

The Claude Shannon Institute Workshop on

Coding & Cryptography

18th & 19th May 2009

Boole Lecture 1, UCC

Abstracts

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**

ABSTRACTS
MONDAY 18th MAY 2009

SESSION 1

10.45 – 11.25 PAULO BARRETO, ESCOLA POLITÉCNICA, UNIVERSITY OF SÃO PAULO

“How to obtain short McEliece keys using Goppa codes”

The classical McEliece cryptosystem is built upon Goppa codes, which remain secure to this date but lead to very large keys. I will describe a subclass of Goppa codes that reduce the size of McEliece keys by an almost linear factor, with the added benefit of improving the efficiency of cryptographic operations to subquadratic time.

11.25 – 11.50 VIJAY G. SUBRAMANIAN, HAMILTON INSTITUTE, NUI MAYNOOTH

“On a class of optimal rateless codes”
Joint work with Doug Leith, Venkatramana Badarla and David Malone.

We analyze a class of systematic fountain/rateless codes constructed using Bernoulli(1/2) random variables. Using simple bounds we then show that this class of codes stochastically minimizes the number of coded packets receptions needed to successfully decode all the information packets. This optimality holds over a large class of random codes that includes Bernoulli(q) random codes with $q \leq 1/2$ and LT codes. We also demonstrate the asymptotic optimality for intermediate decoding of the same codes. Finally, we conclude with an application of these codes in the context of dynamic routing.

11.50 – 12.20 LIANG LU, ECIT, QUEEN’S UNIVERSITY BELFAST

“High performance FPGA evaluation of ECHO function”

In response to the NIST cryptographic SHA-3 hash project, the ECHO hash function was developed and it has been accepted as a candidate in the first round of the competition. ECHO employs the Merkle-Damgard compression technique with the well-known AES block cipher. Its hash output can vary in length from 128 to 512 bits. To date, no attacks have been reported against the ECHO algorithm. As part of the evaluation of this hash function, a high performance hardware architecture has been designed and implemented on a Xilinx Virtex 5 FPGA device. In order to achieve a high throughput rate, a fully autonomous architecture is considered. The design study shows that this architecture can achieve a throughput rate of over 17Gbps. To the authors’ knowledge this is the fastest hash function design reported to date and is 70% faster than other evaluated SHA-3 high speed FPGA implementations. With this significant advantage in throughput rate, ECHO is as strong candidate for employment in satellite communication or network communication applications that require significant real-time data processing.

12.20 – 12.45 MARK FLANAGAN, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“Weight Distributions of Doubly-Generalized LDPC Codes”

Doubly-generalized LDPC (D-GLDPC) codes provide a means of imposing structure on sparse graph code ensembles. In this talk we provide a complete solution for the asymptotic weight distribution of irregular D-GLDPC codes. For small linear-weight codewords, we present a compact analytical result which identifies a key parameter discriminating between asymptotically good and bad distance behaviour. For the general case, a polynomial-system solution is presented for the asymptotic weight distribution.

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”

The two primary decoding algorithms for Reed-Solomon codes are the Berlekamp-Massey algorithm and the Sugiyama et al. adaptation of the Euclidean algorithm, both designed to solve a key equation. We will present a new version of the key equation and a way to use the Euclidean algorithm to solve it. A straightforward reorganization of the algorithm yields the Berlekamp-Massey algorithm.

2.40 – 3.05 YINGXI LU, ECIT, QUEEN'S UNIVERSITY BELFAST

“Random Delay Insertion: Effective Countermeasure against DPA on FPGAs”

Side-channel attacks (SCA) threaten electronic cryptographic devices and can be carried out by monitoring the physical characteristics of security circuits. Differential power analysis is the most widely studied side-channel attack. In recent years numerous countermeasures against the DPA attack of security algorithm hardware implementations have been proposed. In this talk, we will discuss the Random Delay Insertion (RDI) countermeasure. Previous research has presented RDI for microprocessor implementations, which proved that RDI is not successful on smartcard platform; however, its security properties in relation to hardware implementations have not been investigated in detail. In this work, we implement the first hardware security architecture with RDI on an Field Programmable Gate Array (FPGA) device. We prove both theoretically and practically that it is an effective technique on FPGA devices and we propose a set of critical parameters that can be utilized to optimize a security algorithm design with RDI in terms of area, speed and power.

3.05 – 3.30 VITALY SKACHEK, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“On LP Decoding of Nonbinary Expander Codes”

A linear-programming (LP) decoder for nonbinary expander codes is presented. It is shown that the proposed decoder has the maximum-likelihood certificate properties. It is also shown that this decoder corrects any pattern of errors of a relative weight up to approximately $\frac{1}{4} \frac{\delta_A}{\delta_B}$ (where δ_A and δ_B are the relative minimum distances of the constituent codes). This work can be viewed as a nonbinary generalization of the work of Feldman and Stein, SODA, 2005.

SESSION 3

3.45 – 4.25 CHRIS MITHELL, ROYAL HOLLOWAY, UNIVERSITY OF LONDON

“A simple construction for perfect factors in the Bruijn graph”

In this paper we address the existence question for Perfect Factors in the de Bruijn graph (which, for simplicity, we refer to as Perfect Factors). Such Perfect Factors correspond to sets of uniformly long cycles with elements drawn from an alphabet of size c , and in which every possible v -tuple (or ‘window’) of elements occurs exactly once. They are of significance for two main reasons (apart from combinatorial interest in their own right).

- They can be used to construct Perfect Maps (or two-dimensional de Bruijn arrays), which are of practical importance in certain position-location applications.
- They are special cases of Perfect Maps themselves, and hence their existence is significant in deciding whether Perfect Maps exist for all parameter sets satisfying certain simple necessary conditions (these necessary conditions are known to be sufficient for prime power size alphabets).

It has been conjectured that the simple necessary conditions for the existence of a Perfect Factor are sufficient for all finite alphabets and for all window sizes. This conjecture has been shown to be true for specific classes of alphabet size c (for every v), and it has also been shown to be true for small values of v regardless of the alphabet size.

The truth of the conjecture was established by Etzion (1988) for $c=2$ and by Paterson (1995) in the case where c is a prime power. Subsequent work has enabled the existence question for any particular v to be reduced to an existence question concerning a finite number of ‘small’ parameter sets. These ideas were used by Mitchell (1993/1994) to settle the existence question for $v \leq 4$. Further progress was made by Mitchell and Paterson (1998) who resolved the existence question was resolved for $v \leq 6$. In this paper we make further progress on the existence question for Perfect Factors.

4.25 – 4.50 FRANCISCO DANIEL RUÍZ PEREDA, UNIVERSITY OF ALCALÁ

“Performance and application of codes derived from Complementary Set of Sequences”
Joint work with Maria Carmen Pérez Rubio, Jesús Ureña Ureña and Álvaro Hernández Alonso

Proper encoding improves the performance of ultrasonic sensory systems based on times-of-flight measurements in terms of noise immunity, capability of simultaneous measurements and precision in the obtained results. Complementary sets of sequences (CSS) are being employed in such systems because of the ideal properties of the sum of their correlation functions and the possibility of applying an efficient detection algorithm which decreases the time required for their correlation.

However, they limit the number of simultaneous emissions to the number of sequences in the set. Recently, these CSS have been used to construct codes with Zero Correlation Zones (ZCZ) such as Loosely Synchronous (LS) or Three Zero Correlation-Zone (T-ZCZ) codes, which overcome the previous limitation and can be successfully applied in quasi-synchronous CDMA.

This work is devoted to evaluate the performance of CSS, LS and a new family of T-ZCZ codes for their application in a real ultrasonic scenario such as a privacy-oriented local positioning system, where aperiodic emission, multiple-access interference, multipath and near-far effect are quite common.

4.50 – 5.15 ALEXEY ZAYTSEV, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“Explicit equations of maximal and minimal curves of genus 3”

In this talk we discuss the properties of maximal and minimal curves of genus 3 over finite fields of discriminants -19 , -43 , -67 and -163 . We prove that any such curve can be given by an explicit equation of special form. Using these equations we compute some maximal and minimal curves over finite fields with discriminants -19 , -43 and -67 .

TUESDAY 19th May 2009

SESSION 4

9.00 – 9.40 EMMANUEL PROUFF, OBERTHUR TECHNOLOGIES

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

Side Channel Analysis (SCA) is a cryptanalytic technique that consists in analyzing the physical leakage produced during the execution of a cryptographic algorithm embedded on a physical device. This side channel leakage is indeed statistically dependent on the intermediate variables of the computation which enables key recovery attacks. A large variety of SCA performed on embedded devices involve the linear correlation coefficient as wrong-key distinguisher. This coefficient is actually a sound statistical tool to quantify linear dependencies between univariate variables. However, when those dependencies are non-linear, the correlation coefficient stops being pertinent so that another statistical tool must be investigated. Recent works showed that the Mutual Information (MI for short) measure is a promising candidate, since it detects any kind of statistical dependency. Substituting it for the correlation coefficient may therefore be considered as a natural extension of the existing attacks. Nevertheless, the first applications published at CHES 2008 have revealed several limitations of the approach and have raised several questions. In this presentation, we expose the theoretical foundations behind MI-based attacks and we clarify its limitations and assets. We apply it against a flawed countermeasure and we compare its efficiency with the one of correlation-based attacks. We also extend the works recently published at CHES 2008 conference. We argue that in critical contexts (when implementations are protected with masking) MI-based attacks potentially bring improvements compared to existing attacks, because they directly extend to multivariate statistics while, e.g. correlation or Kocher's difference-of-mean generally need to be tweaked to apply to such contexts. Our argumentation will be based on theoretical analyses and on simulations and practical experiments on both hardware and software implementations.

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

“Error Correction for Random Network Coding”

The central idea in network coding is that instead of simply forwarding data, intermediate nodes in a network may combine several incoming independent information flows to produce a new outgoing information flow. The main benefit of the network coding approach is the potential to dramatically increase the throughput of a network. The aim of this poster is to introduce the concepts behind network coding and to outline a recent approach for error correction in network codes.

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

“Network coding with modular lattices”

We introduce a generalisation of the subspace codes for random network coding of Koetter and Kschischang to modular lattices. This generalisation is used to apply submodule lattices for random network coding, especially subgroup lattices of finite abelian p -groups. We present bounds on these codes and an idea for a construction of codes, which are subsets of subgroup lattices.

SESSION 5

10.45 – 11.25 NIGEL BOSTON, UNIVERSITY COLLEGE DUBLIN

“Golay pseudocodewords”

An old question asks if there exists an AWGN pseudocodeword for the extended binary Golay code of pseudoweight < 8 . We explain these terms and the practical importance of pseudoweight and then use a new multivariate weight enumerator to attack it.

11.25 – 12.00 JUNFENG FAN, KATHOLIEKE UNIVERSITEIT LEUVEN, COSIC

“Faster F_p -arithmetic for Cryptographic Pairings on Barreto-Naehrig Curves”

We describe a new method to speed up F_p -arithmetic for Barreto-Naehrig (BN) curves. We explore the characteristics of the modulus defined by BN and choose curve parameters such that F_p multiplication becomes more efficient. The proposed algorithm uses Montgomery reduction in a polynomial ring combined with a coefficient reduction phase using a pseudo-Mersenne number. With this algorithm, the performance of pairings on BN curves can be significantly improved, resulting in a factor 4 speed-up compared with existing hardware implementations.

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

“Asymptotic Weight Distribution of Non-Binary LDPC Codes”

We present the first part of the investigation if one achieves asymptotically the capacity of a binary-input binary-output memoryless symmetric channel under ML decoding by using non-binary LDPC codes.

We consider (l,r) -regular LDPC codes both over finite fields and over the general linear group and compute asymptotic binary weight distributions for these ensembles in the limit of large blocklengths and of large alphabet sizes.

A surprising fact, average binary weight distributions that we obtain do not tend to the binomial one for values of normalized binary weights smaller than $1 - 2^{-(l/r)}$.

However, it does not mean that non-binary codes do not achieve the capacity asymptotically, but rather that there exists some exponentially small fraction of codes in the ensemble, which contains an exponentially large number of codewords of poor weight. At the end of the talk, we present the justification of such behaviour.

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

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

Let A be an abelian variety defined over a non-prime finite field F_q that has embedding degree k with respect to a subgroup of prime order r . In this presentation we give explicit conditions on q , k , and r that imply that the minimal embedding field of A with respect to r is F_{q^k} . When these conditions hold, the embedding degree k is a good measure of the security level of a pairing-based cryptosystem that uses A . We apply our theorem to supersingular elliptic curves and to supersingular genus 2 curves, in each case computing a maximum ρ -value for which the minimal embedding field must be F_{q^k} . Our results are in most cases stronger (i.e., give larger allowable ρ -values) than previously known results for supersingular varieties, and our theorem holds for general abelian varieties, not only supersingular ones.

SESSION 6

1.50 – 2.30 ROLANDO CARRASCO, UNIVERSITY OF NEWCASTLE UPON TYNE

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

This presentation introduces the design methods of different non-binary error-correction codes and their suitable applications. Efficient decoding systems for these codes are proposed with methods to reduce complexity and the performance is evaluated demonstrating the impressive error-correction capability of non-binary codes. First, several methods of construction for non-binary quasi-cyclic (QC) Low Density Parity Check (LDPC) codes are introduced, using primitive elements in finite fields and also codewords from Reed-Solomon codes with two information symbols. Details on how to construct LDPC codes with large girths are also included. To reduce the complexity of the Belief Propagation (BP) decoding algorithm it is shown that its Horizontal step consists of convolution operations that can be replaced with Fast Fourier Transforms (FFTs). Secondly, Ring-Trellis Coded Modulation (Ring-TCM) codes are introduced. The Ring-TCM codes perform very well in slow fading scenarios, but more importantly they can also achieve a high information throughput which is an important requirement in cooperative systems. Simulation results show Ring-TCM codes can significantly outperform a binary trellis code with high order modulation schemes. Finally, Algebraic-Geometric (AG) codes are introduced. The AG code is constructed from an irreducible projective curve and offer powerful error-correction, particularly for long bursts of errors. They can be seen as a natural replacement to replace Reed-Solomon codes in the future. Several decoding algorithms for AG codes are introduced, including the Sakata decoding algorithm, the hard-decision list decoding algorithm and the soft-decision list decoding algorithm. Simulation results show that AG codes are very good candidates for use in storage devices with high storage densities and significant inter-symbol interference and at the same time are not subject to error floors, which is not the case LDPC and turbo codes.

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”

Hash functions are widely used in, and form an important part of many cryptographic protocols. Currently, a public competition is underway to find a new hash algorithm(s) for inclusion in the NIST Secure Hash Standard (SHA-3). Computational efficiency of the algorithms in hardware will form one of the evaluation criteria. In this presentation, we focus on five of these candidate algorithms, namely CubeHash, Grøstl, Lane, Shabal and Spectral Hash. Using Xilinx Spartan-3 and Virtex-5 FPGAs, we present architectures for each of these hash functions, and explore area-speed trade-offs in each design. The efficiency of various architectures for the five hash functions is compared in terms of throughput per unit area. To the best of the authors' knowledge, this is the first such comparison of these SHA-3 candidates.

2.55 – 3.20 JENS ZUMBRÄGEL, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“The product recovery problem for black box groups”

We propose to study the following problem (product recovery problem): Given a set $S=\{1,2,\dots,n\}$ and oracle access to a hidden binary operation on S as well as some a priori information on the binary operation, what is the minimal number of (single) queries " $x*y=?$ " to the oracle such that the binary operation is uniquely determined by its answers? (Subsequent queries may depend on given answers. The a priori information is specified by a set of possible binary operations, for example the set of all group operations.)

We present general lower bounds for the number of queries. We also give an upper bound together with an algorithm for the case that the operation is an abelian group operation. Finally, we report on ongoing work concerning the case of nonabelian 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”

Distinct-difference configurations are combinatorial objects that can be seen as a generalisation of Costas arrays. They were proposed for use in the distribution of keys to the nodes in a wireless sensor network in which the nodes are arranged in a square grid. In this talk we present some recent bounds on certain properties of these configurations, and we discuss techniques for constructing configurations that lead to key predistribution schemes with useful connectivity properties.

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

“Upper Bounds for Codes over Finite Rings”

The important discovery in the 1990s that several families of good binary nonlinear codes have a \mathbf{Z}_4 -linear representation reinvigorated the study of algebraic codes over finite rings. By now several papers have been written on the subject, on topics ranging from MacWilliams’ extension and duality theorems, to code optimality to decoding. A linear $[n, d]$ code C over a finite ring R is a submodule of ${}_R R^n$ such that the minimum weight of any word of C for a given weight function is d . A fundamental question in coding theory is to determine the value of $B_R(n, d)$, the maximal number of codewords a linear $[n, d]$ code over R can have. For this reason upper bounds on $B_R(n, d)$ are sought. A new weight function (which may be viewed as a natural generalisation of the Hamming weight for codes over finite rings), namely the homogeneous weight has emerged as useful in the context of finite rings. Examples of homogeneous weights include the Hamming weight on finite fields and the Lee weight on \mathbf{Z}_4 . In this talk we discuss bounds on codes over finite rings for the homogeneous weight, including generalizations of the classical Plotkin, Elias, linear programming and Singleton bounds. We give some examples of codes meeting these bounds.

4.15 CLOSE