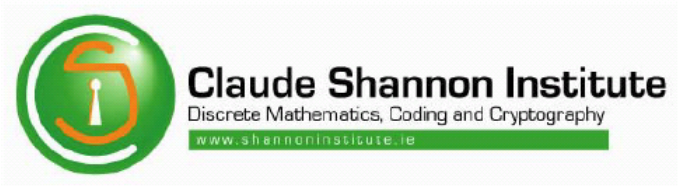

THE CLAUDE SHANNON INSTITUTE WORKSHOP ON CODING AND CRYPTOGRAPHY

21ST & 22ND MAY 2012

G2, Kane Building, UCC

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

School of Engineering, UCC

School of Mathematical Sciences, UCC

Monday 21 May 2012

10.30-11 Registration and Coffee

11-11.05 Opening address(Prof. Bernard Hanzon, School of Mathematical Sciences, UCC)

11.05-11.30 Gary McGuire(CSI-UCD), Supersingular Algebraic Curves in Cryptography and Coding Theory

11.30-12 Nalin Kumara Jayakody(CSI-UCD), Performance comparison of LDPC coded Estimate-Forward and Direct-Soft-Forward relay on soft information

12-12.30 Ted Hurley(UCG), Abstract algebraic structures as building blocks

12.30-1.30 Lunch

1.30-2 Victor Cionca(Tyndall), Security and vulnerabilities in networked embedded systems

2-2.30 Jens Zumbraegel(CSI-UCD), On the algebraic representation of certain optimal non-linear binary codes

2.30-3 Oliver Gnilke(CSI-UCD), A two-party key establishment protocol based on semirings

3-3.30- Coffee

3.30-4 Michael Clear(TCD), Towards Fully-Homomorphic Predicate Encryption

4-4.30 Richard McSweeney(CSI-UCC), Low Latency Reed-Solomon Decoder for High Duty-Cycle Applications

4.30-5 Robert Granger(CSI-DCU), Faster algorithms for Crandall prime field arithmetic for ECC

7.30 Banquet (Cornstore Restaurant, Cornmarket street, Cork city centre)

Tuesday 22 May 2012

9.30-10.30 Neeli Prasad(CTIF), WSN MAC Layer Security issues: A UML Approach

10.30-11 Danny Lynch(CSI-UCD), On Properties of the Mirimanoff Polynomial

11-11.15 Coffee

11.15-11.45 David Boyle(Tyndall), Practical considerations for the implementation of coding and cryptography in current generation networked embedded systems – an applied perspective

11.45-12.15 Naoise Mac Suibhne(Tyndall), An Introduction to Optical Modulation

12.15-12.45 Cathy McFadden(CSI-UCD), Graph-Based Decoding of Ring-Linear Low-Density Parity-Check Codes

12.45-1.15 Mark Hamilton(CSI-UCC), FPGA Implementation of an Elliptic Curve Digital Signature Processor

1.15 Close