Thomas PORNIN
2977 rue de Deschambault
Québec G1W 1B4
Québec – Canada
Tel : +1 (418) 558-0148
<pornin@bolet.org>

Né en 1975 à Dreux (Eure-et-Loir, France). Citoyenneté française et canadienne.

EXPÉRIENCE PROFESSIONNELLE

depuis Janvier 2016 — **Architecte en sécurité (Desjardins)**

- conception et analyse d'infrastructures logicielles et matérielles dans une grande institution financière
- analyse et déploiement de protocoles de paiement sur architectures redondantes sécurisées
- expertise cryptographique à largeur de l'organisation

Février 2012 à Janvier 2016 — Conseiller en sécurité (CGI)

- mandaté en tant qu'architecte de sécurité
- implantation d'une solution de PKI et gestion d'identités utilisant Microsoft ADCS et FIM 2010 pour l'émission et la gestion de plusieurs milliers de cartes à puce
- développement .NET (VB et C#)
- support d'intégration de certificats et cartes à puce en environnement Microsoft (Active Directory, SSL/TLS,...)

Septembre 2001 à Février 2012 — Co-fondateur de Cryptolog International

- consultation de haut niveau en cryptographie
- gestion de projets de développement logiciel sur les PKI
- développement avancé en Java, C et Assembleur
- développement sur plateformes embarquées

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 cryptographiques

Juin et Juillet 1995 — Stage à l'Institut d'Électronique Fondamentale (Université Paris XI)

- traitement d'images sur architecture parallèle SIMD

ACTIVITÉS DE RECHERCHE

Thèse de doctorat en cryptographie au Laboratoire d'Informatique de l'École Normale Supérieure (Paris), soutenue en 2001

- 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)

Participation à des compétitions internationales de sélection d'algorithmes cryptographiques :

- AES (Advanced Encryption Standard, 1997 à 2000) : co-auteur de l'algorithme de chiffrement par blocs DFC
- eSTREAM (ECRYPT Stream Cipher Project, 2004 à 2008) : co-auteur de l'algorithme de chiffrement en flux SOSEMANUK (admis dans la liste finale)
- SHA-3 (2007 à 2012) : co-auteur de la fonction de hachage cryptographique Shabal (admise au deuxième tour)
- PHC (Password Hashing Competition, 2013 à 2015) : auteur de la fonction de hachage de mots de passe Makwa (finaliste, a obtenu une « special recognition »)

Auteur de la bibliothèque `sphlib` : implémentation optimisée de nombreuses fonctions de hachage cryptographique, en C et Java : `http://www.saphir2.com/sphlib/`

Auteur de la RFC 6979 : spécification de signatures déterministes compatibles avec DSA et ECDSA : `http://tools.ietf.org/html/rfc6979`

Auteur de la fonction de hachage de mots de passe Makwa : conception, spécification et implémentations de référence en C et Java : `http://www.bolet.org/makwa/`

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*^{v2}, 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.

T. Pornin, *Comparative Performance Review of the SHA-3 Second-Round Candidates*, présenté à la « Second SHA-3 Candidate Conference », août 2010.

T. Pornin, *The Makwa Password Hashing Function*, soumis à la « Password Hashing Competition », février 2014 (avril 2015 pour la version 1.1).

T. Pornin, *Optimizing Makwa on GPU and CPU*, note technique soumise à la « Password Hashing Competition », mai 2015.

DIVERS

- Français : langue maternelle.
- Anglais écrit et parlé couramment.
- Solide expérience en développement (plus de 20 ans).
- Principaux langages informatiques connus : Java, C, C#, shell, Pascal, Forth, Basic, Assembleur (x86, PowerPC, ARM, MIPS, AVR, 6809, Alpha).
- Connaissance de la programmation de FPGA.
- Très bonne connaissance du protocole SSL/TLS.
- Auteur du livre *Prometheus's Brother* : `http://www.prometheusbrother.com/`