FSE 2006 Rump session

16 March 2006

FSE 2006 Rump Session

- 15:00-15:06 Matt Robshaw: A status update on eSTREAM
- 15:06-15:12 Eli Biham: Pypy: Another version of Py
- 15:12-15:18 Vincent Rijmen, Joan Daemen: Plateau trails
- 15:18-15:24 Yusuke Naito: Improving collision search on SHA-0
- 15:24-15:30 Yu Sasaki: Message modification for MD5
- 15:30-15:36 M. Gebhardt, G. Ilies, W. Schindler: The impact of IV on multiblock hash collision attacks
- 15:36-15:42 conference announcements
  - Alexander Veith: Sightseeing in St. Petersburg
  - Carlos Cid: Gröbner bases in cryptography, coding theory, and algebraic combinatorics
  - Bart Preneel: ECRYPT events in 2006, FSE 2007
- 15:42-15:48 Yossie Oren, Adi Shamir: Power analysis of RFID tags
- 15:48-15:54 Stefan Tillich, Johann Großschädl: Supporting cryptography on embedded processors: coprocessor vs. instruction set extensions

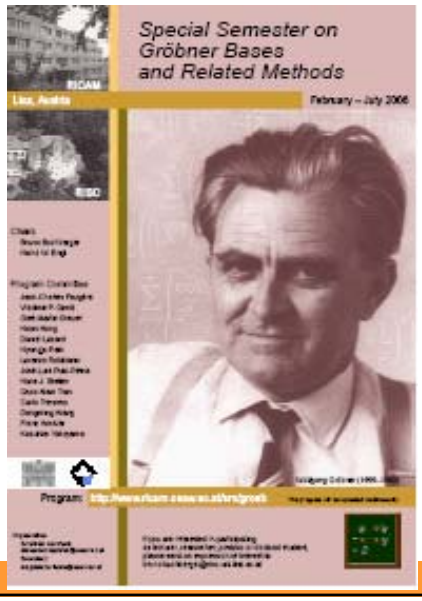
Eurocrypt 2006

- 28 May – 1 June
- St. Petersburg, Russia
- General Chair – Anatoly Lebedev
- Program Chair – Serge Vaudenay

- !visa application

Special Semester on Groebner Bases and Related Methods (Linz – Austria, 2006)

- Organised by Bruno Buchberger (RISC and RICAM – Linz)
- Main goal is to bring together researchers for joint research on Gröbner bases and related theories and methods.
- Part of the effort during the special semester will also go into special lectures, tutorials, and training.
- Both established researchers as well as junior researchers, postdocs, and PhD students are welcome to participate.



Special Semester on Groebner Bases and Related Methods (Linz – Austria, 2006)

- Of special interest:

  Workshop on

  Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics

  May 01 - May 06 , 2006

Workshop on Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics
Linz, Austria - May 01 - 06 , 2006

- The Crypto special session will mainly consist of a number of invited talks plus a poster session.
- It will concentrate on all aspects of Groebner bases in cryptography, including recent advances in this area.
  - Very active area of research: applications of commutative algebra and computer algebra in cryptography.
    - Multivariate Cryptography (HFE, sFlash, etc);
    - Algebraic Attacks against stream ciphers and (possibly) block ciphers;
    - Hash Functions, other applications?
- The goal of the workshop is to bring experts in cryptography together with a community of people working in Groebner bases.

Workshop on Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics
Linz, Austria - May 01 - 06 , 2006

- **CONFIRMED INVITED SPEAKERS**
  - F. Armknecht (Mannheim University, Germany)
  - O. Billet (France Télécom R&D, France)
  - C. Cid (Royal Holloway, UoL, UK)
  - C. Diem (Univ. of Leipzig, Germany)
  - J.C. Faugère (INRIA & CNRS, France)
  - M. Kreuzer (Univ. of Dortmund, Germany)
  - F. Levy-dit-Vehel (ENSTA, France)
  - L. Perret (Crypto Group, UCL, Belgium)
  - H. Park (KIAS, Korea)
  - M. Sugita (ISEC, IPA, Japan)
  - T. Rai (Univ. of Missouri, USA)
  - R.P. Weinmann (Univ. of Darmstadt, Germany)

Workshop on Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics
Linz, Austria - May 01 - 06 , 2006

- Very interesting event for researchers with interest in cryptography/coding theory and applications of Groebner Bases.
- Registration is open to all (to join, register on web page of the Special Semester by April, 10th).
- More information about activities at:
  - the event website
    `http://www.ricam.oeaw.ac.at/srs/groeb/index.htm`
  - or with Ludovic Perret (Louvain-La-Neuve):
    ludovic.perret@uclouvain.be

ECRYPT Calendar:

http://www.ecrypt.eu.org

- 3-4 April '06: Special-Purpose Hardware for Attacking Cryptographic Systems (Cologne, DE)
- 24-26 May '06: Post Q Workshop (Leuven, BE)
- *12-15 June '06: School on Cryptographic Hardware, Side-Channel and Fault Attacks (Louvain-la-Neuve, BE)*
- 28-29 July '06 9 (after ANTS): Algebraic number theory workshop (Berlin, DE)
- 31 July – Aug. 1 '06: Workshop on models for cryptographic protocols (Århus, DK)
- July '06: Workshop on Watermark Security and Benchmarking (Magdeburg/Munich, DE)
- *12-14 July '06: RFID workshop (Graz, AT)*
- *28 Oct.-3 Nov. '06: School on zero-knowledge: foundations and applications (Bertinoro, IT)*
- *Jan '07: School on Cryptographic Algorithm Design*

Workshop on recent advances in hash functions and stream ciphers

- June 28-30, 2006
- QUT, Brisbane, Queensland, Australia
- Contact: Ed Dawson

Vietcrypt

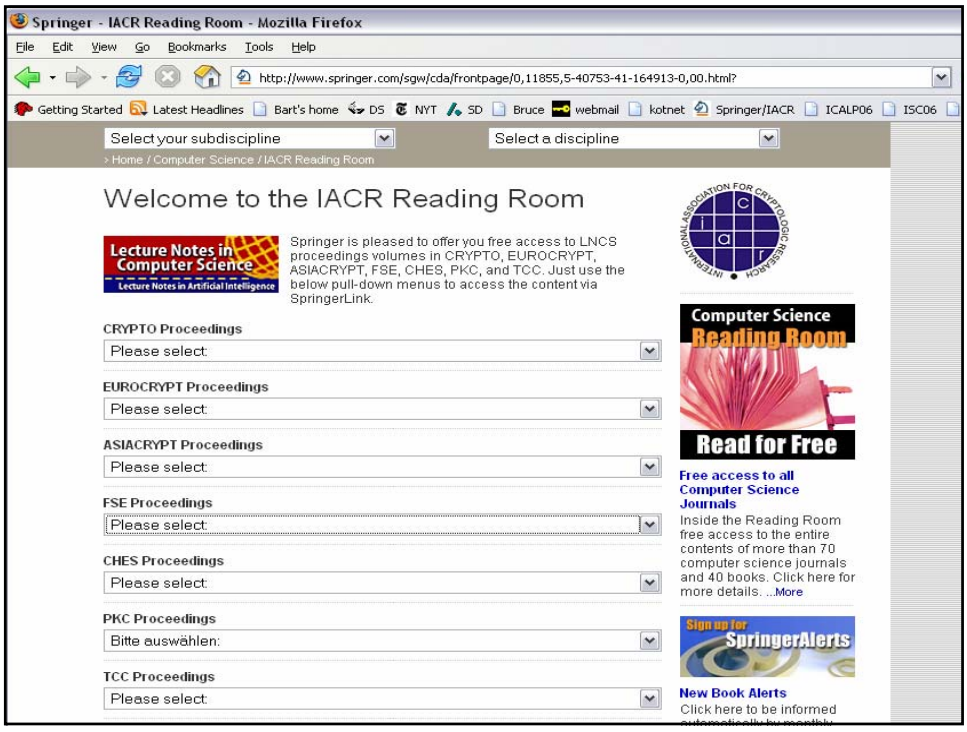
- See additional slides

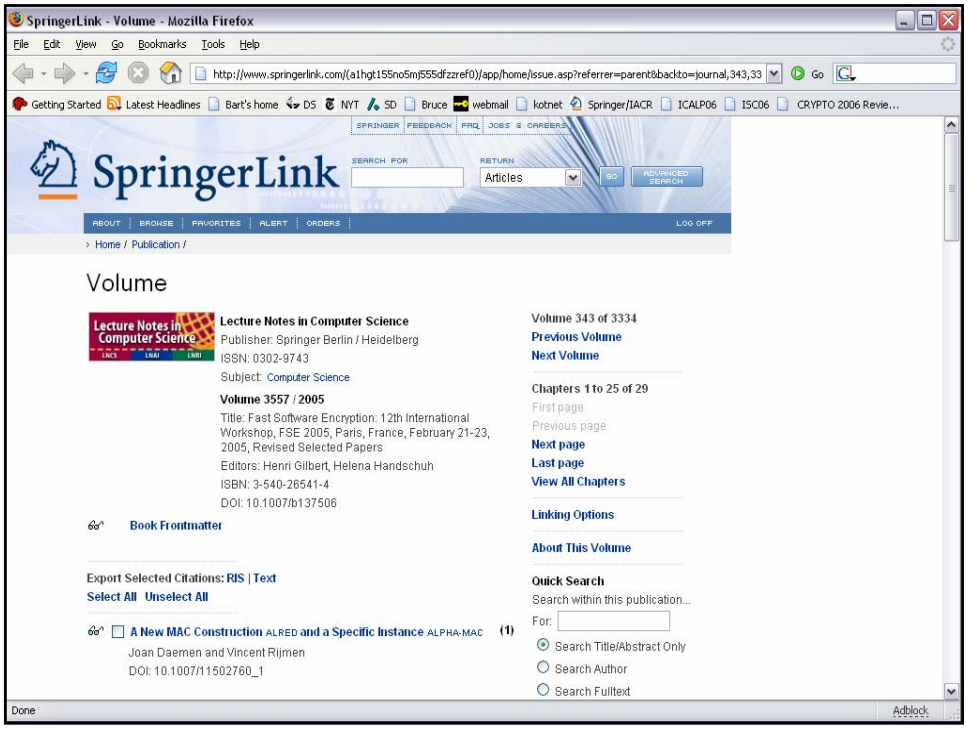
You are a 2007 member of IACR

- Delivering to our members
  - Eurocrypt, Crypto, Asiacrypt
  - FSE, PKC, CHES, TCC
  - Journal of Cryptology and Newsletter
  - Eprint Archive
    - http://eprint.iacr.org/
  - Main website
    - www.iacr.org

Springer-Verlag

- Publisher of IACR's conference and workshop proceedings in the LNCS series and the Journal of Cryptology
- All issues of the Journal of Cryptology are available online to all IACR members: http://link.springer.de
- new: IACR reading room: proceedings of all IACR conferences and workshops





FSE 2007 in Luxembourg (tentative)

March 26-28, 2007 (tentative)

Submission: 20 Dec, 2006 (alternative 1 October 2006)

Program chair: Prof. Alex Biryukov,
University of Luxembourg

General chair: Prof.Jean-Claude Asselborn,
University of Luxembourg

Support Staff: Marianne Graffe and Nathalie Leruth

UNIVERSITÉ DU LUXEMBOURG

Local Information

- City of **Luxembourg** (83,000 inhabitants) is a capital of Luxembourg, a small country in the heart of Europe, between France, Belgium and Germany. Luxembourg is known for its financial institutions and several key European institutions. Luxembourg was chosen cultural capital of Europe 2007.
- The conference will take place in a conference hall in the historic city center.
- **Attractions in the city:** walk in the valey of river Alzette, spanish bastions and casemates, museum of city history, Grand-Ducal palace.
- **Attractions around (within 30 km):** Petit Suisse (beautiful nature park) *** in Michelin guide; Shengen castle; the valley of Moselle river
- **Attractions nearby (within 60 km):** old town of Trier (Germany); old town of Metz (France); Ardennes.

Local Information (cont.)

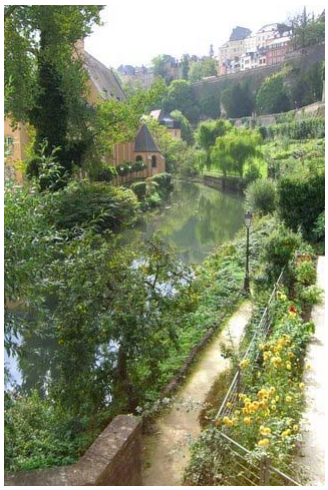
- Plenty of hotels walking distance from the conference location: 100-200 eur/day.
- Youth hostel offering budget accomodations for students is walking distance from the conference location.

Transportation

- Luxair flights to: Berlin, Copenhagen, Frankfurt, Geneve, London, Madrid, Munich, Paris, Rome, Vienna

  http://www.luxair.lu/
- Train: 2:40-3:00 hours from Brussels (direct), 3:30 hours from Paris (direct)

  http://www.b-rail.be/main/E/
- From airport to the city center (5km) (bus #16, 1.20 eur, every 15-20 minutes. Taxi: 15-25 eur, 10-15 minutes. http://www.luxembourg.co.uk/airport.html



FSE 2008?

please send proposals for 2008 to
bart.preneel(AT)esat.kuleuven.be