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

Born on 1975, in France. French and Canadian citizenships.

PROFESSIONAL EXPERIENCE

since January 2016

Security architect (Desjardins)

- design and security analysis of software and hardware infrastructures in a large financial institution
- analysis of payment protocols and their deployment on secured, redundant infrastructures
- enterprise-wide cryptography expertise

February 2012 to January 2016

Consultant in security (CGI)

- appointed as security architect
- deployment of a PKI and Identity Management solution using Microsoft ADCS and FIM 2010, to issue and manage thousands of smart cards
- .NET development (VB and C#)
- integration of certificates and smart cards in a Microsoft environment (Active Directory, SSL/TLS,...)

September 2001 to February 2012

Co-founder of Cryptolog International

- conducted high-level consulting in cryptography
- lead PKI-related software development projects
- advanced development in Java, C and Assembly
- development on embedded platforms

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 optimizations 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

RESEARCH ACTIVITIES

PhD thesis in cryptography at the "Laboratoire d'Informatique de l'École Normale Supérieure" (Paris), defended in 2001

- 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)

Participation to international competitions for the selection of cryptographic algorithms:

- AES (Advanced Encryption Standard, 1997 to 2000): co-author of the block cipher DFC
- eSTREAM (ECRYPT Stream Cipher Project, 2004 to 2008): co-author of the stream cipher SOSEMANUK (admitted in the final portfolio)
- SHA-3 (2007 to 2012): co-author of the cryptographic hash function Shabal (selected for second round)
- PHC (Password Hashing Competition, 2013 to 2015): author of the password hashing function Makwa (finalist, was awarded a "special recognition")

Author of the `sphlib` library: optimized implementations of many cryptographic hash functions, both in C and Java: `http://www.saphir2.com/sphlib/`

Author of RFC 6979: Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA): `http://tools.ietf.org/html/rfc6979`

Author of the password hashing function Makwa: design, specification and reference implementations in C and 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*, 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, Danemark, May 26 and 27, 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, May 26 and 27, 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, 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.

T. Pornin, *Comparative Performance Review of the SHA-3 Second-Round Candidates*, presented at the Second SHA-3 Candidate Conference, August 2010.

T. Pornin, *The Makwa Password Hashing Function*, submitted to the Password Hashing Competition, February 2014 (Appril 2015 for version 1.1).

T. Pornin, *Optimizing Makwa on GPU and CPU*, technical report submitted to the Password Hashing Competition, May 2015.

MISCELLANEOUS

- French: mother language.
- English fluently spoken and written.
- Strong experience in development (more than 20 years).
- Main known computer languages: Java, C, C#, shell, Pascal, Forth, Basic, Assembly (x86, PowerPC, ARM, MIPS, AVR, 6809, Alpha).
- Knowledge of FPGA programming.
- Strong knowledge of the SSL/TLS protocol internals.
- Author of the book *Prometheus's Brother*: `http://www.prometheusbrother.com/`