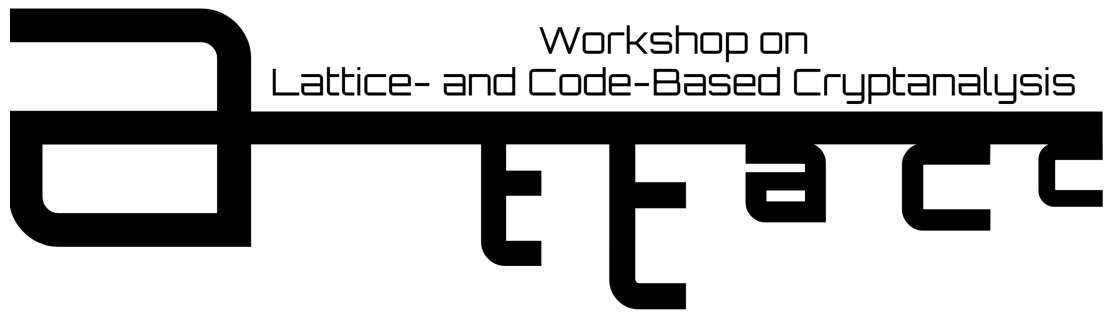


Workshop on Lattice- and Code-Based Cryptanalysis



February 5-8, 2024 — German Aerospace Center (DLR), Oberpfaffenhofen, Germany
www.dlr.de/kn/attacc

	Monday	Tuesday	Wednesday	Thursday
09:00	09:00–09:30 welcome	09:00–10:00 lecture 2 – part 1 Phong Nguyen	09:00–10:00 lecture 3 – part 1 Andre Esser	09:00–10:00 lecture 4 – part 1 Anna-Lena Horlemann
10:00	09:30–10:30 lecture 1 – part 1 Thomas Debris-Alazard	10:00–10:30 coffee break	10:00–10:30 coffee break	10:00–10:30 coffee break
11:00	10:30–11:00 coffee break	10:30–11:15 lecture 2 – part 2 Phong Nguyen	10:30–11:15 lecture 3 – part 2 Andre Esser	10:30–11:15 lecture 4 – part 2 Anna-Lena Horlemann
	11:00–11:45 lecture 1 – part 2 Thomas Debris-Alazard	11:15–11:30 break	11:15–11:30 break	11:15–11:30 break
12:00	11:45–12:00 break	11:30–12:30 talks – session 3	11:30–12:30 talks – session 5	11:30–12:30 talks – session 6
	12:00–12:30 talks – session 1	12:30–13:30 lunch break	12:30–13:30 lunch break	12:30–13:30 lunch break
13:00	12:30–13:30 lunch break	13:30–14:30 talks – session 4	13:30–13:45 photo	13:30–15:30 coworking session
14:00	13:30–14:00 talks – session 2	14:30–15:30 coworking session	13:45–15:45 GSOC tours/ coworking session	
15:00	14:00–15:00 open problems	15:30–16:00 coffee break	15:45–16:15 coffee break	15:30–16:00 coffee break
16:00	15:00–15:30 coffee break	16:00–17:30 coworking session	16:15–17:30 coworking session	16:00–17:30 coworking session
17:00	15:30–17:30 coworking session			

Lecture 1	Monday, 09:30–11:45
09:30–11:45	Thomas Debris-Alazard Codes and Lattices: Real Twins or Distant Cousins?
Session 1	Monday, 12:00–12:30
12:00–12:30	Charles Meyer-Hilfiger Reduction from sparse-LPN to plain-LPN, dual attacks 3.0
Session 2	Monday, 13:30–14:00
13:30–14:00	Ludo Pulles Accurate Score Prediction for Dual-Sieve Attacks
Lecture 2	Tuesday, 09:00–11:15
09:00–11:15	Phong Nguyen Lattice Algorithms: Where Do We Go From Here?
Session 3	Tuesday, 11:30–12:30
11:30–12:00	Eamonn Postlethwaite Introduction to short integer solutions
12:00–12:30	Jean-Christophe Deneuville Practical cryptanalytic gains using the ideal structure
Session 4	Tuesday, 13:30–14:30
13:30–14:00	Shane Gibbons Hull Attacks on the Lattice Isomorphism Problem
14:00–14:30	Simona Samardjiska Graph-based attacks against equivalence problems
Lecture 3	Wednesday, 09:00–11:15
09:00–11:15	Andre Esser Basics of Information Set Decoding & Sieving for Codes
Session 5	Wednesday, 11:30–12:30
11:30–12:00	Simona Etinski Sieving for Codes and Lattices
12:00–12:30	Marc Stevens MCCL: Modular Code Cryptanalysis Library
Lecture 4	Thursday, 09:00–11:15
09:00–11:15	Anna-Lena Horlemann Code-Based Cryptography in Different Metrics
Session 6	Thursday, 11:30–12:30
11:30–12:00	Lars Ran Algebraic Algorithm for the Alternating Trilinear Form Equivalence Problem
12:00–12:30	Marc Newman Lee metric decoding and ℓ_1 norm lattices

Abstracts of Invited Lectures

Thomas Debris-Alazard

Monday

Codes and Lattices: Real Twins or Distant Cousins?

Codes and lattices share many mathematical similarities; a code is defined as a subspace of a vector space over a finite field, and typically endowed with the Hamming metric, while a lattice is a discrete subgroup of an Euclidean vector space. Both objects have found over the last two decades similar applications in cryptography.

Code and lattice-based crypto-systems can be built relying either on the hardness of finding a close codeword or a close lattice point from a given target, a task called decoding. In both disciplines, a considerable amount of work has been made to study the decoding difficulty by identifying its sources of hardness (via reductions) and by designing algorithms to solve it (via cryptanalysis). However, despite many similarities, very few works brought closer codes and lattices in a cryptographic context by studying them in parallel via a common language.

The aim of this talk is to exhibit a dictionary between codes and lattices showing that techniques for studying the decoding difficulty turned out to be the same. We will mainly focus our attention on Fourier duality which is, as we will see, the crucial tool to obtain worst-to-average case reductions (classical or quantum) or to understand recent dual attacks for both codes and lattices.

Phong Nguyen

Tuesday

Lattice Algorithms: Where Do We Go From Here?

Basics of Information Set Decoding

Decoding linear codes is one of the most fundamental problems in coding theory and code-based cryptography. The best known algorithms for decoding random linear codes (almost) all fall into the realm of Information Set Decoding (ISD). In this lecture we will first revisit the definition of an information set and understand how these sets can be used to construct a basic decoding routine. Next we discuss how combinatorial techniques can be used to enhance this basic routine and learn how to derive asymptotic complexity exponents for these algorithms, which are used to classify their efficiency. We then present selected, more advanced improvements with regards to ISD algorithms, including the embedding of representations and nearest-neighbor techniques.

Sieving for Codes

The second part of the lecture introduces the recent framework of SievingISD. This framework uses the usual ISD embedding of combinatorial improvements, but relies, inspired by lattice-techniques, on a sieving-style routine to perform the enumeration. We highlight the essential differences between code- and lattice-sieving that make this technique work. However, despite these differences, at the heart of sieving for codes lies, similar to the lattice-setting, a nearest-neighbor routine (on the Hamming-Sphere). We then discuss different algorithms to instantiate this routine, ranging from basic techniques to a procedure tailored to the code-based setting achieving close to optimal complexities. We conclude with future perspectives and open questions.

Code-Based Cryptography in Different Metrics

Classically code-based cryptography uses the Hamming metric, however, one can replace it by any other coding metric and the respective isometries, as long as the metric is defined on a vector space (as the ambient space). The most studied alternative metric in code-based cryptography is the rank metric, for which many results are known. Furthermore, the Lee and the sum-rank metric have recently gotten a lot of attention in this context. We will give an overview of known results and open questions for those metrics, including:

- public key cryptosystems
- identification schemes and digital signatures
- generic decoding
- structural attacks on public keys

Finally, we will show how the metrics are related to each other (or other metrics) and which metric bears similarities with lattice-based cryptography.

Abstracts of Contributed Talks

Charles Meyer-Hilfiger

Monday, 12:00–12:30

Reduction from sparse-LPN to plain-LPN, dual attacks 3.0

The security of code-based cryptography relies primarily on the hardness of decoding generic linear codes. Until very recently, all the best algorithms for solving the decoding problem were primal attacks, more commonly called information set decoders. While originally uncompetitive, the first dual attack introduced by Al-Jabri in 2001 was recently drastically improved by two new algorithms, namely RLPN (2022) and then double-RLPN (2023); the latter outperforms significantly information set decoders for rates smaller than 0.42. The main idea of Al-Jabri’s algorithm is to recover a position of the error using many parity-checks of small weight on the whole support. RLPN improves Al-Jabri’s algorithm by recovering multiple positions of the error at a time: it reduces decoding to some LPN problem where the samples are obtained by computing efficiently many parity-checks of small weight when restricted to some positions. Lastly, double-RLPN improves RLPN by noticing that the previous LPN problem is in fact sparse, namely with a secret whose Hamming weight is small, and it reduces it to a plain-LPN problem with a coding approach inspired by coded-BKW. The goal of this talk is to recap previous dual attacks and present the double-RLPN algorithm.

Ludo Pulles

Monday, 13:30–14:00

Accurate Score Prediction for Dual-Sieve Attacks

The lattice-based dual attack has seen many improvements in the recent years, leading to claims that it is the most efficient attack against certain cryptoschemes. The claims are based on a heuristic, which states that the inner products of one point in space with dual lattice vectors behave independently. However, the work of Ducas–Pulles (Crypto ’23) reveals using experiments that an analysis based on this heuristic overestimates the success probability of the dual attack, invalidating the recent claims. In this presentation, we provide a theoretical explanation and intuition why the heuristic mispredicts the success probability of the dual attack. Moreover, we give a novel heuristic, which gives very accurate predictions in experiments. The presentation finishes with some future directions that may be pursued. Based on ePrint: <https://ia.cr/2023/1850>.

Eamonn Postlethwaite

Tuesday, 11:30–12:00

Introduction to short integer solutions

In this introductory lecture we will discuss the short integer solution problems and variants. Such problems appear frequently, especially in the design of lattice based signatures. Cryptanalysis (mostly) comprises lattice reduction on a particular class of related lattices, but we will also mention recent results on attacks that occur when parameters are pushed too far.

Jean-Christophe Deneuville

Tuesday, 12:00–12:30

Practical cryptanalytic gains using the ideal structure

Using structured codes or lattices is a common approach for improving parameters hence efficiency of cryptographic constructions. It is generally assumed that the best attacks against such constructions are the generic best known attacks, i.e. those for unstructured objects. In this talk, we try to exhibit some aspects that could yield practical improvements, if not theoretical ones. Disclaimer: this talk should be taken as a call for interest to dig more into the subject, rather than a strong claim that constructions leveraging structured objects might actually be weaker than their unstructured counterparts.

Shane GibbonsTuesday, 13:30–14:00

Hull Attacks on the Lattice Isomorphism Problem

The lattice isomorphism problem (LIP) asks one to find an isometry between two lattices. It has recently been proposed as a foundation for cryptography in two independent works [Ducas & van Woerden, EUROCRYPT 2022, Bennett et al. Eurocrypt 2023]. This problem is the lattice variant of the code equivalence problem, where the notion of the hull of a code can lead to devastating attacks. In this work we study the cryptanalytic role of an adaptation of the hull to the lattice setting, namely, the s -hull. We show that the hull can be helpful for geometric attacks on the lattice isomorphism: for certain lattices the minimal distance of the hull is relatively smaller than that of the original lattice, and this can be exploited. The attack cost remains exponential, but the constant in the exponent is halved. This result gives a counterexample to the general hardness conjecture of LIP proposed by Ducas & van Woerden. Moreover, it is an instance of an attack on a code-based problem being adapted to solve a lattice problem. Our results suggest that one should be very considerate about the geometry of hulls when instantiating LIP for cryptography. They also point to unimodular lattices as attractive options, as they are equal to their dual and their hulls, leaving only the original lattice to an attacker. This is already the case in proposed instantiations, namely the trivial lattice Z^n and the Barnes-Wall lattices.

Simona SamardjiskaTuesday, 14:00–14:30

Graph-based attacks against equivalence problems

In the past few years, there has been an increased interest in hard equivalence problems, especially with NIST's announcement of a fourth round for new designs of digital signatures. On a high level, such a problem can be defined as follows: Given two algebraic objects, find - if any - an equivalence that maps one object into the other. Several instantiations have been considered for cryptographic purposes, for example - Isomorphism of polynomials (Pattarin '96), Code equivalence (Biasse et al. '20), Matrix Code equivalence (Chou et al. '22), Alternating trilinear form equivalence (Tang et al. '22), Lattice isomorphism (Ducas & van Woerden '22). All of these problems are believed to be hard even for quantum adversaries. Conveniently, they can generically be used to build a Sigma protocol and further a post-quantum secure signature using the Fiat-Shamir transform. In this talk I will consider some graph-based algorithms against code-based equivalence problems, their applications to different objects and isometries and the differences that arise depending on the usecase.

Simona Etinski

Wednesday, 11:30–12:00

Sieving for Codes and Lattices

In this talk, I will compare and contrast sieving techniques used for attacking code-based and lattice-based problems. Namely, I will focus on a sieving technique used for attacking code-based problems originally introduced in [GJN22] and further improved and formalized in [DEEK23]. I will then compare it to its closest lattice-based equivalent, introduced in [BDGL17], and highlight the differences between the two approaches.

References:

- [BDGL16] Becker, Ducas, Gama, Laarhoven (2015/2016). New directions in nearest neighbor searching with applications to lattice sieving. <https://eprint.iacr.org/2015/1128.pdf>
- [DEEK23] Ducas, Esser, Etinski, Kirshanova (2023). Asymptotics and Improvements of Sieving for Codes. <https://eprint.iacr.org/2023/1577.pdf>
- [GJN23] Guo, Johansson, Nguyen (2023). A new sieving-style information-set decoding algorithm. <https://eprint.iacr.org/2023/247.pdf>

Marc Stevens

Wednesday, 12:00–12:30

MCCL: Modular Code Cryptanalysis Library

MCCL strives to be a flexible and optimized playground for code cryptanalysis. It is built in C++ with the ISD-generic + sub-ISD structure, allowing subISD algorithms to be added easily. We hope it aids our community in code cryptanalysis research.

Lars Ran

Thursday, 11:30–12:00

Algebraic Algorithm for the Alternating Trilinear Form Equivalence Problem

In NIST's additional call for signatures at least 4 schemes have been proposed that are based on equivalence problems. One of these is based on the Alternating Trilinear Form Equivalence (ATFE). In this talk we explore an algorithm for solving ATFE algebraically by treating it as a matrix code equivalence problem. We find that the resulting system has less variables and less equations than earlier algebraic models, and generally, is easier to solve.

Marc Newman

Thursday, 12:00–12:30

Lee metric decoding and ℓ_1 norm lattices

There are several generic decoding algorithms for the Lee metric, all of which are analogous to generic decoders in the Hamming metric. However, Lee metric decoding is also reducible to the closest vector problem and related problems in ℓ_1 norm lattices. While these problems appear in the literature, most results are related to reductions to-and-from their better-studied variants in the ℓ_2 norm. In this talk we will present the link between Lee decoding and lattice problems, the existing methods to solving these problems, and our ongoing work attempting to exploit this link to achieve more efficient Lee metric decoding.