

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.
- 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.

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.
 - Management of a team of 8 developers/mathematicians.
 - Design of hardware and software products.
 - Creation of long-term development strategies.
 - Research and development in cryptography, authoring of standards.
 - Author of white papers on local network and storage network security.

- 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
 - Research in cryptography
 - System administration

- 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.
Securization of the network (60 workstations, 5 servers).

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

- 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

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

Personal Knowledge

OS	- GNU/Linux (kernel architecture and administration well-mastered). - Excellent knowledge of Solaris, AIX, BSDs, Windows 2000, XP, 2003, HP-UX, WinCE/Windows Mobile 2003, RIMOS, PalmOS, Mac OS X
Networks	- Local networks (Ethernet) and storage networks (SAN/Fiber Channel) - Low level:IP, TCP, UDP, ICMP, High level: HTTP, DNS, SMTP, DHCP, NFS
Programming	- Low level : x86 assembly (well-mastered), sparc32, sparc64, arm, ppc (good level). - High level : C (excellent knowledge), C++, Java, Common LISP, Scheme. - Scripting languages : POSIX shell, sed, awk, Python, PHP.
Administration	- 7 years of Unix and Windows administration. - Firewall, intrusion detection, audits - Veritas, Legato, Tivoli Storage Manager
Databases	- MySQL, PostgreSQL
Miscellaneous	- Computer algebra: Maple, Mathematica, Pari-GP, NTL - Formatting languages : LaTeX2e, MathML, HTML, XHTML, CSS.
Standards	- FIPS xxx, Common Criteria EALxx, ANSI X9.xx, IEEE P1363, P1619, RSA PKCS #x, - Membre of IEEE

Extra-Curricular Activities

Music	Clarinet. Indian classical music.
Sports competitions.	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