Adresse
Paris, France

E-mail
prest↺ens•fr

Site Web & Git
di.ens.fr/~prest
github.com/tprest

ThomasPrest

Ingénieur cryptologue

Compétences scientifiques
Cryptologie ★★★★☆
Algorithmique ★★★★☆
Mathématiques ★★★★☆

Programmation
C/C++ ★★★☆☆
Python/Sage ★★★☆☆
Magma ★★★☆☆
CAML ★★★☆☆

Outils de programmation
Valgrind ★★★☆☆
SVN/Git ★★★☆☆
Doxygen ★★★☆☆
Gcov ★★★☆☆

Systèmes d'exploitation
Unix ★★★☆☆
Windows ★★★☆☆

Expériences professionnelles

01/16 - Maintenant — **Ingénieur cryptologue** — Thales Communications & Security, Gennevilliers
Mon travail comprend la fourniture de spécifications cryptographiques pour des produits Thales, l'assistance à des équipes de développement, la veille technologique, la rédaction de rapports pour des clients externes ainsi que du développement logiciel opérationnel.

10/12 - 12/15 — **Thèse de doctorat** — Thales et École Normale Supérieure
Ma thèse s'intitule "Gaussian Sampling in Lattice-Based Cryptography" et a été encadré par Vadim Lyubashevsky (ÉNS) et Sylvain Lachartre (Thales). J'y ai développé et implémenté des outils algorithmiques, statistiques et algébriques pour rendre plus efficace la cryptographie basée sur les réseaux.

04/12 - 09/12 — **Stage de fin d'études** — Thales Communications & Security, Colombes
J'ai développé et qualifié une librairie cryptographique, sous la direction de Sylvain Lachartre et Olivier Orcière.

06/10 - 07/10 — **Stage de Master I** — INRIA, équipe "CARAMEL", Nancy
J'ai travaillé sur l'amélioration de la sélection polynomiale pour le crible NFS, sous la direction de Paul Zimmermann. Mon travail a été intégré dans le projet CADO-NFS et a donné lieu à la publication d'un article.

06/09 - 07/09 — **Stage de Licence** — Institut de mathématiques de Jussieu, Paris
J'ai étudié les applications des courbes elliptiques en cryptographie, sous la direction de Marc Hindry.

Scolarité

2011 - 2012 — **Master 2 Cryptologie & sécurité informatique** — Université Bordeaux I, Talence
J'ai choisi la spécialité cryptographie lors de mon cursus.

2008 - 2011 — **Magistère de mathématiques** — ÉNS de Rennes, Bruz
Le cursus en 4 ans s'étale de la License 3 au Master 2, et inclut le passage de l'agrégation, que j'ai passé en option informatique.

2007 - 2008 — **Première année d'école d'ingénieurs** — Supélec, Rennes
J'ai démissionné pour préparer les concours des ÉNS.

2005 - 2007 — **CPGE scientifique, MPSI et MP*** — Lycée Fabert,Metz

Langues

Français ★★★★★
Anglais ★★★★☆

Mise en page

LaTeX ★★★★☆
Beamer ★★★★☆
Word ★★★☆☆
Excel ★★☆☆☆
HTML/CSS ★★☆☆☆

Divers

Mes 100 films favoris

Publications

Fast Fourier Orthogonalization. ISSAC 2016.
Avec Léo Ducas.

Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices. Eurocrypt 2015.
Avec Vadim Lyubashevsky.

Efficient Identity-Based Encryption over NTRU Lattices. Asiacrypt 2014.
Avec Léo Ducas et Vadim Lyubashevsky.

Non-Linear Polynomial Selection for the Number Field Sieve. Journal of Symbolic Computation, Volume 47 Issue 4.
Avec Paul Zimmermann.

Exposés invités et en conférence

Fast Fourier Orthogonalization

- 05/2016: Séminaire de cryptographie, Université Rennes I.
- 03/2016: Séminaire d'algorithmique, Université de Caen.
- 01/2016: "Lattice Meetings", École Normale Supérieure.
- 10/2015: Journées C2, La Londe-les-Maures.

Gaussian Sampling in Lattice-based Cryptography

- 03/2016: Séminaire de cryptologie, Université de Caen.

Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices

- 04/2015: Eurocrypt, Sofia.
- 01/2015: Séminaire AriC, ÉNS de Lyon.

Efficient Identity-Based Encryption over NTRU Lattices

- 12/2014: Asiacrypt, Kaohsiung.
- 10/2014: Séminaire de cryptographie, Université Rennes I.
- 03/2014: Journées C2, les Sept Laux.

Tous mes articles et exposés peuvent être trouvés sur mon site. C'est également le cas pour les implémentations associées, ma thèse de doctorat, mes rapports de stage, etc.

Références

Nom	Fonction	Adresse e-mail
◦Éric Garrido	◦Chef d'équipe	◦eric•garrido↺thalesgroup•com
◦Vadim Lyubashevsky	◦Directeur de thèse	◦vad↺zurich•ibm•com
◦David Pointcheval	◦Ancien chef d'équipe	◦david•pointcheval↺ens•fr