Mathematical Applications in Cryptography
Applications des mathématiques en cryptographie
(Org: **Francis N. Castro** (Puerto Rico University), **T. Aaron Gulliver** (University of Victoria) and/et **Amr Youssef** (Concordia University))

FRANCIS N. CASTRO, University of Puerto Rico, Rio Piedras Campus
Diophantine Equations with Binomials Coefficents and Perturbations of Symmetric Boolean Functions

This work presents a study of perturbations of symmetric Boolean functions. In particular, it establishes a connection between exponential sums of these perturbations and Diophantine equations of the form

$$\sum_{l=0}^{n} \binom{n}{l} x_l,$$

where x_l belongs to some fixed bounded subset Γ of $\mathbb{Z}$. The concepts of trivially balanced symmetric Boolean function and sporadic balanced Boolean function are extended to this type of perturbations. An observation made by Canteaut and Videau for symmetric Boolean functions of fixed degree is extended. To be specific, it is proved that, excluding the trivial cases, balanced perturbations of fixed degree do not exist when the number of variables grows. Some sporadic balanced perturbations are presented. Finally, a beautiful but unexpected identity between perturbations of two very different symmetric Boolean functions is also included in this work. This is a joint work with Oscar Gonzalez and Luis Medina.

CLAUDE CRÉPEAU, McGill University
Relativistic Commitments and Zero-Knowledge Proofs

We present techniques for zero-knowledge proofs of NP statements using very few relativistic commitments, making it possible for two synchronized verifiers, far enough from each other, to test two synchronized provers, close enough to the verifiers, in such a way that

* under the assumption that information cannot travel faster than the speed of light, only valid statements can be demonstrated by the provers (soundness)

* the answers obtained by the verifiers are useless to convince an off-line third party of the validity of the statement (zero-knowledge).

We achieve this by presenting a new interactive proof for NP languages that uses only 6 commitments at any point in the proof to be perfect zero-knowledge.

Joint work with Lucas Stinchcombe and Nan Yang

JINTAI DING, University of Cincinnati
Post-Quantum Key Exchange from the LWE

In this lecture, we present practical and provably secure (authenticated) key exchange protocol and password authenticated key exchange protocol, which are based on the learning with errors problems. These protocols areconceptually simple and have strong provable security properties. This type of new constructions were started in 2011-2012. These protocols are shown indeed practical. We will explain that all the existing LWE based key exchanges are variants of this fundamental design. In addition, we will explain some issues with key reuse and how to use the signal function invented for KE for authentication schemes.

KENZA GUENDA, University of Victoria
A Secure New Variant of the McEliece Cryptosystem

In this work joined with H. Mofek and T.A Gulliver we will be presenting a new version of the McEliece cryptosystem based on quasi-cyclic (QC) low density parity check (LDPC) codes and QC moderate density parity check (MDPC) codes. A modified self-shrinking generator is used to obtain random bits which are utilized in the cryptosystem. It is shown that this system is secure against the known attacks.

PETR LISONEK, Simon Fraser University

Non-existence results for vectorial bent functions with Dillon-type exponents

Vectorial bent functions with Dillon-type exponents have attracted attention because they are hyperbent whenever they are bent, and they achieve the highest possible algebraic degree among all bent functions on the same domain. We study monomial functions $f(x) = \mathrm{Tr}_k^{2m}(ax^{2^m-1})$ where $a \in \mathbb{F}_{2^{2m}}^*$ and Tr_k^{2m} denotes the trace from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_{2^k}$. Muratović-Ribić, Pasalic and Bajrić (IEEE Trans. Inform. Theory 2014) proved that f is not bent when $k = m$. Lapierre and Lisoněk (Proceedings ISIT 2016) proved that f is not bent when $k = m/2$, $k \geq 2$. In the current work we further introduce new proof techniques and we prove that f is not bent when $k = m/3$ where k is odd, $k \geq 3$. Our techniques use results that relate the divisibility of the Kloosterman sum $K(a)$ by powers of 2 and the coefficients of the characteristic polynomial of a due to Göloğlu, Lisoněk, McGuire and Moloney (IEEE Trans. Inform. Theory 2012). This is joint work with Luc Lapierre.

SIHEM MESNAGER, University of Paris 8, Paris 13 and Telecom ParisTech

Recent advances on bent functions for symmetric cryptography

Boolean functions are important objects in discrete mathematics. They play a role in mathematics and in many domains of computer science. We will be mainly interested in their relationships with private-key cryptography.

The talk is devoted to special families of Boolean functions which are viewed as important objects in combinatorics and the information theory framework (namely, cryptography and coding theory) : the so-called bent functions.

Bent functions are maximally nonlinear Boolean functions. They are wonderful creatures introduced by O. Rothaus in the 1960's and initially studied by J. Dillon since 1974. For their own sake as interesting combinatorial objects, but also for their relations to coding theory (e.g. Reed-Muller codes, Kerdock codes, etc.), combinatorics (e.g. difference sets), design theory, sequence theory, and applications in cryptography (design of stream ciphers and of S-boxes for block ciphers), they have attracted a lot of research for four decades.

We give a survey of the main results in bent functions and present new ones.

DANIEL PANARIO, Carleton University

Ambiguity, deficiency and differential spectrum of low degree normalized permutation polynomials over finite fields

Let $\mathbb{F}_q$ be the finite field of q elements, q a prime power. If $f : \mathbb{F}_q \to \mathbb{F}_q$ induces a bijection, f is a *permutation polynomial*; if f is monic, $f(0) = 0$, and, when the degree n of f is not divisible by the characteristic of $\mathbb{F}_q$, the coefficient of x^{n-1} is zero, f is in *normalized* form. Normalized permutation polynomials are known exhaustively up to degree six.

For $a \in \mathbb{F}_q^*$, the *difference map* of f is defined as $\Delta_{f,a}(x) = f(x + a) - f(x)$. This map plays a central role in differential cryptanalisis. To resist linear and differential cryptanalysis, we want permutations functions f such that $|\Delta_{f,a}^{-1}(b)|$ is low for all $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. We define $n_k(f)$ as the number of pairs (a, b) such that $f(x+a) - f(x) = b$ has exactly k solutions. The vector $[n_0(f), \ldots, n_q(f)]$ is the *spectrum* vector of the difference map of f. The *deficiency* of f is $D(f) = n_0(f)$; it measures how close the $\Delta_{f,a}$'s are to be surjective. The *(weighted) ambiguity* of f is $A(f) = \sum_{0 \leq k \leq n} n_k(f)\binom{k}{2}$; it measures how close the $\Delta_{f,a}$'s are to be injective.

We give exact formulas for the differential spectrum, deficiency and ambiguity of all normalized permutation polynomials of degree up to six over finite fields.

Joint work with Daniel Santana (Federal University of Santa Catarina, Brazil) and Qiang Wang (Carleton University, Canada)

DR. VALENTIN SUDER, UVSQ

Two Notions of Differential Equivalence on Sboxes

In this work, we discuss two notions of differential equivalence on Sboxes. First, we introduce the notion of *DDT-equivalence* which applies to vectorial Boolean functions that share the same difference distribution table (DDT). Next, we compare this notion, to what we call the γ-*equivalence*, applying to vectorial Boolean functions whose DDTs have the same support. We discuss the relation between these two equivalence notions and provide an algorithm for computing the DDT-equivalence and the γ-equivalence classes for a given function. We study the sizes of these classes for some families of Sboxes. Finally, we prove a result that shows that the rows of the DDT of an APN permutation are pairwise distinct. (Joint work with Christina Boura, Anne Canteaut and Jérémy Jean).