Nathalie Casati

Curriculum Vitæ

+41 79 393 96 90
+41 32 510 96 96
nca@zurich.ibm.com
Date of birth: 11.02.1985
Driver's license

Education

2010–present **PhD in Computer Science**, *IBM Zurich Research Lab*, Switzerland.
2007–2009 **MSc in Computer Science**, *EPF Lausanne*, Switzerland. are optional
2003–2007 **BSc in Computer Science**, *EPF Lausanne*, Switzerland.
2000–2003 **Maturité Fédérale**, *Lycée Blaise-Cendrars, La Chaux-de-Fonds*, Switzerland.

Master Thesis

title, year *Universally Composable Secret Handshakes with Credentials, 2009*
supervisors Arjen K. Lenstra, Martijn Stam
Laboratory For Cryptologic Algorithms @ EPF Lausanne, Switzerland.
supervisors Jan Camenish, Thomas R. Groß, Victor Shoup
Cryptography group @ IBM Zurich Research Lab, Switzerland.
description Design of a new Secret Handshake cryptographic primitive with enhanced features such as credentials matching and improved security using the Universal Composability framework.

Semester Project

title, year *Optimized Implementation of SHA-1 on the Cell processor, 2008*
supervisors Arjen K. Lenstra, Dag Arne Osvik
Laboratory For Cryptologic Algorithms @ EPF Lausanne, Switzerland.
description Fast implementation of SHA-1 on the Cell processor, in the context of high throughput hashing and collision attacks. In collaboration with IAIK Krypto Group, TU Graz, Austria.

Experience

Academic experience

2006–2008 **Student assistant**, *Processor Architecture Laboratory*, EPF Lausanne, Switzerland.
Student assistant for Computer Architecture I and II classes, FPGA used is FPGA4U.
2006–2008 **Student assistant**, *Poseidon Project*, EPF Lausanne, Switzerland.
Hardware and software support, purchasing advice.

Work Experience

2009–2010 **Internship**, *Computational Scaling Team*, IBM Zurich Research Lab, Switzerland.
Source-mask optimization efficiency improvements using pattern recognition techniques.
2008 **Internship**, *Cryptography group*, IBM Zurich Research Lab, Switzerland.
Cryptographic primitives design.

Associations

2007–2009 **Vice president**, *GNU Generation*, EPF Lausanne, Switzerland.
Promoting open source software.

Languages

French **Native** *Swiss and French citizenship*
English **Fluent** *Two linguistic trips to England (2001 and 2002)*
German **High school level**
Spanish **High school level**

Publications and recent projects

Kafai Lai, Maria Gabrani, David L. DeMaris, Nathalie Casati, Andres Torres, Sankha Sarkar, Phil Strenski, Saeed Bagheri, Daniele. P. Scarpazza, Alan E. Rosenbluth, David O. Melville, Andreas Waechter, Jon Lee, Vernon Austel, Marc Szeto-Millstone, Kehan Tian, and Francisco Barahona. Design-specific joint optimization of masks and sources on a very large scale. In Mircea V. Dusa, editor, *Optical Microlithography XXIV, proceedings of SPIE Advanced Lithography 2011*, volume 7973, April 2011.

Jan Camenisch, Nathalie Casati, Thomas Gross, and Victor Shoup. Credential Authenticated Identification and Key Exchange. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 255–276. Springer Berlin / Heidelberg, August 2010.

Joppe Bos, Nathalie Casati, and Dag Arne Osvik. Multi-Stream Hashing on the PlayStation 3. In *Proceedings of the 9th International Workshop on State-of-the-Art in Scientific and Parallel Computing (PARA2008)*.

Nathalie Casati. Benchmarking the Memory Interface Controller bus of the Cell processor. 2007.