ThomasPrest

Ingénieur et chercheur en cryptologie

Contact

prest↺ens•fr

Site Web & Git

tprest.github.io
github.com/tprest

Compétences scientifiques

Cryptologie, Algorithmique, Mathématiques

Programmation

C/C++, Python, Magma, CAML

Outils de programmation

Valgrind, SVN/Git, Doxygen, Gcov, Klocwork

Systèmes d'exploitation

Unix, Windows

Langues

Français, Anglais

Mise en page

Latex, Beamer, Office Suite, HTML/CSS

Divers

Mes 100 films favoris

Expériences professionnelles

01/16 - Maintenant **Ingénieur cryptologue** — Thales Communications & Security, Gennevilliers
Spécifications cryptographiques, aide à équipes de développement, rédaction de rapports scientifique, recherche, développement logiciel.

10/12 - 12/15 **Thèse de doctorat** — Thales et École Normale Supérieure
Gaussian Sampling in Lattice-Based Cryptography. Thèse encadrée par Vadim Lyubashevsky (ÉNS) et Sylvain Lachartre (Thales).

04/12 - 09/12 **Stage de fin d'études** — Thales Communications & Security, Colombes
Développement d'une librairie cryptographique. Tuteur: S. Lachartre.

06/10 - 07/10 **Stage de Master I** — INRIA, équipe "CARAMEL", Nancy
Sélection polynomiale pour le crible NFS. Tuteur: Paul Zimmermann.

06/09 - 07/09 **Stage de Licence** — Institut de mathématiques de Jussieu, Paris
Courbes elliptiques en cryptographie. Tuteur: Marc Hindry.

Scolarité

2011 - 2012 **Master 2 Cryptologie & sécurité informatique** — Université Bordeaux I, Talence
Spécialité cryptographie, mention bien.

2008 - 2011 **Magistère de mathématiques** — ÉNS de Rennes, Bruz
L3, M1, agégation (option informatique), M2.

2007 - 2008 **Première année d'école d'ingénieurs** — Supélec, Rennes
Démission en première année pour préparer les concours des ÉNS.

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

Publications

Uns liste complète est disponible sur mon site (`tprest.github.io`) ou sur DBLP (`dblp.uni-trier.de/pers/hd/p/Prest:Thomas`).

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