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. Accomplie sous la supervision de I.M. Sigal.

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.
Notamment:
- conférences ECC à Waterloo, Canada et à Essen, Allemagne
- conférence Certicom à Washington, USA
- conférence PIMS à Edmonton, Canada
- conférences diverses au Fields Institute, Toronto, Canada

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.
  - ➔ *Spécification et implémentation d'une bibliothèque de cryptographie certifiée FIPS-140-2 (niveau 2).*
  - ➔ *Design de protocoles d'authentification afin de sécuriser les réseaux de stockage SAN. (Certification EAL4+)*
- Management d'une équipe de 8 développeurs/mathématiciens.
- Design de produits software et hardware.
  - ➔ *Design et implémentation d'une carte PCI-X accélératrice pour AES-128/256 (circuit FPGA capable de 6Gbit/s) et compression ADLC ainsi que RSA, DSA et ECC sur processeur embarqué PPC. Implémentation de pilotes pour Windows, GNU/Linux, Solaris et AIX.*
  - ➔ *Optimisation de l'algorithme AES pour implémentation hardware (FPGA).*
- Définition de stratégies de développement à long terme.

➔ *Mise au point des « Development Roadmap » pour la section R&D du groupe.*

- Recherche et développement en cryptographie, développement de standards.
  - ➔ *Recherche pour le groupe de travail IEEE-P1619 – Security in Storage. Auteur du standard et du code de référence pour LRW-AES (cryptage avec tweak).*
  - ➔ *Amélioration de l'arithmétique sur les Jacobiennes de courbes hyperelliptiques de genre 3 (environ 20% plus performant).*
  - ➔ *Recherche sur les courbes hyperelliptiques: IBE (Identity-based encryption) et systèmes cryptographiques basés sur les couplages (Weil, Tate).*

- Veille technologique en sécurité des réseaux locaux et des réseaux de stockage.
  - ➔ *Auteur de publications internes ayant trait à la sécurité des réseaux*

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
  - ➔ *Spécification et implémentation d'une bibliothèque de cryptographie (ECC, RSA, AES, DES, SkipJack, HMAC, ...) haute-performance extrèmement portable (Trusted Solaris (espace utilisateur et noyau), AIX (ibid.), Linux (ibid.), Windows (ibid.), WinCE, RIMOS, PalmOS et BIOS (x86).*
  - ➔ *Audit approfondie de code source et recherche de vulnérabilités.*
- Recherche en cryptographie
  - ➔ *Recherche d'algorithmes efficaces d'arithmétique dans un corps fini, et sur une courbe elliptique.*
- Administration système
  - ➔ *Administration d'un parc de 30 serveurs et stations de travail (Unix, Windows)*

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.

Réalisations:

- Sécurisation du réseau (60 stations de travail, 5 serveurs).
- Expert GNU/Linux
- Veille technologique

1999 – 2001 **Enseignant assistant à l'Université de Toronto - Toronto**

Cours de 2ème année undergraduate (DEUG) sur les Équations Différentielles Partielles.

Réalisations:

- Enseignement des TDs
- Correction des examens du cours d'Equations Différentielles Partielles.

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

Systèmes d'exploitation:

- GNU/Linux / x86, PPC, sparc32, sparc64
  - ➔ *Maîtrise de l'architecture du noyau et de l'administration.*
  - ➔ *Développement de pilotes Linux pour software et hardware*
  - ➔ *Développement de nombreuses applications de plus de 5000 lignes de code en espace utilisateur et espace noyau*
- Windows 95, 2000, XP, 2003
  - ➔ *Maîtrise de l'administration et connaissance approfondie de l'architecture du noyau*
  - ➔ *Développement de pilotes Windows pour software et hardware*
  - ➔ *Développement de plusieurs applications de plus de 5000 lignes de code à la fois en espace utilisateur et en espace noyau*
- Solaris (8/9/10, Trusted Solaris)
  - ➔ *Maîtrise de l'administration et bonne connaissance de l'architecture du noyau*
  - ➔ *Développement de pilotes Solaris pour software et hardware*
- FreeBSD, OpenBSD, NetBSD...
  - ➔ *Maîtrise de l'administration et bonne connaissance de l'architecture du noyau*
- WinCE/Windows Mobile 2003, RIMOS, PalmOS
  - ➔ *Design et port d'une bibliothèque de cryptographie pour Windows Mobile 2003/ARM, RIMOS/386 et PalmOS*
- HP-UX
  - ➔ *Design et port d'une bibliothèque de cryptographie pour HP-UX*
- Mac OSX
  - ➔ *Bonne connaissance de l'administration*
  - ➔ *Port d'une bibliothèque de cryptographie pour Mac OSX/PPC*

Réseaux:

- Connaissance approfondie de la structure des réseaux locaux Ethernet
  - ➔ Bas niveau: IP, TCP , UDP, ICMP, IGMP, PPP
  - ➔ Haut niveau: HTTP, DNS, SMTP, DHCP, NFS, TFTP, BOOTP
- Bonne connaissance des réseaux de stockage SAN/Fiber Channel et NAS et de leur administration

Programmation:

- Langages bas niveau
  - ➔ Assembleur x86 (maîtrisé)
  - ➔ Assembleur ppc (bon niveau)
  - ➔ Assembleur sparc32, sparc64
  - ➔ Assembleur arm
- Langages 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
- Pare-feu (netfilter, ipfilter), détection d'intrusions (snort), audits (nessus, satan)
- 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: 46, 81, 140-1, 140-2, 180, 186-2, 197
- Common Criteria EAL
- ANSI X9.31, X9.42, X9.62, X9.63
- IEEE P1363, P1619
- Membre de l'IEEE
- RSA PKCS #1, PKCS #5, PKCS #11

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). Linguistique.

Références disponibles sur demande

Pour un CV plus concis: http://www.zoy.org/~cyril/CV/CV_FR_court.pdf
Pour un CV en anglais: http://www.zoy.org/~cyril/CV/CV_EN_long.pdf