

WCC 2022

The Twelfth International Workshop on Coding and Cryptography

Monday, 7 March 2022

09:00 - 09:05 (UTC+1): Welcome

09:05 - 10:20 (UTC+1): Symmetric Cryptography

Chair: Subadheep Banik

Quantum impossible differential attacks: Applications to AES and SKINNY

Nicolas David, María Naya-Plasencia and André Schrottenloher

[Paper](#)

On the hardness of monomial prediction and zero-sum distinguishers for Ascon

Pranjal Dutta, Mahesh Rajasree and Santanu Sarkar

[Paper](#)

On the Algebraic Degree of Iterated Power Functions

Clémence Bouvier, Anne Canteaut and Leo Perrin

[Paper](#)

10:35 - 11:50 (UTC+1): Public Key Cryptography

Chair: Jens Zumbärgel

Analysis of a Public-Key Encryption Scheme based on distorted Gabidulin codes

Pierre Loidreau

[Paper](#)

An analysis of Coggia-Couvreur Attack on Loidreau's Rank-metric public-key encryption scheme in the general case

Pierre Loidreau and Ba Duc Pham

[Paper](#)

On the (In)security of optimized Stern-like signature schemes

André Chailloux

[Paper](#)

14:00 - 14:45 (UTC+1): Discussions in breakout rooms

15:00 - 15:50 (UTC+1): Invited Talk

Quantum Safe Symmetric Cryptography

María Naya-Plasencia

Chair: Léo Perrin

During this talk we will introduce the context and summarize the state-of-the-art of the main quantum symmetric cryptanalysis results, providing the details of some particularly interesting cases. We will also present the scenario of some related open problems that are yet to be solved or improved.

16:00 - 17:15 (UTC+1): Side Channel Attacks and Hardware Components

Chair: Antoine Joux

Exploiting ROLLO's Constant-Time Implementations with a Single-Trace Analysis

Agathe Cheriére, Lina Mortajine, Tania Richmond and Nadia El Mrabet

[Paper](#)

Analysis of Communication Channels Related to Physical Unclonable Functions

Georg Maringer, Marvin Xhemrishi, Sven Puchinger, Kathrin Garb, Hedongliang Liu, Thomas Jerkovits, Ludwig Kürzinger, Matthias Hiller and Antonia Wachter-Zeh.

[Paper](#)

Estimating the Strength of Horizontal Correlation Attacks in the Hamming Weight Leakage Model: A Side-Channel Analysis on HQC KEM

Guillaume Goy, Antoine Loiseau and Philippe Gaborit

[Paper](#)

Tuesday, 8 March 2022

09:00 - 09:05 (UTC+1): Rostock Impressions

09:05 - 10:45 (UTC+1): Codes, Rings and Groups

Chair: Alfred Wassermann

Classification of Extremal Type II \mathbb{Z}_4 -codes of Length 24

Rowena Alma Betty and Akihiro Munemasa

[Paper](#)

Dense packings via lifts of codes to division rings

Nihar Gargava and Vlad Serban

[Paper](#)

On $\mathbb{Z}_p\mathbb{Z}_{p^2}$ -linear generalized Hadamard codes

Dipak Kumar Bhunia, Cristina Fernández-Córdoba and Mercè Villanueva

[Paper](#)

On some batch code properties of the simplex code

Henk D.L. Hollmann, Karan Khathuria, Ago-Erik Riet and Vitaly Skachek

[Paper](#)

11:00 - 12:40 (UTC+1): Algebraic Geometry Codes

Chair: Elisa Gorla

Efficient multivariate low-degree tests via interactive oracle proofs of proximity for polynomial codes

Daniel Augot, Sarah Bordage and Jade Nardi

[Paper](#)

Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes

Sarah Bordage and Jade Nardi

[Paper](#)

On the dimension and structure of the square of the dual of alternant codes and Goppa codes

Rocco Mora and Jean-Pierre Tillich

[Paper](#)

On Subfield Subcodes Obtained from Restricted Evaluation Codes

Cem Güneri, Ferruh Özbudak and Selcen Sayıcı

[Paper](#)

14:00 - 14:45 (UTC+1): Discussions in breakout rooms

15:00 - 15:50 (UTC+1): Invited Talk

Algebraic Quantum Codes

Markus Grassl

Chair: Jean-Pierre Tillich

The talk will discuss connections between quantum error-correcting codes (QECCs) and algebraic coding theory. A quantum error-correcting code is a subspace of a complex Hilbert space that allows to protect quantum information against certain errors. Using the so-called stabilizer formalism, we illustrate how QECCs can be constructed using techniques from algebraic coding theory. We will also present some open problems in classical coding theory that are motivated by the link to quantum error-correcting codes. The talk will also briefly introduce relevant concepts of quantum mechanics.

[Slides](#)

16:00 - 17:40 (UTC+1): Algorithms

Chair: Anton Betten

A new family of quantum codes from duadic codes

Reza Dastbasteh and Petr Lisoněk

[Paper](#)

Cryptographic Group and Semigroup Actions

Oliver W. Gnilke and Jens Zumbrägel

[Paper](#)

Analysis and Computation of Multidimensional Linear Complexity of Periodic Arrays

Rafael Arce, Carlos Hernández, José Ortiz-Ubarri, Ivelisse Rubio and Jaziel Torres

[Paper](#)

Solutions to the Conjugacy Search Problem in Various Platform Groups

Simran Tinani, Carlo Matteotti and Joachim Rosenthal

[Paper](#)

Wednesday, 9 March 2022

09:00 - 09:05 (UTC+1): Rostock Impressions

09:05 - 10:20 (UTC+1): Algebraic Aspects of Coding Theory

Chair: Joachim Rosenthal

A note on the duality of skew module codes

Delphine Boucher

[Paper](#)

q -ary propelinear perfect codes from the regular subgroups of the $GA(r, q)$ and their ranks

Ivan Mogilnykh

[Paper](#)

The Density of MDS Codes With Subfield Linearity

Nadja Willenborg and Anna-Lena Horlemann

[Paper](#)

11:00 - 12:15 (UTC+1): Reed-Solomon Codes

Chair: Ferruh Özbudak

Efficient Decoding of Folded Linearized Reed-Solomon Codes in the Sum-Rank Metric

Felicitas Hörmann and Hannes Bartz

[Paper](#)

Quadratic-Curve-Lifted Reed-Solomon Codes

Hedongliang Liu, Lukas Holzbaur, Nikita Polyanskii, Sven Puchinger and Antonia Wachter-Zeh

[Paper](#)

Maximum Sum-Rank Distance Codes over Finite Chain Rings

Umberto Martinez-Peñas and Sven Puchinger

[Paper](#)

14:00 - 14:45 (UTC+1): Discussions in breakout rooms

15:00 - 15:50 (UTC+1): Invited Talk

List-Decoding for Reed-Solomon Codes

Lisa Sauermann

Chair: Gohar Kyureghyan

Reed-Solomon codes are an important and intensively studied class of error-correcting codes. After giving some background, this talk will discuss the so-called list-decoding problem for Reed-Solomon codes. More specifically, we prove that for any fixed list-decoding parameters, there exist Reed-Solomon codes with a certain rate, which is optimal up to a constant factor. This in particular answers a question of Guo, Li, Shangguan, Tamo, and Wootters about list-decodability of Reed-Solomon codes with radius close to 1. Joint work with Asaf Ferber and Matthew Kwan.

16:00 - 17:40 (UTC+1): Perfect Nonlinear Functions and Related Objects

Chair: Felix Ulmer

On partially APN functions

Nurdagül Anbar, Tekgül Kalaycı and Alev Topuzoğlu

[Paper](#)

A note on exceptional APN functions of Gold and Kasami-Welch type

Nurdagül Anbar, Tekgül Kalaycı and Nihal Yurdakul

[Paper](#)

Classification of all DO planar polynomials with prime field coefficients over \mathbb{F}_{3^n} for $n \leq 7$

Diana Davidova and Nikolay Kaleyski

[Paper](#)

Counting the number of non-isotopic semifields inside some known semifield families

Faruk Göloğlu and Lukas Kölsch

[Paper](#)

Thursday, 10 March 2022

09:00 - 09:05 (UTC+1): Rostock Impressions

09:05 - 10:20 (UTC+1): Weight and Distance Distribution

Chair: Subhamoy Maitra

On almost perfect linear Lee codes of minimum distance 5

Xiaodong Xu and Yue Zhou

[Paper](#)

Weight distributions of a class of codes with parameters of Reed – Muller codes

Ivan Mogilnykh and Faina Solov'eva

[Paper](#)

On the Size Distribution of Levenshtein Balls with Radius One

Geyang Wang and Qi Wang

[Paper](#)

10:35 - 12:15 (UTC+1): Network Coding

Chair: Faina Solov'eva

Hybrid Elementary Linear Subspace codes

Ermes Franch and Chunlei Li

[Paper](#)

Right-hand side decoding of Gabidulin codes and applications

Maxime Bombar and Alain Couvreur

[Paper](#)

The Curious Case of the Diamond Network

Allison Beemer and Alberto Ravagnani

[Paper](#)

Hardness estimates of the Code Equivalence Problem in the Rank Metric

Krijn Reijnders, Simona Samardjiska and Monika Trimoska

[Paper](#)

14:00 - 14:45 (UTC+1): Discussions in breakout rooms

15:00 - 15:50 (UTC+1): Invited Talk
Function-Correcting Codes
Antonia Wachter-Zeh

Chair: Alexander Pott

Motivated by applications in machine learning and archival data storage, we introduce function-correcting codes, a new class of codes designed to protect a function evaluation of the data against errors. We show that function-correcting codes are equivalent to irregular-distance codes, i.e., codes that obey some given distance requirement between each pair of codewords. Using these connections, we study irregular-distance codes and derive general upper and lower bounds on their optimal redundancy. Since these bounds heavily depend on the specific function, we provide simplified, suboptimal bounds that are easier to evaluate. We further employ our general results to specific functions of interest and compare our results to standard error-correcting codes which protect the whole data. This is a joint work with Andreas Lenz, Rawad Bitar, and Eitan Yaakobi.

16:00 - 17:40 (UTC+1): MRD and Storage Codes

Chair: Pierre Loidreau

On a family of MRD codes with parameters $[n \times n, 2n, n - 1]_q$, n even
Olga Polverino, Marco Timpanella, Giovanni Zini and Ferdinando Zullo

[Paper](#)

The Proportion of (Non-)Linear MRD Codes

Anina Gruica and Alberto Ravagnani

[Paper](#)

Antipodal two-weight rank-metric codes

Rakhi Pratihar and Tovohery Hajatiana Randrianarisoa

[Paper](#)

High-rate storage codes on triangle-free graphs

Alexander Barg and Gilles Zémor

[Paper](#)

Friday, 11 March 2022

09:00 - 09:05 (UTC+1): Rostock Impressions

09:05 - 10:20 (UTC+1): Boolean Functions I

Chair: Anne Canteaut

An asymptotic lower bound on the number of bent functions

Vladimir Potapov, Anna Taranenko and Yuriy Tarannikov

[Paper](#)

On Boolean Functions with Low Polynomial Degree and Higher Order Sensitivity

Subhamoy Maitra, Chandra Sekhar Mukherjee, Pantelimon Stănică and Deng Tang

[Paper](#)

A Modified Patterson-Wiedemann Construction Having Nonlinearity Greater Than Bent Concatenation Bound

Selçuk Kavut

[Paper](#)

Introducing Nega-Forrelation: Quantum Algorithms in Analyzing Nega-Hadamard and Nega-crosscorrelation Spectra

Suman Dutta and Subhamoy Maitra

[Paper](#)

11:00 - 12:15 (UTC+1): Arithmetic of Finite Fields

Chair: Maria Montanucci

Secure Private and Adaptive Matrix Multiplication Beyond the Singleton Bound

Christoph Hofmeister, Rawad Bitar, Marvin Xhemrishi and Antonia Wachter Zeh

[Paper](#)

Constructing irreducible polynomials recursively with a reverse composition method

Anna-Maurin Graner and Gohar Kyureghyan

[Paper](#)

Multiplication in finite fields with Chudnovsky-type algorithms over the projective line

Stéphane Ballet, Alexis Bonnetaze and Bastien Pacifico

[Paper](#)

14:00 - 14:45 (UTC+1): Discussions in breakout rooms

15:00 - 15:50 (UTC+1): Invited Talk

Biprojectivity in cryptographic functions and related algebraic structures

Faruk Göloğlu

Chair: Alev Topuzoglu

In this talk, we will consider biprojective nonlinear functions, permutations, and semifields. Biprojective functions can be viewed as bivariate functions over a two dimensional extension of a finite field K that exploit nice properties of projective polynomials over K in two variables. Projective polynomials over finite fields have found many applications in cryptography, coding theory and combinatorics with a renewed interest in recent years. Biprojective functions were recently employed to exhibit large numbers of combinatorially and cryptographically interesting objects. We will explain construction and enumeration

methods for bijective structures and methods to determine "inequivalence" between them. The talk is mostly on the material from our recent joint works with Lukas Kölsch.

16:00 - 17:15 (UTC+1): Boolean Functions II

Chair: Petr Lisoněk

On Constructions of Binary Locally Repairable Codes with Locality Two and Multiple Repair Alternatives via Autocorrelation Spectra of Boolean Functions

Deng Tang, Jian Liu and Sihem Mesnager

[Paper](#)

Vectorial Boolean Functions with the Maximum Number of Bent Components outside the $\mathcal{M}^\#$ class

Amar Bapić, Enes Pasalic, Alexandr Polujan and Alexander Pott

[Paper](#)

C -differential uniformity for functions constructed via the Maiorana-McFarland bent function

Pantelimon Stănică

[Paper](#)

17:15 (UTC+1): Closing