Oberseminar Coding and Cryptography

Sommersemester 2025

February 27 **Speaker:** Martino Borello, Université Paris 8

Location and Time: Theresienstrasse 90, building N4, room 2405, 11:00

Title: Intersecting Codes: Geometry and Applications

Abstract:

Intersecting codes are classical objects in coding theory that find applications in various contexts, such as secret sharing, oblivious transfer, hash functions, separating systems, digital fingerprinting, and even certain theoretical problems in additive combinatorics. In this talk, we will present a geometric perspective on such codes. It is well known that a nondegenerate linear code of length n and dimension k can be associated with a set of n points (with multiplicities) in a projective space of dimension $k-1$. Some coding-theoretical properties can be interpreted geometrically. In particular, intersecting codes correspond to non-2-cohyperplanar sets, meaning sets in projective space that are not contained in any pair of hyperplanes. We will illustrate some recent results obtained using this geometric approach and discuss how this perspective can be extended to the rank metric.

April 3 **Speaker:** Anurag Bishnoi, TU Delft

Location and Time: Theresienstrasse 90, building N4, room 2408, 11:00

Title: Oddtowns, partial ovoids, and the rank-Ramsey problem

Abstract:

What is the largest size of a family of subsets of $\{1, \ldots, m\}$ such that every set in the family has odd cardinality and among any three distinct sets there is at least one pair that intersects in an even number of elements?

We show that this natural generalization of the classic Oddtown problem is equivalent to finding the largest size of a partial 2-ovoid in a binary symplectic space and that of finding the largest set of nearly orthogonal vectors in $\mathbb{F}_2^m$. Moreover, we show that it's intimately linked to the following recently introduced rank-Ramsey problem: for a given t, find the largest number of vertices for which there exists a triangle-free graph whose adjacency matrix satisfies $\operatorname{rank}(A + I) \leq t$.

We give new constructions of these equivalent objects, improving the state of the art, using a triangle-free Cayley graph associated with BCH codes. Moreover, by using binary projective caps we improve the best construction for the rank-Ramsey problem over the reals.

Joint work with John Bamberg, Ferdinand Ihringer, and Ananthakrishnan Ravi

April 24 **Speaker:** Alessandro Neri, University of Naples Federico II

Location and Time: Theresienstrasse 90, building N4, room 2408, 11:00

Title: On the Etzion-Silberstein conjecture

Abstract:

In 2009 Etzion and Silberstein proposed a conjecture on the largest dimension of a space of matrices over a finite field whose nonzero elements are supported on a given Ferrers diagram and all have rank lower bounded by a fixed positive integer d. Since then, their conjecture has been verified in a number of cases, but as of today it still remains widely open. In this talk I will provide an overview on the state of the art on the topic, starting from the first findings, until some very recent results.

May 19 **Speaker:** Giuseppe D’Alconzo, Politecnico di Torino

Location and Time: Theresienstrasse 90, building N4, room 2408, 11:00

Title: Relaxed Cryptanalysis on Code-based schemes from the NIST’s call

Abstract:

In 2023, the USA National Institute of Standardization and Technology (NIST) started a call to diversify post-quantum digital signature schemes. In fact, two of the first three quantum-resistant standardized signature schemes are based on lattices (Dilithium and Falcon). Many new proposals base their security on linear codes assumptions, from syndrome decoding to code equivalence. In this talk, we will investigate the ”relaxed” cryptanalysis of LESS, MIRA, MiRitH and RYDE, i.e., when other additional information apart from the public key is provided. For LESS, we investigate the security of exposing multiple public keys using the same private key. For the rank-based schemes MIRA, MiRitH and RYDE we analyze the partial key exposure scenario where a partial or erroneous secret key is leaked.

June 16 **Speaker:** Andre Esser, TII

Location and Time: Theresienstrasse 90, building N4, room 2408, 11:00

Title: Solving Code Equivalence via Codeword Search

Abstract:

The Code Equivalence Problem has gained increasing attention in recent years as a foundation for constructing code-based signature schemes that overcome some of the limitations of Syndrome Decoding–based designs. From a cryptanalytic perspective, however, many of the most effective attacks against Code Equivalence still share structural similarities with those against Syndrome Decoding, relying heavily on the ability to identify low-weight codewords in the underlying codes. In this talk, we present a structured overview of the main algorithmic approaches to Linear Code Equivalence (LCE), with a focus on the general framework based on codeword search. We compare different algorithmic instantiations, including classical as well as more recent techniques, and evaluate them both asymptotically and concretely against parameters proposed in cryptographic settings. We conclude by highlighting a recent improvement that shows that the amount of information required to solve LCE can be significantly reduced, leading to faster attacks and notable decreases in estimated security margins for cryptographic parameters.