

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

Né le 6 juin 1975 à Dreux (Eure-et-Loir, France).

## EXPÉRIENCE PROFESSIONNELLE

*depuis*  
*Septembre 2001*

### **Co-fondateur de Cryptolog International**

- consultation de haut niveau en cryptographie
- gestion de projets de développement logiciel sur les PKI
- développement de nouveaux protocoles brevetés

*Août 1999*  
*à Novembre 2000*

Service militaire et stage auprès du Ministère de l'Intérieur (sujet confidentiel)

*Avril*  
*à Juillet 1996*

Stage auprès de l'équipe cryptographique de Gemplus (maintenant Gemalto)

- optimisation de l'implémentation de RSA
- développement de nouveaux algorithmes d'authentification et de signature

*Juin et*  
*Juillet 1995*

Stage à l'Institut d'Électronique Fondamentale (Université Paris XI)

- conception et implémentation de fonctions de traitement d'images de bas niveau sur une architecture parallèle SIMD

## ÉTUDES

*Septembre 1996*  
*à Août 2001*

**Thèse de doctorat en cryptographie** au Laboratoire d'Informatique de l'ÉNS (Paris)

- conception d'outils automatiques d'optimisation d'algorithmes de chiffrement symétrique sur plateforme logicielle
- implémentation d'algorithmes de chiffrement symétrique sur FPGA
- travail sur la cryptanalyse du système A5/1 (sécurité GSM)

*Juillet 1996*

DEA « Algorithmique » de l' Université Paris VI (filiale « cryptographie »)

*Septembre 1994*  
*à Septembre 1998*

Scolarité à l'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*, thèse de doctorat, soutenue le 25 octobre 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, Danemark, 26 et 27 mai 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, Danemark, 26 et 27 mai 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<sup>v2</sup>*, Proceedings of SASC 2006 – ECRYPT Workshop on stream ciphers, Leuven, Belgique, février 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, numéro 1, Springer-Verlag, 2007.

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

## DIVERS

- Français : langue maternelle.
- Anglais écrit et parlé couramment.
- Principaux langages informatiques connus : C, Java, shell, Pascal, Basic, Assembleur (80x86, 6809, Alpha).
- Connaissance de la programmation de FPGA.
- Solide expérience en programmation (15 ans), programmation système sous Unix (12 ans) et administration réseau (10 ans).
- Membre de l'International Association for Cryptologic Research depuis 1997.