

Norsk Kryptoseminar, Bergen, November 9-10, 2011

Place: Department of Informatics, University of Bergen,
Høyteknologisenteret i Bergen,
Thormøhlensgt. 55 (Datablokken)
Room 2142

Organiser: Tor Helleseeth, Mob: 95702773, E-mail: Tor.Helleseeth@ii.uib.no

Suggested hotels close by:

- Hotel Park Bergen, Harald Haarfagresgate 35, N-5007 Bergen
- Rica Travel Hotel, Christies gate 5-7, 5008 Bergen, Ph: 55 36 29 00

List of Participants (Preliminary)

1. Lilya Budaghyan, UiB
2. Yanling Chen, NTNU
3. Mehdi Hassanzadeh, UiB
4. Tor Helleseeth, UiB
5. Oleksandr Kazymyrov, UiB
6. Alexander Kholosha, UiB
7. Chunlei Li, UiB
8. Stig Frode Mjølsnes, NTNU
9. Simona Samardjiska, NTNU
10. Thorsten Schilling, UiB
11. Igor Semaev, UiB
12. Reza Sohizadeh, UiB
13. Asgeir Steine, NTNU
14. Mohsen Toorani, UiB
15. Joe-Kai Tsay, NTNU

Program, Norsk Kryptoseminar, Bergen, 2011

9. November - Wednesday

10:45 – 11:00 Tor Helleseeth, Welcoming remarks

11:00 – 11:30 Igor Semaev, Improvements on Circuit Lattices, hardware tool for cryptanalysis

11:30 – 12:00 Simona Samardjiska, On a class of left MQQs with degree invariant to parastrophy

12:00 – 12:30 Yanling Chen, On Orthogonal Latin Squares

12:30 – 14:00 LUNCH

14:00 – 14:30 Asgeir Steine, En protokoll for anonym betaling

14:30 – 15:00 Mohsen Toorani, Certificateless Public Key Cryptography

15:00 – 15:30 Thorsten Schilling, Analysis of Trivium Using Compressed Right Hand Side Equations

15:30 – 16:15 Mehdi Hassanzadeh, GSM Security

19:30 – Dinner in the evening (On own cost)

10. November - Thursday

10:00 – 10:30 Stig Frode Mjølsnes, Disruption of 802.11 Availability

10:30 – 11:00 Alexander Kholosha, Bent functions

11:00 – 11:30 Lilya Budaghyan, APN functions and S-boxes

11:30 – 12:00 Oleksandr Kazymyrov, Block ciphers

12:00 – 12:30 Joe-Kai Tsay, Modular Soundness Proofs for Equational Theories via Deduction Games

12:30 – 14:00 LUNCH

14:00 – 14:30 Reza Abinayeh, Minimalistic cryptography

14:30 – 15:00 Chunlei Li, Algebraic immunity of stream ciphers