

Jean-Luc Beuchat

Laboratory of Cryptography and Information Security
University of Tsukuba
1-1-1 Tennodai, Tsukuba, Ibaraki, 305-8573, Japan
Phone: +81 (0)29 853 5586
Fax: +81 (0)29 861 7348
jeanluc.beuchat@gmail.com
<http://www.cipher.risk.tsukuba.ac.jp/~beuchat>

Date of birth: March 2nd, 1973
Place of birth: Vevey, Switzerland
Citizenship: Swiss

Career Path

- Since 2007 **Associate Professor**
Graduate School of Systems and Information Engineering,
University of Tsukuba,
Tsukuba, Japan
- 2006–2007 **Researcher**
Laboratory of Cryptography and Information Security,
University of Tsukuba,
Tsukuba, Japan
- 2006 **Hardware Designer and Developer**
Cinetis SA
Martigny, Switzerland
- 2003–2005 **Researcher**
(Swiss National Science Foundation Fellowship for Advanced Researchers)
Arénaire project-team, Laboratoire de l'Informatique du Parallélisme,
École Normale Supérieure de Lyon,
Lyon, France
- 2001–2003 **Postdoctoral Fellow**
(Swiss National Science Foundation Fellowship for Prospective Researchers)
Arénaire project-team, Laboratoire de l'Informatique du Parallélisme,
École Normale Supérieure de Lyon,
Lyon, France
- 1997–2001 **Research Assistant and Ph.D. Candidate**
Logic Systems Laboratory,
Swiss Federal Institute of Technology at Lausanne,
Lausanne, Switzerland
- 1996–1997 **Internship Student**
Dalle Molle Institute for Perceptual Artificial Intelligence,
Martigny, Switzerland
- 1995 **Internship Student**
Dalle Molle Institute for Perceptual Artificial Intelligence,
Martigny, Switzerland

Short-Term Invitations

- 2010 Computer Science Department, Centro de Investigación y de Estudios Avanzados del IPN, México City, México (2 weeks)
- 2008 Computer Science Department, Centro de Investigación y de Estudios Avanzados del IPN, México City, México (2 weeks)
- 2005 ATIPS and CISaC laboratories, University of Calgary, Calgary, Canada (1 month)
- 2004 ERMETIS, Département des sciences appliquées, Université du Québec à Chicoutimi, Chicoutimi, Canada (2 weeks)

Education

- 2009 **Qualification for applying to professor positions in France**
French National Board of Universities (CNU), Section 27 (computer science)
- 1997–2001 **Ph.D. in Computer Science and Engineering**
Swiss Federal Institute of Technology at Lausanne
Lausanne, Switzerland
- 1992–1997 **Diploma in Computer Science**
Swiss Federal Institute of Technology at Lausanne
Lausanne, Switzerland

Languages

- French Native speaker
- German Basic notions
- English Fluent
- Japanese Basic notions

Awards

- 2009 **Best Paper Award** with J. Detrey, N. Estibals, E. Okamoto, and F. Rodríguez-Henríquez at **CHES 2009** for the paper *Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers*.
- 2007 **Best Paper Award** with N. Brisebarre, J. Detrey, and E. Okamoto at **CHES 2007** for the paper *Arithmetic Operators for Pairing-Based Cryptography*.
- 1997 **NCR Golden Mouse Award, Prix de la Société Académique du Valais, and Anaheim Foundation Award**
Received for the diploma thesis *Reconnaissance de caractères manuscrits à l'aide de réseaux neuromimétiques* (Handwritten Digit Recognition Using Artificial Neural Networks).
- 1997 **Swiss Informaticians Society Award**
Awards the second best diploma.

Current Research Interests

Public Key Cryptography

Elliptic curve cryptography, pairing-based cryptography, post-quantum cryptography, identity-based encryption, digital signature.

Cryptographic Hardware

Hardware architectures for public key and symmetric cryptography, reconfigurable hardware for cryptography, cryptography for pervasive computing (sensor networks, RFID, etc.), attacks against implementations and countermeasures.

Cryptographic Software

Software implementations for embedded processors, multi-core libraries for cryptography.

Computer Arithmetic

Number systems, finite field arithmetic, on-line arithmetic, residue arithmetic and conversion algorithms, arithmetic processor design, elementary function evaluation.

Computer Architecture

Instruction set architectures, instruction-level parallelism, multiprocessors, pipelining, hardware design languages.

Research Activities

- Since 2006 **Cryptographic Pairings over Elliptic and Hyperelliptic Curves**
Algorithmic improvements (pairing computation, tower field arithmetic, etc.) and proposal of the fastest hardware and software architectures for the computation of the cryptographic Tate pairing in characteristics two and three.
In collaboration with N. Brisebarre, J. Detrey, N. Estibals, E. López-Trejo, L. Martínez-Ramos, S. Mitsunari, E. Okamoto, F. Rodríguez-Henríquez, M. Shirase, and T. Takagi.
- 2004–2005 **RN-Codings**
Study of radix- β signed-digit representations of numbers for which rounding to the nearest is always identical to truncation.
In collaboration with J.-M. Muller.
- 2003–2008 **Modular Multiplication on FPGA**
Design of modular multipliers based on Horner's rule for FPGA devices.
In collaboration with J.-M. Muller.
- 2003–2006 **Code-Based Cryptography**
Development of hardware operators for cryptographic applications based on the algebraic theory of codes.
In collaboration with the LIRMM (Montpellier, France) and the Codes project (INRIA Rocquencourt, Paris, France).
- 2002–2005 **Hardware Operators for Elliptic Curve Cryptography**
Development of hardware operators for cryptographic applications on FPGAs. The project focused in particular on problems related to finite fields and elliptic curves.
In collaboration with the LIRMM (Montpellier, France) and the GTA team (Université Montpellier II, France).
- 2001–2002 **Multiplier-Based Arithmetic Operators**
Design of large multipliers and SRT dividers based on the multiplier blocks embedded in several FPGA families.
In collaboration with A. Tisserand.
- 1999–2002 **On-Line Arithmetic**
Design of algorithms and FPGA implementation for the on-line computation of arithmetic, algebraic, and elementary functions.

1997–1999 **Hardware Implementation of Artificial Neural Networks**
Investigation of hardware-friendly training and pruning algorithms for multilayer perceptrons.

Development

Since 2009 **Multi-Core Library for the Cryptographic Tate Pairing**
Design of a fast software library for the computation of the Tate pairing on supersingular elliptic curves.

In collaboration with E. López-Trejo, L. Martínez-Ramos, S. Mitsunari, and F. Rodríguez-Henríquez.

Since 2007 **Hardware Accelerators for Pairing-Based Cryptography**
VHDL library of parametrizable coprocessors for the cryptographic Tate pairing in characteristics two and three.

In collaboration with J. Detrey and N. Estibals.

2006–2008 **NEDO “Pairing Lite” Project**
Contribution to the first ASIC implementation of the η_T pairing in characteristic three: study of arithmetic over \mathbb{F}_{3^m} and $\mathbb{F}_{3^{6m}}$, design of arithmetic coprocessors.

Industrial project supported by the New Energy and Industrial Technology Development Organization (NEDO), Japan.

2006 **Digitization of Super 8 Films**
Design of an innovative system to transfer Super 8 films to DVD.

Industrial project with Cinetis SA, Martigny, Switzerland.

2004–2006 **VHDL Library of Arithmetic Operators**
Design of a GPL library of integer and modular operators for cryptographic applications.

1999–2000 **CryptoBooster**
Design and FPGA implementation of a modular cryptographic processor.
Industrial project with Lightning Ltd., Lausanne, Switzerland. Project leader.

Recent Collaborations

Since 2009 Cybozu Labs, Inc., Tokyo, Japan

Since 2009 Intel Guadalajara Design Center, México

Since 2008 CACAO project-team, INRIA Nancy–Grand Est, Nancy, France

Since 2008 Computer Science Department, Centro de Investigación y de Estudios Avanzados del IPN, México City, México

Since 2006 Arénaire project-team, École Normale Supérieure de Lyon, Lyon, France

2006–2008 FDK Corporation, Japan.

2006–2008 School of Systems Information Science, Future University–Hakodate, Hakodate, Japan

2006–2008 Graduate School of Information Security, Institute of Information Security, Yokohama, Japan

List of Publications

International Journals

1. Jean-Luc Beuchat, Hiroshi Doi, Kaoru Fujita, Atsuo Inomata, Piseth Ith, Akira Kanaoka, Masayoshi Katouno, Masahiro Mambo, Eiji Okamoto, Takeshi Okamoto, Takaaki Shiga, Masaaki Shirase, Ryuji Soga, Tsuyoshi Takagi, Ananda Vithanage, and Hiroyasu Yamamoto. *FPGA and ASIC Implementations of the η_T Pairing in Characteristic Three*. Computers and Electrical Engineering, 36(1):73–87, 2010.
2. Jean-Luc Beuchat and Jean-Michel Muller. *Automatic Generation of Modular Multipliers for FPGA Applications*. IEEE Transactions on Computers, 57(12):1600–1613, 2008.
3. Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, Eiji Okamoto, Masaaki Shirase, and Tsuyoshi Takagi. *Algorithms and Arithmetic Operators for Computing the η_T Pairing in Characteristic Three*. In R. Steinwandt, W. Geiselmann, and Ç.K. Koç, editors, IEEE Transactions on Computers—Special Section on Special-Purpose Hardware for Cryptography and Cryptanalysis, 57(11):1454–1468, 2008.
4. Jean-Luc Beuchat, Takanori Miyoshi, Jean-Michel Muller, and Eiji Okamoto. *Horner’s Rule-Based Multiplication over $GF(p)$ and $GF(p^n)$: A Survey*. International Journal of Electronics, 95(7):669–684, 2008.
5. Jean-Luc Beuchat and Jean-Michel Muller. *Modulo M Multiplication-Addition: Algorithms and FPGA Implementation*. Electronics Letters, 40(11):654–655, 2004.
6. Jean-Luc Beuchat and Jacques-Olivier Haenni. *Von Neumann’s 29-state Cellular Automaton: A Hardware Implementation*. IEEE Transactions on Education, 43(3):300–308, 2000.
7. Eduardo Sanchez, Moshe Sipper, Jacques-Olivier Haenni, Jean-Luc Beuchat, André Stauffer, and Andrés Perez-Urbe. *Static and Dynamic Configurable Systems*. IEEE Transactions on Computers, 48(6):556–564, 1999.

Book Chapters

1. Jean-Luc Beuchat and Arnaud Tisserand. Opérateurs arithmétiques sur circuits FPGA. In J.-C. Bajard and J.-M. Muller, editors, *Calcul et arithmétique des ordinateurs*, Traité IC2, pages 109–152, Lavoisier 2004.
2. Moshe Sipper, Eduardo Sanchez, Jacques-Olivier Haenni, Jean-Luc Beuchat, André Stauffer, and Andrés Perez-Urbe. *From configurable circuits to bio-inspired systems*. In H.-N. Teodorescu, D. Mlynek, A. Kandel, and H.J. Zimmermann, editors, *Intelligent Systems and Interfaces*, vol. 15 of Intelligent Technologies Series. Kluwer Academic Publishers, Boston, 2000.

International Conferences

1. Jean-Luc Beuchat, Emmanuel López-Trejo, Luis Martínez-Ramos, Shigeo Mitsunari, and Francisco Rodríguez-Henríquez. *Multi-core Implementation of the Tate Pairing over Supersingular Elliptic Curves*. In J.A. Garay, A. Miyaji, and A. Otsuka, editors, *Cryptology and Network Security—CANS 2009*, number 5888 in Lecture Notes in Computer Science, pages 413–432. Springer, 2009.
2. Jean-Luc Beuchat, Jérémie Detrey, Nicolas Estibals, Eiji Okamoto, and Francisco Rodríguez-Henríquez. *Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers*. In C. Clavier and K. Gaj, editors, *Cryptographic Hardware and Embedded Systems—CHES 2009*, number 5747 in Lecture Notes in Computer Science, pages 225–239. Springer, 2009. **Best Paper Award**.

3. Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, Eiji Okamoto, and Francisco Rodríguez-Henríquez. *A Comparison Between Hardware Accelerators for the Modified Tate Pairing over \mathbb{F}_{2^m} and \mathbb{F}_{3^m}* . In S.D. Galbraith and K.G. Paterson, editors, *Pairing 2008*, number 5209 in Lecture Notes in Computer Science, pages 297–315. Springer, 2008.
4. Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, and Eiji Okamoto. *Arithmetic Operators for Pairing-Based Cryptography*. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems—CHES 2007*, number 4727 in Lecture Notes in Computer Science, pages 239–255. Springer, 2007. **Best Paper Award**.
5. Jean-Luc Beuchat, Nicolas Brisebarre, Masaaki Shirase, Tsuyoshi Takagi, and Eiji Okamoto. *A Coprocessor for the Final Exponentiation of the η_T Pairing in Characteristic Three*. In C. Carlet and B. Sunar, editors, *Proceedings of WAIFI 2007*, number 4547 in Lecture Notes in Computer Science, pages 25–39. Springer, 2007.
6. Jean-Luc Beuchat, Masaaki Shirase, Tsuyoshi Takagi, and Eiji Okamoto. *An Algorithm for the η_T Pairing Calculation in Characteristic Three and its Hardware Implementation*. In P. Kornerup and J.-M. Muller, editors, *Proceedings of the 18th IEEE Symposium on Computer Arithmetic*, pages 97–104, IEEE Computer Society, 2007.
7. Jean-Luc Beuchat, Takanori Miyoshi, Yoshihito Oyama, and Eiji Okamoto. *Multiplication over \mathbb{F}_{p^m} on FPGA: A Survey*. In P.C. Diniz, E. Marques, K. Bertels, M.M. Fernandes, and J.M.P. Cardoso, editors, *Reconfigurable Computing: Architectures, Tools and Applications—Proceedings of ARC 2007*, number 4419 in Lecture Notes in Computer Science, pages 214–225. Springer, 2007.
8. Rachid Beguenane, Jean-Luc Beuchat, Jean-Michel Muller, and Stéphane Simard. *Modular Multiplication of Large Integers on FPGA*. In *Proceedings of the 39th Asilomar Conference on Signals, Systems & Computers*. IEEE Signal Processing Society, 2005.
9. Jean-Luc Beuchat and Jean-Michel Muller. *Multiplication Algorithms for Radix-2 RN-Codings and Two's Complement Numbers*. In S. Vassiliadis, N. Dimopoulos, and S. Rajopadhye, editors, *Proceedings of the 16th IEEE International Conference on Application-Specific Systems, Architectures, and Processors (ASAP 2005)*, pages 303–308. IEEE Computer Society, 2005.
10. Jean-Luc Beuchat. *FPGA Implementations of the RC6 Block Cipher*. In P.Y.K. Cheung, G.A. Constantinides, and J.T. de Sousa, editors, *Field-Programmable Logic and Applications*, number 2778 in Lecture Notes in Computer Science, pages 101–110. Springer, 2003.
11. Jean-Luc Beuchat, Laurent Imbert, and Arnaud Tisserand. *Comparison of Modular Multipliers on FPGAs*. In F.T. Luk, editor, *Advanced Signal Processing Algorithms, Architectures and Implementations XIII*, volume 5205, pages 490–498, San Diego, CA, August 2003. SPIE.
12. Jean-Luc Beuchat. *Modular Multiplication for FPGA Implementation of the IDEA Block Cipher*. In E. Depretere, S. Bhattacharyya, J. Cavallaro, A. Darte, and L. Thiele, editors, *Proceedings of the 14th IEEE International Conference on Application-Specific Systems, Architectures, and Processors (ASAP 2003)*, pages 412–422. IEEE Computer Society, 2003.
13. Jean-Luc Beuchat. *Some Modular Adders and Multipliers for Field Programmable Gate Arrays*. Proceedings of the 17th International Parallel & Distributed Processing Symposium. IEEE Computer Society, 2003.
14. Jean-Luc Beuchat and Arnaud Tisserand. *Small Multiplier-based Multiplication and Division Operators for Virtex-II Devices*. In M. Glesner, P. Zipf, and M. Renovell editors, *Field-Programmable Logic and Applications—Reconfigurable Computing Is Going Mainstream*, number 2438 in Lecture Notes in Computer Science, pages 513–522. Springer, 2002.

15. Jean-Luc Beuchat and Eduardo Sanchez. *An On-Line Arithmetic-Based Reconfigurable Neuroprocessor*. In J. Rolim, editor, *Parallel and Distributed Processing*, number 1586 in Lecture Notes in Computer Science, pages 700–702. Springer, 1999.
16. Jean-Luc Beuchat and Eduardo Sanchez. *Using On-Line Arithmetic and Reconfiguration for Neuroprocessor Implementation*. In J. Mira and J.V. Sánchez-Andrés, editors, *Engineering Applications of Bio-Inspired Artificial Neural Networks*, number 1607 in Lecture Notes in Computer Science, pages 129–138. Springer, 1999.
17. Jean-Luc Beuchat, Jacques-Olivier Haenni, and Eduardo Sanchez. *Hardware Reconfigurable Neural Networks*. In J. Rolim, editor, *Parallel and Distributed Processing*, number 1388 in Lecture Notes in Computer Science, pages 91–98. Springer, 1998.
18. Jean-Luc Beuchat and Eduardo Sanchez. *A Reconfigurable Neuroprocessor with On-chip Pruning*. In L. Niklasson and M. Bodén and T. Ziemke, editors, *ICANN 98, Perspectives in Neural Computing*, pages 1159–1164. Springer, 1998.

National Journals

1. Jean-Luc Beuchat and Arnaud Tisserand. *Évaluation polynomiale en-ligne de fonctions élémentaires sur FPGA*. *Technique et Science Informatiques*, 23(10):1247–1267, 2004.
2. Jean-Luc Beuchat, Jacques-Olivier Haenni, Hector Fabio Restrepo, Christof Teuscher, Francisco J. Gómez, and Eduardo Sanchez. *Approches matérielles et logicielles de l'algorithme de chiffrement IDEA*. *Technique et Science Informatiques*, 21(2):203–224, 2002.
3. Jean-Luc Beuchat, Jacques-Olivier Haenni, Erik Bruchez, and Eduardo Sanchez. *Une plate-forme pour le développement et le prototypage de systèmes reconfigurables*. *Informatik/Informatique*, (1):21-24, 1998.

National Conferences

1. Vithanage Ananda, 猪俣 敦夫, 岡本 栄司, 岡本 健, 金岡 晃, 上遠野 昌良, 志賀 隆明, 白鷗 政明, 曾我 竜司, 高木 剛, 土井 洋, 藤田 香, Jean-Luc Beuchat, 満保 雅浩, and 山本 博康. *ペアリング演算ASICの開発*. In *Proceedings of CSEC 2008*, pages 31–35. 2008.
2. Jean-Luc Beuchat and Jean-Michel Muller. *RN-codes : algorithmes d'addition, de multiplication et d'élévation au carré*. *SympA'2005 : 10^{ème} édition du SYMPOsium en Architectures nouvelles de machines*, pages 73–84, 2005.
3. Jean-Luc Beuchat and Jean-Michel Muller. *Multiplication-addition modulaire : algorithmes itératifs et implantations sur FPGA*. In M. Auguin, F. Baude, D. Lavenier, and M. Riveill, editors, *Actes de RenPar'15, CFSE'3 et SympAAA'2003*, pages 235–242, 2003.
4. Jean-Luc Beuchat and Arnaud Tisserand. *Opérateur en-ligne sur FPGA pour l'implantation de quelques fonctions élémentaires*. In *Actes de la conférence Sympa'8-Symposium en Architectures Nouvelles de Machines*, pages 267–274, 2002.
5. Jean-Luc Beuchat, Jacques-Olivier Haenni, Christof Teuscher, Francisco J. Gómez, Hector Fabio Restrepo, and Eduardo Sanchez. *Une comparaison entre quelques implantations logicielles et matérielles de l'algorithme de chiffrement IDEA*. In *Actes de la conférence Sympa'6-Symposium en Architectures Nouvelles de Machines*, pages 25–34, 2000.
6. Jean-Luc Beuchat. *Conception d'un neuroprocesseur reconfigurable proposant des algorithmes d'apprentissage et d'élagage : une première étude*. In F. Alexandre and J.-D. Kant, editors, *Actes des journées NSI'98*, 1998.

Ph.D. and Master's Theses

1. Jean-Luc Beuchat. *Étude et conception d'opérateurs arithmétiques optimisés pour circuits programmables*. Ph.D. thesis, École Polytechnique Fédérale de Lausanne, 2001.
2. Jean-Luc Beuchat. *Reconnaissance de caractères manuscrits à l'aide de réseaux neuronniques*. Master's thesis, École Polytechnique Fédérale de Lausanne. Available as research report IDIAP-RR 97–18, Dalle Molle Institute for Perceptual Artificial Intelligence, 1997.

Unpublished Work

1. Jean-Luc Beuchat, Jérémie Detrey, Nicolas Estibals, Eiji Okamoto, and Francisco Rodríguez-Henríquez. *Fast Architectures for the η_T Pairing over Small-Characteristic Supersingular Elliptic Curves*. Cryptology ePrint Archive, Report 2009/398, 2009.
2. Nidia Cortez-Duarte, Francisco Rodríguez-Henríquez, Jean-Luc Beuchat, and Eiji Okamoto. *A Pipelined Karatsuba-Ofman Multiplier over $GF(3^{97})$ Amenable for Pairing Computation*. Cryptology ePrint Archive, Report 2008/127, 2008.
3. Jean-Luc Beuchat, Masaaki Shirase, Tsuyoshi Takagi, and Eiji Okamoto. *A Refined Algorithm for the η_T Pairing Calculation in Characteristic Three*. Cryptology ePrint Archive, Report 2007/311, 2007.
4. Jean-Luc Beuchat. *Further Comments on "Residue-to-Binary Converters Based on New Chinese Remainder Theorems"*. ArXiv:0707.3732v1, 2007.
5. Jean-Luc Beuchat. *A Family of Modulo $(2^n + 1)$ Multipliers*. LIP Research Report 2004–39, September 2004. (Also available as Inria Research Report 5316, September 2004.)
6. Jean-Luc Beuchat, Nicolas Sendrier, Arnaud Tisserand, and Gilles Villard. *FPGA Implementation of a Recently Published Signature Scheme*. LIP Research Report 2004–14, March 2004. (Also available as Inria Research Report 5158, March 2004.)
7. Jean-Luc Beuchat. *More on Modulo $2^n - 1$ Addition*. LIP Research Report 2003–14, February 2003.
8. Jean-Luc Beuchat, Christof Teuscher, Francisco J. Gómez, and Hector Fabio Restrepo. *Un premier prototype de coprocesseur cryptographique*. Rapport technique de projet CTI, 2000.

Selected Talks

1. *Une introduction à la cryptographie à clef publique*. 26^{ème} Rencontre Scientifique Francophone de Tokyo, Tokyo, Japan. October 17, 2009.
2. *Hardware Operators for Pairing-Based Cryptography*. Nara Institute of Science and Technology, Nara, Japan. October 7, 2009.
3. *Multi-core Implementation of the Cryptographic Tate Pairing*. Centre Universitaire d'Informatique, University of Geneva, Geneva, Switzerland. September 25, 2009.
4. *Hardware Operators for Pairing-Based Cryptography*.
 - Haute École d'Ingénierie et de Gestion du Canton de Vaud, Yverdon, Switzerland. September 24, 2009.
 - Department of Informatics, University of Fribourg, Fribourg, Switzerland. September 23, 2009.
 - Cryptography Seminar, Université de Rennes 1, Rennes, France. March 13, 2009.

- Arénaire project-team, LIP, École Normale Supérieure de Lyon, Lyon, France. March 11, 2009.
 - ARITH team, LIRMM, Montpellier, France. March 5, 2009.
 - Dali team, Université de Perpignan Via Domitia, Perpignan, France. March 3, 2009.
 - CACAO project-team, LORIA, Nancy, France. February 27, 2009.
5. *Hardware Accelerators for the Tate Pairing Based on Karatsuba-Ofman Multipliers*. Pairing Forum, Tokyo, Japan. November 7, 2008.
 6. *Hardware Operators for Pairing-Based Cryptography*.
 - Facultad de Ciencias de la Computación, Universidad Autónoma de Puebla, Puebla, México. July 21, 2008.
 - Computer Science Section, Electrical Engineering Department, Centro de Investigación y de Estudios Avanzados del IPN, México City, México. July 14, 2008.
 7. *FPGA Coprocessors for the Tate Pairing over \mathbb{F}_{2^m} and \mathbb{F}_{3^m}* . Pairing Forum, Tokyo, Japan. April 22, 2008.
 8. *Arithmetic Operators for Pairing-Based Cryptography*. Pairing Forum, Tokyo, Japan. September 20, 2007.
 9. *Arithmetic Operators for Pairing-Based cryptography*. Laboratory for Cryptologic Algorithms, Swiss Federal Institute of Technology, Lausanne, Switzerland. September 6, 2007.
 10. *Arithmetic Operators for Pairing-Based Cryptography*. Cryptographic Architectures Embedded in Reconfigurable Devices–CryptArchi 2007, Montpellier, France. June 19–22, 2007.
 11. *Radix-2 and High-Radix Carry-Save Modular Multipliers for FPGAs*.
 - Future University-Hakodate, Hakodate, Japan. July 24, 2006.
 - Los Alamos National Laboratory, Los Alamos, New Mexico, United States. October 27, 2005.
 12. *Addition and Multiplication Algorithms for Radix-2 RN-Codings and Two's Complement Numbers*. ARITH team, LIRMM, Montpellier, France. October 10, 2005.
 13. *Trois problèmes d'arithmétique des ordinateurs liés à l'implantation matérielle d'algorithmes de cryptage*. id Quantique, Geneva, Switzerland. November 2004.
 14. *Modulo M Multiplication-Addition: Algorithms and FPGA Implementation*. Cryptographic Architectures Embedded in Reconfigurable Devices–CryptArchi 2004, Abbaye de la Bussière, France. June 16–19, 2004.

Teaching

Graduate Course

Since 2008 *Advanced Course in Authentication Systems* (with E. Okamoto). University of Tsukuba, Japan.

Tutorials

- Since 2009 *Hardware Evaluation of SHA-3 Candidates* (weekly lecture for undergraduate and graduate students). Laboratory of Cryptography and Information Security, University of Tsukuba, Japan.
- Since 2006 *Hardware Implementation of Pairing-Based Cryptography* (weekly lecture for undergraduate and graduate students). Laboratory of Cryptography and Information Security, University of Tsukuba, Japan.
- 2006 *Algorithms and Number Systems for Digital Arithmetic*. Laboratory of Cryptography and Information Security, University of Tsukuba, Japan.

Guest Lectureships

- 2008 *An Introduction to Pairing-Based Cryptography*. Computer Science Section, Electrical Engineering Department, Centro de Investigación y de Estudios Avanzados del IPN, México City, México. (Master's and Ph.D students.)
- 2004 *Une introduction à l'arithmétique des ordinateurs* (An Introduction to Computer Arithmetic). Département des sciences appliquées, Université du Québec à Chicoutimi, Chicoutimi, Canada. (Master's and Ph.D students.)
- 2004 Graduate course *Opérateurs arithmétiques* (Arithmetic Operators), École Normale Supérieure de Lyon, Lyon, France.
- 1997–2001 Graduate course *Réseaux de neurones artificiels* (Artificial Neural Networks), Swiss Federal Institute of Technology, Lausanne, Switzerland.
- 1998–2001 Graduate course *Systèmes et programmation génétiques* (Genetic Systems and Programs), Swiss Federal Institute of Technology, Lausanne, Switzerland.

Teaching Assistance (Swiss Federal Institute of Technology, Lausanne, Switzerland)

- 1997–2001 Undergraduate course *Logique élémentaire* (Elementary Logic). Prof. J. Zahnd.
- 1998–2000 Undergraduate course *Automates et calculabilité* (Automata and Computation). Prof. J. Zahnd.
- 1999–2001 Undergraduate course *Conception des processeurs* (Processor Architecture). Prof. E. Sanchez.
- 1997–1998 Undergraduate course *Systèmes logiques* (Logic Systems). Prof. D. Mange.

Teaching Material

Jean-Luc Beuchat and Jacques-Olivier Haenni. *Automate cellulaire autoréplicateur de von Neumann*. Logic Systems Laboratory, Swiss Federal Institute of Technology at Lausanne. March 2001. (40 pages)

Jean-Luc Beuchat. *Systèmes neuromimétiques à apprentissage supervisé*. Logic Systems Laboratory, Swiss Federal Institute of Technology at Lausanne. April 1999. (115 pages)

Program Committees

- 2010 International Conference on Pairing-based Cryptography (Pairing 2010)
- 2010 Workshop on Cryptographic Hardware and Embedded Systems 2010 (CHES 2010)
- 2009 Cryptology and Network Security (CANS 2009)
- 2009 Workshop on Cryptographic Hardware and Embedded Systems 2009 (CHES 2009)
- 2009 ReConFig'09 (special track on reconfigurable computing for security and cryptography)

Occasional Referee

International and National Journals

Communications and Computer Sciences; Computers and Electrical Engineering; IEEE Transactions on Circuits and Systems I; IEEE Transactions on Circuits and Systems II; IEEE Transactions on Computers; IEICE Transactions on Fundamentals of Electronics; IET Circuits, Devices & Systems; Integration, the VLSI Journal; International Journal of Electronics; Iranian Journal of Electrical and Computer Engineering; Microelectronics Journal; Technique et science informatiques.

International Conferences

Australasian Conference on Information Security and Privacy (ACISP); IEEE Symposium on Computer Arithmetic (ARITH); IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP); International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT); International Conference on Cryptology and Network Security (CANS); Workshop on Cryptographic Hardware and Embedded Systems (CHES); International Conference on Computational Science (ICCS); International Conference on Information Security and Cryptology (ICISC); International Workshop on Security (IWSEC); International Conference on Field Programmable Logic and Applications (FPL); Pairing-Based Cryptography (Pairing); Public Key Cryptography (PKC).

Grants

- 2009–2010 Recruitment of Dr Simon Kramer as a JSPS post-doctoral fellow:
- Maintenance allowance: 364,000 JPY per month.
 - Supplementary research allowance: 1,600,000 JPY.
- 2008–2009 Investigator, *Software and Hardware Components for Pairing-Based Cryptography*, Japan-France Integrated Action Program (Ayame/Sakura), 2,000,000 JPY.
- 2004–2005 Principal investigator, *Opérateurs arithmétiques pour circuits programmables*, Swiss National Science Foundation Fellowship for Prospective Researchers, 91,150 CHF.
- 2003–2006 Investigator, *Opérateurs Cryptographiques et Arithmétique Matérielle*, Ministère délégué à la Recherche (ACI “Security in Computer Science”), 103,000 EUR.
- 2002–2005 Investigator, *Opérateurs Arithmétiques pour la Cryptographie*, Ministère délégué à la Recherche (ACI “Cryptology”), 60,000 EUR.
- 2002–2003 Principal investigator, *Opérateurs arithmétiques pour circuits programmables*, Swiss National Science Foundation Fellowship for Prospective Researchers, 35,500 CHF.
- 2001–2002 Principal investigator, *Opérateurs arithmétiques pour circuits programmables*, Swiss National Science Foundation Fellowship for Prospective Researchers, 35,500 CHF.