

Thomas PORNIN
2977 rue de Deschambault
Québec G1W 1B4
Québec – Canada
Tel: +1 (418) 977-7531
<pornin@bolet.org>

PROFESSIONAL EXPERIENCE

*since
September 2001*

Co-founder of Cryptolog International

- conducted high-level consulting in cryptography
- lead PKI-related software development projects
- developed new patented protocols

*August 1999
to November 2000*

Military service and internship at the French Ministry of Interior (confidential work)

*April
to July 1996*

Internship at the cryptography team of Gemplus (now Gemalto)

- worked on the optimization of RSA algorithm implementations
- developed new signature and authentication algorithms

*June and
July 1995*

Internship at the “Institut d’Électronique Fondamentale” (Paris XI University)

- designed and implemented low-level image processing functions on a parallel SIMD computer

EDUCATION

*September 1996
to August 2001*

PhD in cryptography at “Laboratoire d’Informatique de l’ÉNS” (Paris)

- designed automatic tools of optimization of symmetric cryptography algorithms on software architectures
- implemented symmetric cryptography algorithms on FPGA chips
- worked on the cryptanalysis of the A5/1 cipher (GSM security)

July 1996

DEA (\approx 3rd year of Master Degree) “Algorithmique” (generic algorithmic studies, specialization in cryptography) of Paris VI University

*September 1994
to September 1998*

Scholarship at the École Normale Supérieure, rue d’Ulm, Paris

PUBLICATIONS

T. Pornin, *Optimal Resistance Against the Davies and Murphy Attack*, Advances in Cryptology – ASIACRYPT’98, LNCS 1514, Springer-Verlag, 2000.

H. Gilbert, M. Girault, P. Hoogvorst, F. Noilhan, T. Pornin, G. Poupard, J. Stern, S. Vaudenay, *Decorrelated Fast Cipher: an AES Candidate*, Proceedings of the First Advanced Encryption Standard (AES) Candidate Conference, 1998.

O. Baudron, H. Gilbert, L. Granboulan, H. Handschuh, R. Harley, A. Joux, P. Nguyen, F. Noilhan, D. Pointcheval, T. Pornin, G. Poupard, J. Stern, S. Vaudenay, *DFC Update*, Proceedings of the Second Advanced Encryption Standard (AES) Candidate Conference, 1999.

O. Baudron, H. Gilbert, L. Granboulan, H. Handschuh, A. Joux, P. Nguyen, F. Noilhan, D. Pointcheval, T. Pornin, G. Poupard, J. Stern, S. Vaudenay, *Report on the AES Candidates*, Proceedings of the Second Advanced Encryption Standard (AES) Candidate Conference, 1999.

T. Pornin, J. Stern, *Software-Hardware Trade-offs*, Cryptographic Hardware and Embedded Systems – CHES 2000, LNCS 1965, Springer-Verlag, 2000.

T. Pornin, *Transparent Harddisk Encryption*, Cryptographic Hardware and Embedded Systems – CHES 2001, LNCS 2162, Springer-Verlag, 2000.

T. Pornin, *Implantation et optimisation des primitives cryptographiques*, PhD thesis, defended on October 25th, 2001.

D. Catalano, D. Pointcheval, T. Pornin, *IPAKE: Isomorphisms for Password-based Authenticated Key Exchange*, Advances in Cryptology – CRYPTO 2004, LNCS 3152, Springer-Verlag, 2004.

C. Berbain, O. Billet, A. Canteaut, N. Courtois, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, H. Sibert, *SOSEMANUK, a fast software-oriented stream cipher*, Proceedings of SKEW – Symmetric Key Encryption Workshop, Network of Excellence in Cryptology ECRYPT, Aarhus, Denmark, May 26th and 27th, 2005.

C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, H. Sibert, *DECIM, a new stream cipher for hardware applications*, Proceedings of SKEW – Symmetric Key Encryption Workshop, Network of Excellence in Cryptology ECRYPT, Aarhus, Denmark, May 26th and 27th, 2005.

T. Pornin, J. P. Stern, *Digital Signatures Do Not Guarantee Exclusive Ownership*, Applied Cryptography and Network Security – ACNS 2005, LNCS 3531, Springer-Verlag, 2005.

C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, H. Sibert, *DECIM^{v2}*, Proceedings of SASC 2006 – ECRYPT Workshop on stream ciphers, Leuven, Belgium, February 2006.

D. Catalano, D. Pointcheval, T. Pornin, *Trapdoor Hard-to-Invert Group Isomorphisms and Their Application to Password-Based Authentication*, Journal of Cryptology, volume 20, number 1, Springer-Verlag, 2007.

L. Granboulan, T. Pornin, *Perfect Block Ciphers with Small Blocks*, Fast Software Encryption – FSE 2007, LNCS 4593, Springer-Verlag, 2007.

MISCELLANEOUS

- French: mother language.
- English spoken and written fluently
- Main computer languages known: C, Java, shell, Pascal, Basic, Assembly (80x86, 6809, Alpha)
- Knowledge of FPGA programming
- Strong experience in programming (15 years), system programming on Unix systems (12 years) and system administration (10 years)
- Member of the International Association for Cryptologic Research since 1997