. Lattice Enumeration for Tower NFS : a 521-bit Discrete Logarithm Computation. In *ASIACRYPT 2021*, volume 13090 of *LNCS*, pages 67–96. Springer, 2021.

[7] Pierrick Gaudry and Alexander Golovnev. Breaking the encryption scheme of the Moscow Internet voting system. In *Financial Cryptography and Data Security*, pages 32–49. Springer, 2020.

[8] Pierrick Gaudry, Florian Hess, and Nigel Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, 15 :19–46, 2002.

[9] Pierrick Gaudry and Éric Schost. Genus 2 point counting over prime fields. *Journal of Symbolic Computation*, 47(4) :368–400, 2012.

[10] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, K. Lenstra, Arjen, Emmanuel Thomé, W. Bos, Joppe, Pierrick Gaudry, Alexander Kruppa, L. Montgomery, Peter, Dag Arne Osvik, Herman Te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768-bit RSA modulus. In *CRYPTO 2010*, volume 6223 of *LNCS*, pages 333–350. Springer Verlag, 2010.