Andrea RÖCK

Contact Information

Aalto University - School of Science
Department of Information and Computer Science
P.O. Box 15 400
FI-00076 AALTO
Finland

Phone: +358(0)9-470-23254
Email: andrea.rock@aalto.fi
Homepage: http://www.tcs.hut.fi/~arock/

Personal Details

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

Research Interests

My interests lie in symmetric cryptography, including random number generators, stream ciphers, block ciphers and hash functions. Currently I'm working on linear cryptanalysis of block ciphers, online entropy estimation for RNG sources and cryptanalysis of hash functions.

Academic Records

Since 2009	Post-doctoral position at the Aalto University School of Science, Finland
2005–2009	PhD of Computer under the supervision of Nicolas Sendrier INRIA Paris–Rocquencourt, Team SECRET, Paris, France Diploma: Docteur de l'École Polytechnique with excellent success
2000–2005	Mathematics at the University of Salzburg, Austria Diploma: Magistra der Naturwissenschaften with excellent success
1998–2005	Applied Computer Science at the University of Salzburg, Austria Diploma: Diplom-Ingenieurin with excellent success
2001–2002	Bowling Green State University, Ohio, USA Diploma: Master of Science in the field of Computer Science
1993–1998	Technical High School for Communications Engineering, Innsbruck, Austria Diploma: Reifeprüfungszeugnis with excellent success

Working Experience

1999–2005	Applications developer in Java, SBS Software Ges.m.b.H. Weiserhofstraße 19, 5020 Salzburg, Austria, www.sbs.co.at [except during my stay in the USA 2001–2002]

Teaching

2001-2002	Teaching assistant for programming courses in C++ Bowling Green State University, Ohio, USA
2007-2009	Teaching assistant for programming course in Java (beginner and advanced level) 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
2010	Teaching assistant for cryptology course and postgraduate course in theoretical computer science, Aalto University School of Science, Finland

Visit To Other Laboratories

January 2008	Princeton University, New Jersey, USA Cooperation with Cédric Lauradoux
February 2010	1 week, FHNW Windisch, Switzerland Cooperation with María Naya-Plasencia

Participation In Research Projects

2007-2010	RAPIDE: Design and analysis of stream ciphers dedicated to constrained environments. Funded by the French National Research Agency (ANR). Partners: LORIA, INRIA, INSA Lyon, Université de Limoges
2004-2012	ECRYPT I - ECRYPT II: European Network of Excellence in Cryptology With 31 European partners from academia and industry

Competences

Programming: Java, C++, C, MPI

German: Native

English: Fluent

French: Fluent

Miscellaneous

Reviews for the following international conferences: WCC 2009, FSE 2010, Crypto 2010, SAC 2010, Asiacrypt 2010, Nordsec 2010, FSE 2011

General Co-chair together with Helger Lipmaa of the Ecrypt II Hash function workshop in Tallinn, Mai 2011

Publications

Thesis

[1] Andrea Röck. *Quantifying Studies of (Pseudo) Random Number Generation for Cryptography.* Doctoral dissertation, INRIA Paris-Rocquencourt, Project SECRET and École Polytechnique, France, 2009.

[2] Andrea Röck. Pseudorandom number generators for cryptographic applications. Master's thesis, University of Salzburg, Austria, Austria, 2005.

Full papers in international peer-reviewed conference proceedings

[1] Andrea Röck and Kaisa Nyberg. Exploiting Linear Hull in Matsui's Algorithm 1. In *The Seventh International Workshop on Coding and Cryptography, WCC 2011, April 11-15, 2011, Paris, France*, to appear.

[2] Dmitry Khovratovich, María Naya-Plasencia, Andrea Röck, and Martin Schläffer. Cryptanalysis of Luffa v2 components. In Alex Biryukov, Guang Gong, and Douglas Stinson, editors, *Selected Areas in Cryptography - SAC 2010*, volume 6544 of *LNCS*, pages 388–409. Springer, Heidelberg, 2011.

[3] María Naya-Plasencia, Andrea Röck, Jean-Philippe Aumasson, Yann Laigle-Chapuy, Gaëtan Leurent, Willi Meier, and Thomas Peyrin. Cryptanalysis of ESSENCE. In Seokhie Hong and Tetsu Iwata, editors, *Fast Software Encryption - FSE 2010*, volume 6147 of *Lecture Notes in Computer Science*, pages 134–152. Springer, 2010.

[4] Cédric Lauradoux and Andrea Röck. Parallel generation of ℓ-sequences. In Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, editors, *SETA*, volume 5203 of *Lecture Notes in Computer Science*, pages 299–312. Springer, 2008.

[5] Andrea Röck. Stream ciphers using a random update function: Study of the entropy of the inner state. In Serge Vaudenay, editor, *AFRICACRYPT*, volume 5023 of *Lecture Notes in Computer Science*, pages 258–275. Springer, 2008.

[6] Andrea Röck. Entropy of the internal state of an FCSR in Galois representation. In Kaisa Nyberg, editor, *FSE*, volume 5086 of *Lecture Notes in Computer Science*, pages 343–362. Springer, 2008.

[7] Andrea Röck and Ray Kresman. On petri nets and predicate-transition nets. In Hamid R. Arabnia and Hassan Reza, editors, *Software Engineering Research and Practice*, pages 903–909. CSREA Press, 2006.

Invited talks and seminars

[1] Cryptanalysis of ESSENCE. Seminar of the Center for Advanced Security Research Darmstadt (CASED) - Germany, November 2009.

[2] Analysis of the Linux random number generator. Cryptography seminar at the University of Rennes - France, October 2009.

[3] Entropy approximation for FCSRs. Cryptography seminar at the University of Caen - France, March 2007.

[4] Entropy approximation for FCSRs. Seminar of the project PI2C, Limoges - France, February 2007.

[5] Andrea Röck and Cédric Lauradoux. Parallel generation of l-sequences. In Helena Handschuh, Stefan Lucks, Bart Preneel, and Phillip Rogaway, editors, *Symmetric Cryptography*, number 09031 in Dagstuhl Seminar Proceedings, Dagstuhl, Germany, 2009. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany.

International workshops

[1] Andrea Röck. The impact of entropy loss caused by random functions. In *WEWoRC 2007, Western European Workshop on Research in Cryptology*, Bochum, Germany, July 2007.

National workshops

[1] Étude du générateur d'aléa du noyau Linux. Journées "Codages et Cryptographie", Fréjus (Var) - France, October 2009.

[2] Parallel generation of ℓ-sequences. Kryptowochenende, Tabarz - Germany, November 2007.

[3] Synthèse des ℓ-séquences décimées. Journées "Codages et Cryptographie", Carcans (Gironde) - France, March 2008.

[4] Entropy of the inner state of an FCSR. 7. Kryptotag, Bonn - Germany, November 2007.

[5] Attaques par collision basés sur la perte d'entropie causée par des fonctions aléatoires. In *MajecSTIC 2007*, pages 115–124, october 2007.

[6] Entropy loss and random functions. Journées "Codages et Cryptographie", Eymoutiers (Haute-Vienne) - France, October 2006.

Collaborative projects

[1] Jonathan Etrog, Dmitry Khovratovich, Willi Meier, Nicky Mouha, Jorge Nakahara Jr., Andrea Röck, Vincent Rijmen, Christian Rechberger, Martin Schläffer, and Vesselin Velichkov. D.SYM.6 - New developments in symmetric key cryptanalysis. In Svetla Nikova, editor, *Ecrypt II – SymLab deliverables*, June 2010. `http://www.ecrypt.eu.org/documents`.

Patents

[1] Andrea Röck. Online entropy estimator for random sources. Filed at the National Board of Patents and Registration of Finland (PRH) under application number FI 20106291, December 2010.