Program Norsk kryptoseminar 2012

Onsdag 7. November

10:00-11:45
"PRINCE" a New Block Cipher to Appear at ASIACRYPT
On the Distribution of Linear Biases: Three Instructive Examples

Gregor Leander, Danske Tekniske Universitet (DTU)

(Kaffe)

11:50-12:20 ***Tilfeldighet i Kryptografi***

Leif Nilsen, Thales

(Lunsj)

13:00-13:45 ***Effektive Implementasjoner***

Dag-Arne Osvik

13:45-14:15 ***Compressed Right Hand Side Equation Systems***

Thorsten Schilling, Ernst&Young

(Kaffe og Kaker)

14:30-15:10 ***Kryptografi og Nettlesere***

Håvard Molland, Opera Software

15:10-15:30 ***AES-like Representation of Russian Hash Function Stribog***

Oleksandr Kazymyrov, Universitetet i Bergen (UiB)

15:30-15:50 ***Efficient Padding Oracle Attacks on Cryptographic Hardware***

Joe-Kai Tsay, Norges Tekniske og Naturvitenskaplige Universitet (NTNU)

15:50-16:15 ***Disruption of Cryptoprotocols***

Stig-Frode Mjølsnes, Norges Tekniske og Naturvitenskaplige Universitet (NTNU)

Torsdag 8. November

09:15-11:00 ***Even Mansour Revisited: Building Ideal Ciphers from a Few Random Permutations***
Efficient AES-Based Authenticated Encryption with Applications

Andrey Bogdanov, Danske Tekniske Universitet (DTU)

(Kaffe)

11:15-12:00 ***Hvordan Modellere Alice og Bob?***

Kristian Gjøsteen, Norges Tekniske og Naturvitenskaplige Universitet (NTNU)

(Lunsj)

12:45-13:15 ***Norsk Kryptohistorie***

Hans Morten Synstnes, Nasjonal sikkerhetsmyndighet

13:15-14:00 ***Boolean Functions and the Quaternary Symmetric Channel***

Matthew G. Parker, Universitetet i Bergen (UiB)

14:00-14:30 ***Sikkerhet i Digitale Kinoer***

Øyvind Grinde, Direktoratet for forvaltning og IKT (Difi)

(Kaffe og Kaker)

14:40-15:10 ***Multivariate Quadratic Public-Key Crypto***

Håkon Jacobsen, Norges Tekniske og Naturvitenskaplige Universitet (NTNU)

15:10-15:30 ***Towards a Secure Multivariate Identity-Based Encryption***

Simona Samardjiska, Norges Tekniske og Naturvitenskaplige Universitet (NTNU)

Generell Informasjon

Sted

Oslo Kongressenter (www.oslokongressenter.no) ligger i samme bygg som Folkets Hus ved Youngstorget (Youngs gate 11, 0181 Oslo, Norge)

Lunsj

Lunsj består av "husets" stående buffet. Det serveres oppskåret frukt ved starten av dagen, samt kaker på ettermiddagen. Kaffe, te og mineralvann er tilgjengelig hele dagen

Middag Onsdag 07. November

Vi satser på at så mange som mulig deltar på en hyggelig sammenkomst på kvelden. Viss ingen har store innvendinger så prøver vi oss på Smelteverket på Mathallen (http://www.mathallenoslo.no/butikkene#smelteverket).

Kontaktinformasjon

Viss noen lurer på noe så ta kontakt med Sondre Rønjom på sondre.ronjom@nsm.stat.no eller tlf. 99 64 93 01