Address
Paris, France

Mail
prest↺ens•fr

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

ThomasPrest

Cryptography engineer

Scientific Skills
Cryptology ★★★★☆
Algorithmics ★★★★☆
Mathematics ★★★★☆

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

Programming Tools
Valgrind ★★★☆☆
SVN/Git ★★★☆☆
Doxygen ★★★☆☆
Gcov ★★★☆☆

Operating Systems
Unix ★★★☆☆
Windows ★★★☆☆

Experience

01/16 - Now **Cryptography engineer** Thales Communications & Security, Gennevilliers, FR
My work includes writing cryptographic specifications for Thales products, providing assistance to development teams, technology watch, writing scientific reports to external clients, and operational software development.

10/12 - 12/15 **PhD thesis** Thales and École Normale Supérieure, FR
The title of my thesis was “Gaussian Sampling in Lattice-Based Cryptography”, and I was directed by Vadim Lyubashevsky (ÉNS) and Sylvain Lachartre (Thales). I used algorithmic, statistical and algebraic tools to make lattice-based cryptography more practical and also worked on efficient implementations of it.

04/12 - 09/12 **Graduation internship** Thales Communications & Security, Colombes, FR
I developped and qualified a cryptographic library, directed by Sylvain Lachartre and Olivier Orcière.

06/10 - 07/10 **Mid-graduate internship** INRIA, “CARAMEL” team, Nancy, FR
I worked on improving the polynomial selection for the NFS sieve, directed by Paul Zimmermann. My work was integrated in the CADO-NFS project and led to the publication of a research article.

06/09 - 07/09 **Bachelor internship** Mathematics institute of Jussieu, Paris, FR
I studied elliptic curves and their applications in cryptography, directed by Marc Hindry.

Education

2011 - 2012 **Master 2 Cryptography & Computer Security** Bordeaux I University, Talence, FR
I specialized in cryptography and cryptanalysis.

2008 - 2011 **Mathematics magister** ÉNS de Rennes, Bruz, FR
This school delivers a 4-year training (essentially from the middle of Bachelor to a Master degree). I took mathematics as my major, computer science as my minor. During my scholarship, I passed the selective national examination “agrégation”.

2007 - 2008 **First year of engineer school** Supélec, Rennes, FR
I left to prepare exams for the ÉNS schools.

2005 - 2007 **Scientific CPGE preparatory classes** Lycée Fabert,Metz, FR

Languages

French ★★★★★
English ★★★★☆

Layout Tools

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

Miscellaneous

My top 100 movies

Publications

Fast Fourier Orthogonalization. ISSAC 2016.
With Léo Ducas.

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

Efficient Identity-Based Encryption over NTRU Lattices. Asiacrypt 2014.
With Léo Ducas and Vadim Lyubashevsky.

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

Invited and conference talks

Fast Fourier Orthogonalization

- 05/2016: Cryptography seminar, Rennes I University.
- 03/2016: Algorithmics seminar, Caen University.
- 01/2016: Lattice Meetings, École Normale Supérieure.
- 10/2015: “Journées C2”, La Londe-les-Maures.

Gaussian Sampling in Lattice-based Cryptography

- 03/2016: Cryptology seminar, Caen University.

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

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

Efficient Identity-Based Encryption over NTRU Lattices

- 12/2014: Asiacrypt, Kaohsiung.
- 10/2014: Cryptography seminar, Rennes I University.
- 03/2014: “Journées C2”, les Sept Laux.

All my publications and talks can be found on my website. This is also the case for associated implementations, my PhD thesis, internships reports, etc.

References

Name	Function	E-mail address
◦Éric Garrido	◦Team leader	◦eric•garrido↺thalesgroup•com
◦Vadim Lyubashevsky	◦Thesis director	◦vad↺zurich•ibm•com
◦David Pointcheval	◦Former team leader	◦david•pointcheval↺ens•fr