

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

Abstracts

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*



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



BOOLE CENTRE
FOR RESEARCH IN **INFORMATICS**

Sponsored by:



science foundation ireland
fondúireacht eolaíochta éireann

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

MONDAY 23rd MAY 2011

OPENING

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

10.30-10.45 WELCOME ADDRESS

PROF PATRICK FITZPATRICK AND PROF GARY MCGUIRE

SESSION 1

10.45 – 11.25 MAX SALA, UNIVERSITY OF TRENTO

“On the provable security of BEAR/LION schemes”

Abstract:

BEAR, LION and LIONESS are block ciphers presented by Biham and Anderson (1996), inspired by the famous Luby-Rackoff constructions of block ciphers from other cryptographic primitives (1988). The ciphers proposed by Biham and Anderson are based on one stream cipher and one hash function. Clearly, good properties of the primitives ensure good properties of the block cipher. In particular, they are able to prove that their ciphers are immune to any efficient known-plaintext key-recovery attack that can use as input ONE plaintext-ciphertext pair. Our contribution is showing that they are actually immune to any efficient known-plaintext key-recovery attack that can use as input ANY number of plaintext-ciphertext pairs. We are able to get this improvement by using weaker hypotheses on the primitives.

This is joint work with Anna Rimoldi, Lara Marines and Matteo Piva. This work has been supported by TELS Y Elettronica e Telecomunicazioni S.p.A, an Italian company working in Information and Communication Security.

11.25 – 11.50 GEOFFREY WALSH, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
“q-Analogues of Combinatorial Design”

Abstract:

In the 1970's Delsarte introduced the notion of a q -analogue of a combinatorial design, in which point sets are replaced by vector spaces over a finite field of order q [2]. Since 2008 there has been resurgence of interest in these q -analogues, due to the observation that the q -analogues of certain combinatorial designs are in fact optimal error correction codes for random network coding. This talk details recent research into a class of q -analogue designs, that exhibit a high degree of regularity. These are collections of k -dimensional vector spaces over a finite field which are completely regular, in the sense defined by Delsarte [1]. In particular, we investigate the existence and geometric structure of completely regular q -analogue designs, with small strength. This research generalizes the work of Martin [3] [4], on classical combinatorial designs.

References

- [1] P. Delsarte An algebraic approach to association schemes of coding theory. Phillips Res. Repts. Suppl., vol. 10, 1973.
- [2] P. Delsarte Association schemes and t -designs in regular semilattices. J. Combin. Theory Ser. A, vol. 20, 1976.
- [3] W.J. Martin Completely regular subsets. Ph.D. Thesis, University of Waterloo, 1992.
- [4] W.J. Martin Completely regular designs of strength one. J. Combin. , vol. 3, pp.177-185, 1994.

11.50 – 12.15 CATHY McFADDEN, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“Invariant Weights Related to Code Equivalence over Rings”

Abstract:

In network applications providing a high data throughput is of great importance. To increase the performance of a network a hardware accelerator can be used to perform computationally intensive cryptographic operations. We describe a FPGA implementation of a System on Chip capable of providing hardware acceleration for various cryptographic protocols such as the TLS protocol. A Xilinx Microblaze processor is used to control all data transfer operations on the chip while various hardware blocks are used to perform elliptic curve arithmetic, data hashing, data encryption and random number generation.

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”

Abstract:

Using the EXIT chart approach, a necessary and sufficient condition is developed for the local stability of iterative decoding of multi-edge-type (MET) doubly-generalized low-density parity-check (D-GLDPC) code ensembles. In such code ensembles, the use of arbitrary linear block codes as component codes is combined with the further design of local Tanner graph connectivity through the use of multiple edge types. The stability condition for these code ensembles is shown to be succinctly described in terms of the value of the spectral radius of an appropriately defined polynomial matrix.

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”

Abstract:

Lattices of complex matrices form a natural choice for a multi-antenna radio signal constellation. Theoretical work ties the minima of determinants over non-trivial choices of signals to the asymptotic performance of the communication system. The behavior of the minimum determinant as a function of the size of the lattice coefficients then emerges as a natural problem. There is a sharp contrast between the single user and multiple user cases in that in the former case the determinants can be bounded away from zero, but in the latter case it is impossible to do so, and the determinants necessarily will decay towards zero. I will explain the mathematical reasons for this different behavior, and survey explicit and conjectural lattice constructions as well as what is known about the decay function. All the proposed constructions rely on algebraic number theory, and the lower bounds to the decay function rely on the theory of Diophantine approximation.

14.40 – 15.05 PHIL HODGES, CSIT, QUEEN’S UNIVERSITY BELFAST
“Side Channel Attacks with Power Spectral Density Analysis”

Abstract

Cryptographic algorithms are used widely today to help secure important personal and financial information. Although these encryption algorithms have been designed to be computationally secure, it has been shown that when implemented in hardware, that these devices leak Side Channel Information that can be used to mount an attack that recovers the secret encryption key. In this presentation an overlapping window Power Spectral Density (PSD) Side Channel Attack (SCA), targeting an FPGA device running the Advanced Encryption Standard (AES) is proposed. It is shown that it is possible to extract the relevant information from both aligned and misaligned data set, whilst also overcoming the issues of sampling boundaries.

15.05 – 15.30 DAVID CONTI, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN
“Tail-Biting Trellises and Pseudocodewords”

Abstract:

Tail-Biting Trellises (TBT) are labeled graphs that represent codes and are used for decoding purposes. For a given code C one can construct different TBT’s that represent C . A standard problem is to find a TBT for C of smallest size, since the complexity of trellis-based decoding algorithms depends on the size of the chosen TBT. On the other hand iterative decoding failure on a TBT can arise from so called pseudocodewords, and small trellises can have many pseudocodewords. In this talk we will introduce the language of trellises and pseudocodewords, by presenting some problems and a motivating conjecture on a special TBT for the Golay code. We will show as well how an algebraic framework can be constructed to help us studying and understanding pseudocodewords.

15.30-15.45 COFFEE BREAK

SESSION 3

15.45 – 16.25 NATASA ZIVIC, UNIVERSITY OF SIEGEN

“Robustness of Secure Messages”

Abstract:

The messages which will be considered are secured by Message Authentication Codes, to provide security services as data integrity and authentication of origin for the receiver. Data integrity provides the recognition of any modification or manipulation of the message. Authentication convinces the receiver that the message is originated by the sender who shares the used secret key with the receiver. The Message Authentication Codes are very sensitive to any change of the message, which causes the modification of around 50% of the bits of the Message Authentication Code. Such error propagation is known as ‘avalanche effect.’

The verification process calculates the Message Authentication Code over the received message and compares it with the received Message Authentication Code. The message is accepted only if both Message Authentication Codes are identical. This condition is too strict for some applications, when many errors occur during transmission or storage, because not all of them can be corrected before the verification is performed. This presentation will give an overview of different approaches to overcome this problem and to introduce robustness of secure messages. One approach is to accept messages which result in slightly different Message Authentication Codes and a new approach is to correct messages using ‘avalanche effect’ of Message Authentication Codes.

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”

Abstract:

This presentation presents a performance comparison of two different channel coding techniques for use with an orthogonal frequency-division multiplexing (OFDM) system. The system operates in an outdoor environment and achieves coding gain by the use of a low-density parity-check (LDPC) code or a concatenated Reed Solomon -convolutional code (RS-CC). A concatenated code is a popular class of block code which operates by consecutively combining an outer code and inner code; this is a solution to the problem of finding a code with an exponential decrease in error probability as the block length increases, together with polynomial-time decoding complexity. LDPC codes are a relatively new channel code class capable of near-Shannon-limit performance over many practical communication channels. In this paper, we provide link level performance results for both LDPC and RS-CC coding used in a non-line-of-sight QPSK-OFDM system over Rayleigh fading channels. Performance results are documented for the COST 207 (Typical Urban and Bad Urban) channel as well as the Winner 2.8 scenario NLOS channel.

16.50 – 17.15 ANDREAS KENDZIORRA, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“Invertible matrices over finite simple semirings with zero”

Abstract:

In 2007 Monico, Maze and Rosenthal proposed new methods for public key cryptography based on semigroup actions. Some of these actions involve matrices over finite simple semirings and especially matrices over proper finite simple semirings with zero. If one uses matrices for cryptography the question arises when a matrix is invertible and how easy it is to find the inverse of an invertible matrix. To answer these questions we use the classification of finite simple semirings by Zumbrägel which says that every proper finite simple semiring with zero and more than two elements is isomorphic to a certain semiring of residuated mappings (complete supremum-morphisms) of a finite lattice. With this we find a characterization of invertible matrices over proper finite simple semirings with zero, a construction for the inverse of an invertible matrix and the number of invertible matrices in a matrix semiring over a proper finite simple semiring with zero.

TUESDAY 24th May 2011

SESSION 4

9.00 – 9.40 NORBERT GOERTZ, VIENNA UNIVERSITY OF TECHNOLOGY

“LDPC Convolutional Codes: Polynomial Description and Cycle Analysis”

Abstract:

Time-invariant LDPC Convolutional Codes (LDPCccs) generated from quasi-cyclic block codes are known to perform well at limited block size, and they are interesting for practical applications: they can be terminated as required to obtain a desired block size, they can be efficiently encoded, and known LDPCcc constructions from quasi-cyclic LDPC block codes allow for reasonably good code designs for a variety of code rates. Moreover, they can be efficiently decoded by a pipelined decoder that can be scheduled in parallel, allowing for fast realisation in programmable hardware.

We show that the LDPCccs under consideration can be equivalently described by a polynomial syndrome former of limited size, in which code analysis is much easier than in the original semi-infinite time-domain syndrome former. We show how to obtain the polynomial syndrome former from the parity-check matrix, and we discuss how cycles form in both code representations. We then analyse cycles in the polynomial syndrome former and we demonstrate that time-invariant LDPCccs based on quasi-cyclic block codes must have 12 cycles. This is known to be a structural property of the code design, no matter what the specific choice of the parity-check matrix is. We extend the analysis to the more general case that the polynomial syndrome former contains polynomial entries (not only monomials) and we demonstrate that unavoidable cycles, even shorter than length 12, start to form: hence, we conclude that non-monomial entries should be avoided by the code design.

We also use the polynomial description to find codes with better cycle properties that, by simulation, are shown to have better bit-error performance (under message-passing decoding) than LDPCccs (with comparable rate and blocksize) derived from quasi-cyclic block codes.

Joint work with Hua Zhou, TU Wien

9.40 – 10.05 WEIBO PAN, UNIVERSITY COLLEGE CORK

“A Correlation Power Analysis attack against Tate pairing on FPGA”

Abstract:

Pairings on elliptic curves are deeply researched and used in applications such as identity based schemes. Recently there have been several hardware implementations of the Tate Pairing. Along with the algorithms, their security has to be considered. We will present a correlation power analysis (CPA) attack against a Tate pairing implementation.

Real power traces are taken from the FPGA implementation. The experimental result shows a successful attack.

10.05 – 10.30 JENS ZUMBRAEGEL, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“Algebraic Decoding of Negacyclic Codes over Z_4 ”

Abstract:

We investigate Berlekamp's negacyclic codes and discover that these codes, when considered over the integers modulo 4, do not suffer any of the restrictions on the minimum distance observed in Berlekamp's original papers. We present an algebraic decoding algorithm for this class of codes that corrects any error pattern of Lee weight up to t . Our treatment uses Grobner bases, the decoding complexity is quadratic in t . We also indicate how the decoding method can be applied to correct more than t errors when the minimum Lee distance is larger than $2t+1$.

Joint work with Eimear Byrne, Marcus Greferath, and Jaume Pernas.

10.30–10.45 COFFEE BREAK

SESSION 5

10.45 – 11.25 PARIS KITSOS, HELLENIC OPEN UNIVERSITY

“FPGA-based Considerations of SEED Block Cipher”

Abstract:

SEED block cipher has been adopted by the International Organization for Standardization (ISO/IEC 18033-3) standard. In this presentation FPGA-based designs are presented. Designs for high throughput and low

hardware resources will be presented. The new embedded functions of the XILINX SPARTAN-3A and VIRTEX-5 such as DSP blocks and BRAMs are used in order to examine the efficiency of each design. The above features minimize the usage of registers and Look-Up-Tables (LUTs).

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

Abstract:

Modern medical wireless systems, such as wireless body area networks (WBANs), are applications of wireless networks that can be used as a communication tool between clients and medical personnel. In a WBAN, miniature sensors are attached to a client to send health information (such as heart rate or blood pressure) via relays to a receiver. Accuracy of data is highly demanded for WBANs, while coding schemes for WBANs require less complexity and computations so as to be used by low-power devices. In this talk, we will present a coding scheme, based on a scheme proposed by S. Marinkovic and E. Popovici, which is robust to packet erasures. We consider a graph representation of such a coding scheme and define its decoding probability which can be a measurement of the robustness against packet erasures. We also provide some properties of graph representations with high decoding probabilities.

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

Abstract:

Binary and nonbinary Low-Density Parity-Check (LDPC) codes have attracted much attention in the research community in the past decade. LDPC codes are generally decoded by the iterative Belief Propagation (BP) algorithm which performs remarkably well at moderate noise levels. However, at low noise levels BP suffers from so called error-floor problem. In recent years, the new approach of Linear Programming (LP) decoding is emerging as an attractive alternative to the BP decoding. In LP decoding, the maximum likelihood decoding problem is modelled as an LP problem. The resulting LP program can then be solved with the help of standard LP solvers such as Simplex. However, the time complexity of the Simplex is known to be exponential in number of variables. Hence, the earliest LP decoders proposed for binary and nonbinary LDPC codes which relies on Simplex are not suitable for use at moderate and large code lengths. To overcome this problem, Vontobel et al. developed an iterative Low-Complexity LP (LCLP) decoding algorithm for binary LDPC codes. This binary LCLP decoding algorithm is related to the binary BP algorithm and has complexity linear in block length. This work was generalized to derive an iterative LCLP decoding algorithm for nonbinary linear codes by present authors. Contrary to binary LCLP, the variable and check node calculations of this algorithm are in general different from that of nonbinary BP. The overall complexity of nonbinary LCLP decoding is linear in block length; however the complexity of its check node calculations is exponential in the check node degree. In this talk, we present a modified BCJR algorithm for efficient check node processing for the nonbinary LCLP decoding algorithm. The proposed algorithm has complexity linear in the check node degree. Simulation results are presented for (504, 252) and (1008, 504) nonbinary LDPC codes over Z_4 .

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

Abstract:

Kloosterman sums are exponential sums related to finite fields, and have applications in coding theory, the construction of bent functions, and number theory. We show that the values taken by such sums (modulo powers of the characteristic of the underlying field) are related to the values taken by the trace, and similar functions. We also give some results on their minimal and characteristic polynomials. This talk is based on joint work with Faruk Göloğlu, Gary McGuire. Part of the talk is also joint work with Petr Lisoněk.

12.40-14.00 LUNCH

SESSION 6

14.00 – 14.30 ARNAUD TISSERAND, CNRS-IRISA, LANNION

“Circuits for True Random Number Generation with On-Line Quality Monitoring”

Abstract:

Random numbers are required in many applications such as cryptography, telecommunications, digital simulations or VLSI circuits testing.

Pseudo random number generators (PRNGs) usually lead to very high throughput with software and hardware implementations. But they are based on deterministic algorithms. This is a problem in many security applications. True random number generators (TRNGs) are based on the extraction of some physical noise in hardware implementations (jitter variations, meta-stability, radioactive decay...).

For ASIC and FPGA circuits, a widely used TRNG solution is based on oscillator sampling. The physical noise source is the jitter (the phase deviation) produced by one or several free running oscillators. One part of the jitter is produced by random noise but another part is produced by deterministic noise (power supply, clock or chip activity, cross talk...). So the randomness quality depends on noise source characteristics but also on other parameters such as TRNG architecture, implementation details and many environment parameters (circuit temperature, power supply, in-chip activity, electromagnetic radiations, clock signal quality). All those parameters may be used to attack the TRNG, reduce the quality of the produced random sequence and then reduce the security of the complete system (e.g. weak key).

In this talk, we will introduce context and standard architectures for TRNG circuits. Statistical methods for randomness quality evaluation will be recalled. Then we will detail two ASIC circuits (130 nm technology) designed in the CAIRN team for TRNGs based on oscillator sampling with on-line and real-time evaluation of the quality of TRNG output. FPGA versions will also be presented and discussed. The on-line and real-time monitoring of the generated random sequence is useful to prevent randomness quality reduction due to environment variations or physical attacks against the TRNG.

14.30 – 14.55 SHRADDHA SRIVASTAVA, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE CORK

“Efficient decoding of BCH codes beyond the error correction capability”

Abstract :

A lower complexity and computationally efficient list decoding algorithm is developed for BCH codes based on the property that BCH codes are subfield subcodes of Reed-Solomon codes. The polynomial evaluating to the codeword in the subfield, i.e. evaluation polynomial for BCH codes, has some special properties based on the cyclotomic cosets structure. Using these properties, the list decoding algorithm via syndrome variety is modified and simplified. The decoding problem can be written as an algebraic system of equations in different variables whose solution is related to the error occurred. Because of the large number of variables, the complexity of previously discussed algorithms are quite high and it becomes difficult to compute the Groebner basis even for the small code length. The complexity of our algorithm is reduced as the number of variables is decreased significantly using the properties of evaluation polynomial related to cyclotomic cosets structure. Hence, the time and memory footprint of the algorithm can be also decreased substantially.

14.55 – 15.20 VIJAYKUMAR SINGH, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“On Characteristic polynomial of supersingular abelian varieties over finite fields”

Abstract:

We give the list of characteristic polynomials of supersingular abelian varieties of dimensions up to 7, and the simple procedure to find them which can in principle be extended to all dimensions.

15.20 – 15.45 OLIVER GNILKE, CLAUDE SHANNON INSTITUTE, UNIVERSITY COLLEGE DUBLIN

“Semigroup action problems”

Abstract:

In 2003 Maze suggested a generalization of the classical Diffie-Hellman key exchange protocol. Instead of utilizing the action of Z/nZ on a cyclic subgroup of Z/mZ^ or the group of points on an elliptic curve over a finite field, a general semigroup action on a set is considered. Monico, Maze and Rosenthal proposed a system based on this idea in 2007 using the action of a semiring on a semimodule. We investigate the possibility to extend known algorithms for solving the underlying discrete logarithm problem to this new setting. Especially a Pohlig-Hellman like reduction is considered.*

15.45 – 16.00 CLOSE