

ThomasPrest

Cryptography researcher

Contact

thomas•prest
📧 pqshield•com

Web & Git

tprest.github.io
pqshield.com
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

10/18 - Now **Senior cryptography researcher** PQShield, Oxford, UK
Research, consulting.

01/16 - 10/18 **Cryptography engineer** Thales, Gennevilliers, FR
Research, consulting, development, project management.

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, Colombes, FR
Development of a cryptographic library. Directed by Sylvain Lachartre.

06/10 - 07/10 **Mid-graduate internship** INRIA, "CAMEL" 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 or on DBLP.

References

Name	Function	E-mail address
• Ali El Kaafarani	• CEO	• elkaafarani 📧 pqshield • com
• David Pointcheval	• Former team leader	• david•pointcheval 📧 ens • fr