

*The Claude Shannon Institute Workshop on
Coding & Cryptography
18th & 19th May 2009
Boole Lecture 1, UCC*

Schedule

Hosted by:

*The Claude Shannon Institute for Discrete Mathematics, Coding, Cryptography and Information Security,
The Boole Centre for Research in Informatics, UCC
Department of Electrical and Electronic Engineering, UCC
Department of Microelectronic Engineering, UCC
School of Mathematical Sciences, UCC*



Claude Shannon Institute
Discrete Mathematics, Coding and Cryptography
www.shannoninstitute.ie



Sponsored by:



**This 2-day Workshop on Coding and Cryptography will be held in UCC on Monday 18th & 19th May 2009.
There is no registration fee but those interested in attending are
requested to register for the event by emailing r.sarteschi@ucc.ie**

SCHEDULE

MONDAY 18th MAY 2009

OPENING

10:00 – 10:30 COFFEE AND REGISTRATION (Boole 1)

10.30-10.45 WELCOME ADDRESS

PROF PATRICK FITZPATRICK AND PROF GARY MCGUIRE

SESSION 1

10.45 – 11.25 PAULO BARRETO, ESCOLA POLITÉCNICA, UNIVERSITY OF SÃO PAULO
“How to obtain short McEliece keys using Goppa codes”

11.25 – 11.50 VIJAY G. SUBRAMANIAN, HAMILTON INSTITUTE, NUI MAYNOOTH
“On a class of optimal rateless codes”

11.50 – 12.20 LIANG LU, ECIT, QUEEN’S UNIVERSITY BELFAST
“High performance FPGA evaluation of ECHO function”

12.20 – 12.45 MARK FLANAGAN, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
“Weight Distributions of Doubly-Generalized LDPC Codes”

12.45-2.00 LUNCH

SESSION 2

2.00 – 2.40 MARIA BRAS AMORÓS, UNIVERSITAT ROVIRA I VIRGILI
“From the Euclidean Algorithm for Solving a Key Equation for Dual Reed-Solomon Codes to the Berlekamp-Massey Algorithm”

2.40 – 3.05 YINGXI LU, ECIT, QUEEN’S UNIVERSITY BELFAST
“Random Delay Insertion: Effective Countermeasure against DPA on FPGAs”

3.05 – 3.30 VITALY SKACHEK, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
“On LP Decoding of Nonbinary Expander Codes”

3.30-3.45 COFFEE BREAK

SESSION 3

3.45 – 4.25 CHRIS MITHELL, ROYAL HOLLOWAY, UNIVERSITY OF LONDON
“A simple construction for perfect factors in the Bruijn graph”

4.25 – 4.50 FRANCISCO DANIEL RUÍZ PEREDA, UNIVERSITY OF ALCALÁ
“Performance and application of codes derived from Complementary Set of Sequences”

4.50 – 5.15 ALEXEY ZAYTSEV, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
“Explicit equations of maximal and minimal curves of genus 3”

**7:00 - DINNER IN RISTORANTE CASANOVA (€23.00 per person to be paid at the Registration, drinks are not included)
87 North Main Street, Cork City**

!!!(PLEASE BOOK WITH Rita Sarteschi, r.sarteschi@ucc.ie)

TUESDAY 19th May 2009

SESSION 4

9.00 – 9.40 EMMANUEL PROUFF, OBERTHUR TECHNOLOGIES

“Combining Information Theory and Side Channels to Attack (Secure) Implementations”

9.40 – 10.05 GEOFFREY WALSH, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“Error Correction for Random Network Coding”

10.05 – 10.30 ANDREAS KENDZIORRA, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“Network coding with modular lattices”

10.30–10.45 COFFEE BREAK

SESSION 5

10.45 – 11.25 NIGEL BOSTON, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“Golay pseudocodewords”

11.25 – 12.00 JUNFENG FAN, KATHOLIEKE UNIVERSITEIT LEUVEN, COSIC

“Faster \mathbb{F}_p -arithmetic for Cryptographic Pairings on Barreto-Naehrig Curves”

12.00– 12.25 IRYNA ANDRIYANOVA, ENSEA/UNIVERSITY OF CERGY-PONTOISE/CNRS, ETIS GROUP

“Asymptotic Weight Distribution of Non-Binary LDPC Codes”

12.25 – 12.50 NAOMI BENGER, CLAUDE SHANNON INSTITUTE, DUBLIN CITY UNIVERSITY

“On the security of pairing-friendlyabelian varieties over non-prime fields”

12.50-1.50 LUNCH

SESSION 6

1.50 – 2.30 ROLANDO CARRASCO, UNIVERSITY OF NEWCASTLE UPON TYNE

“Design of Non-Binary Error-Correction Codes and their Applications”

2.30 – 2.55 BRIAN BALDWIN, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE CORK

“FPGA Implementations of SHA-3 Candidates: CubeHash, Grøstl, Lane, Shabal and Spectral Hash”

2.55 – 3.20 JENS ZUMBRÄGEL, UNIVERSITY COLLEGE DUBLIN

“The product recovery problem for black box groups”

3.20 – 3.45 MAURA PATERSON, ROYAL HOLLOWAY, UNIVERSITY OF LONDON

“Properties of distinct-difference configurations and lightweight key predistribution schemes for grid-based networks”

3.45 – 4.10 EIMEAR BYRNE, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“Upper Bounds for Codes over Finite Rings”

4.15 CLOSE