Cyril GUYOT
Lotissement Carrot Chavanne
42400 SAINT CHAMOND
26 year old – Married
French citizenship

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

IT-Security R&D Manager

Cryptography Specialist

Education

1999 – 2001 **Masters of Science** in Mathematics - University of Toronto.
Thesis on data segmentation algorithms using entropy criteria.
Supervised by I.M. Sigal

1997 – 1999 **Graduate from Ecole Centrale de Paris**, specialized in Applied Mathematics.
Second year project on software simulation of city traffic.

1995 – 1997 Preparatory class **MP*(3/2)** - Lycée Claude Fauriel (Saint Étienne).

– 1995 Bac S (specialization: mathematics). **Grade: Excellent** - Lycée Claude Lebois (Saint Chamond)

1999 – Participated in numerous conferences on cryptography and mathematics.
Most notably:
- ECC conference in Waterloo, ON, Canada and in Essen, Germany
- Certicom conference in Washington, DC, USA
- PIMS conference in Edmonton, Canada
- miscellaneous conferences in Fields Institute, Toronto, Canada

Work Experience

2002 – 2005 **Kasten Chase Applied Research Ltd. - Mississauga/Toronto**
Company(70 employees), specialized in storage systems security and data protection. ISO 9001 certified. (http://www.kastenchase.com)
Senior Cryptographic Architect, Leader of the « Cryptography Performance Group » (8 people), Member of the Office of the Chief Technological Officer (OCTO).

Achievements:

- Security architecture of products.
  - ➔ *Specification and implementation of a FIPS-140-2 (level 2) certified cryptographic library.*
  - ➔ *Design of authentication protocols to render SAN storage networks secure. (CC EAL4+ certification)*
- Management of a team of 8 developers/mathematicians.
- Hardware and software design.
  - ➔ *Design and implementation of an AES-128/256 and ADLC compression PCI-X accelerator board (FPGA design capable of a 6Gbit/s throughput). Embedded PPC is used for RSA, DSA and ECC. Implementation of Windows, GNU/Linux, Solaris and AIX drivers.*
  - ➔ *AES algorithm optimization for hardware FPGA implementation.*
- Creation of long-term development strategies.
  - ➔ *Production of the Development Roadmap for the R&D department.*
- Research and development in cryptography; authoring of standards..

- ➔ *Research for the IEEE-P1619 working group on Security in Storage. Author of the standard and of the reference implementation for LRW-AES (encryption with tweak).*
- ➔ *Improvement of the arithmetics on Jacobians of genus 3 hyperelliptic curves (20% faster).*
- ➔ *Research on hyperelliptic curves: IBE (Identity-based encryption) and pairing-based cryptographic systems (Weil, Tate).*

- Technological monitoring of security of local networks and storage networks..
  - ➔ *Author of internal white papers on security of networks and cryptography.*

2001 – 2002 **Karthika Technologies Inc. - Toronto**
Canadian start-up specialized in cryptography. Team: 5 employees in 2001, 25 in 2002 when acquired by Kasten Chase Applied Research Ltd.
Mathematician / Developer

Achievements:

- Design and implementation of cryptographic software.
  - ➔ *Specification and implementation of a high-performance, extremely portable cryptographic software library. (ECC, RSA, AES, DES, SkipJack, HMAC...) for Trusted Solaris (user and kernel space), AIX (ibid.), Linux (ibid.), Windows (ibid.), WinCE, RIMOS, PalmOS and BIOS (x86).*
  - ➔ *Source code audit and security vulnerability testing.*
- Research in cryptography.
  - ➔ *Study of efficient algorithms for arithmetic on finite fields and elliptic curves.*
- System administration.
  - ➔ *Administration of 30 Unix and Windows servers and workstations.*

1999 – 2001 **The Fields Institute – University of Toronto. - Toronto**
Centre for mathematical research: 70 researchers (http://www.fields.utoronto.ca/).
Part-time assistant system administrator.

Achievements:

- Local network securization (60 workstations, 5 servers).
- GNU/Linux expert.
- Technological monitoring.

1999 – 2001 **Teaching assistant at the University of Toronto - Toronto**
Second-year undergraduate Partial Differential Equations course.

Achievements:

- Teaching of TAs
- Correction of examinations.

Summer 1998 Six-weeks placement in Aberdeen (Scotland) and in North Hoy(Orkney Islands) as an Assistant Warden in an ornithological reserver.

Publications

C. Guyot, V.M. Patankar, *Multiple doubling algorithms for hyperelliptic Jacobians of genus 3*, in progress.
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, June 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.

Languages

French	Native language.
English	Bilingual; spent 5 years in Toronto.
German	Good level; 8 years of study.
Spanish	Good written and oral comprehension; 2 years of study.
Polish	Four years of on-and-off study.

Personal Knowledge

OS:

- GNU/Linux / x86, PPC, sparc32, sparc64
  - ➔ *Kernel architecture and administration well-mastered.*
  - ➔ *GNU/Linux software and hardware driver development.*
  - ➔ *Development of numerous applications larger than 5000 lines of code both in user space and kernel space.*
- Windows 95, 2000, XP, 2003
  - ➔ *Administration well-mastered and good knowledge of the kernel architecture.*
  - ➔ *Windows software and hardware driver development.*
  - ➔ *Development of several applications larger than 5000 lines of code, both in user space and kernel space.*
- Solaris (8/9/10, Trusted Solaris)
  - ➔ *Administration well-mastered and good knowledge of the architecture of the kernel.*
  - ➔ *Solaris software and hardware driver development.*
- FreeBSD, OpenBSD, NetBSD...
  - ➔ *Administration well-mastered and good knowledge of the kernel architecture.*
- WinCE/Windows Mobile 2003, RIMOS, PalmOS
  - ➔ *Design and port of a cryptographic library for the following Oses: Windows Mobile 2003/ARM, RIMOS/386 et PalmOS*
- HP-UX
  - ➔ *Design and port of a cryptographic library for HP-UX*
- Mac OSX
  - ➔ *Good knowledge of the administration*
  - ➔ *Port of a cryptographic library for Mac OSX/PPC*

Networks:

- Excellent knowledge of the structure of Ethernet local networks.
  - ➔ Low level: IP, TCP , UDP, ICMP, IGMP, PPP
  - ➔ High level: HTTP, DNS, SMTP, DHCP, NFS, TFTP, BOOTP
- Good understanding of SAN/Fiber Channel and NAS storage networks.

Programming:

- High level languages
  - ➔ x86 assembly (well-mastered)
  - ➔ ppc assembly (good level)
  - ➔ sparc32, sparc64 assembly
  - ➔ arm assembly
- High level languages
  - ➔ C (excellent knowledge)
  - ➔ C++
  - ➔ Java
  - ➔ Common LISP, Scheme.
  - ➔ Scripting languages : POSIX shell, sed, awk, Python, PHP

Administration:

- 7 years of experience in Unix and Windows administration.
- Firewall (netfilter, ipfilter), Intrusion detection (snort), audits (nessus, satan)
- Veritas, Legato, Tivoli Storage Manager

Databases:

- MySQL
- PostgreSQL

Others:

- Computer algebra
  - ➔ Maple
  - ➔ Mathematica
  - ➔ Pari-GP, NTL
- Formatting languages
  - ➔ 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
- Member of IEEE
- RSA PKCS #1, PKCS #5, PKCS #11

Extra-Curricular Activities

Music	Clarinet. Indian classical music.
Sports	Table tennis: **Winner of the Challenge Centrale Lyon** and of numerous regional competitions.
	Ski and mountaineering.
Miscellaneous	Astronomy. Photography (http://www.zoy.org/~cyril/gallery).

References available upon request

For a more concise version: http://www.zoy.org/~cyril/CV/CV_EN_short.pdf
For a French CV: http://www.zoy.org/~cyril/CV/CV_FR_long.pdf