The Claude Shannon Institute Workshop on Coding & Cryptography
23rd & 24th May 2011
Kane Building, UCC

Schedule

Hosted by:
The Claude Shannon Institute for Discrete Mathematics, Coding, Cryptography and Information Security,
The Boole Centre for Research in Informatics, UCC
School of Engineering, UCC
School of Mathematical Sciences, UCC

Sponsored by:

This 2-day Workshop on Coding and Cryptography will be held in UCC on Monday 23rd & 24th May 2011. There is no registration fee but those interested in attending are requested to register for the event by emailing ni.osullivan@ucc.ie
SCHEDULE
MONDAY 23rd MAY 2011

OPENING
10:00 – 10:30 COFFEE AND REGISTRATION (Kane Building G2)

10.30-10.45 WELCOME ADDRESS
PROF JOHN MORRISON and PROF GARY McGUIRE

SESSION 1
10.45 – 11.25 MAX SALA, UNIVERSITY OF TRENTO
"On the provable security of BEAR/LION schemes”
11.25 – 11.50 GEOFFREY WALSH, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
"q-Analogues of Combinatorial Design”
11.50 – 12.15 CATHY McFADDEN, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
"Invariant Weights Related to Code Equivalence over Rings”
12.15 – 12.40 MARK FLANAGAN, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
"Stability of Iterative Decoding of Multi-Edge Type Doubly-Generalized LDPC Codes over the Binary Erasure Channel”

12.40-14.00 LUNCH

SESSION 2
14.00 – 14.40 JYRKI LAHTONEN, UNIVERSITY OF TURKU
"Estimating minimum determinants in a lattice of complex matrices”
14.40 – 15.05 PHIL HODGES, ECIT, QUEEN'S UNIVERSITY BELFAST
"Side Channel Attacks with Power Spectral Density Analysis”
15.05 – 15.30 DAVID CONTI, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
"Tail-Biting Trellises and Pseudocodewords”

15.30-15.45 COFFEE BREAK

SESSION 3
15.45 – 16.25 NATASA ZIVIC, UNIVERSITY OF SIEGEN
"Robustness of Secure Messages”
16.25 – 16.50 DUSHANTHA N.K. JAYAKODY, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
"Performance of QPSK-OFDM with LDPC and Concatenated Reed Solomon / Convolutional Coding in Outdoor Environments”
16.50 – 17.15 ANDREAS KENDZIORRA, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
"Invertible matrices over finite simple semirings with zero”

19:00 - DINNER IN CORNSTORE RESTAURANT (£25.00 per person to be paid at the Registration)
!!! (PLEASE BOOK WITH Ms Niamh O'Sullivan, ni.osullivan@ucc.ie)
TUESDAY 24th May 2011

SESSION 4
9.00 – 9.40 NORBERT GOERTZ, VIENNA UNIVERSITY OF TECHNOLOGY
“LDPC Convolutional Codes: Polynomial Description and Cycle Analysis”

9.40 – 10.05 WEIBO PAN, UNIVERSITY COLLEGE CORK
“A Correlation Power Analysis attack against Tate pairing on FPGA”

10.05 – 10.30 JENS ZUMBRAEGEL, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
“Algebraic Decoding of Negacyclic Codes over Z4”

10.30–10.45 COFFEE BREAK

SESSION 5
10.45 – 11.25 PARIS KITSOS, HELLENIC OPEN UNIVERSITY
“FPGA-based Considerations of SEED Block Cipher”

11.25 – 11.50 AKIKO MANADA, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
“A graph theoretical approach for wireless body area networks”

11.50–12.15 MAYUR PUNEKAR, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
“Trellis-Based Check Node Processing for Low-Complexity Nonbinary LP Decoding”

12.15–12.40 RICHARD MOLONEY, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
“Divisibility Properties of Kloosterman Sums”

12.50-14.00 LUNCH

SESSION 6
14.00 – 14.30 ARNAUD TISSERAND, CNRS-IRISA, LANNION
“Circuits for True Random Number Generation with On-Line Quality Monitoring”

14.30 – 14.55 SHRADDHA SRIVASTAVA, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE CORK
“Efficient decoding of BCH codes beyond the error correction capability”

14.55 – 15.20 VIJAYKUMAR SINGH, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
“On Characteristic polynomial of supersingular abelian varieties over finite fields”

15.20 – 15.45 OLIVER GNILKE, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
“Semigroup action problems”

15.45 – 16.00 CLOSE