Cyril GUYOT
Lotissement Carrot Chavanne
42400 SAINT CHAMOND
26 ans – Marié
Nationalité française

+33(0) 6 73 33 27 74
cyril.guyot@centraliens.net

Responsable R&D en Sécurité IT

Spécialiste en Cryptographie

Formation

1999 – 2001 **Masters of Science** en Mathématiques - Université de Toronto.
Thèse sur les algorithmes de segmentation de données utilisant des critères d'entropie.

1997 – 1999 **Ingénieur de l'Ecole Centrale de Paris**, option Mathématiques Appliquées.
Projet de deuxième année sur la simulation logicielle des flux de trafic urbains.

1995 – 1997 Classe préparatoire **MP*(3/2)** - Lycée Claude Fauriel (Saint Etienne).

– 1995 Bac S (spécialité mathématiques). **Mention Très Bien** - Lycée Claude Lebois (Saint Chamond)

1999 – Participation à de nombreuses conférences en mathématiques et en cryptographie.

Expérience Professionnelle

2002 – 2005 **Kasten Chase Applied Research Ltd. - Mississauga/Toronto**
SSII(70 personnes), spécialisée dans la sécurité des systèmes de stockage et la protection des données. Certifiée ISO 9001. http://www.kastenchase.com
Architecte en Cryptographie Expérimenté (Senior Cryptographic Architect), Directeur du groupe « Performance et Cryptographie » (8 personnes), Membre du groupe de Direction Technologique de l'entreprise (CTO)

Réalisations
- Architecture des produits en matière de sécurité.
- Management d'une équipe de 8 développeurs/mathématiciens.
- Design de produits software et hardware.
- Définition de stratégies de développement à long terme.
- Recherche et développement en cryptographie, développement de standards.
- Veille technologique en sécurité des réseaux locaux et des réseaux de stockage.

2001 – 2002 **Karthika Technologies Inc. - Toronto**
Start-up canadienne spécialisée dans la cryptographie. Effectif: 5 personnes en 2001, 25 personnes en 2002 lors de l'acquisition par Kasten Chase Applied Research Ltd.
Mathématicien / Développeur

Réalisations
- Design et implémentations de logiciels cryptographiques
- Recherche en cryptographie
- Administration système

1999 – 2001 **The Fields Institute – Université de Toronto. - Toronto**
Centre de recherche en mathématiques, 70 chercheurs. http://www.fields.utoronto.ca
Assistant administrateur système à temps partiel.
Sécurisation du réseau (60 stations de travail, 5 serveurs).

1999 – 2001 **Enseignant assistant à l'Université de Toronto - Toronto**
Cours de mathématiques de deuxième année undergraduate (DEUG).

Eté 1998 Stage de 6 semaines à Aberdeen (Ecosse) et à North Hoy (Iles Orcades) en tant qu'assistant gardien dans une réserve ornithologique.

Publications

C. Guyot, V.M. Patankar, *Multiple doubling algorithms for hyperelliptic Jacobians of genus 3*, en cours de rédaction

C. Guyot, K. Kaveh, V.M. Patankar, *Explicit algorithms for the arithmetic on hyperelliptic Jacobians of genus 3*, 2004, Journal of the Ramanujan Mathematical Society, Juin 2004.

C. Guyot, C. Kent, *IEEE-P1619 standard – LRW-AES*, 2004, Proceedings of IEEE-P1619.

I.F. Blake, C. Guyot, C. Kent, V.K. Murty, *Encryption of stored data in networks: analysis of a tweaked block cipher*, 2003, Proceedings of IEEE-P1619.

Langues

Français	Langue maternelle.
Anglais	Bilingue; 5 ans de vie à Toronto.
Allemand	Bon niveau; 8 ans d'études.
Espagnol	Bonne compréhension écrite et orale; 2 ans d'études.
Polonais	Débutant; 4 ans de pratique.

Connaissances Personnelles

OS	- GNU/Linux (maîtrise de l'architecture du noyau et de l'administration). - Connaissance approfondie de Solaris, AIX, des Unix BSD, Windows 2000, XP, 2003, HP-UX, WinCE/Windows Mobile 2003, RIMOS, PalmOS, Mac OS X
Réseaux	- Réseaux locaux (Ethernet) et réseaux de stockage (SAN/Fiber Channel) - Bas niveau:IP, TCP, UDP, ICMP, Haut niveau: HTTP, DNS, SMTP, DHCP, NFS
Programmation	- Bas niveau : assembleur x86 (maîtrisé), sparc32, sparc64, arm, ppc (bon niveau). - Haut niveau : C (excellente maîtrise), C++, Java, Common LISP, Scheme. - Langages de script : shell POSIX, sed, awk, Python, PHP.
Administration	- 7 ans d'expérience en administration Unix et Windows. - Firewall, détection d'intrusions, audits - Veritas, Legato, Tivoli Storage Manager
Bases de données	- MySQL, PostgreSQL
Autres	- Calcul formel: Maple, Mathematica, Pari-GP, NTL - Langages de mise en page : LaTeX2e, MathML, HTML, XHTML, CSS.
Standards	- FIPS xxx, Common Criteria EALxx, ANSI X9.xx, IEEE P1363, P1619, RSA PKCS #x, - Membre de l'IEEE

Centres d'Intérêts

Musique	Clarinette. Musique classique indienne.
Sports régionaux.	Tennis de table: **Vainqueur du Challenge Centrale Lyon** et de nombreux trophées
	Ski et randonnée en montagne.
Divers	Astronomie. Photographie: http://www.zoy.org/~cyril/gallery.

Références disponibles sur demande

Pour un CV plus détaillé: http://www.zoy.org/~cyril/CV/CV_FR_long.pdf
Pour un CV en anglais: http://www.zoy.org/~cyril/CV/CV_EN_short.pdf