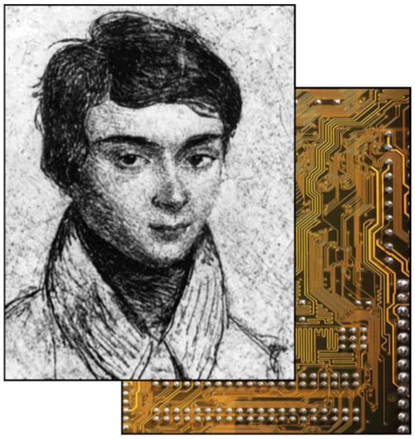
Workshop on Arithmetic in Finite Fields WAIFI 2024



June 10-12, 2024

Carleton Dominion-Chalmers Centre,
Woodside Hall
355 Cooper Street, Ottawa, Canada

Sponsors

The Fields Institute for Research in Mathematical Sciences

FIELDS

The Tutte Institute for Mathematics and Computing

INSTITUT
TUTTE
INSTITUTE

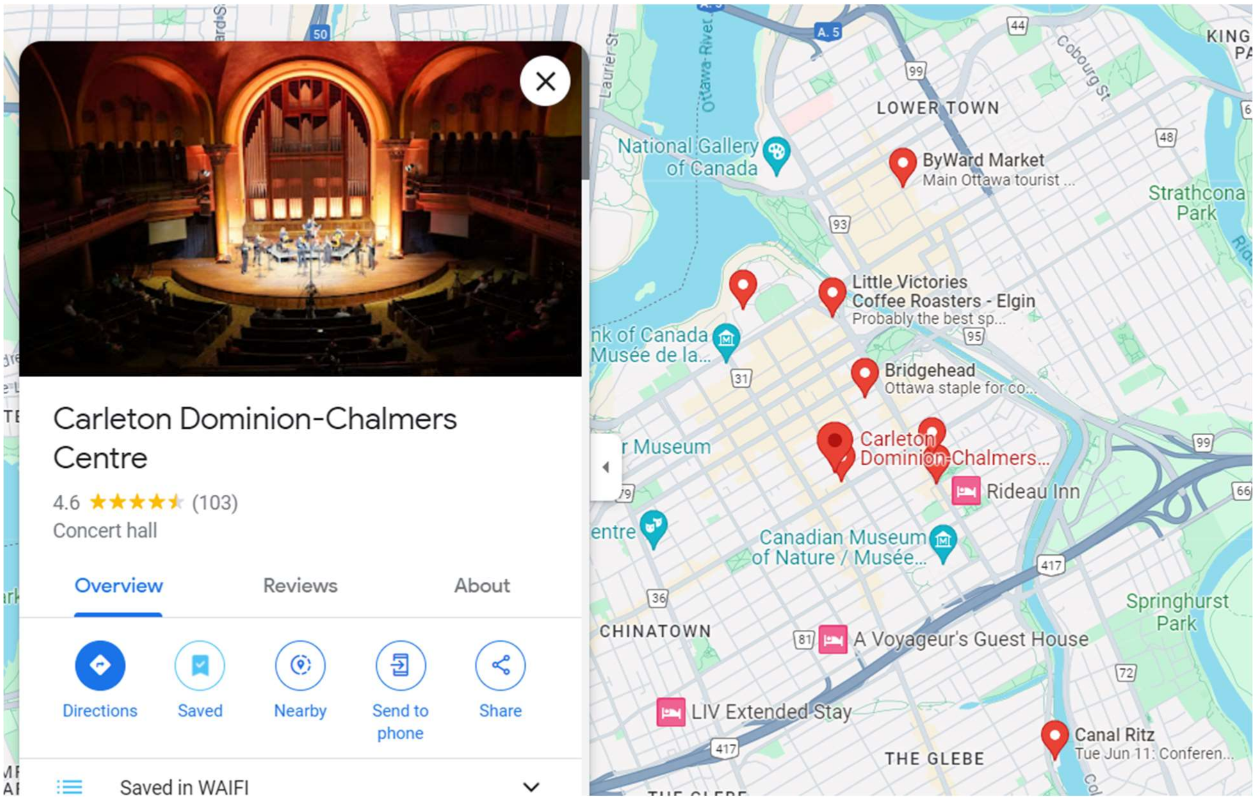
The Institute for Combinatorics and its Applications

ICA
The Institute
of Combinatorics
and its Applications

The School of Mathematics and Statistics, Carleton University

Carleton
University
School of Mathematics
and Statistics

Conference Map (https://maps.app.goo.gl/tNrgRPcUcNDTWu366)



Points of Interest:

Conference Locations:

1. **Woodside Hall: Carleton Dominion-Chalmers Centre**, 355 Cooper St.
2. **The Business Inn & Suites,** 180 MacLaren St.
3. (Mon Jun 10) Welcome reception @ **Union Local 613** (upstairs), 315 Somerset Ave. W
4. (Tue Jun 11) Conference dinner @ **Canal Ritz**, 375 Queen Elizabeth Dr.

Coffee:

1. Little Victories: 44 Elgin St.
2. Bridgehead: 160 Elgin St.
3. Happy Goat Coffee: 326 Elgin St

Tourism:

1. Parliament Hill
2. Byward Market

Schedule

Monday June 10, 2024

09:15-09:30	Welcome	
09:30-10:30	Invited talk: Marco Baldi (Università Politecnica delle Marche)	The restricted decoding problem and its application to post-quantum cryptography
10:30-11:00	Coffee break	
11:00-11:30	Gerardo Vega, Félix Hernández	Determining the complete weight distributions of some families of cyclic codes
11:30-12:00	Chin Hei Chan, Maosheng Xiong	Central limit theorem for linear eigenvalue statistics of random matrices from binary linear codes
12:00-13:30	Lunch	
13:30-14:00	Eduardo Camps-Moreno, Ignacio García-Marco, Hiram H. López, Irene Márquez-Corbella, Edgar Martínez-Moro, Eliseo Sarmiento	On decoding hyperbolic codes
14:00-14:30	Dongxia Luo, Lucia Moura	Fast decoding of group testing results from Reed-Solomon d-disjunct matrices
14:30-15:00	Coffee break	
15:00-15:30	Lucas Da Silva Reis	Prescribing traces of primitive elements in finite fields
15:30-16:00	Mohit Pal	On Cryptographic Properties of a Class of Power Permutations in Odd Characteristic
16:00-16:30	Francisco Javier Soto, Ana Isabel Gómez Pérez, Domingo Gómez Pérez	Generating gaussian pseudorandom noise with binary sequences
16:30-17:00	Amund Askeland	An FPGA Accelerated Search Method for Maximum Period NLFSRs File
18:00-20:00	Welcome Reception: Union Local 613 (upstairs): 315 Somerset Ave. W	

Tuesday June 11, 2024

09:30-10:30	Invited talk: Maria Montanucci (Technical University of Denmark)	Algebraic curves over finite fields: rational points and birational invariants
10:30-11:00	Coffee Break	
11:00-11:30	Olga Polverino, Paolo Santonastaso, Ferdinando Zullo	On fat linearized polynomials
11:30-12:00	Simon Kuttner, Jason Gao, Steven Wang	Counting polynomials with distinct roots in finite fields using the subset sum problem
12:00-13:30	Lunch	

13:30-14:30	Invited talk (remote): Chloe Martindale (University of Bristol)	Making and breaking post-quantum cryptography from elliptic curves
14:30-15:00	Coffee Break	
15:00-15:30	Sarah Arpin, Wouter Castryck, Jonathan Komada Eriksen, Gioella Lorenzon, Frederik Vercauteren	Generalized class group actions on oriented elliptic curves with level structure
15:30-16:00	Daniele Bartoli, Lukas Koelsch, Giacomo Micheli	Differential biases, c-differential uniformity, and their relation to differential attacks
16:00-16:30	Claude Carlet, Ulises Pastor-Díaz, José M. Tornero	On the Walsh and Fourier-Hadamard Supports of Boolean Functions From a Quantum Viewpoint
16:30-17:00	Reza Dastbasteh, Olatz Sanz Larrarte, Josu Etxezarreta Martínez, Antonio Demarti Iolius, Javier Oliva del Moral, Pedro Crespo Bofill	Quantum CSS Duadic and Triadic Codes: New Insights and Properties
19:00-21:00	Conference Dinner: Canal Ritz – 375 Queen Elizabeth Driveway	

Wednesday June 12, 2024

09:30-10:30	Invited talk: Koray Karabina (National Research Council, Canada)	An overview of mathematical problems, cryptosystems, and their interconnections
10:30-11:00	Coffee Break	
11:00-11:30	Nazli Deniz Türe, Murat Cenk	Efficient Batch Post-Quantum Signatures with Crystals Dilithium
11:30-12:00	Mohammadtaghi Badakhshan, Guiwen Luo, Tanmayi Jandhyala, Guang Gong	Ursa Minor: The Implementation Framework for Polaris
12:00-12:30	Jiafeng Xie, Pengzhou He, Samira Carolina Oliva Madrigal, Çetin Kaya Koç	SMALL: Scalable Matrix OriginAted Large Integer PoLynomial Multiplication Accelerator for Lattice-based Post-Quantum Cryptography
12:30	Closing Remarks	

Invited Talk

The restricted decoding problem and its application to post-quantum cryptography

Marco Baldi

Universita Politecnica delle Marche

Code-based cryptographic trapdoors, along with lattice-based ones, are at the basis of some of the most interesting post-quantum cryptographic primitives. Starting from the original McEliece cryptosystem, the problem of decoding in the Hamming metric searching for solutions with low weight has classically been used to design code-based cryptosystems. Later, the alternative decoding problem searching for solutions with large weight, which are also rare, began to be considered in code-based cryptography. More recently, new variants of the decoding problem have been introduced that look for solutions subject to certain restrictions, such as having only entries belonging to a restricted subset of the finite field over which the code is defined. The talk will describe these new variants of the decoding problem, known as restricted decoding problem, and show how they can be used to design new post-quantum digital signature schemes, such as the CROSS scheme that is among the candidates in the current NIST process for selection and standardization of post-quantum digital signature schemes.

Invited Talk

An overview of mathematical problems, cryptosystems, and their interconnections'

Koray Karabina

National Research Council, Canada

Integer factorization, discrete logarithm, subset-sum, and lattice problems have significantly influenced cryptosystem design and motivated the development of algorithms to efficiently tackle the underlying problem instances. This talk presents an overview of these problems and cryptosystems, focusing on their noteworthy interconnections, key applications, and security claims in the post-quantum era.

—–

Invited Talk

Making and breaking post-quantum cryptography from elliptic curves

Chloe Martindale

University of Bristol

Most of the public-key cryptography in use today relies on the hardness of either factoring or the discrete logarithm problem in a specially chosen abelian group. Here "hard" does not mean mathematically impossible but that the best known algorithm to solve the problem has complexity (sub-)exponential in the size of the input. However, once scalable quantum computers become a reality, both factoring and the discrete logarithm problem will no longer be hard problems, due to Shor's polynomial-time quantum algorithm to solve both problems. Post-quantum cryptography is about designing new cryptographic primitives based on different hard problems in mathematics for which there is no known polynomial-time classical or quantum algorithm. In this talk we will show how to design post-quantum cryptographic primitives from the hard problem of, given two elliptic curves over a large finite field, find and compute and isogeny between them (if it exists). We will then discuss recent work giving an attack on one of these primitives, Supersingular Isogeny Diffie-Hellman (SIDH).
This is joint work with Luciano Maino, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski.

—–

Invited Talk

Algebraic curves over finite fields: rational points and birational invariants

Maria Montanucci

Technical University of Denmark

Algebraic curves over a finite field $\mathbb{F}_q$ have been a source of great fascination, ever since the seminal work of Hasse and Weil in the 1930s and 1940s. Many fruitful ideas have arisen out of this area, where number theory and algebraic geometry meet, and many applications of the theory of algebraic curves have been discovered during the last decades.

A very important example of such application was provided in 1977-1982 by Goppa, who found a way to use algebraic curves in coding theory. The key point of Goppa's construction is that the code parameters are essentially expressed in terms of the features of the curve, such as the number N_q of $\mathbb{F}_q$-rational points and the genus g. In this light, Goppa codes with good parameters are constructed from curves with large N_q with respect to their genus g.

Given a smooth projective, algebraic curve of genus g over $\mathbb{F}_q$, an upper bound for N_q is a corollary to the celebrated Hasse-Weil Theorem,

$$N_q \leq q + 1 + 2g\sqrt{q}.$$

Curves attaining this bound are called $\mathbb{F}_q$-maximal.

The Hermitian curve is a key example of an $\mathbb{F}_q$-maximal curve, as it is the unique curve, up to isomorphism, attaining the maximum possible genus of an $\mathbb{F}_q$-maximal curve. It is a result commonly attributed to Serre that any curve which is $\mathbb{F}_q$-covered by an $\mathbb{F}_q$-maximal curve is still $\mathbb{F}_q$-maximal. In particular, quotient curves of $\mathbb{F}_q$-maximal curves are $\mathbb{F}_q$-maximal. Many examples of $\mathbb{F}_q$-maximal curves have been constructed as quotient curves of the Hermitian curve by choosing a subgroup of its very large automorphism group.

It is a challenging problem to construct maximal curves that cannot be obtained in this way, as well as to construct maximal curves with many automorphisms (in order to use the machinery described above). A natural question arises also: given two maximal curves over the same finite field, how can one decide whether they are isomorphic or not? A way to try to give an answer to this question is to look at the birational invariants of the two curves, that is, their properties that are invariant under isomorphism.

In this talk, we will describe our main contributions to the theory of maximal curves over finite fields and their applications to coding theory. In relation with the question described before, during the talk, the behaviour of the birational invariant of maximal curves will also be discussed.

Determining the complete weight distributions of some families of cyclic codes

Gerardo Vega and Félix Hernández

Obtaining the complete weight distributions for nonbinary codes is an even harder problem than obtaining their Hamming weight distributions. In fact, obtaining these distributions is a problem that usually involves the evaluation of sophisticated exponential sums, which leaves this problem open for most of the linear codes. In this work we present a method that uses the known complete weight distribution of a given cyclic code, to determine the complete weight distributions of other cyclic codes. In addition we also obtain the complete weight distributions for a particular kind of one- and two-weight irreducible cyclic codes, and use these distributions and the method, in order to determine the complete weight distributions of infinite families of cyclic codes. As an example, and as a particular instance of our results, we determine in a simple way the complete weight distribution for one of the two families of reducible cyclic codes studied by Bae, Li and Yue [Discrete Mathematics, 338 (2015) 2275-2287].

Central limit theorem for linear eigenvalue statistics of random matrices from binary linear codes

Chin Hei Chan and Maosheng Xiong

It was known that the empirical spectral distribution of random matrices constructed from binary linear codes of increasing length converges to the Marchenko-Pastur law as long as the dual distance of the codes is at least 5, and the condition of the dual distance 5 is optimal because there are binary linear codes of dual distance 4 that do not satisfy this property. In this article, we push this result a little further: we show that a Gaussian central limit theorem holds for the linear spectral statistics associated with such random matrices from binary linear codes of increasing length when the dual distance is at least 7. We also show that the condition of dual distance 7 is optimal as there are binary linear codes of dual distance 6 that do not satisfy this property. This result can be interpreted as that pseudorandom sequences constructed from long binary linear codes of dual distance 7 in general satisfy a more stringent pseudorandom test than those from binary linear codes of dual distance 5.

On decoding hyperbolic codes

Eduardo Camps-Moreno,
Ignacio García-Marco,
Hiram H. López,
Irene Márquez-Corbella,
Edgar Martínez-Moro,
Eliseo Sarmiento

This work studies several decoding algorithms for hyperbolic codes based on known Reed-Muller decoders. We use some previous ideas to describe how to decode a hyperbolic code using the largest Reed-Muller code contained in it or using the smallest Reed-Muller code that contains it. A combination of these two algorithms is proposed when hyperbolic codes are defined by polynomials in two variables. Then, we compare hyperbolic codes and Cube codes (tensor product of Reed-Solomon codes) and propose decoding algorithms of hyperbolic codes based on their closest Cube codes. Finally, we adapt to hyperbolic codes the Geil and Matsumoto's generalization of Sudan's list decoding algorithm.

Fast decoding of group testing results from Reed- Solomon d-disjunct matrices

Dongxia Luo and Lucia Moura

Non-adaptive combinatorial group testing has applications in disease screening as well as in many problems in digital security and communications. Matrices that are d-disjunct (also called d-cover-free) can be build using codes and allows for the detection of d defective items using group testing. In this paper, we study d-disjunct matrices build from Reed-Solomon codes, and design a specialized algorithm for decoding the results of group testing using these matrices. We do an experimental comparison between our method and the naive one that only uses the d-disjunct property of the matrix, and show that the former outperforms the latter as the size of the problem grows.

Prescribing traces of primitive elements in finite fields

Lucas Da Silva Reis

Let F be a finite field and let E be an n-degree extension of F. Given a family $\{F_1, \dots, F_k\}$ of intermediate fields, we discuss the existence of primitive elements of E whose traces over the fields F_i are prescribed. In 2022, S. Ribas and the author studied this problem and, by employing a very standard approach, we provided asymptotic results under some mild restrictions on the intermediate fields. Moreover, we observed that such element can never exist if $[E : F_i] = 2$ for some $1 \le i \le k$ and the corresponding prescribed trace is zero. In this paper we show that, up to this genuine exception, such element exists if n is fixed and $\#F$ is large enough. In contrast to the ideas employed in our previous work, here our approach basically relies on showing that the corresponding set of elements in E with prescribed traces comprises an affine space with a generic algebraic property. The affine spaces satisfying this property were recently studied by the author, where it is shown that they present a good cancellation through multiplicative character sums (hence they contain a large number of primitive elements).

On Cryptographic Properties of a Class of Power Permutations in Odd Characteristic

Mohit Pal

Recently, interest in bijective functions over finite fields of odd characteristic with good cryptographic properties increased as many cryptographic primitives have been proposed in the literature which operate on prime field $\mathbb{F}_p$ for some large prime p. Here, we consider the boomerang uniformity and algebraic degree of a class of differentially 4-uniform power permutations over finite fields of odd characteristic. We also determine the compositional inverse of this class of power permutations and compute the algebraic degree of its compositional inverse.

Generating gaussian pseudorandom noise with binary sequences

Francisco Javier Soto,
Ana Isabel Gómez Pérez,
Domingo Gómez Pére

Gaussian random number generators attract a widespread interest due to their applications in several fields. Important requirements include easy implementation, tail accuracy, and, finally, a flat spectrum. In this work, we study the applicability of uniform pseudorandom bi- nary generators in combination with the Central Limit Theorem to propose an easy to implement, efficient and flexible algorithm that leverages the properties of the pseudorandom binary generator used as an input, specially with respect to the correlation measure of higher order, to guarantee the quality of the generated samples. Our main result provides a relationship between the pseudorandomness of the input and the statistical moments of the output. We propose a design based on the combination of pseudonoise sequences commonly used on wireless communications with known hardware implementation, which can generate sequences with guaranteed statistical distribution properties sufficient for many real life applications and simple machinery. Initial computer simulations on this construction show promising results in the quality of the output and the computational resources in terms of required memory and complexity.

An FPGA Accelerated Search Method for Maximum Period NLFSRs File

Amund Askeland

Maximum period nonlinear feedback shift registers (NLFSRs) are promising building blocks for stream ciphers and pseudo-random number generators. Unfortunately, many fundamental problems related to NLFSRs remain open, and in particular, it is not known how to construct ones whose periods are of maximum length. In this paper, we describe a search method for finding maximum period NLFSRs. The method is based on using an accelerator implemented on a field programmable gate array (FPGA) to test NLFSR periods, and an initial pruning step that checks for short cycles. We use this method to build a dataset containing complete lists of maximum period NLFSRs of certain forms up to a bit width of 32. We also release the source code for our FPGA implementation together with the dataset.

On fat linearized polynomials

Olga Polverino,
Paolo Santonastaso,
Ferdinando Zullo

Fat polynomials have been recently introduced as a generalization of scattered polynomials. These polynomials define linear sets on the projective line with r points of weight greater than one and also rank-metric codes with a certain number of matrices of lower rank. In this paper we explore 1- and 2-fat polynomials, by providing examples and some classification results.

Counting polynomials with distinct roots in finite fields using the subset sum problem

Simon Kuttner,
Zhicheng Gao,
Qiang Wang

Let G be a finite additive abelian group. For each $\alpha \in G$, let $M(\alpha)$ be a subset of non-negative integers. We study the number of partitions of $b \in G$ with r parts such that the multiplicity of α belongs to $M(\alpha)$. That is, we study the cardinality of the set

$$\left\{ m : \sum_{\alpha \in G} m(\alpha)\alpha = b,\ \sum_{\alpha \in G} m(\alpha) = r,\ m(\alpha) \in M(\alpha) \right\}.$$

When $M(\alpha) = \{0, 1\}$ for each $\alpha \in D$ and $M(\alpha) = 0$ for each $\alpha \notin D$, where $D \subseteq G$, this becomes the classical subset sum problem. Our approach uses generating functions and character sums. Simple explicit formulas are derived for some special types of abelian groups.

Generalized class group actions on oriented elliptic curves with level structure

Sarah Arpin,
Wouter Castryck,
Jonathan Komada Eriksen,
Gioella Lorenzon,
Frederik Vercauteren

We study a large family of generalized class groups imaginary quadratic number fields K and prove that they act freely and (essentially) transitively on the set of O_K-oriented elliptic curves over a field k (assuming this set is non-empty) equipped with appropriate level structure. This extends, in several ways, a recent observation due to Galbraith, Perrin and Voloch for the ray class group. We show that this leads to a reinterpretation of the action of the class group of a suborder $O \subseteq O_K$ on the set of O-oriented elliptic curves, discuss several other examples, and briefly comment on the hardness of the corresponding vectorization problems.

Differential biases, c-differential uniformity, and their relation to differential attacks

Daniele Bartoli,
Lukas Koelsch,
Giacomo Micheli

Differential cryptanalysis famously uses statistical biases in the propagation of differences in a block cipher to attack the cipher. In this paper, we investigate the existence of more general statistical biases in the differences. To this end, we discuss the c-differential uniformity of S-boxes, which is a concept that was recently introduced to measure certain statistical biases that could potentially be used in attacks similar to differential attacks. Firstly, we prove that a large class of potential candidates for S-boxes necessarily has large c-differential uniformity for all but at most B choices of c, where B is a constant independent of the size of the finite field q. This result implies that for a large class of functions, certain statistical differential biases are inevitable. In a second part, we discuss the practical consequences of this result; in particular we discuss the practical possibility of designing a differential attack based on weaknesses of S-boxes related to their c-differential uniformity.

On the Walsh and Fourier-Hadamard Supports of Boolean Functions From a Quantum Viewpoint

Claude Carlet,
Ulises Pastor-Díaz,
José M. Tornero

In this paper, we focus on the links between Boolean function theory and quantum computing. In particular, we study the notion of what we call fully-balanced functions and analyze the Fourier-Hadamard and Walsh supports of those functions having such property. We study the Walsh and Fourier supports of other relevant classes of functions, using what we call balancing sets. This leads us to revisit and complete certain classic results and to propose new ones. We complete our study by extending the previous results to pseudo-Boolean functions (in relation to vectorial functions) and giving an insight on its applications in the analysis of the possibilities that a certain family of quantum algorithms can offer.

Quantum CSS Duadic and Triadic Codes: New Insights and Properties

Reza Dastbasteh,
Olatz Sanz Larrarte,
Josu Etxezarreta Martínez,
Antonio Demarti Iolius,
Javier Oliva del Moral,
Pedro Crespo Bofill

In this study, we investigate the construction of quantum CSS duadic codes with dimensions greater than one. We introduce a method for extending smaller splittings of quantum duadic codes to create larger, potentially degenerate quantum duadic codes. Furthermore, we present a technique for computing or bounding the minimum distances of quantum codes constructed through this approach. Additionally, we introduce quantum CSS triadic codes, which can generate codes with a rate of at least $\frac{1}{3}$.

Efficient Batch Post-Quantum Signatures with Crystals Dilithium

Nazli Deniz Türe and Murat Cenk

Digital signatures ensure authenticity and secure communication. They are used to verify the integrity and authenticity of signed documents and are widely utilized in various fields such as information technologies, finance, education, and law. They are crucial in securing servers against cyberattacks and authenticating connections between clients and servers. Performing multiple signature generation simultaneously and efficiently is highlighted as a beneficial approach for many systems. This work focuses on efficient batch signature generation using Crystal Dilithium, NIST's post-quantum digital signature standard. One of the main operations of signature generation using Dilithium is the matrix-vector product with polynomial entries. So, the naive approach to generate m signatures where $m > 1$ is to perform m such multiplications. In this paper, we propose to use efficient matrix multiplications of sizes greater than four to generate m signatures. To this end, a batch algorithm that trans- forms the polynomial matrix-vector multiplication in Dilithium's structure into polynomial matrix-matrix multiplication is designed. The batch numbers and the sizes of the matrices to be multiplied based on the number of repetitions of Dilithium's signature algorithm are determined. Moreover, many efficient matrix-matrix multiplication algorithms, such as Strassen-like multiplications and commutative matrix multiplications, are analyzed to design the best algorithms that are compatible with the specified dimensions and yield improvements. Various multiplication formulas are derived for different security levels of Dilithium, and improvements up to 27.28%, 32.0%, and 30.31% in the arithmetic complexities are observed at three different security levels, respectively. The proposed batch Dilithium signature algorithm and the efficient multiplication algorithms are also implemented, and 18.37%, 9.34%, and 7.19% improvements for three security levels are obtained.

Ursa Minor: The Implementation Framework for Polaris

Mohammadtaghi Badakhshan,
Guiwen Luo,
Tanmayi Jandhyala,
Guang Gong

This paper conducts an analysis of algorithms within Po- laris, a plausibly post-quantum zero-knowledge succinct non-interactive argument of knowledge (zkSNARK) protocol, by decomposing it into its construction components for detailed investigation. Recognizing the need for fast implementation in real-world applications, we introduce the Ursa Minor, an implementation framework tailored to evaluate Polaris's efficiency. Our contribution in this framework are twofold: Firstly, we proposed a concrete GKR arithmetic circuit to be integrated in Polaris. Secondly, we optimized the efficiency of FRI protocol employed in Po- laris, by eliminating the field inversion operations.

SMALL: Scalable Matrix OriginAted Large Integer PoLynomial Multiplication Accelerator for Lattice- based Post-Quantum Cryptography

Jiafeng Xie,
Pengzhou He,
Samira Carolina Oliva Madrigal,
Çetin Kaya Koç

Along with the rapid development in quantum computing, more attention has been switched to post-quantum cryptography (PQC) and related research including their hardware implementations. Follow- ing this trend, this paper presents a novel strategy to implement a special type of polynomial multiplication used in lattice-based PQC, where the coefficients of two input polynomials are unequal, and modulus and polynomial size are power-of-two numbers (not in favor of deploying number theoretic transform). In particular, we have proposed a Scalable Matrix originAted Large integer poLynomial multiplication Accelerator (SMALL) for flexible and compact implementation of the targeted polynomial multiplication. In total, our efforts include: (i) we have formulated and derived a scalable matrix originated computation strategy for the targeted polynomial multiplication in a general format; (ii) we have then presented the detailed internal structures for the proposed polynomial multiplication accelerator based on novel algorithm-to-architecture design techniques; (iii) we have implemented the proposed accelerator based on two case study PQC schemes to demonstrate the superior efficiency of the proposed design over the state-of-the-art solutions. We hope the outcome of this work will be useful for further PQC development.