MANDAG:

09:00-09:30
Tor Helleseth - “Introduksjon”

09:30-10:15
Kristian Gjøsteen
Foredragstittel: "Protokollanalyse ved hjelp av sammensetning"

10:15-10:45
André Klingsheim
Foredragstittel: “Personvern på Internett”

10:45-11:00
Kaffepause

11:00-11:30
Christian Robenhagen Ravnshøj
Foredragstittel: "Egenskaber for hyperelliptiske kurver"

11:30-13:00
Lunch

13:00-13:30
Loren Olson
Foredragstittel: "Nye implementasjoner av ECC"

13:30-14:00
Hilja Huru
Foredragstittel: “Eliptiske kurver og kvantisering”

14:00-14:30
Øyvind Grinde
Foredragstittel: "ECC i akademia vs. industrien"

14:30-15:00
Øystein Thuen
Foredragstittel: "Paring-basert kryptografi"

15:00-15:10
Kaffepause

15:10-15:30
Tor Erling Bjørstad
Foredragstittel: "Båndbreddeeffektiv kryptering med RSA"

15:30-16:00
Michal Hojsik
Foredragstittel: "Fault attacks on cryptosystems"

TIRSDAG:

09:00-09:30
Igor Semaev
Solving MRHS linear equations

09:30-10:00
Johannes Mykkeltveit
Foredragstittel: "Irredusible ikkje-linær rekursjon"

10:00-10:10
Kaffepause

10:10-10:40
Slobodan Petrovic
Foredragstittel: "Rekonstruksjon av taktstyring sekvens i generalisert shrinking generator"

10:40-11:10
Olaf Garnaas
Foredragstittel: “Visualisering av kryptosystemer og andre flytdiagram”

11:10-11:40
Anders Paulshus
Foredragstittel: "Passord, entropi og kryptologi"

11:40-13:15
Lunch

13:15-13:45
Terje Jensen
Foredragstittel: "NSMs kryptoaktiviteter"

13:45-14:15
Turid Herland
Foredragstittel: "Rotorchiffer"

14:15-14:30
Kaffepause

14:30-15:00
Ole Kasper Klanderud Olsen
Foredragstittel: "SCIP: En interoperabel kryptoprotokoll"

15:00-15:45
Guang Gong "Stream Ciphers and Applications"