# Thomas**Prest**

Cryptography engineer and researcher


## Contact

prest↺ens•fr

## Web & Git

tprest.github.io
github.com/tprest


## Scientific Skills

Cryptology, Algorithmics, Mathematics

## Programming

C/C++, Python, Magma, CAML

## Programming Tools

Valgrind, SVN/Git, Doxygen, Gcov, Klocwork

## Operating Systems

Unix, Windows

## Languages

French, English

## Layout Tools

Latex, Beamer, Office Suite, HTML/CSS

## Miscellaneous

My top 100 movies

## Experience

01/16 - Now **Cryptography engineer** Thales Communications & Security, Gennevilliers, FR
Writing of cryptographic specifications, assistance to development teams, research, scientific reports for external clients, development.

10/12 - 12/15 **PhD thesis** Thales and École Normale Supérieure, FR
*Gaussian Sampling in Lattice-Based Cryptography*. Directed by Vadim Lyubashevsky (ÉNS) and Sylvain Lachartre (Thales).

04/12 - 09/12 **Graduation internship** Thales Communications & Security, Colombes, FR
*Development of a cryptographic library*. Directed by Sylvain Lachartre.

06/10 - 07/10 **Mid-graduate internship** INRIA, "CARAMEL" team, Nancy, FR
*Polynomial selection for the NFS sieve*. Directed by Paul Zimmermann.

06/09 - 07/09 **Bachelor internship** Mathematics institute of Jussieu, Paris, FR
*Elliptic curves & 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). Major: maths, minor: computer science.

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

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

## Publications

A complete list can be found either on my website (`tprest.github.io`) or on DBLP (`dblp.uni-trier.de/pers/hd/p/Prest:Thomas`).

## 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 |