Workshop on 20th Anniversary of Institute of Applied Mathematics

BOOK OF ABSTRACTS

Middle East Technical University
Culture and Convention Center
Ankara, Turkey
November 4, 2022

Contents

FOREWORD

Institute of Applied Mathematics (IAM) is an interdisciplinary centre fostering multi- and interdisciplinary research opportunities in mathematical sciences. A major aim of IAM is to coordinate mathematics-based research at METU and to initiate and undertake collaborative research with industry.

The Institute of Applied Mathematics began functioning in the academic year 2002-03 by offering Master of Science (MSc) degrees in Financial Mathematics, Scientific Computing and Cryptography. The Cryptography department was the only department offering Doctor of Philosophy (PhD) at that time. In the spring semester of the academic year 2004-05, IAM offered PhD in Financial Mathematics and Scientific Computing to cater the growing demands of professionally skilled manpower in Applied Mathematics. In the academic year 2008-09, Actuarial Sciences started to offer MSc degree as fourth program in the IAM.

Two decades of IAM have given its fruits as successful 264 graduates holding M.Sc or Ph.D degrees, many international and national projects, conferences, uncountable publications and research groups whose achievements are highly acknowledged.

IAM keeps moving along with the recent developments in multidisciplinary areas, expands it horizon in research, but remains in line with theoretical Mathematics. As being the unique multidisciplinary institute abridging Mathematics with other sciences, IAM looks forward to many other decades ahead.

Organizing Committee

- **Steering Committee**
  - A. Sevtap Selçuk-Kestel
  - Önder Türk
  - Oğuz Yayla
- **Technical Assistance**
  - Gülçin Akarsu Şengöz
  - Pelin Çiloğlu
  - Hasan Bartu Yünüak

SPONSORS

We thank cordially our sponsors for their contributions and supports for the workshop organized to celebrate 20th Anniversary of the Institute of Applied Mathematics.

PROGRAMME

<table>
<tr><td>08:00-09:00</td><td colspan="2">Registration</td></tr>
<tr><td>09:00-09:30</td><td colspan="2">Opening Talks</td></tr>
<tr><td></td><td colspan="2">Plenary Talks I
Chair: Önder Türk</td></tr>
<tr><td>09:30-10:15</td><td colspan="2">Ramon Codina
Hybrid Intrusive/ML-based Reduced Order Model for the Optimisation of Aerodynamic Profiles</td></tr>
<tr><td>10:15-11:00</td><td colspan="2">Corina Constantinescu
Subsidizing Inclusive Insurance to Reduce Impoverishment</td></tr>
<tr><td>11:00 - 11:30</td><td colspan="2">Break (Workshop photo session in foyer)</td></tr>
<tr><td rowspan="4">11:30 - 12:30</td><td colspan="2">Parallel Sessions I</td></tr>
<tr><td>Hall A, Chair: Ömür Uğur</td><td>Hall D, Chair: Ferruh Özbudak</td></tr>
<tr><td>Alev Atak
Information Disclosure and Financial Sentiment Index using a Machine Learning Approach</td><td>Fatih Sulak
Randomness in Cryptography</td></tr>
<tr><td>Abdullah Karasan
Factor Analysis through SEC Announcements: A Machine Learning Approach</td><td>Pınar Gürkan Balıkçıoğlu
Dealing with Real Life Use Cases of Cryptography</td></tr>
<tr><td></td><td>Neşe Koçak
Challenges in Post-Quantum</td></tr>
<tr><td>12:30 - 14:00</td><td colspan="2">Lunch Break</td></tr>
<tr><td rowspan="4">14:00 - 15:00</td><td colspan="2">Parallel Sessions II</td></tr>
<tr><td>Hall A, Chair: Hamdullah Yücel</td><td>Hall D, Chair: Ali Devin Sezer</td></tr>
<tr><td>Ahmet Melih Selçuk
Machine Learning Extending Boundaries: Smart Machines, Smart Cities, Smart Agriculture</td><td>Mert C. Demir
An Alternative Approach to the Mean-Variance Markowitz Model</td></tr>
<tr><td>Oktay Ölmez
Moving from Academia to Industry</td><td>Şirzat Çetinkaya
New Technology Age for Insurance Industry</td></tr>
<tr><td>15:00 - 15:30</td><td colspan="2">Break</td></tr>
<tr><td></td><td colspan="2">Plenary Talks II
Chair: Oğuz Yayla</td></tr>
<tr><td>15:30 - 16:15</td><td colspan="2">Zehra Ekşi-Altay
Mean-Reversion and Momentum Trading under Partial Information</td></tr>
<tr><td>16:15 - 17:00</td><td colspan="2">Michal Zajac
A Short Introduction to ZkSNARKs: Recent Results and Open Problems</td></tr>
<tr><td>17:00 - 17:30</td><td colspan="2">Closing Talks</td></tr>
<tr><td>18:00 - 20:00</td><td colspan="2">Reception: Main foyer at Art and Science Faculty Building</td></tr>
</table>

ABSTRACTS

Hybrid Intrusive/ML-based Reduced Order Model for the Optimisation of Aerodynamic Profiles

Ramon Codina[1]

[1] *Department of Civil and Environmental Engineering, Universitat Politecnica de Catalunya, Spain*
ramon.codina@upc.edu

There are several applications in computational fluid mechanics that require solving many times the flow equations, and one of them is the optimisation of aerodynamic profiles. Considering only shape optimisation problems, the geometry needs to be parametrised and the parameters need to be determined from the minimisation of a cost function, for example the drag. This requires many evaluations of this cost function and, therefore, many solves of the flow equations. A fast numerical solution of the flow problem is thus peremptory, and a means to achieve this is using reduced order models (ROMs). In particular, we propose to use ROMs based on proper orthogonal decomposition (POD) and having a finite element (FE) approximation as full order model (FOM). POD-based ROMs start from collecting results from the FOM, for example instances of the unknown at different time instants or for different values of the geometric parameters. These are the so-called snapshots. A basis of a reduced space is then constructed, typically from a singular value decomposition (SVD) of the snapshot collection. The dimension of the ROM space is taken much smaller than that of the FOM space. The flow equations are then projected onto the ROM space and solved there, being this solve much cheaper than that of the FOM (sometimes, after the introduction of some hyper- reduction techniques). ROMs that use the FOM equations, as the projected ROMs described, are often called intrusive. In contrast, there are also ROMs purely designed based on existing data of high fidelity and using machine learning (ML) techniques; these are called non-intrusive models. In this work we propose to design a hybrid model, essentially of intrusive type but incorporating a correction term based on ML techniques. The idea is to start from a purely POD-based ROM, projecting the equations onto the ROM space, and then add a nonlinear correction that depends on the ROM unknowns to enhance the final ROM model. This correction is based on the fact that we do have some available high fidelity data, namely, the snapshots. Thus, the correcting term is built as an artificial neural network (ANN) constructed with the snapshots as training set, i.e., considering that the loss function is the norm of the difference between the snapshots and the outputs predicted by the model. The resulting hybrid ROM has a significant higher accuracy than the original intrusive one.

Subsidizing Inclusive Insurance to Reduce Impoverishment

Corina Constantinescu[1]

[1] *Department of Mathematical Science, University of Liverpool, UK*
c.constantinescu@liverpool.ac.uk

We consider inclusive insurance, namely insurance for financially vulnerable populations. We show that, although insurance alone may not be sufficient to reduce the likelihood of impoverishment for specific groups of households, since premium payments constrain their capital growth, government subsidies can provide maximum social benefits while reducing governmental costs.

Mean-Reversion and Momentum Trading under Partial Information

Zehra Ekşi-Altay[1]

[1] *Institute for Statistics and Mathematics, WU Vienna, Austria*
zehra.eksi-altay@wu.ac.at

Momentum and long-term reversal are past return characteristics that are used frequently to predict future returns. There is well-established finance literature on stock price models with momentum and mean reversion. By its very definition, the momentum factor is observable, whereas the mean-reversion factor is generally unobservable. The existing literature assumes both factors to be observable. Accordingly, it is accustomed to using proxies to estimate the unobservable mean-reversion factor. In this study, we bring the unobservable character of the mean-reversion variable into play. Overall, we solved a utility maximization problem that accommodates both momentum and mean reversion by postulating continuous-time asset price dynamics whose drift can only be partially observed. The Gaussian nature of the problem allowed us to use the Kalman filter methodology to obtain estimates for unobservable mean-reversion level. Since the filtering and stochastic optimal control problems are essentially separable, we reduced the optimization problem under partial information to one with complete information. We solved the reduced control problem and obtained the optimal trading strategies and the value function. Next, we estimated the model based on the CRSP value-weighted index data using a maximum likelihood approach in conjunction with the Kalman filter. We compared the optimal trading strategies under partial and complete information and computed the loss of utility due to partial information. This talk is based on a joint project with Sühan Altay, Katia Colaneri and Eva Flonner.

A Short Introduction to ZkSNARKs: Recent Results and Open Problems

Michał Zając[1]

[1] *Head of Cryptographic Research, Nethermind* michal@nethermind.io

In this talk, I will introduce a special kind of zero-knowledge protocols (ZKP) called zkSNARKs. As usual for ZKP, in zkSNARKs, we define an NP relation $R = \{x, w\}$ and two parties, one called prover and another verifier. The prover gets as input an instance–witness pair (x, w) and produces a proof to convince the verifier who knows x that x belongs to the language L_R induced by R. A ZKP should have the following properties. First, it needs to be complete. An honest verifier should always accept an honest prover's proof. Second, it needs to be sound. That is, a malicious prover should not be able to make the verifier accept a proof for x outside L_R. Third, the verifier should not learn anything from the proof besides that x belongs to L_R. Zk-SNARKs have one additional property, namely *succinctness*. This property states that the proof produced by the prover is sublinear to the size of the instance x and witness w. Zk-SNARKs got their popularity thanks to their useability in verifiable computations. Namely, a computationally limited client playing the role of a ZKP verifier may ask a powerful server, playing the role of a ZKP prover, to evaluate a program 'Prog' on some input 'inp' such that in the end, the client is convinced that the evaluation is correct. To that end, the prover-server evaluates the program and provides a zkSNARK proof of the correctness of the computation. Since zkSNARK proofs are short and easy to verify, they can be verified by the computationally limited client. Even more recently, the zkSNARKs started seeing adoption as a blockchain scaling tool. Namely, they allow building so-called zero-knowledge rollups. In this talk, I will begin by showing how the most popular zkSNARKs are constructed. I will explain the essential building blocks, introduce the the notion of arithmetization and briefly discuss some approaches to that problem. Then I will present what security properties zkSNARKs have, what trusted setup is, and in what cases allowing it is beneficial. Finally, I will discuss what problems are still open.

Information Disclosure and Financial Sentiment Index using a Machine Learning Approach

Alev Atak[1]

[1] *Department of Economics, METU, Turkey* alevatak@metu.edu.tr

In this paper, we aim to investigate the causal effects of voluntary information disclosures on a bank's expected default probability, enterprise risk, and value by creating a financial sentiment index. We extract relevant financial information for sentiment analysis through Natural Language Processing. We retrieve structured content from BIST 100 companies' financial reports for the period 1998-2018. We measure strategy-related disclosures, and their cross-sectional variation and classify report content into generic sections using synonym lists divided into four main categories according to their liquidity risk profile, risk positions, intra-annual information, and their exposure to risk. Therefore, we create an adequate analytical tool and a financial dictionary to depict the importance of granular financial disclosure for investors to identify correctly the risk-taking behavior and hence make the aggregated effects traceable.

Dealing with Real Life Use Cases of Cryptography

Pınar Gürkan Balıkçıoğlu[1],

[1] *Chief Cryptography Officer, InterProbe Information Technologies*
pinar.gb@pavotek.com.tr

In this talk, when dealing with real-life use cases of cryptography, it will be mentioned at which points there are different areas of expertise other than cryptography. The relations of these different fields with cryptography and how they are used together will be explained.

New technology age for insurance industry

Şirzat Çetinkaya[1]

[1] *Director, Sompo Insurance*
President of Turkish Actuarial Society sirzat.cetinkaya@gmail.com

Our environment, technologies and methodologies that we use, risks that we face, parties that we collaborate , business that we govern in a nut shell our world is changing. This presentation aims to show the fast changing environment in actuarial and insurance business in the aspect of practitioners.

An alternative approach to the mean-variance Markowitz model

Mert C. Demir[1], **Ezdin Aslancı**[2]

[1] *Managing Partner, Adendum* mert.demir@adendum.com.tr
[2] *Software Engineer, Adendum* ezdin.aslanci@adendum.com.tr

This manuscript aims at explaining the fund proposal method used in AddVICE©. One of the shortcomings of the efficient market hypothesis optimization model is its dependence to variability of expected returns. Another shortcoming is that it uses an a priori solution and optimizes only future investments. AddVICE model tries to find solutions to both of these shortcomings by making use of extra inputs and by means of a nonlinear mathematical programming model.

Factor Analysis through SEC Announcements: A Machine Learning Approach

Abdullah Karasan[1]

[1] *University of Maryland Baltimore County, USA*
Senior Data Science Consultant, TFI TAB Food Investments abdullahkarasan@gmail.com

Identifying risk is always the key to the success of factor modeling. Though there is a large body of research in risk identification, this study embraces a different method to update financial risk in a timely fashion. That is to say, corporate risk is detected via parsing Item-1A in annual SEC announcements. Subsequent to detecting risk, topic modeling is run and risks are clustered using hierarchical clustering method. Covering the period of 2015/Jan - 2022/Jan and top 10 companies based on market valuation, the result shows that certain types of risk factors have an important impact on the return volatility.

Challenges in Post-Quantum Cryptography

Neşe Koçak[1]

[1] *Aselsan A.Ş.* nesekocak@aselsan.com.tr

The development of quantum computers threatens some cryptographic algorithms used today. Main purpose of the post quantum cryptography is to develop secure cryptographic systems against both quantum and classical computers. In this talk, the challenges encountered in applications of post-quantum cryptographic algorithms will be mentioned.

Moving from Academia to Industry

Oktay Ölmez[1]

[1] *Lead Research Scientist, Afiniti* olmezoktay@gmail.com

As a part of my job, I read industry-related research articles, examine toy examples, mentor people in their career development, and give talks for knowledge transfer purposes in the corporate environment. These activities are similar to my previous daily academic life. After moving out from academia, I realized there is also a set of hard skills and soft skills, which I need to learn shortly and practice daily in the industry. In this talk, I will talk about my career path from academia to industry focusing on the challenges of knowledge-related collaboration.

Machine Learning Extending Boundaries: Smart Machines, Smart Cities, Smart Agriculture

Ahmet Melih Selçuk[1]

[1] *Chief Data Scientist, Managing Partner, Analythinx* ahmet.selcuk@analythinx.com

Early adopters of data analytics were banks, telco operators, retailers trying to optimize human decisions or manipulate human preferences. Predicting human behavior is a mature field of study, we are surrounded by recommendation engines, fraud prevention systems and so on. Recent advances in storing, processing and modeling data -together with cost reductions- enabled extension of big data analytics into other industries. Machine learning might be the key for solving problems in energy consumption, industrial/agricultural inefficiencies or human safety; leading to a greater cause than profit maximization. The presentation will be focused on dissemination of data science and accompanying advances in artificial intelligence.

Randomness in Cryptography

Fatih Sulak[1]

[1] *Department of Mathematics, Atılım University, Turkey* fatih.sulak@atilim.edu.tr

In this talk, we will give a brief introduction about statistical randomness tests. Afterwards, cryptographic randomness tests for block ciphers and hash functions will be introduced. New statistical randomness tests to test outputs of cryptographic primitives will be discussed.

Index of Speakers

VENUE AND LOCAL INFO

Venue

Congress will be held in **Culture and Convention Center of Middle East Technical University**, Ankara, Türkiye.

Middle East Technical University (METU) is a leading national university which is internationally acknowledged and renowned in research, education and public service for society, humanity, and nature, in an environment nurturing, creative and critical thinking, innovation, leadership, and universal values. There are 107 graduate and 69 doctorate programs available in Graduate Schools of Natural Sciences, Social Sciences, Informatics, Applied Mathematics and Marine Sciences. Marine Sciences conducts the academic program studies at İçel-Erdemli. The language of instruction at METU is English. METU School of Foreign Languages takes the initiative to teach English to students at Preparatory School. Owing to the quality academic education that emphasizes merit and excellence in scientific, cultural and intellectual studies as well as owing to the accomplished and qualified METU graduates, the University has become one of the distinguished and respectable institutions of Turkey.

Institute of Applied Mathematics (IAM) is an interdisciplinary graduate school which offers programs in Actuarial Sciences, Cyrptography, Financial Mathematics, Scientific Computing. It is one and first research center in Türkiye which abridges many research and education areas in national and international platforms.

Local Info

Food on campus: There are various options at campus:

- Çatı cafe (Ac31 at the map) has wide range of options and it is a 2 min walk from the venue.
- The Social Building (Sosyal Bina, Hc1 at the map) also has somewhat wide range of options, again 2 min walk from the venue.
- There is a small shopping mall on campus across the tennis courts (Çarşı, M1 at the map) where you can find various restaurants and fast food places.

Accommodation at METU

The Organizing Committee has not booked any guest house located inside the campus of Middle East Technical University for accommodation of delegates. However, delegates can make booking at

- METU Guest House
- Aysel Sabuncu Guest House

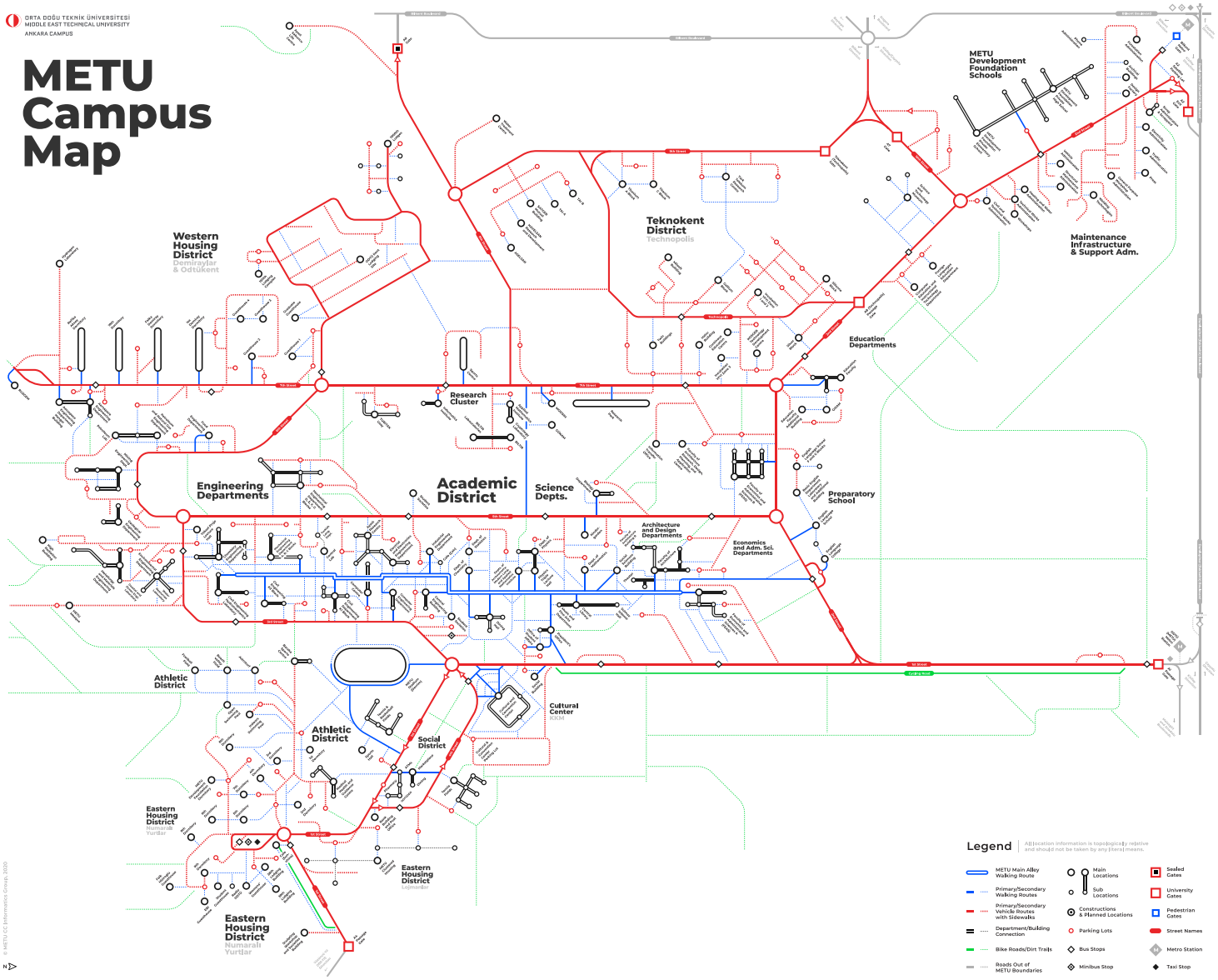
Please, check METU Accommodation (http://stm.metu.edu.tr/) for more information.

Accommodation at Hotels

Hotels close to METU include: Movenpick, JW Marriot Hotel Ankara, Dafne, Holiday Inn, The Green Park Hotel Ankara, Merya Palace, Bilkent hotel and Conference Center Ankara. These are in a distance between 3 and 4 km from the Metu campus entrance.

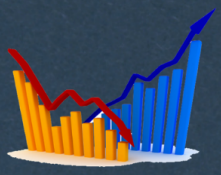
ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY
ANKARA CAMPUS

METU Campus Map



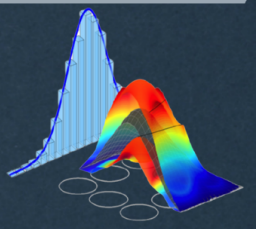
ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

Workshop on 20th Anniversary of Institute of Applied Mathematics



FINANCIAL MATHEMATICS

SCIENTIFIC COMPUTING



ACTUARIAL SCIENCES

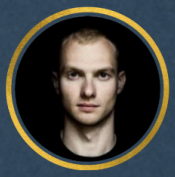
CRYPTOGRAPHY

Invited Speakers

Ramon Codina
Polytechnic University of Catalonia, Spain

Corina Constantinescu
University of Liverpool, UK

Zehra Ekşi-Altay,
WU Vienna, Austria



Michal Zajac
Nethermind

November 4, 2022
09:00 - 17:30

Culture and Convention Center, Halls A & D, METU

www.iam.metu.edu.tr

Sponsors

HALKBANK Adendum FAMECRYPT INTER PROBE INTELLIGENCE & ANALYTICS TARSİM tarımın sigortasıyız aselsan METU siam STUDENT CHAPTER