Yevgeniy Dodis (NYU): *Key Derivation Without Entropy Waste.*

We revisit the classical question of converting an imperfect source X of min-entropy k into a usable m-bit cryptographic key for some underlying application P. If P has security delta (against some class of attackers) with a uniformly random m-bit key, we seek to design a key derivation function (KDF) h that allows us to use R=h(X) as the key for P and results in comparable security delta' close to delta.

Seeded randomness extractors provide a generic way to solve this problem provided that $k > m + 2 * \log(1/\delta)$, and this lower bound on k (called "RT-bound") is known to be tight in general. Unfortunately, in many situation the "waste" of $2 * \log(1/\delta)$ bits of entropy is significant, motivating the question of designing KDFs with less waste for important special classes of sources X or applications P. I will discuss several positive and negative results in this regard. The most surprising of them will be a positive result for all unpredictability applications P, yielding a provably secure KDF with entropy "waste" only $\log\log(1/\delta)$ - an expenential improvement over the RT-bound.

Parikshit Gopalan (Microsoft Research): *Locally Testable Codes and their Guises.*

A locally testable code (LTC) is an error correcting code which admits a very efficient procedure for testing membership in the code: a local tester queries few locations in the received word but still distinguishes codewords from words that are far from the code. The rate-distance-query tradeoffs possible for such codes are not well understood: for instance, we do not know if there exist asymptotically good codes with 3-query testers.

We will briefly survey what is known about tradeoffs for such codes and then talk about other guises of LTCs. We will see that LTCs are equivalent to a certain class of Cayley expander graphs and to certain metric spaces with good L_1 embeddings. These equivalences let us translate known constructions of LTCs into constructions of other combinatorial objects, and existence questions about LTCs into existential questions about these objects. We will speculate about other possible uses of these translations.

Based on joint works with Boaz Barak (MSR), Johan Hastad (KTH), Raghu Meka (IAS), Prasad Raghavendra (UC Berkeley), David Steurer (Cornell), Salil Vadhan (Harvard) and Yuan Zhou (CMU).

Hendrik Lenstra (Leiden University): *Lattices with symmetry.*

It is a notoriously difficult algorithmic problem to decide whether a given lattice admits an orthonormal basis. However, this problem becomes doable if the lattice is given along with a suitably large abelian group of symmetries. The lecture is devoted to a precise formulation of this result and to an outline of the algorithm that underlies its proof. One of the ingredients is an elegant algorithmic technique that C. Gentry and M. Szydlo introduced several years ago in the context of cryptography, but that can be recast in algebraic language. Other ingredients are taken from analytic number theory and from commutative algebra. Part of the work reported on was done jointly with Alice Silverberg and René Schoof.

Harald Niederreiter (Austrian academy of Sciences): *Large Remarkable Sequences Obtained from Global Function Fields.*

We discuss two types of applications of global function fields to the construction of sequences with useful properties. One application concerns the construction of keystream sequences for stream ciphers with pseudorandomness properties. The other refers to the construction of sequences of quasirandom points

with strong uniformity properties. In the latter case, constructions that are in a sense asymptotically optimal are obtained by methods based on global function fields.

Renato Renner (ETH Zurich): *Smooth entropy in physics and information theory.*

Abstract: The notion of smooth entropy plays an important role in one-shot information theory and, in particular, information-theoretic cryptography. For example, smooth entropy characterises the amount of key that can be extracted, using privacy amplification, from weakly secret data. Remarkably, the very same concept of smooth entropy is also used in physics. For example, smooth entropy quantifies the amount of usable energy that can be drawn from a thermodynamic system. In this talk, I will discuss these remarkable links between information theory and physics and demonstrate how they help us making progress in both fields.

Henning Stichtenoth (Sabanci University): *On Ihara's constant $A(q)$ over non-prime finite fields.*

For a curve $\mathcal{C}$ over the fienite field $\mathbb{F}_q$, we denote by $N(\mathcal{C})$ and $g(\mathcal{C})$ the number of rational points (the genus, resp.) of $\mathcal{C}$. There is a real number $A(q)$ (called Ihara's constant) such that

$$N(\mathcal{C}) \lesssim A(q) \cdot g(\mathcal{C})$$

for any family of curves with $g(\mathcal{C}) \to \infty$. It has been known since around 1980 that $A(q) \leq \sqrt{q} - 1$ (Drinfeld-Vladut), and equality holds for q being a square (Ihara and Tfasman-Vladut-Zink). Good lower bounds for $A(q)$ are of high interest since they provide curves of large genus having "many" rational points. Such curves have interesting applications (e.g., in Coding Theory, Secret Sharing, Low Discrepancy Sequences, ...).

There is a lower bound for $A(q)$ due to J.-P. Serre: $A(q) \geq c \cdot \log q$ with an absolute constant $c > 0$. However, this lower bound is very weak as q is large. In some cases (in particular for $q = p^3$ or $q = p^n$ with a prime number p and certain exponents $n \gg 0$), improvements of Serre's bound have been obtained.

In this talk I present a lower bound for $A(q)$ for all non-prime q as follows:

Theorem 1 *(A. Bassa, P. Beelen, A. Garcia, H.S.) Let $q = p^{2m+1}$ with $m \geq 1$. Then*

$$A(q) \geq H(p^m - 1, p^{m+1} - 1),$$

where $H(.,.)$ denotes the harmonic mean of two real numbers.

This lower bound coincides with the best known bound for $q = p^3$, for all exponents $n = 2m + 1 > 3$, it is much better than all previous bounds. As a simple consequence we obtain

Corollary 1 *For all non-prime fields $\mathbb{F}_q$ with $q \neq 4, 8, 9, 16, 25, 27, 32, 125$, the Gilbert-Varshamov bound can be improved on a large interval $I \subseteq (0, 1 - q^{-1})$.*

Reference: A. Bassa, P. Beelen, A. Garcia and H. Stichtenoth: *Towers of function fields over non-prime finite fields*, arXiv:1202.5922v1[math.AG], 27 Feb 2012

Madhu Sudan (Microsoft Research): *Locality in codes and Lifting.*

Locally decodable codes (LDCs) are error-correcting codes that allow for highly-efficient recovery of "pieces" of information even after arbitrary corruption of a codeword. Locally testable codes (LTCs)

are those that allow for highly-efficient testing to see if some given word is close to a codeword. Codes derived from evaluations of low-degree multivariate polynomials give the simplest example of LDCs and LTCs, and these codes and their locality properties played a significant role in many results in complexity theory in the 90s. Attempts to construct better LTCs and LDCs (those that offer better coding efficiency, while achieving a desired level of locality) have been quite successful in the past decade. However the constructions often tend to be complex and have inevitably led to codes which satisfy one of the two properties, but not both! In this talk we will show how small codes can be lifted to longer ones retaining the locality of the small ones, while achieving high rate. In particular we give codes of rate close to arbitrarily one with locality n^ϵ for arbitrary $\epsilon > 0$. The only previous LDCs with such properties are the multiplicity codes of Kopparty, Saraf, and Yekhanin. Our codes are naturally LTCs also, whereas this aspect remains open for the multiplicity codes.

We will use these codes as an excuse to give an overview of some of the work in "affine-invariant codes" - of which lifted codes are a subclass. The testability and rate of our lifted codes follows from some of the analysis of the general class. One surprising fact that leads to our high-rate codes is that the set of multivariate functions that project to a univariate polynomial of degree d on every line, is *not* the set of degree d multivariate polynomials, but an overwhelmingly larger set over fields of small characteristic. This fact turns out to lead to some strong lower bounds on the size of "Nikodym sets" (sets that contain "most points of at least one line" through every point in the space).

Joint work with Alan Guo (MIT) and Swastik Kopparty (Rutgers)

Amos Beimel (Ben Gurion University): *Multi-Linear Secret Sharing Schemes.*

A secret-sharing scheme is a method by which a dealer distributes shares to parties such that only authorized subsets of parties can reconstruct the secret and all other sets get no information on the secret. Secret-sharing schemes are an important tool in cryptography and they are used as a building box in many secure protocols, e.g., general protocol for multiparty computation, Byzantine agreement, threshold cryptography, access control, attribute-based encryption, and generalized oblivious transfer.

Multi-linear secret-sharing schemes are the most common secret-sharing schemes. In these schemes the secret is composed of some field elements and the sharing is done by applying some fixed linear mapping on the secret and some randomly chosen field elements. If the secret contains one field element, then the scheme is called linear. The importance of multi-linear schemes is that they provide a simple non-interactive mechanism for computing shares of linear combinations of previously shared secrets. In this talk, I will discuss the power of multi-linear secret-sharing schemes. On one hand, we prove that multi-linear secret-sharing schemes in which the secret is composed of p field elements are more powerful than schemes in which the secret is composed of less than$p$ field elements (for every prime p). On the other hand, we prove super-polynomial lower bounds on the share size in multi-linear secret-sharing schemes. Previously, such lower bounds were known only for linear schemes.

This talk is based on a joint work with Aner Ben-Efraim, Carles Padro, and Ilya Tyomkin.

Chaoping Xing (Nanyang Technological University): *List Decoding Reed-Solomon, Algebraic Geometry and Gabidulin Subcodes.*

We consider Reed-Solomon (RS) codes whose evaluation points belong to a subfield, and give a linear-algebraic list decoding algorithm that can correct a fraction of errors approaching the code distance, while pinning down the candidate messages to a well-structured affine space of dimension a constant factor smaller than the code dimension. By pre-coding the message polynomials into a subspace-evasive set,

we get a Monte Carlo construction of a subcode of Reed-Solomon codes that can be list decoded from a fraction $(1 - R - \epsilon)$ of errors in polynomial time (for any fixed $\epsilon > 0$) with a list size of $O(1/\epsilon)$. Our methods extend to algebraic-geometric (AG) codes, leading to a similar claim over constant-sized alphabets. This matches parameters of recent results based on folded variants of RS and AG codes, but our construction here gives subcodes of Reed-Solomon and AG codes themselves (albeit with restrictions on the evaluation points). Further, the underlying algebraic idea also extends nicely to Gabidulin's construction of rank-metric codes based on linearized polynomials. This gives the first construction of positive rate rank-metric codes list decodable beyond half the distance, and in fact gives codes of rate R list decodable up to the optimal $(1 - R - \epsilon)$ fraction of rank errors.

Oriol Farras (URV Tarragona): *Secret Sharing Schemes for Very Dense Graphs.*

A secret-sharing scheme realizes a graph if every two vertices connected by an edge can reconstruct the secret while every independent set in the graph does not get any information on the secret. Similar to secret-sharing schemes for general access structures, there are gaps between the known lower bounds and upper bounds on the share size for graphs. Motivated by the question of what makes a graph "hard" for secret-sharing schemes (that is, require large shares), we study very dense graphs, that is, graphs whose complement contains few edges.

We show that if a graph with n vertices contains $\binom{n}{2} - n^{1+x}$ edges for some constant $0 \leq x < 1$, then there is a scheme realizing the graph with total share size of $\tilde{O}(n^{5/4+3x/4})$. This should be compared to $O(n^2/\log n)$ – the best upper bound known for the share size in general graphs. Thus, if a graph is "hard", then the graph and its complement should have many edges. We generalize these results to nearly complete k-homogeneous access structures for a constant k. To complement our results, we prove lower bounds for secret-sharing schemes realizing very dense graphs, e.g., for linear secret-sharing schemes we prove a lower bound of $\Omega(n^{1+x/2})$ for a graph with $\binom{n}{2} - n^{1+x}$ edges.

This is a joint work with Amos Beimel and Yuval Mintz, and was presented at CRYPTO 2012.

Gilles Zemor (Bordeaux Mathematics Institute): *Low Rank Parity Check codes and their application to cryptography.*

We introduce a new family of rank metric codes that come together with an efficient probabilistic decoding algorithm. This family can be seen as an equivalent to classical LDPC codes transposed in the rank metric, and has otherwise very poor structure. It is shown how they can be used efficiently in a public-key cryptosystem reminiscent of the NTRU cryptosystem but transposed in a rank-metric context. Joint work with Philippe Gaborit, Gaetan Murat, Olivier Ruatta.

Manoj Prabhakaran (Univ. of Illinos at Urbana Champaign): *Towards Quantitative Cryptographic Complexity.*

We formulate a quantitative notion of "cryptographic complexity" of a (multi-party) function, as the amortized number of "crypto gates" needed to securely evaluate the function. Due to recent results, we can show that up to constants, this quantity does not depend on the specific choice of crypto gate, as long as it is "complete."

In contrast to communication complexity, a function's cryptographic complexity can potentially be super-linear in the size of the inputs to the function. Indeed, we conjecture that most functions have

super-linear, if not exponential, cryptographic complexity.

We shall discuss the state of the art information-theoretic techniques for lower-bounds on cryptographic complexity. But these techniques are inherently limited to linear bounds.

Due to standard results in secure function evaluation, cryptographic complexity is a lower-bound on circuit complexity. In principle, this suggests an approach to proving circuit complexity lower-bounds. However, we do not have any results even on the existence of functions with super-linear cryptographic complexity. We pose this "existential question" as the main open problem of cryptographic complexity.

Iwan Duursma (Univ. of Illinos at Urbana Champaign): *Algebraic aspects of secret sharing.*

To share a secret, Shamir proposed to use polynomials over a finite field. Unknown values of a polynomial can be obtained from a large enough subset of known values through interpolation. Applications of secret sharing include multiparty computation protocols, encoding schemes for the wiretap channel and secure network coding. Various more general schemes have been proposed that accomodate different access structures or that can be realized over smaller fields. We summarize the algebraic principles that determine the parameters of such schemes.

Tarik Kaced (Institute of Network Coding, The Chinese University of Hong Kong): *Essentially Conditional Inequalities Might Help.*

Given a secret, the goal of a perfect secret-sharing scheme is to assign each participant some information to achieve the following twofold objective:
- Authorized groups of participants can recover the secret (functional dependency)
- Forbidden groups do not learn any information on the secret (independence)
The secret sharing problem is now clear: try to finding the smallest pieces of information for participants. Sometimes, a participant's share is inevitably large and the basic technique to obtain such a lower bound is to use linear information inequalities (for Shannon Entropy).

We introduce a quasi-perfect model of secret sharing in the sense that its parameters tend to the one of a perfect scheme. In this model, a structure is implemented by a sequence of secret-sharing scheme with possible leaks. The idea is to capture the asymptotic behavior of the optimization of perfect secret-sharing schemes.

There are cases where a quasi-perfect implementation is sometimes better that a perfect one in a weak sense. However, it is still open as to whether quasi-perfect schemes can achieve substantially better information ratios than perfect ones or not. We suspect that certain conditional information inequalities might help separating the two notions in the strong sense.

The information inequalities that have been extensively used to derive lower bounds are in fact conditional. This talk will present new properties of some conditional information inequalities:
1. Some conditional inequalities cannot be extended to any unconditional inequalities (and thusly called "essentially" conditional).
2. Some essentially conditional inequalities do not hold for all almost entropic points.

Ruud Pellikaan (TU Eindhoven): *Error-correcting pairs and arrays from algebraic*

geometry codes.

In this lecture it will be shown how an efficient decoding algorithm can be retrieved from an algebraic geometry code by means of error-correcting pairs and arrays directly, that is without the detour via the representation (X, P, E) of the code, where X is an algebraic curve, P is an n-tuple of mutually distinct points and E is a divisor. As a consequence algebraic geometry codes with certain parameters are not secure for the code based McEliece public crypto system.

Olav Geil (Aalborg University): *Further improvements on the Feng-Rao bound for dual codes.*

Salazar, Dunn and Graham in [Salazar et. al., 2006] presented an improved Feng-Rao bound for the minimum distance of dual codes. In this work we take the improvement a step further. Both the original bound by Salazar et. al., as well as our improvement are lifted so that they deal with generalized Hamming weights. We also demonstrate the advantage of working with one-way well-behaving pairs rather than weakly well-behaving or well-behaving pairs.

Alexander May (Ruhr-University Bochum): *Recent Progress in Decoding Random Linear Codes.*

Abstract: We review some recent algorithmic progress that led to faster algorithms for decoding random linear codes over F_2^n. The worst case complexity for decoding these codes dropped from roughly $2^{(1/8)n}$ to $2^{(1/10)n}$.

Frantisek Matus (Institute of Info. Theory and Automation, Academy of Sciences of the Czech Republic): *Ideal secret sharing in quantum setting.*

When studying entropy functions of multivariate probability distributions, polymatroids and matroids emerge. Entropy functions of pure multiparty quantum states give rise to analogous notions, called polyquantoids and quantoids. The polymatroids and polyquantoids will be related via linear mappings and duality. We will briefly review the quantum secret sharing from the viewpoint of polyquantoids and describe ideal sharing via selfdual matroids.

Yvo Desmedt (Univ. of Texas at Dallas): *Functional secret sharing.*

Functional encryption is now receiving a lot of attention. However, the topic of functional encryption was preceded by functional secret sharing (SIAM Journal on Discrete Mathematics, 2000).

In this lecture, we explain some of the motivations behind functional secret sharing. We note that in functional secret sharing, we have, as in normal secret sharing a dealer. However, after the participants received shares from the dealer, a function f will be chosen and the participants will be asked to evaluate f(secret), without help of the dealer.

We observe that functional secret sharing is different from secure multiparty computation. Parties are allowed to leak information about their inputs (the shares) as long as they do not leak any additional information on the secret.

Two approaches are surveyed. The first one is non-interactive in the sense that the participants need to broadcast some partial evaluation of f(secret). Since broadcast is used, these partial evaluations should not facilitate a non-authorized set to compute f'(secret), except if f'(secret) follows logically from f(secret). The second approach is interactive in which stricter privacy requirements can be enforced.

We conclude with giving open problems.

Tal Rabin (IBM Research): *Full Characterization of Functions that Imply Fair Coin Tossing and Ramifications to Fairness.*

It is well known that it is impossible for two parties to toss a coin fairly (Cleve, STOC 1986). This result implies that it is impossible to securely compute with fairness any function that can be used to toss a coin fairly. In this paper, we focus on the class of deterministic Boolean functions with finite domain, and we ask for which functions in this class is it possible to information-theoretically toss an unbiased coin, given a protocol for securely computing the function with fairness. We provide a *complete characterization* of the functions in this class that imply and do not imply fair coin tossing. This characterization extends our knowledge of which functions cannot be securely computed with fairness. In addition, it provides a focus as to which functions may potentially be securely computed with fairness, since a function that cannot be used to fairly toss a coin is not ruled out by the impossibility result of Cleve (which is the *only* known impossibility result for fairness). In addition to the above, we draw corollaries to the feasibility of achieving fairness in two possible fail-stop models.

Joint work with Gilad Asharov and Yehuda Lindell

Juan Garay (AT&T Labs-Research): *Broadcast-Efficient Secure Multiparty Computation.*

Secure multiparty computation (MPC) is perhaps the most popular paradigm in the area of cryptographic protocols. It allows several mutually untrustworthy parties to jointly compute a function of their private inputs, without revealing to each other information about those inputs. In the case of unconditional (information-theoretic) security, protocols are known which tolerate a dishonest minority of players, who may coordinate their attack and deviate arbitrarily from the protocol specification.

It is typically assumed in these results that parties are connected pair-wise by authenticated, private channels, and that in addition they have access to a "broadcast" channel. Broadcast allows one party to send a consistent message to all other parties, guaranteeing consistency even if the broadcaster is corrupted. Because broadcast cannot be simulated on the point-to-point network when more than a third of the parties are corrupt, it is impossible to construct general MPC protocols in this setting without using a broadcast channel (or some equivalent addition to the model). A great deal of research has focused on increasing the efficiency of MPC, primarily in terms of round complexity and communication complexity. In this work we propose a refinement of the round complexity which we term broadcast complexity. We view the broadcast channel as an expensive resource and seek to minimize the number of rounds in which it is invoked.

We construct an MPC protocol which uses the broadcast channel only three times in a preprocessing phase, after which it is never required again. The protocol relies on new constructions of Pseudosignatures and Verifiable Secret Sharing (VSS), both of which might be of independent interest, as in addition to the low broadcast complexity they require a constant number of rounds overall.

This is joint work with Clint Givens (Maine School of Science and Mathematics) and Rafail Ostrovsky (UCLA).

Diego Mirandola (CWI): *On powers of codes.*

Given a linear code C, one can define the d-th power of C as the span of all componentwise products of d elements of C. A power of C may quickly fill the whole space. Our purpose is to reply to the following question: does the square of a code "typically" fill the whole space? We show that this is the case, when the codes have dimension larger than the square root of the length. In our proof we need results about the number of zeros of quadratic forms. Finally we discuss the implications on multiplicative secret sharing.

Joint work with Ignacio Cascudo, Ronald Cramer, Gilles Zemor.

Suhas Diggavi (UCLA): *On interactive wireless network security.*

The fundamental tenet of information-theoretic security for wireless networks is that the legitimate receiver and the eavesdropper have different "views" (i.e., channels) of the transmitted signal. This poses a difficult challenge: how can we guarantee such channel conditions? In this talk, we start by studying simpler channel models, that can be instantiated in a controlled channel environment. The model is the erasure broadcast channel, with all nodes in the network experiencing statistically identical (but independent) erasures. For this model we develop several results for optimal secrecy rates, including group key generation, message security and private message broadcasting. We will conclude our talk with broader horizons of information theoretic security, with applications to (distributed) control.

Serge Fehr (CWI): *The monogamy of entanglement, and one-sided device independent QKD.*

We introduce a new quantum game, which captures the "monogamy of entanglement" that is inherent to quantum mechanics, and we show a strong parallel repetition theorem for this game. As an application, we show that standard BB84 quantum key distribution remains provably secure, even when Bob's quantum measurement device is arbitrarily malicious.

Alp Bassa (Sabanci University): *Rational points on curves over finite fields and Drinfeld modular varieties.*

In the past modular curves of various type (classical, Drinfeld, Shimura) have been used successfully to construct high genus curves with many rational points over finite fields of square cardinality. In this talk I will explain how Drinfeld modular varieties can be used similarly to obtain high genus curves over any non-prime finite field with many rational points. This way one obtains lower bounds for the Ihara constant A(q) for all non-prime q, which are better then all previously known bounds. This is joint work with Beelen, Garcia, Stichtenoth.