

CURRICULUM VITAE

ANDREA RÖCK



CONTACT INFORMATION

Team SECRET
INRIA Paris–Rocquencourt, B.P. 105
78153 Le Chesnay Cedex
France

Phone: +33(0)1-39-63-50-75
Fax: +33(0)1-39-63-50-51
Email: andrea.roeck@inria.fr
Homepage: <http://www-rocq.inria.fr/secret/Andrea.Roeck/>

PERSONAL DETAILS

Date of birth: 12th of September, 1979
Place of birth: Innsbruck, Austria
Marital status: Single
Citizenship: Austria

EDUCATION

1993–1998 Technical High School for Communications Engineering, Innsbruck, Austria
Diploma: Reifeprüfungszeugnis with excellent success

1998–2005 Applied Computer Science at the University of Salzburg, Austria
Diploma: Diplom-Ingenieurin with excellent success

2000–2005 Mathematics at the University of Salzburg, Austria
Diploma: Magistra der Naturwissenschaften with excellent success

Since 2005 PhD of Computer Science
INRIA Paris–Rocquencourt, Team SECRET, Paris, France

WORKING EXPERIENCE

Summer 1995 Tiroler Wasserkraftwerke Aktiengesellschaft (TIWAG) (Tyrolean energy provider)
Eduard Wallnoefer-Platz 2, 6020 Innsbruck, Austria
4 weeks training

Summer 1996 Austrian Broadcasting Corporation (ORF), Landesstudio Tirol
Rennweg 14, 6020 Innsbruck, Austria
4 weeks training

1999–2005 Applications developer in Java, SBS Software Ges.m.b.H.
Weiserhofstraße 19, 5020 Salzburg, Austria

TEACHING EXPERIENCE

- 2001-2002 Teaching assistant for programming courses in C++
Bowling Green State University, Ohio, U.S.A
- 2007/2008 Teaching assistant for programming course in Java
École Polytechnique, Palaiseau, France
- 2008 Teaching assistant for parallel programming course
Polytech'Paris, Université Pierre et Marie Curie, France
- 2008 Teaching assistant for algorithms course
École National Supérieure de Techniques Avancées (ENSTA), Paris, France

FOREIGN LANGUAGES

English, oral and written

French, oral and written

ADDITIONAL QUALIFICATIONS

Programming:

- Java
- C++
- C
- MPI

STUDIES ABROAD

- 2001–2002 Bowling Green State University, Ohio, U.S.A
Computer Science, Graduation as Master of Science
- October 2004 INRIA Rocquencourt, Project CODES,
Paris, France (4 weeks visit)
- January 2008 Princeton University, New Jersey, USA
co-operation with Cédric Lauradoux

PUBLICATIONS

- 2006 Ray Kresman and Andrea Röck. **On petri nets and predicate-transition nets.** In Proceedings of *Software Engineering Research and Practice*, pages 903–909, CSREA Press, 2006
- 2007 Andrea Röck. **The Impact of Entropy Loss Caused by Random Functions.** In Proceedings of *WEWoRC 2007, Western European Workshop on Research in Cryptology*, pages 130–135, July 4-6, 2007, Ruhr-University, Bochum, Germany.
- Andrea Röck. **Attaques par collision basées sur la perte d’entropie causée par des fonctions aléatoires.** In Proceedings of *MajecSTIC 2007*, pages 115–124, 29-31 October, 2007, Caen, France.
- 2008 Andrea Röck. **Entropy of the Internal State of an FCSR in Galois Representation.** In Proceedings of *FSE 2008, Fast Software Encryption*, volume 5086 of *Lecture Notes in Computer Science*, pages 343–362, Springer, 2008
- Andrea Röck. **Stream ciphers using a random update function: Study of the entropy of the inner state.** In Proceedings of *AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 258–275, Springer, 2008
- Cédric Lauradoux and Andrea Röck. **Parallel generation of ℓ -sequences.** In Proceedings of *SETA 2008, Sequences and Their Applications*, volume 5203 of *Lecture Notes in Computer Science*, pages 299–312, Springer, 2008