Norsk Kryptoseminar, Bergen, November 9-10, 2011

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

Organiser: Tor Helleseth, Mob: 95702773, E-mail: Tor.Helleseth@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. Reza Abinyaheh, UiB
2. Lilya Budaghyan, UiB
3. Yanling Chen, NTNU
4. Sergiy Gladysh, NTNU
5. Mehdi Hassanzadeh, UiB
6. Tor Helleseth, UiB
7. Alexander Kholosha, UiB
8. Chunlei Li, UiB
9. Stig Frode Mjølsnes, NTNU
10. Simona Samardjiska, NTNU
11. Thorsten Schilling, UiB
12. Igor Semaev, UiB
13. Asgeir Steine, NTNU
14. Joe-Kai Tsay, NTNU
15. Mohsen Toorani, UiB

Program, Norsk Kryptoseminar, Bergen, 2011

9. November - Wednesday

10:45 – 11:00 Tor Helleseth, 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 Stene, 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 FrodeMjølsnes, Disruption of 802.11 Availability
10:30 – 11:00 Alexander Kholosha, Pomaranch streamcipher
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