Coding Theory and Cryptography

Monday June 21st

1.30-2.00 PM	Coding from within unit schemes - Ted Hurley
2.05-2.35 PM	Codes over non-unital rings - Patrick Solé
2.40-3.10 PM	Optimal Error Correcting Codes Derived from Codes over Mixed Alphabets - Taher Abualrub
3.15-3.45 PM	Break
3.50-4.20 PM	Abelian Group Factorization from Perfect and Cyclic Codes - Abdulla Eid
4.25-4.55 PM	On the generalized Hamming weights of certain Reed-Muller-type code - Delio Jaramillo
5.00-5.30 PM	Random Nonsingular Matrix Generation over GF(2) via Circulant Matrices and Applications to Code-Based Cryptography - Bahattin Yildiz

Session Chair: Dr. Abdulla Eid

Virtual Room 1C

Coding Theory and Cryptography

Tuesday June 22nd

1.30-2.00 PM	An Approach to Cryptanalysis by Local Inversion - Virendra Sule
2.05-2.35 PM	Codes for multimedia fingerprinting, cover-freefamilies and compressed sensing - Grigory Kabatiansky
2.40-3.10 PM	A linear algebraic (t; n)–threshold secret image sharing scheme - Ali Kanso
3.15-3.45 PM	Break
3.50-4.20 PM	Number Theory from Z to A - Ahmad El-Guindy
4.25-4.55 PM	A New Primality Test for Mersenne Primes - Moustafa Ibrahim
5.00-5.30 PM	Quasi-Frobenius Rings and Coding Theory - Henry Chimal Dzul

Session Chair: Dr. Abdulla Eid

Virtual Room 1C

Coding Theory and Cryptography

Abstracts

Dr. Ted Hurley (ted.hurley@nuigalway.ie)
National University of Ireland, Galway. Ireland

Coding from within unit schemes

Linear Coding Theory is: $GH^T=0$ where G is a generator matrix of size $r \times n$ and H is a check matrix of size $(n-r) \times n$. Thus in some sense G looks like a zero divisor but G and H are not in the same system. In a cyclic code, for example, G is a submatrix of a zero divisor $n \times n$ matrix.

In cryptography, unit schemes with $ED = I$ are considered where E is known but D is computationally impossible to obtain from just knowing E. However linear coding schemes can be derived from unit schemes. Indeed coding schemes may be derived from within unit schemes with very efficient decoding algorithms. Maximum distance separable codes of required types, and with efficient decoding algorithms, may be derived from within unit

Dr. Patrick Solé (patrick.sole@telecom-paris.fr)
Telecom Paris Tech. France

Codes over non-unital rings

Non unital rings of order 4 have been classified by Raghavandran in 1969. We study self-orthogonal codes over the rings E (local, noncommutative), I (local, commutative) and H (non-local, noncommutative). We introduce the notions of quasi self-dual (QSD), Type IV, and quasi Type IV (QT4) over these rings. A mass formula for QSD and QT4 codes over I is derived. We classify these codes in short lengths, and construct them recursively by the build-up method. Joint work with Adel Alahmadi and Alexis Bonnecaze.

Coding Theory and Cryptography

Abstracts

Dr. Taher Abualrub (abualrub@aus.edu)
American University in Sharjah, United Arab Emirates

Optimal Error Correcting Codes Derived from Codes over Mixed Alphabets

The Hamming distance of any error correcting code provides information related to the number of errors such a code can detect or correct. In this talk, I will study the class of Z2Z4-additive codes, Z2Z3-cyclic codes and F2F4-additive linear codes. I will introduce different Gray mappings that map these codes to codes over finite fields. As an applications of these codes, I will provide examples of optimal error correcting codes that are derived from codes over mixed alphabets as images under Gray mappings.

Dr. Abdulla Eid (aeid@uob.edu.bh)
University of Bahrain

Abelian Group Factorization from Perfect and Cyclic Codes

In this talk, we introduce the concept of group factorization and recall some definition in coding theory including the perfect and cyclic codes. These codes will be used to find group factorization of certain p--groups.

Session Chair: Dr. Abdulla Eid

Virtual Room 1C

Coding Theory and Cryptography

Abstracts

Dr. Delio Jaramillo (djaramillo@math.cinvestav.mx)
Cinvestav-IPN, Mexico

On the generalized Hamming weights of certain Reed-Muller-type code

We give an easy to evaluate formula to compute the r-th generalized Hamming weight of certain family of Reed-Muller-type codes from the formula for the r-th generalized Hamming weight of affine cartesian codes, given by P. Beelen and M. Datta. We determine the basic parameters and the generalized Hamming weights of the Veronese type codes and their dual codes in terms of the basic parameters and the generalized Hamming weights of the corresponding projective Reed–Muller-type codes and their dual codes.

Dr. Bahattin Yildiz (Bahattin.Yildiz@nau.edu)
Northern Arizona University

Random Nonsingular Matrix Generation over GF(2) via Circulant Matrices and Applications to Code-Based Cryptography

In this work we give a new method for generating a random nonsingular nxn matrix over GF(2) given a bitstream of length n by constructing a circulant matrix. We first give background about circulant matrices. We then compare the computational complexity of other random nonsingular matrix generation techniques to the computational complexity of our technique. We discuss special cases where the matrix generation is faster. We then describe applications of this, including to the McEliece and Niederreiter cryptosystems, and provide an example of this technique using an SRAM PUF as the bitstream generator.

Coding Theory and Cryptography

Abstracts

Dr. Virendra Sule (vrs@ee.iitb.ac.in)
Indian Institute of Technology, Bombay, India

An Approach to Cryptanalysis by Local Inversion

This talk presents an approach to Cryptanalysis of Block and Stream ciphers as an application of an algorithm for local inversion of maps F : F^n_2 \to F^n_2, that of finding all solutions x in F^n_2 of the equation y = F(x) where y constitutes an online data. A complete algorithm for local inversion is first briefly presented and then an incomplete but practically useful algorithm is presented. In short the approach shows that when the iterative sequence S(F; y) = fy; F(y); F(2)(y); : : :g has small linear complexity of polynomial order O(nk) then one solution of the inverse can be computed very quickly and can be disastrous to a cipher algorithm under a known plaintext attack. The complete algorithm evaluates in detail all the computational efforts required to find all solutions of the equation and shows that the computation can be divided in two parts, offline (without knowledge of y) and online (dependent on y) and provides a computational methodology to evaluate strengths of cipher algorithms. The computations of the complete algorithm show that the problem offline computation involves hard problems but are possible by parallel computation. Hence this approach can be used for estimating computational resources in time and memory for strength verification of practical ciphers.

Dr. Grigory Kabatiansky (G.Kabatyansky@skoltech.ru)
Skolkovo Institute of Science and Technology, Russia

Codes for multimedia fingerprinting, cover-freefamilies and compressed sensing

A comprehensive overview of recent results in the area of multimedia fingerprinting codes will be given. We shall pay especial attention to so-called cover-free families introduced in \cite{Erdos}, but known before as superimposed codes \cite{super}, and compressed sensing \cite{Donoho,Tao}. Main tools for constructing the corresponding codes are linear algebra over finite fields and probabilistic method of Paul Erdős. Let us note that multimedia fingerprinting codes appear useful not only for IP protection but also as multiple access channel coding and as binary robust compressed sensitive matrices.

Coding Theory and Cryptography

Abstracts

Dr. Ali Kanso (ali.kanso@ku.edu.kw)
Kuwait University, Kuwait

A linear algebraic (t; n)–threshold secret image sharing scheme

A (t, n)-threshold secret image sharing scheme is an algorithm that produces n shadow images from a secret image S and distributes them among n participants such that any set of participants of cardinality at least t can reconstruct S, while that of cardinality less than t does not reveal any useful information about S. In this work, we propose a linear algebraic (t, n)-threshold secret image sharing scheme that produces equally-sized shadow images, each of size t=1 the size of S. For each secret block B of S, the scheme assigns a signature vector vi to participant Pi such that vectors v1, v2,..., vn satisfy some admissibility conditions. The i-th share is then constructed as a linear combination of the t vectors from the secret block B with coefficients from vi. Simulation results demonstrate the effectiveness and robustness of the proposed scheme against standard statistical and security attacks. Furthermore, the proposed scheme is shown to be competitive with existing ones.

Dr. Ahmad El-Guindy (a.elguindy@gmail.com)
Cairo University, Egypt

Number Theory from Z to A

The ring of polynomials in a single variable over a finite field (commonly denoted by A) bears many similarities with the classical ring of integers Z. Studying analogs of arithmetic questions over A and its generalizations has played an important role in modern developments of number theory as highlighted by the work of Carlitz, Drinfeld and many others. In this talk we give an overview of the theory of Drinfeld modules and discuss some of the similarities and differences between the classical case and the function field case.

Coding Theory and Cryptography

Abstracts

Dr. Moustafa Ibrahim (mimohamed@uob.edu.bh)
University of Bahrain

A New Primality Test for Mersenne Primes

Given any odd prime P, the number $MP=2P-1$is called Mersenne prime if MP is prime. Mersenne primes have a long history because of their close connection to perfect numbers: the Euclid–Euler theorem asserts a one-to-one correspondence between even perfect numbers and Mersenne primes. Mersenne primes hold a special place in encryption too. Applying some differential operators to certain expansions, we give a new primality test for Mersenne primes.

Dr. Henry Chimal Dzul (hc118813@ohio.edu)
Ohio University, United States

Quasi-Frobenius Rings and Coding Theory

The theory of linear codes over finite fields has been shown to extend to a theory of linear codes over finite over finite rings (not necessarily commutative). In this talk we review the main notions of this new theory and rise some questions concerning Quasi-Frobenius Rings and the famous McWilliam Extension Theorem. A classification of finite rings up to isomorphism stands out along the way.