

## Jerome MILAN

<http://www.lix.polytechnique.fr/Labo/Jerome.Milan/>

Téléphone : <voir page web>

E-mail : <voir page web>

Adresse : <voir page web>

Nationalité française

### Objectif

Trouver un emploi d'ingénieur d'études dans un département de recherche et développement, dans le domaine de la cryptologie ou de la sécurité des systèmes d'information

### Domaines de compétences

- **Cryptologie**

*Cryptosystèmes à clés secrète et publique, cryptanalyse, stéganographie et codage de l'information*

- **Sécurité des systèmes informatiques**

*Sécurisation locale et en réseau, sécurité des cartes à puces, architectures PKI*

- **Génie logiciel**

*Motifs de conception, gestion de projet, contrôle d'assurance qualité, gestion des risques*

- **Physique subatomique**

*Physique nucléaire et physique des particules, mécanique quantique et statistique*

## Expérience professionnelle

- 2005 - présent: **Ingénieur**  
Equipe cryptologie du Laboratoire d'Informatique de l'Ecole polytechnique (LIX), PALAISEAU, FRANCE. Sujets d'études :
- factorisation d'entiers
  - cryptographie dans le contexte des réseaux ad hoc
  - couplages sur les courbes elliptiques

## Formation en informatique

- 2003-2004: **Master Mathématiques et Informatique**  
**Mention: Cryptologie, sécurité et codage de l'information**  
Université Joseph FOURIER, GRENOBLE
- 2002-2003: **DESS Génie Informatique**  
**Option: Systèmes répartis et réseaux**  
Université Joseph FOURIER, GRENOBLE

## *Stages*

- 03-09/2004: **Laboratoire des Images et des Signaux, CNRS**  
Analyse stéganographique d'images numériques par classifieurs
- 01-09/2003: **Laboratoire TIMC, Institut d'Informatique et de Mathématiques Appliquées de Grenoble (IMAG)**  
Conception d'une plate-forme de fédération de données médicales
- 01-09/2002: **Laboratoire Leibniz, ENS d'Informatique et de Mathématiques Appliquées de Grenoble (ENSIMAG)**  
Etude théorique des états enchevêtrés de l'informatique quantique

## Formation en physique

- 1998-1999: **DEA Physique de la matière et du rayonnement**  
**Spécialité: Physique nucléaire et physique des particules**  
Université Joseph FOURIER, GRENOBLE

## *Stages*

- 03-07/1998: **Laboratoire d'Annecy-le-Vieux de Physique des Particules**  
Influence de la fonction de transfert de l'interféromètre VIRGO sur un algorithme de recherche de coalescences d'étoiles binaires
- 07-09/1997: **Institut des Sciences Nucléaires de Grenoble (ISN)**  
Etude de faisabilité d'une caméra gamma à Xéon liquide pour l'imagerie médicale

## Expériences internationales

- 2000-2001: **Université de New York à Stony Brook**  
**Groupe de chimie nucléaire**  
Etude du flot elliptique sur l'expérience PHENIX au Relativistic Heavy Ion Collider du Brookhaven National Laboratory
- 1997-1998: **Université de Californie à Los Angeles**  
Maîtrise de Physique effectuée en échange dans le cadre du programme "Education Abroad Program"

## Compétences techniques

- Systèmes:** UNIX (OSF1 v4, Solaris), GNU/Linux (Red Hat, Debian), Mac OS X, OpenVMS 7, Windows NT4/2000
- Langages:** C/C++, Objective-C, Java, Ada 95, Fortran 77, Oracle SQL, Prolog, Perl, principaux shells UNIX, assembleur SPARC, HTML, Javascript
- Logiciels:** *Applications scientifiques:*  
Maple, PAW, ROOT, Octave  
*Applications bureautiques:*  
L<sup>A</sup>T<sub>E</sub>X, OpenOffice.org, MS Word, MS Powerpoint

## Divers

- Langues:** Anglais courant (deux ans passés aux Etats-Unis)  
Espagnol rudimentaire