



ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

Uygulamalı Matematik Enstitüsü (UME)

Faaliyet Raporu 2023

Orta Doğu Teknik Üniversitesi
Uygulamalı Matematik Enstitüsü
Mart 2024

Önsöz	2
İnsan Kaynakları	4
Bağlantılı Öğretim Üyeleri - ODTÜ	7
Bağlantılı Öğretim Üyeleri - Diğer Üniversite ve Kurumlar	8
Araştırma	11
Yayınlar	11
SCIE - SSCI Dergilerde Makaleler	12
Diğer Uluslararası Hakemli Dergilerde Makaleler	16
Konferans Makaleleri (Proceedings)	16
Kitap ve Kitap Bölümleri	16
Konferans ve Çalıştay Katılımları	17
Bilimsel Etkinlikler	19
Genel Seminer ve Kolokyum	19
Özel Seminer	20
SIAM Student Chapter Seminerleri	21
Kısa Süreli Ziyaretler Gelen Ziyaretçiler	21
Giden Mensuplarımız	22
Projeler	23
TÜBİTAK, Döner Sermaye ve Diğer Projeler	24
ODTÜ Bilimsel Araştırma Projeleri (DOSAP)	26
Eğitim	27
Başvurular, Kabul ve Kayıtlar	27
Enstitü Öğrencilerinin Programlara Göre Dağılımı ve İstatistikler	29
Enstitüdeki Dersler, Öğrenci Sayıları ve İstatistikler	32
Doktora Programları	38
Doktora Mezunları	39
Yüksek Lisans Programları	40
Tezli Yüksek Lisans Mezunları	40
Tezsiz Yüksek Lisans Mezunları	42
Ödüller	43
Ek Bilgiler	44
Yeni Açılan Dersler (2023 Yılı)	44
2023 - 2024 Güz Dönemi	44

Önsöz

Türkiye’deki Matematik alanında ilk disiplinler arası araştırma kurumu olan Uygulamalı Matematik Enstitüsü (UME) lisansüstü programları ve araştırmaları ile uluslararası düzeyde saygın ve öncü bir araştırma enstitüsü olmayı hedeflemektedir. 2022 yılında kuruluşunun 20. yılını tamamlayan Uygulamalı Matematik Enstitüsü’nde Aktüerya Bilimleri, Bilimsel Hesaplama, Finansal Matematik ve Kriptografi olmak üzere dört anabilim dalında yüksek eğitim olanağı sunulmaktadır. Kriptoloji Laboratuvarımız bilgi güvenliği alanında ihtiyaç duyulan araştırma faaliyetlerine ulusal ve uluslararası boyutta devam etmektedir. Enstitümüz, ayrıca Üniversitemizde 2022 yılında kurulan Data and Decision Science (Veri ve Karar Bilimleri) lisansüstü eğitim programını Bilgisayar Mühendisliği, Elektrik-Elektronik Mühendisliği, Endüstri Mühendisliği ve İstatistik Bölümleri ile ortak yönetmektedir.

Disiplinlerarası ve çoklu disiplinlerdeki alanlarda başarılı çalışmalar ve projeler gerçekleştiren UME, birçok araştırma grubuna ev sahipliği yapmaktadır. Applied Cryptography (Uygulamalı Kriptografi), Blockchain (Blokzincir), Post-quantum Cryptography (Post-kuantum Kriptografi), Algorithmic Trading (Algoritmik Ticaret), Dependent Risks (Bağımlı Riskler), Longevity & Pension (Uzun Yaşam ve Emeklilik), Uncertainty Quantification (Belirsizlik Ölçümü) başlıkları altında toplanan bu araştırma-çalışma gruplarına ait çalışma çıktıları Enstitü web sayfasında (www.iam.metu.edu.tr) Yayınlar ve Projeler bölümlerinde detaylı olarak yer almaktadır. Ayrıca devlet kurumları ve özel sektörle ortaklaşa çalışmalar/projeler sürdürülmekte ve bunların sayısının artırılması hedeflenmektedir.

Enstitümüz bünyesinde doktora programına kayıtlı 77 öğrencimizden yaklaşık (5 öğrenci) %4’üne Kriptoloji/Siber Güvenlik, Hesaplamalı Bilim ve Mühendislik ve Yapay Zeka ve Makine Öğrenmesi alanlarında olmak üzere Yüksek Öğretim Kurumu tarafından verilen YÖK 100/2000 bursları sağlanmaktadır. Bu burslar aracılığıyla öncelikli araştırma alanlarının Enstitümüzde görünürlüğünün artırılması hedeflenmektedir.

Covid-19 küresel salgınının birçok akademik etkinliği ve uluslararası ziyaretleri engellemesine rağmen Enstitümüz yayın ve proje sayılarında artış gözlenmiştir. Enstitümüz bünyesinde gerçekleştirilen çalışmaların %88,6’sı SCI-E, %6,9 kadarı diğer kategorisindeki dergilerde ve konferans tam bildirisi kategorisinde, %4,5 kadarı ise kitapta bölüm ve kitap olarak yayınlanmıştır. Uluslararası akademik veri tabanı platformlarından Enstitümüz öğretim ve bağlantılı öğretim üyeleri yayınlarına 2023 yılında yapılan toplam Web of Science (WoS) atıf sayısı 993 olarak gerçekleşmiştir.

Kuruluşundan bugüne 124 doktora, 295 tezli yüksek lisans, 155 tezsiz yüksek lisans olmak üzere toplam 574 mezunu olan Enstitümüz; 2023 yılında 15 doktora, 19 tezli ve 6 tezsiz yüksek lisans öğrencisine diploma vermiştir. Bunların yanı sıra, 2022-2023 akademik yılı ODTÜ Tez, Yayın ve Ders Performans Ödülleri kapsamında mezunlarımızdan 2 doktora, 1 yüksek lisans mezunumuz ODTÜ Tez ödülünü ve 1 doktora öğrencimiz Ders Performans Ödülünü almaya hak kazanmışlardır.

Uygulamalı Matematik Enstitüsü'nün bugüne kadar göstermiş olduğu başarısında emeği olan tüm öğretim üyeleri ve bağlantılı öğretim üyeleri, eski yöneticileri ve yardımcıları, araştırma görevlileri ve öğrenci asistanları, idari personel ve mezunlarımıza teşekkür ederim.

Saygılarımla,

Prof. Dr. A. Sevtap Kestel
Uygulamalı Matematik Enstitüsü Müdürü

İnsan Kaynakları

Enstitü Yönetimi
Müdür
Prof. Dr. A. Sevtap Kestel
Müdür Yardımcıları
Doç. Dr. Önder Türk
Doç. Dr. Oğuz Yayla

Enstitü Anabilim Dalı Başkanları

Dr. Öğr. Üyesi Büşra Z. Temoçin*
(Aktüerya Bilimleri)

Doç. Dr. Önder Türk
(Bilimsel Hesaplama)

Prof. Dr. A. Sevtap Kestel
(Finansal Matematik)

Doç. Dr. Oğuz Yayla
(Kriptografi)

Enstitü Yönetim Kurulu

Prof. Dr. A. Sevtap Kestel
(Uygulamalı Matematik Enstitüsü)

Doç. Dr. Önder Türk
(Uygulamalı Matematik Enstitüsü)

Doç. Dr. Serdar Göktepe
(İnşaat Mühendisliği)

Doç. Dr. Seza Danışoğlu
(İşletme)

Prof. Dr. Songül Kaya Merdan**
(Matematik)

Doç. Dr. Oğuz Yayla
(Uygulamalı Matematik Enstitüsü)

* Prof. Dr. A. Sevtap Kestel, 01.12.2023 tarihine kadar Aktüerya Bilimleri EABD Başkanlığı görevini yürütmüştür.

**Prof. Dr. Ferruh Özbudak, 15.03.2023 tarihine kadar Yönetim Kurulu üyeliği yapmıştır.

Enstitü Personeli

Öğretim Üyeleri	Araştırma Görevlileri
Murat Cenk, Prof. Dr. *	Gülçin Akarsu
A. Sevtap Kestel, Prof. Dr.	Pelin Çiloğlu, Dr.
Buket Özkaya, Dr. Öğr. Üyesi	Tugay Dağlı*
Ali Devin Sezer, Prof. Dr.	Esra Günsay*
Büşra Z. Temoçin, Dr. Öğr. Üyesi	Burcu Ecem Karakaş
Önder Türk, Doç. Dr.	Zeynelabidin Karakaş, Dr. (35. madde)
Ömür Uğur, Prof. Dr.	Kübra Kaytancı, Dr.
Oğuz Yayla, Doç. Dr.	
Hamdullah Yücel, Doç. Dr.	

Öğretim Görevlisi	DOSAP
İrem Kesinkurt Paksoy, Dr.*	Buket Özkaya, Dr.** Bükre Yıldırım Külekci, Dr.

İdari Personel
Saffet Aykın (İdari Amir)
Serkan Demiröz (Sekreter)
Nejla Erdoğan (Enstitü Sekreteri)
Ömer Ergüven (Bilgisayar İşletmeni)
Ebru Gündoğdu (Sekreter)
Muharrem Kayabel (Görevli)
Cafer Topal (Görevli)

*2023 yılı içinde Enstitüdeki görevinden ayrılmıştır.

** 2023 yılı içinde Doktor Öğretim Üyesi olarak atanmıştır.

Bağlantılı Öğretim Üyeleri - ODTÜ

Matematik	Songül Kaya Merdan, Prof. Dr. Yıldırım Ozan, Prof. Dr. Muhiddin Uğuz, Dr.
İstatistik	B. Burçak Başbuğ Erkan, Prof. Dr. Özlem İlk Dağ, Prof. Dr. Fulya Gökalp Yavuz, Doç. Dr. Vilda Purutçuoğlu Gazi, Prof. Dr. Ceren Vardar Acar, Doç. Dr. Ceylan Yozgatlıgil, Prof. Dr.
Bilgisayar Mühendisliği	Emre Akbaş, Doç. Dr. Pelin Angın, Doç. Dr. Şeyda Ertekin Bolelli, Doç. Dr. Murat Manguoğlu, Prof. Dr. M. Halit S. Oğuztüzün, Prof. Dr. Ertan Onur, Prof. Dr. Hakan Yıldız, Dr.
Elektrik Elektronik Mühendisliği	Özgür Ergül, Prof. Dr. Yeşim Serinağaoğlu Doğrusöz, Doç. Dr. Ahmed H. Hareedy, Dr.
Havacılık ve Uzay Mühendisliği	Sinan Eyi, Prof. Dr. Ercan Gürses, Doç. Dr.
İktisat	Atak Alev, Dr. Esma Gaygısız-Lajunen, Doç. Dr. Nil İpek Şirikçi, Dr.
İnşaat Mühendisliği	Serdar Göktepe, Doç. Dr.
İşletme	Hande Ayaydın Hacıömeroğlu, Dr. Seza Danişoğlu, Doç. Dr. Z. Nuray Güner, Prof. Dr. Adil Oran, Doç. Dr. İlkay Şendeniz Yüncü, Dr.

Bağlantılı Öğretim Üyeleri - Diğer Üniversite ve Kurumlar

Ankara Üniversitesi	Furkan Başer, Doç. Dr. Murat Osmanoğlu, Dr. Fatih Tank, Prof. Dr.
ARÇELİK A.Ş.	Songül Bayraktar, Dr.
Atılım Üniversitesi	Ümit Aksoy, Prof. Dr. Burcu Gülmez Temür, Prof. Dr. Fatih Sulak, Doç. Dr. Emrah Sercan Yılmaz, Dr.
Başkent Üniversitesi	Özge Sezgin-Alp, Prof. Dr.
Cumhurbaşkanlığı	Ceyda Mangır, Dr. Mehmet Uzunkaya, Dr.
Başkent Üniversitesi	Sinem Kozpınar, Dr. Özge Sezgin Alp, Prof. Dr.
Bilkent Üniversitesi	Çağın Ararat, Dr. Firdevs Ulus, Dr.
Boğaziçi Üniversitesi	Könül Bayramoğlu Kavlak, Doç. Dr.
Çankaya Üniversitesi	Özlem Defterli, Doç. Dr. Nurgül Gökgöz Küçüksakallı, Dr. A. Nurdan Saran Buz, Dr. Özlem Türker Bayrak, Doç. Dr.
Dokuz Eylül Üniversitesi	Erdem Alkım, Dr.
Gazi Üniversitesi	Aytekin Bayram Çıbık, Prof. Dr.
Hacettepe Üniversitesi	Talha Arıkan, Dr. Başak Bulut Karageyik, Dr. Uğur Karabey, Doç. Dr. Mehmet Baha Karan, Prof. Dr. Yasemin Saykan, Dr. Ş. Kasırga Yıldırak, Prof. Dr.
Hacı Bayram Veli Üniversitesi	Seher Nur Sülkü, Prof. Dr.

Interprobe	Pınar Gürkan Balıkçioğlu, Dr.
İzmir Yüksek Teknoloji Üniversitesi	Cüneyt Bazlamaçcı, Prof. Dr.
Karabük Üniversitesi	Oytun Haçarız, Dr. Eda Tekin, Dr.
Kahramanmaraş Sütçü İmam Üniversitesi	Bilgi Yılmaz, Doç. Dr.
Katholieke Universiteit Leuven	Vincent Rijmen, Prof. Dr.
King Fahd University of Petroleum and Minerals (KFUPM)	Günther Glatz, Dr. Umair bin Waheed, Dr.
Koç Üniversitesi	Mine Çağlar, Prof. Dr.
MICRA	Serdar Dalkır, Dr.
Namık Kemal Üniversitesi	Cansu Evcin, Dr.
Necmettin Erbakan Üniversitesi	Ahmet Sınak, Doç. Dr.
Ondokuz Mayıs Üniversitesi	Sedat Akleylek, Prof. Dr.
Poznan University of Technology	Gerhard-Wilhelm Weber, Prof. Dr.
Rice Üniversitesi (A.B.D.)	Tayfun E. Tezduyar, Prof. Dr.
ROKETSAN	Tayfun Çimen, Doç. Dr.
Sabancı Üniversitesi	Ferruh Özbudak, Prof. Dr.
Silent Protocol	İsa Sertkaya, Dr.
Sinop Üniversitesi	Murat Uzunca, Prof. Dr.
Süleyman Demirel Üniversitesi	Barış Bülent Kırklar, Prof. Dr.
Technical University of Kaiserslautern	Ralf Korn, Prof. Dr.
TOBB-ETÜ	Tahir Hanalioğlu, Prof. Dr. Zülfükar Saygı, Prof. Dr. Ali Aydın Selçuk, Prof. Dr.
TÜBİTAK	Onur Koçak, Dr.
Türk Hava Kurumu Üniversitesi	Tuğba Akman Yıldız, Doç. Dr.
Vienna Uni. of Economics and Business	Zehra Ekşi-Altay, Doç. Dr.

Western University	Rogemar S. Mamon, Prof. Dr.
Diğer	Murat Cenk, Prof. Dr. Ali Alper Hekimoğlu, Dr. Öznur Mut Sağdıçoğlu, Dr.

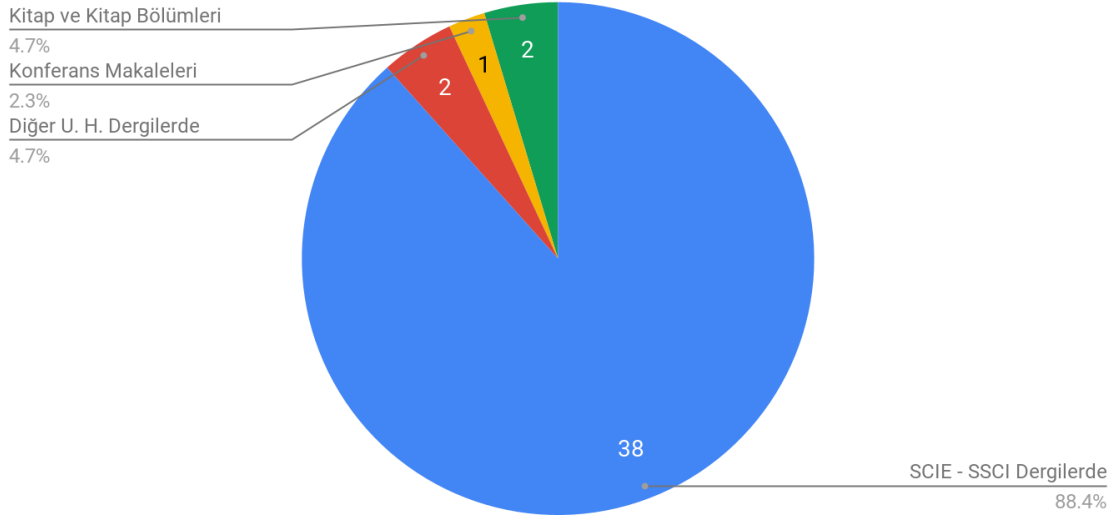
Araştırma

Yayınlar

Enstitümüz adresli yayınlarımızı genellikle SCI-E Tipi ve diğer Hakemli Dergilerdeki makaleler ve konferans bildirileri oluşturmaktadır. Bunun yanı sıra kitaplarda bölümler ve editoryal yayınlar da Enstitümüzün yayın portföyünde yer almaktadır. Raporun devamında bu yayınlara ait detaylı bilgiler ve istatistikler yer almaktadır.

SCIE Tipi yayınların 2022 yılına göre artış gösterdiği belirlenerek, bu yayınların çoğunluğunun WoS tanımlı Q1 ve Q2 kategorisinde yer aldığı gözlemlenmiştir. 2023 yılında Enstitümüz öğretim ve bağlantılı üyeleri tarafından yapılan yayınların çoğunluğunun tez öğrencileri ve mezunlarımızla ortak yapılan çalışmalardan oluşmaktadır.

Yayınlar (2023)



Bunun yanı sıra, 2023 yılı yayın sayılarına bakıldığında %88,6 SCIE tipi dergilerde yayınlanan çalışmaların ağırlıklı olarak tez öğrencileri ile yapılan araştırmalara ait olduğu belirlenmiştir.

SCIE - SSCI Dergilerde Makaleler

Aşağıda SCIE - SSCI Dergilerdeki Uygulamalı Matematik Enstitüsü adresli yayınların listesine yer verilmiştir.

[1]	A novel model for sustainable waste collection arc routing problem: Pareto-based algorithms. Tirkolaei E.B., Goli A., Gütmen S., Weber G.-W., Szwedzka K., Annals of Operations Research, 324(1-2), 189-214, 2023. https://doi.org/10.1007/s10479-022-04557-y
[2]	A robust optimization model to design an IoT-based sustainable supply chain network with flexibility. Goli A., Babaei Tirkolaei E., Golmohammadi A.-M., Atan Z., Weber G.-W., Ali S.S., Central European Journal of Operations Research, 2023. https://doi.org/10.1007/s10100-023-00870-4
[3]	A stabilized FEM formulation with discontinuity-capturing for solving Burgers'-type equations at high Reynolds numbers. Cengizci S., Uğur Ö., Applied Mathematics and Computation, 442, 2023. https://doi.org/10.1016/j.amc.2022.127705
[4]	A stochastic gradient algorithm with momentum terms for optimal control problems governed by a convection-diffusion equation with random diffusivity. Toraman, S. C., Yücel, H., Journal of Computational and Applied Mathematics, 422, 2023. https://doi.org/10.1016/j.cam.2022.114919
[5]	A SUPG formulation augmented with shock-capturing for solving convection-dominated reaction-convection-diffusion equations. Cengizci S., Uğur Ö., Natesan S., Computational and Applied Mathematics, 42(5), 2023. https://doi.org/10.1007/s40314-023-02370-2
[6]	Analytical and numerical assessments of boundary variations in Steklov eigenvalue problems. Bahadır E., Türk Ö., Journal of Computational and Applied Mathematics, 422, 2023. https://doi.org/10.1016/j.cam.2022.114900
[7]	Assessment of dependent risk using extreme value theory in a time-varying framework. Yıldırım Külekci, B., Karabey, U., Selçuk-Kestel, A.S., Hacettepe Journal of Mathematics and Statistics, 52(1), 248-267, 2023. https://doi.org/10.15672/hujms.992699

[8]	Butson-Hadamard matrices and Plotkin-optimal codes over $\mathbb{Z}_p$. Acar D., Saraç B., Yayla O., Journal of Algebra and its Applications, 2023. https://doi.org/10.1142/s0219498824501962
[9]	Comparison of dipole-based and potential-based ECGI methods for premature ventricular contraction beat localization with clinical data. Dogrusoz Y.S., Rasoolzadeh N., Ondrusova B., Hlivak P., Zelinka J., Tysler M., Svehlikova J., Frontiers in Physiology, 14, 2023. https://doi.org/10.3389/fphys.2023.1197778
[10]	Complete characterization of some permutation polynomials of the form $xr(1+axs1(q-1)+bxs2(q-1))$ over F_{q^2} . Özbudak F., Temür B.G., Cryptography and Communications, 15(4), 775-793, 2023. https://doi.org/10.1007/s12095-023-00641-7
[11]	Credit Risk Evaluation Using Clustering Based Fuzzy Classification Method. Baser, F., Koc, O., Selcuk-Kestel, A.S, Expert System with Applications, 119882, 2023. https://doi.org/10.1016/j.eswa.2023.119882
[12]	Direct and inverse problems for a 2D heat equation with a Dirichlet–Neumann–Wentzell boundary condition. I. Ismailov, M. , Türk Ö., Communications in Nonlinear Science and Numerical Simulation, 127, 107519, 2023. https://doi.org/10.1016/j.cnsns.2023.107519
[13]	Estimation of disease progression for ischemic heart disease using latent Markov with covariates. Oflaz, Z., Selcuk-Kestel A.S., Yozgatlıgil, C., Statistical Analysis and Data Mining, 2023. https://doi.org/10.1002/sam.11589
[14]	Further constructions and characterizations of generalized almost perfect nonlinear functions. Sălăgean A., Özbudak F., Cryptography and Communications, 2023. https://doi.org/10.1007/s12095-023-00647-1
[15]	Global energy preserving model reduction for multi-symplectic PDEs. Uzunca, M., Karasözen, B., Aydın, A., Applied Mathematics and Computation, 436 127483, 2023. https://doi.org/10.1016/j.amc.2022.127483
[16]	Improving Performance in Space-Hard Algorithms. Güner H.K., Mangır C., Yayla O., Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13914 LNCS, 398-410, 2023. https://doi.org/10.1007/978-3-031-34671-2_28
[17]	MILP-Aided Cryptanalysis of the FUTURE Block Cipher. İlter M.B., Selçuk A.A., Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13809 LNCS, 153-167, 2023. https://doi.org/10.1007/978-3-031-32636-3_9

[18]	Modeling comorbidity of chronic diseases using coupled hidden Markov model with bivariate discrete copula. Oflaz Z., Yozgatligil C., Selcuk-Kestel A.S., Statistical Methods in Medical Research, 32(4), 829-849, 2023. https://doi.org/10.1177/09622802231155100
[19]	Modification of hybrid RNN-HMM model in asset pricing: univariate and multivariate cases. Aydoğan-Kilic, D., Selcuk-Kestel, A.S., Applied Intelligence, 2023. https://doi.org/10.1007/s10489-023-04762-7
[20]	Multi-objective solid transportation-location problem with variable carbon emission in inventory management: a hybrid approach. Das S.K., Pervin M., Roy S.K., Weber G.W., Annals of Operations Research, 324(1-2), 283-309, 2023. https://doi.org/10.1007/s10479-020-03809-z
[21]	On diamond products ensuring irreducibility of the associated composed product. İrimağzı C., Özbudak F., Communications in Algebra, 51(7), 3134-3142, 2023. http://doi.org/10.1080/00927872.2023.2178656
[22]	On subfield subcodes obtained from restricted evaluation codes. Güneri C., Özbudak F., Sayıcı S., Designs, Codes, and Cryptography, 2023. https://doi.org/10.1007/s10623-023-01261-1
[23]	On Two Applications of Polynomials $x^k - cx - d$ over Finite Fields and More. İrimağzı C., Özbudak F., Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13638 LNCS, 14-32, 2023. https://doi.org/10.1007/978-3-031-22944-2_2
[24]	Optimal placement of the multiple magnetic sources for the MHD flow in a rectangular duct. Evcin C., Uğur Ö., Tezer-Sezgin M., Optimization and Engineering, 2023. https://doi.org/10.1007/s11081-023-09796-x
[25]	Optimal premium allocation under stop-loss insurance using exposure curves. Mert, O.M., Selcuk Kestel, A.S., Hacettepe Journal of Mathematics and Statistics: 51(1) 288-307, 2023. https://doi.org/10.15672/hujms.889619
[26]	Partial Direct Product Difference Sets and Almost Quaternary Sequences. Özden B., Yayla O., Advances in Mathematics of Communications, 17(3), 572-588, 2023. https://doi.org/10.3934/amc.2021010
[27]	Pluricomplex Green functions on Stein manifolds and certain linear topological invariants. A., Aytuna, Bull. London Math. Soc., 2023. https://doi.org/10.1112/blms.12720
[28]	Pluricomplex Green functions on Stein manifolds and certain linear topological

	invariants. A., Aytuna, Bull. London Math. Soc., 2023. https://doi.org/10.1112/blms.12721
[29]	Preface: operations research in neuroscience III, Tikidji-Hamburyan, R.A., Kropat, E., Weber, G.W., Annals of Operations Research, 312(2) 1143-1145, 2022, https://doi.org/10.1007/s10479-022-04697-1
[30]	Random Sequences in Vehicle Routing Problem. Gülen M.E., Yayla O., Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13858 LNCS, 159-170, 2023. https://doi.org/10.1007/978-3-031-32412-3_14
[31]	Recent advances in viable and sustainable supply chain management. Lotfi R., Weber G.-W., Tirkolaee E.B., Environmental Science and Pollution Research, 2023. https://doi.org/10.1007/s11356-023-28810-4
[32]	Reduced-order modeling for Ablowitz–Ladik equation. Uzunca M., Karasözen B., Mathematics and Computers in Simulation, 213, 261-273, 2023. https://doi.org/10.1016/j.matcom.2023.06.013
[33]	Stochastic Discontinuous Galerkin Methods for Robust Deterministic Control of Convection Diffusion Equations with Uncertain Coefficients. Çiloğlu, P., Yücel, H., Advances in Computational Mathematics, 49, 16, 2023. https://doi.org/10.1007/s10444-023-10015-5
[34]	SUPG formulation augmented with YZ β shock-capturing for computing shallow-water equations. Cengizci S., Uğur Ö., ZAMM Zeitschrift für Angewandte Mathematik und Mechanik, 103(6), 2023. https://doi.org/10.1002/zamm.202200232
[35]	The Impact of Large Investors on the Portfolio Optimization of Single-Family Houses in Housing Markets. Yilmaz, B., Korn, R., Selcuk-Kestel, A.S., Computational Economics, 2023. https://doi.org/10.1007/s10614-022-10233-x
[36]	The Impact of simultaneous shocks to financial markets and mortality on pension buy-out prices. Arık A., Uğur Ö., Kleinow T., ASTIN Bulletin, 53(2), 392-417, 2023. https://doi.org/10.1017/asb.2023.11
[37]	Linearly implicit methods for Allen-Cahn equation, Uzunca, M., Karasözen, B., Applied Mathematics and Computation, 450, 127984, 2023. https://doi.org/10.1016/j.amc.2023.127984
[38]	The c-differential uniformity of the perturbed inverse function via a trace function $\text{Tr}(x^2/x+1)$. Kaytancı, K., Özbudak, F., Period Math Hung (2023). https://doi.org/10.1007/s10998-023-00561-2

Diğer Uluslararası Hakemli Dergilerde Makaleler

[1]	Dependence analysis of the ISE100 banking sector using vine copula. Yıldırım Külekci, B., Poyraz, G., Gür, İ., Evkaya, O., Istanbul Journal of Economics, 73(1), 55-82, 2023. http://dx.doi.org/10.26650/ISTJECON2022-1229039
[2]	Dynamics of a Newly Established Agricultural Commodities Market: Financialization, Hedging and Portfolio Diversification in Turkey. Acikgoz T., Alp O.S., Alkan N.B., Annals of Financial Economics, 2023. https://doi.org/10.1142/S2010495223500057
[3]	The prediction power of machine learning on estimating the sepsis mortality in the intensive care unit. Selcuk, M., Koc, O., Selcuk-Kestel, A.S., Informatics in Medicine Unlocked, Volume 28, 100861. ELseiver, 2023. https://doi.org/10.1016/j.imu.2022.100861

Konferans Makaleleri (Proceedings)

[1]	Effects of Torso Inhomogeneities on Spontaneous PVC Localization in Potential and Dipole-Based Methods. Rasoolzadeh N., Ondrusova B., Dogrusoz Y.S., Svehlikov J., Proceedings of the 14th International Conference on Measurement, MEASUREMENT 2023, 2-5, 2023. https://doi.org/10.23919/MEASUREMENT59122.2023.10164347
-----	--

Kitap ve Kitap Bölümleri

[1]	Impact of Outlier-Adjusted Lee–Carter Model on the Valuation of Life Annuities. Yavrum, C., Selcuk-Kestel, A.S., Advances in Econometrics, Operational Research, Data Science and Actuarial Studies. Springer, Cham, 495-513, 2023. https://doi.org/10.1007/978-3-030-85254-2_30
[2]	The Pursuit of Reality: Narrative History of the Quantum and the Great Minds That Made it. Bayın, S.Ş., Springer, 2023. https://doi.org/10.1007/978-981-99-1031-1

Konferans ve Çalıştay Katılımları

Aşağıda Uygulamalı Matematik Enstitüsü öğretim üyeleri, asistanları ve öğrencilerinin Konferans ve Çalıştay katılımları listelenmektedir.

[1]	Oğuz Yayla; 'ALCOCRYPT 2023: Algebraic and Combinatorial Methods for Coding and Cryptography' adlı konferansa bildirili katılmak üzere 19-24 Şubat 2023 tarihleri arasında Marsilya, Fransa' ziyaretinde bulunmuştur.
[2]	Burcu Ecem Karakaş; '3. Ulusal Kripto Günleri' adlı çalıştaya bildirili katılmak üzere 4-8 Mayıs 2023 tarihleri arasında Kocaeli' ziyaretinde bulunmuştur.
[3]	Zeynelabidin Karakaş; '3. Ulusal Kripto Günleri' adlı çalıştaya bildirili katılmak üzere 4-8 Mayıs 2023 tarihleri arasında Kocaeli' ziyaretinde bulunmuştur.
[4]	Pelin Çiloğlu; 'Numerical Analysis of Stochastic Partial Differential Equations' adlı çalıştaya bildirili katılmak üzere 14-18 Mayıs 2023 tarihleri arasında Eindhoven, Hollanda' ziyaretinde bulunmuştur.
[5]	Özenç Murat Mert; '26th International Congress on Insurance: Mathematics and Economics' adlı kongreye bildirili katılmak üzere 3-8 Temmuz 2023 tarihleri arasında Edinburg, İskoçya' ziyaretinde bulunmuştur.
[6]	Cem Yavrum; '26th International Congress on Insurance: Mathematics and Economics' adlı kongreye bildirili katılmak üzere 3-8 Temmuz 2023 tarihleri arasında Edinburg, İskoçya' ziyaretinde bulunmuştur.
[7]	Gülçin Akarsu Şengöz; '26th International Congress on Insurance: Mathematics and Economics' adlı kongreye bildirili katılmak üzere 3-8 Temmuz 2023 tarihleri arasında Edinburg, İskoçya' ziyaretinde bulunmuştur.
[8]	Önder Türk; 'The 10th International Congress on Industrial and Applied Mathematics (ICIAM 2023)' adlı kongreye bildirili katılmak üzere 18-27 Ağustos 2023 tarihleri arasında Tokyo/Japonya' ziyaretinde bulunmuştur.
[9]	Önder Türk; 'The European Conference on Numerical Mathematics and Advanced Applications (ENUMATH) 2023' adlı konferansa bildirili katılmak üzere 3-9 Eylül 2023 tarihleri arasında Lizbon, Portekiz' ziyaretinde bulunmuştur.
[10]	Buket Özkaya; '35. Ulusal Matematik Sempozyumunda sözlü sunum yapmak üzere 3-9 Eylül 2023 tarihleri arasında Trakya Üniversitesi, Edirne' ziyaretinde bulunmuştur.

[11]	Hamdullah Yücel; 'European Conference on Computational Optimization EUCCO 2023' adlı konferansa bildirili katılmak üzere 25-27 Eylül 2023 tarihleri arasında 'Heidelberg, Almanya,' ziyaretinde bulunmuştur.
[12]	A. Sevtap Kestel; 'Stop-Loss Reinsurance Pricing and Exposure Curves under Jump Influence, Financial and Actuarial Mathematics in Liverpool, Leeds and York (FAMILY) Workshop, adlı çalışmaya seminer vermek üzere 7-8 Aralık 2023 tarihleri arasında Liverpool, İngiltere/Birleşik Krallık' ziyaretinde bulunmuştur.

Bilimsel Etkinlikler

Enstitümüzün bilimsel etkinliklerini, dönem boyunca süren ve Salı günleri düzenlenen Genel Seminerler oluşturmaktadır. Ayrıca, farklı zamanlarda Özel Seminerler ve Dersler adıyla programlara özel, alana yönelik etkinlikler yapılmaktadır.

Türkiye’de ilk defa Enstitümüz çatısı altında yer alan Society of Industrial and Applied Mathematics (SIAM) Student Chapter tarafından organize edilen seminerler geniş yelpazedeki davetli konuşmacıları ve etkinlikleri ile Matematik ile Bilim ve Teknoloji alanlarında işbirliği sağlamaktadır. Konferans ve Çalıştaylar düzenlemek, organizasyonuna katkı sağlamak her akademik birim gibi Enstitümüzün de hedefleri arasındadır.

Alanında uzman araştırmacıların ve bilim insanlarının Enstitümüze yaptığı ziyaretler ile Enstitü üyelerimizin farklı kurum ve kuruluşlara yaptığı ziyaretler de akademik çalışmalarımızı olumlu yönde etkilemekte ve işbirlikleri için temel oluşturmaktadır.

Aşağıdaki tablolarda yukarıda belirtilen çerçevede tanımlanan ve 2023 yılında yapılan Bilimsel Etkinliklere yer verilmiştir.

Genel Seminer ve Kolokyum

[1]	Grassl, Markus (International Centre for Theory of Quantum Technologies (ICTQT) University of Gdansk, Poland); 02 Şubat 2023 tarihinde 'Fundamentals of Quantum Error Correction' başlıklı semineri vermiştir.
[2]	Konstantinides, Dimitrios (Department of Statistics and Actuarial - Financial Mathematics, University of the Aegean, Karlovassi, GR-83 200 Samos, Greece); 21 Şubat 2023 tarihinde 'A Note on Product-Convolution for Generalized Subexponential Distributions' başlıklı semineri vermiştir.
[3]	Savin, Sergei (Innopolis University, Center for Technologies in Robotics and Mechatronics Components); 28 Şubat 2023 tarihinde 'Orthogonal Decomposition in Optimal Control for Systems with Explicit Constraints' başlıklı semineri vermiştir.
[4]	Ertem, Mustafa Alp (Industrial Engineering - Çankaya University); 18 Nisan 2023 tarihinde 'A Network Flow Model for Intermodal Transportation in Humanitarian Logistics' başlıklı semineri vermiştir.

[5]	Sönmez Turan, Meltem (National Institute of Standards and Technology (NIST)); 02 Mayıs 2023 tarihinde 'Final Steps of the NIST Lightweight Cryptography Standardizations' başlıklı semineri vermiştir.
[6]	Gülmez Temür, Burcu (Atılım University-Department of Mathematics); 09 Mayıs 2023 tarihinde 'Some Permutation and Complete Permutation Polynomials Over Finite Fields' başlıklı semineri vermiştir.
[7]	Esgin, Muhammed F. (Department of Software Systems & Crbersecurity, Monash University); 30 Mayıs 2023 tarihinde 'A Tale of Practical Verifiable Random Functions based on Post-Quantum Assumptions' başlıklı semineri vermiştir.
[8]	Dalkır, Serdar (CRETC. Competition & Regulation Economics Testimony and Consulting LLC); 13 Haziran 2023 tarihinde 'Estimation of the Probability of a Merger or Acquisition between Two Companies through Analysis of Their Stock Prices' başlıklı semineri vermiştir.
[9]	Feo, Luca De (IBM Research Europe - Zurich, Switzerland); 20 Haziran 2023 tarihinde 'An Overview of SQIsign' başlıklı semineri vermiştir.
[10]	Yılmaz, Emrah Sercan (Department of Mathematics, Atılım University); 17 Ekim 2023 tarihinde 'Computing L-polynomial of a Supersingular Curve by Fewer Coefficients' başlıklı semineri vermiştir.
[11]	Güzel, İsmail (Senior Researcher, TÜBİTAK ULAKBİM); 21 Kasım 2023 tarihinde 'CROCKER Plots: A Visual Topological Exploration of Dynamical Systems' başlıklı semineri vermiştir.
[12]	Ghaffarinasab, Nader (Department of Industrial Engineering, Middle East Technical University); 12 Aralık 2023 tarihinde 'The Risk-Averse Single Allocation Hub Location Problem: a Mean CVaR Approach' başlıklı semineri vermiştir.
[13]	Türkiye Cumhuriyeti'nin kuruluşunun 100. yılına özel olarak; (İlk Dağ Özlem, R , 31.10.2023), (Yayla Oğuz , SageMath, 14.11.2023) ve (Uğur Ömür, Julia, 28.11.2023) tarihlerinde Uygulamalı Matematik Enstitüsü - Kriptografi Laboratuvarında ders serisi düzenlenmiştir.

Özel Seminer

[1]	Hasan Özgür Çıldıroğlu, An Overview of Digital Quantum Computing, 16 Mayıs 2023 (Ankara University, Turkey)
[2]	Orhun Kara, Impossible Differential (ID) Attacks on Substitution Permutation Networks (SPN), 20-21 Haziran 2023 (İzmir Institute of Technology (İYTE), Turkey)

SIAM Student Chapter Seminerleri

[1]	Hakan Eryılmaz, Capital MArkets in Turkey, 23 Mayıs 2023 (Managing Partner / Vice Chairman / CEO, Lydia Yatırım Holding, Türkiye)
-----	---

Kısa Süreli Ziyaretler Gelen Ziyaretçiler

[1]	Savin, Sergei (Innopolis University, Center for Technologies in Robotics and Mechatronics Components); 27 Şubat-3 Mart 2023 tarihleri arasında 'Convex optimization in Control part 1 (lecture)/part II (lecture) ve part III (lecture)' başlıklı semineri vermiştir. The framework of the program Erasmus+ International Credit Mobility (KA171 Partner Countries – non-Europe Exchange)
-----	--

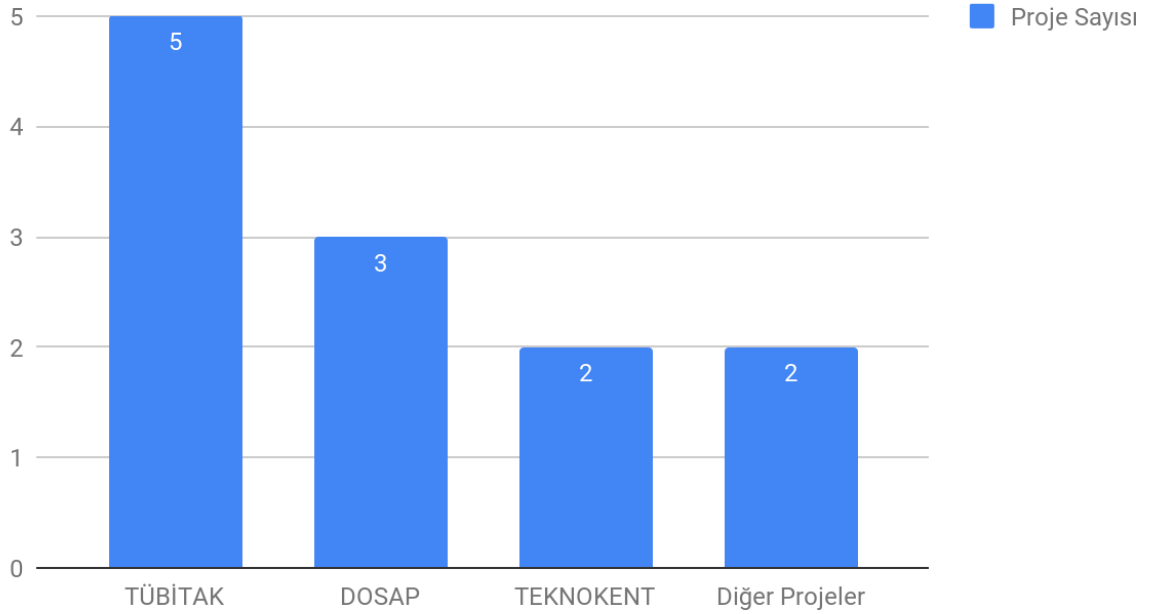
Giden Mensuplarımız

[1]	A. Sevtap Kestel; 'Colorado School of Mines ile ortak araştırma yapmak ve seminer vermek üzere 2-11 Şubat 2023 tarihleri arasında Boulder, Colorado, A.B.D.' ziyaretinde bulunmuştur.
[2]	A. Sevtap Kestel; 'RPTU Kaiserslautern-Landau (TU Kaiserslautern) Üniversitesi Matematik Bölümünde Erasmus Teaching Mobility kapsamında seminer ve ders vermek üzere 16-22 Nisan 2023 tarihleri arasında 'Kaiserslautern Technical University, Almanya' ziyaretinde bulunmuştur.
[3]	Meral Şimşek; 'TÜBİTAK 2214 Doktora Sırası Araştırma Bursu çerçevesinde tez çalışmaları yapmak üzere 9 Nisan 2022-1 Mart 2023 tarihleri arasında University of Liverpool, İngiltere' ziyaretinde bulunmuştur.
[4]	Esra Günsay; 'CISPA Helmholtz Center for Information Security'de seminer vermek üzere 1-22 Nisan 2023 tarihleri arasında Saarbrücken, Almanya' ziyaretinde bulunmuştur.
[5]	Hamdullah Yücel; 'Erasmus+ Mobility Agreement Staff Mobility for Teaching kapsamında ders vermek üzere 7-12 Mayıs 2023 tarihinde Chemnitz University of Technology, Almanya' ziyaretinde bulunmuştur.
[6]	A. Sevtap Kestel; 'Albert-Ludwigs Freiburg Üniversitesi, Ekonomi Fakültesinde yapılan IMP 20. Yıldönümüne katılmak, işbirliği oluşturmak ve seminer vermek üzere 25 Haziran-1 Temmuz 2023 tarihinde Freiburg, Almanya' ziyaretinde bulunmuştur.
[7]	Meral Şimşek; 'Tez çalışmaları kapsamında ortak danışmanı ile çalışmalar yapmak üzere 23 Temmuz-25 Ağustos 2023 tarihinde Liverpool, İngiltere/Birleşik Krallık' ziyaretinde bulunmuştur.
[8]	A. Sevtap Kestel; 'Albert-Ludwigs Freiburg Üniversitesi Ekonomi Fakültesinde seminer vermek ve işbirliği oluşturmak amacıyla 5-11 Kasım 2023 tarihleri arasında Freiburg, Almanya' ziyaretinde bulunmuştur.
[9]	A. Sevtap Kestel; 'Liverpool Üniversitesi, Finansal ve Aktüeryal Matematik Fakültesi tarafından akademik seminer vermek ve Enstitüler arasında işbirliği oluşturmak amacıyla 3-9 Aralık 2023 tarihleri arasında Liverpool, İngiltere/Birleşik Krallık' ziyaretinde bulunmuştur.

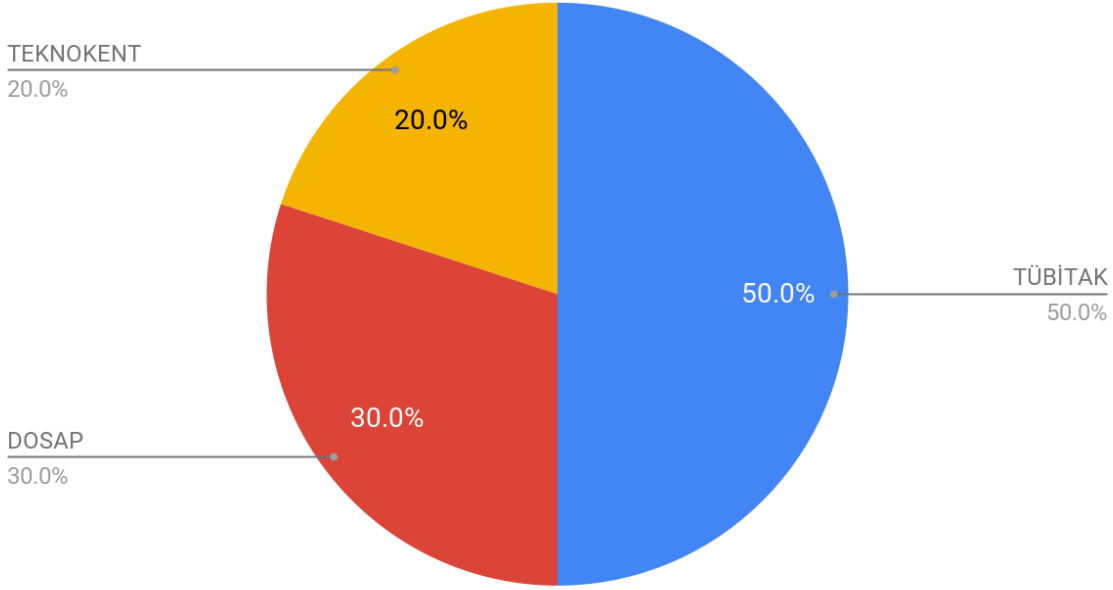
Projeler

Enstitümüzün çatısı altında yürütülen proje sayıları ve öğretim üyelerimizin araştırmacı olarak yer aldıkları proje bilgileri aşağıda verilmektedir. TÜBİTAK (%50) kaynaklı projeler ağırlıklı olmak üzere, Döner Sermaye, DOSAP, TEKNOKENT projeleri aracılığıyla hem Enstitümüz işbirliklerinin artırılması, hem de eğitim ve araştırmaya yönelik olanakların sağlanması sevindiricidir.

Proje Sayıları



Proje Dağılımı



TÜBİTAK, Döner Sermaye ve Diğer Projeler

[1]	Proje Adı: Kriptografik Algoritmaların Tasarımı, Gerçekleştirilmeleri ve Uygulamaları (TÜBİTAK) Yürütücüsü : Oğuz Yayla* Araştırmacılar: Nazlı Deniz Türe, Sermin Çakın, Yaman, N., Kırçalı, M. Başlangıç – Bitiş Tarihleri: 2019 – 2025 *22.09.2022 tarihine kadar Murat Cenk tarafından yürütülmüştür.
[2]	Proje Adı: Kodlama Teorisi ve Uygulamaları Üzerine Araştırma (TÜBİTAK-Güney Kore Ulusal Araştırma Vakfı (NRF)) Yürütücüsü: Ferruh Özbudak Başlangıç – Bitiş Tarihleri: 15 Nisan 2021 – 15 Nisan 2023
[3]	Proje Adı: Bükülmüş Fonksiyonların Genellemeleri ve Permütasyon Polinomları (TÜBİTAK 1001, 120F309) Yürütücüsü: Nurdagül Anbar Meidl UME Araştırmacısı: Oğuz Yayla Başlangıç – Bitiş Tarihleri: 15 Mart 2021 – 15 Mart 2023

[4]	Proje Adı: Siber Güvenlik Tasarım ve Test Çözümleri (TUBITAK 2244-Arçelik) Yürütücüsü: Pelin Angın Araştırmacısı: Yılmaz, B. E. Başlangıç – Bitiş Tarihleri: 2019 – 2023
[5]	Proje Adı: Covid19 Temel Çoğalma Sayısının Ülke Bazında Tahmini ve Pandeminin ABD Finans Piyasasına Etkisi Yürütücüsü: A. Sevtap Kestel Araştırmacılar: Yavrum C., Mert Ö. M., Mermer B. N. Başlangıç – Bitiş Tarihleri: Ocak 2022 - Temmuz 2023
[6]	Proje Adı: Adaptive Multilevel Monte Carlo Methods for Robust Optimal Control Methods Yürütücüsü: Hamdullah Yücel Başlangıç – Bitiş Tarihleri: Ocak 2022 - Mayıs 2023
[8]	Proje Adı: Post-Kuantum Kriptografi Tabanlı Anahtar Paylaşımı Yürütücüsü: Murat Cenk Araştırmacısı: Yıldız H. Başlangıç – Bitiş Tarihleri: Şubat 2021 - Temmuz 2023
[9]	Proje Adı: Mathematical Models for Interacting Dynamics on Networks Yürütücüsü: Hamdullah Yücel, Marjeta Kramar Fijavz Başlangıç – Bitiş Tarihleri: Ekim 2019 - Ekim 2023

ODTÜ Bilimsel Araştırma Projeleri

[1]	Proje Adı: Deprem Hasarlarının Finansal Risk Yönetiminde Katastrofik Bonoların CatBond Katkısının Enflasyon Etkisi Altında Değerlendirilmesi Yürütücü: Sevtap Kestel Başlangıç - Bitiş Tarihleri: 2023 - 2024
[2]	Proje Adı: Kafes-tabanlı Sıfır-Bilgi Aralık İspatı Yürütücü: Murat Cenk Araştırmacılar: Betin Onur, C. Başlangıç - Bitiş Tarihleri: 2021 - 2023
[3]	Proje Adı: Laplace-Steklov Özdeğer Problemlerinin Sınır-Sonlu Elemanları Yöntemleriyle Analizi Yürütücü: Önder Türk Araştırmacılar: Başlangıç - Bitiş Tarihleri: 2023 -

Eğitim

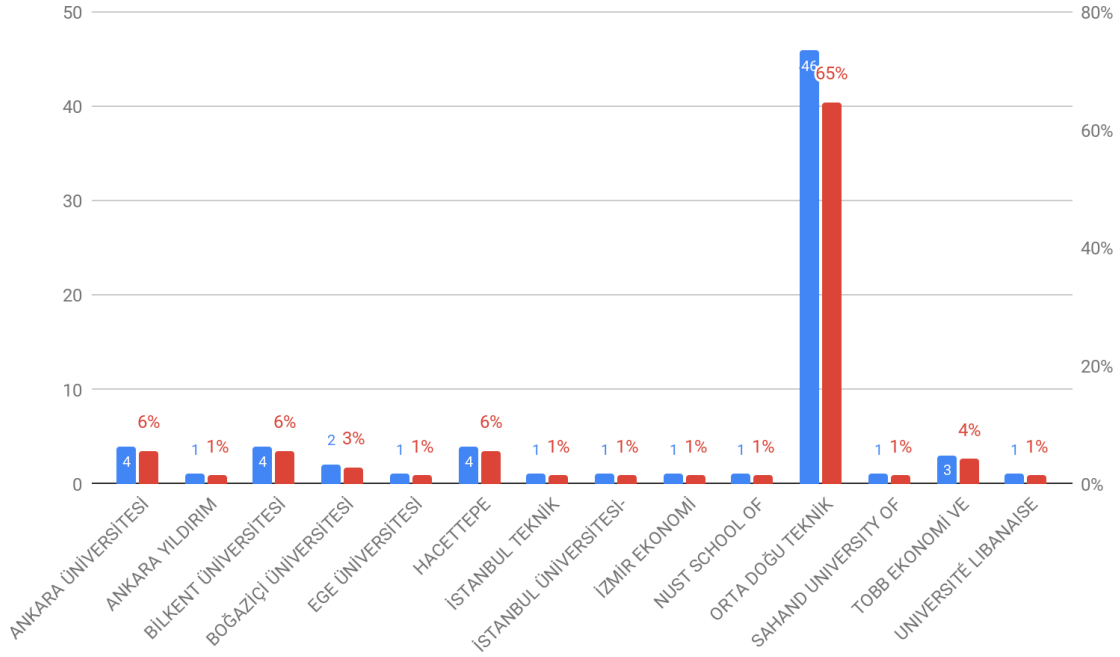
Başvurular, Kabul ve Kayıtlar

Enstitü Anabilim Dallarındaki programlara başvuru yapan ve kabul edilen öğrencilerin toplam başvuru sayılarına oranları aşağıdaki tabloda verilmiştir. Başvuru sayısının düşük olduğu programlar ile ilgili geniş çaplı tanıtım stratejilerinin belirlenmesi hedeflenmektedir.

Enstitü Anabilim Dalları	BAŞVURULAR - 2023		
	Başvuru (%)	Kabul (%)	Kayıt (%)
Aktüerya Bilimleri	7 (%8)	7 (%11)	7 (%13)
Bilimsel Hesaplama	35 (%40)	18 (%28)	16 (%30)
Finansal Matematik	19 (%22)	16 (%25)	13 (%24)
Kriptografi	26 (%30)	23 (%36)	18 (%33)
Toplam	87	64	54

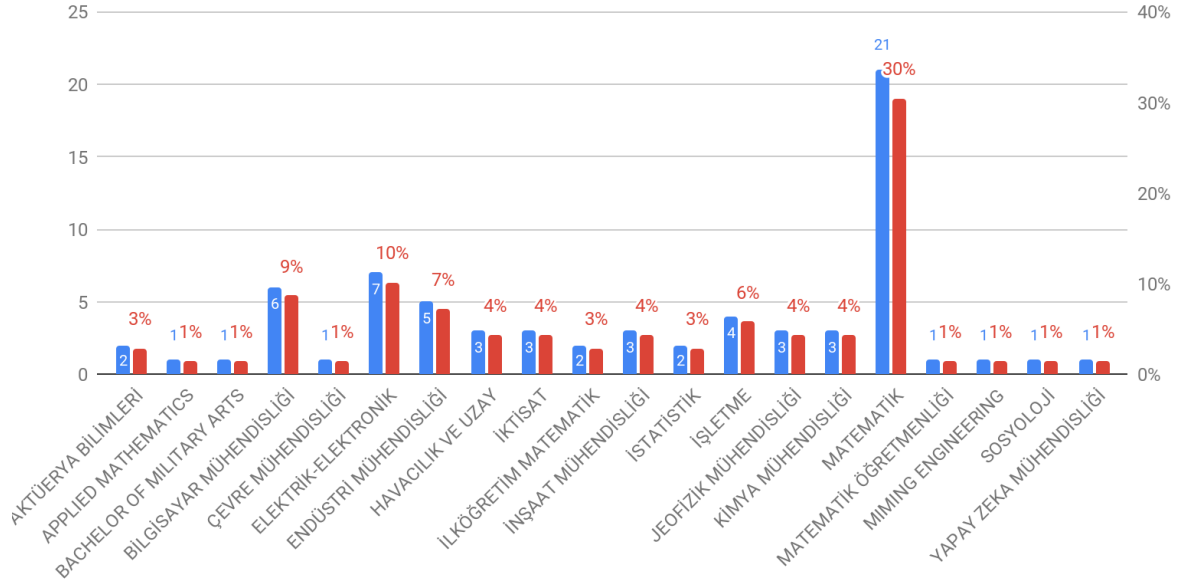
Enstitümüz programlarına kayıt yaptıran öğrencilerimiz hakkındaki diğer istatistiksel bilgiler (başarı ortalamaları, mezun oldukları üniversitelere ve bölümlerine göre dağılımları) aşağıda sunulmuştur. Ağırlıklı olarak ODTÜ mezunlarının başvuruda bulunduğu programlarımıza Hacettepe Üniversitesi ve Bilkent Üniversitesi'nden başvuruların da olduğu görülmektedir.

Kayıt Olan Öğrencilerin Mezun Oldukları Üniversitelere Göre Dağılımı



Programlara göre değişkenlik göstermesine rağmen, ağırlıklı olarak Matematik, Ekonomi, İşletme, Elektrik Elektronik Mühendisliği ve Makine Mühendisliği öğrencilerinin Enstitümüz programlarına kayıt yaptırdıkları gözlenmiştir. Enstitümüz farklı disiplinlerden adayların programlarımızda yer almalarını sağlamak amacıyla sosyal medya ve diğer tanıtım araçları ile geniş kitlelere ulaşmayı amaçlamaktadır.

Kayıt Olan Öğrencilerin Mezun Oldukları Bölümlere Göre Dağılımı



Enstitü Öğrencilerinin Programlara Göre Dağılımı ve İstatistikler

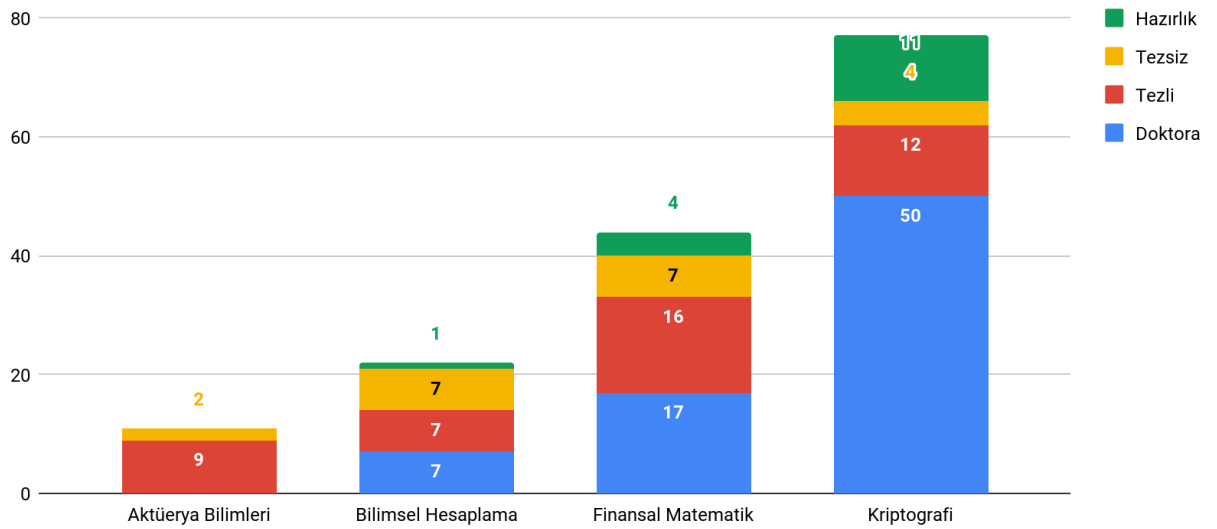
Enstitümüze yeni katılan öğrencilerimiz ile birlikte, mevcut öğrencilerimizin programlara göre dağılımı aşağıdaki “2023-2024 Güz” ve “2022-2023 Bahar” başlıklı tablolarda belirtilmiştir.

2022-2023 Bahar					
Anabilim Dalı	Doktora	Tezli	Tezsiz	Hazırlık	Toplam
Aktüerya Bilimleri		9	2		11
Bilimsel Hesaplama	7	7	7	1	22
Finansal Matematik	17	16	7	4	44
Kriptografi	50	12	4	11	77
Özel Öğrenci					0
	74	44	20	16	154

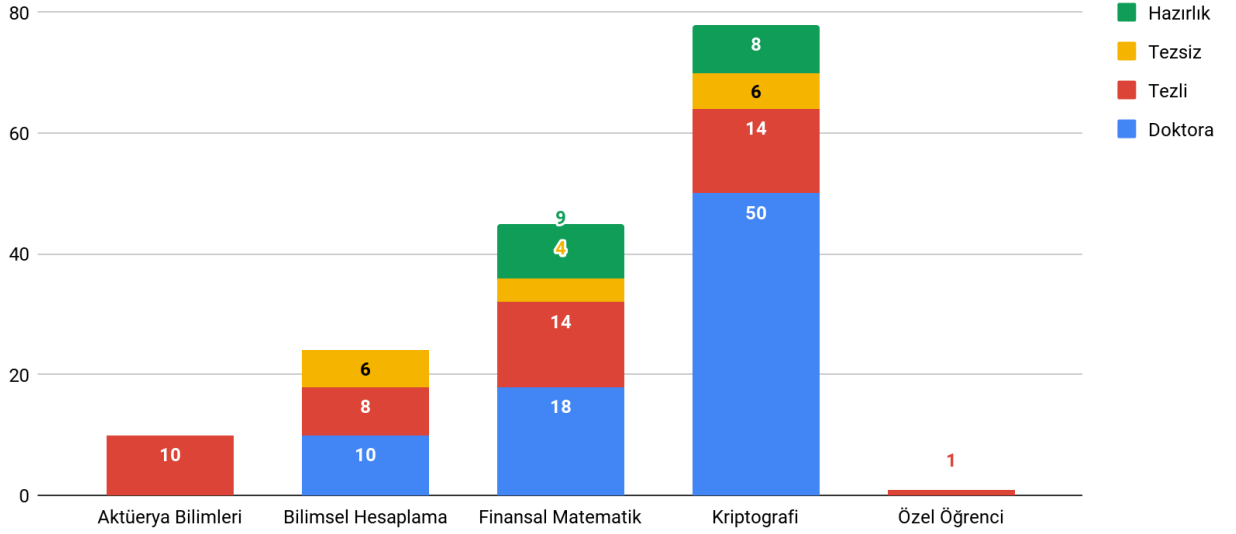
2023-2024 Güz					
Anabilim Dalı	Doktora	Tezli	Tezsiz	Hazırlık	Toplam
Aktüerya Bilimleri		10			10
Bilimsel Hesaplama	10	8	6		24
Finansal Matematik	18	14	4	9	45
Kriptografi	50	14	6	8	78
Özel Öğrenci		1			1
	78	47	16	17	158

Tablolardaki veriler ışığında, programlara göre öğrenci dağılımları aşağıdaki grafiklerde belirtilmiştir.

Doktora, Tezli, Tezsiz Yüksek Lisans ve Bilimsel Hazırlık Öğrencileri Dağılımı (2022-2023 Bahar)

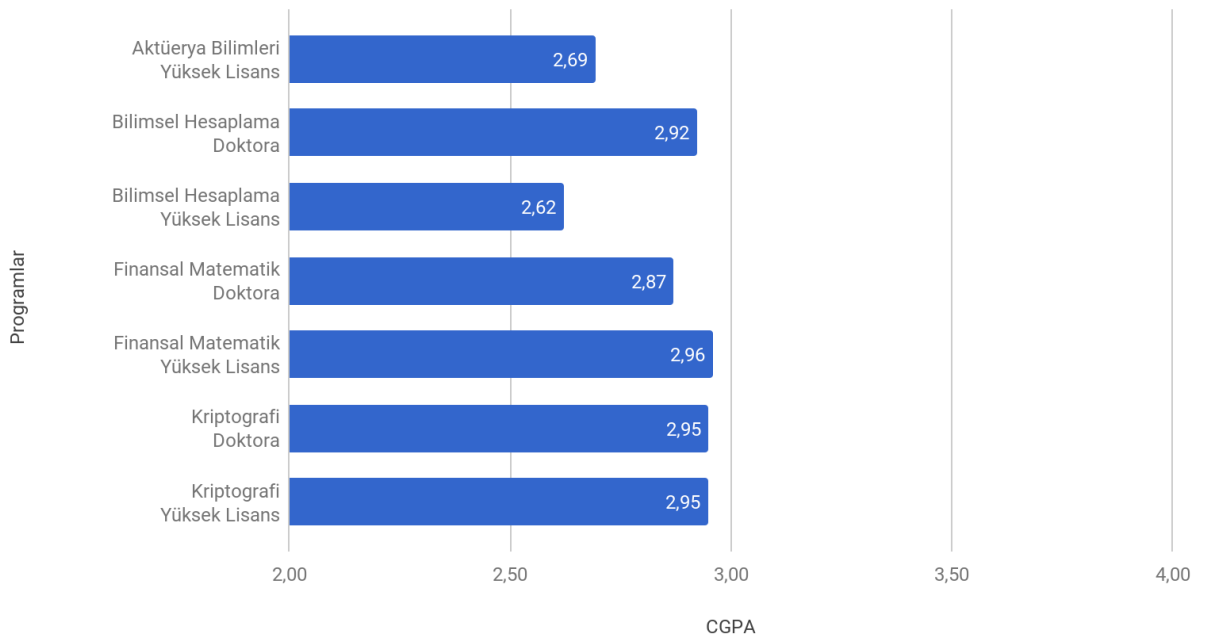


Doktora, Tezli, Tezsiz Yüksek Lisans ve Bilimsel Hazırlık Öğrencileri Dağılımı (2023-2024- Güz)



Enstitümüze kayıt yaptıran öğrencilerin Anabilim Dalı bazında lisans akademik başarı performansları (CGPA ortalamaları) aşağıdaki gibi gerçekleşmiştir.

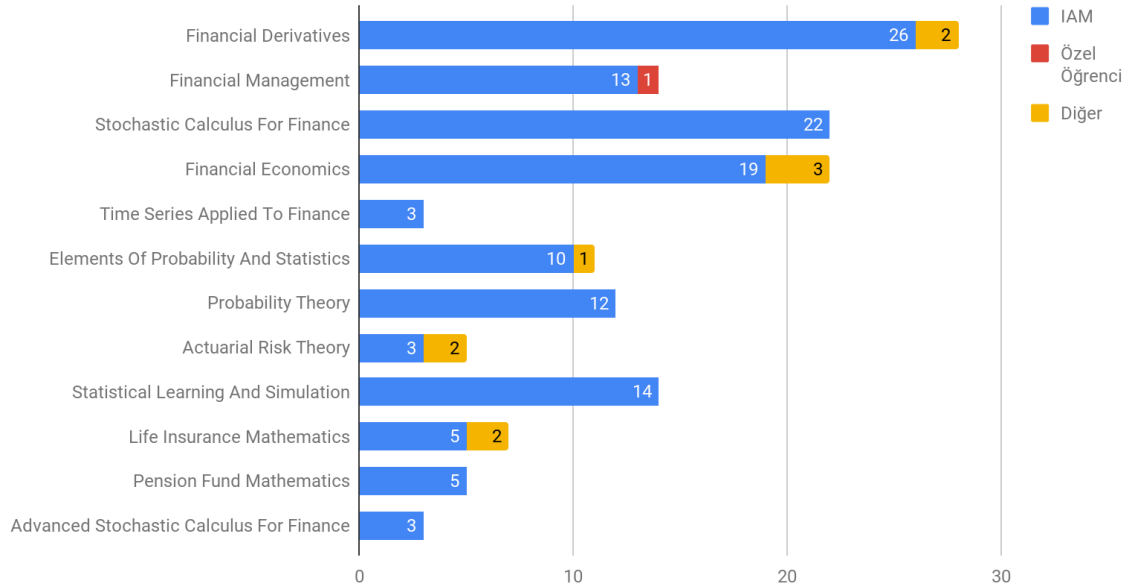
Kayıt Olan Öğrencilerin Lisans CGPA Ortalamaları



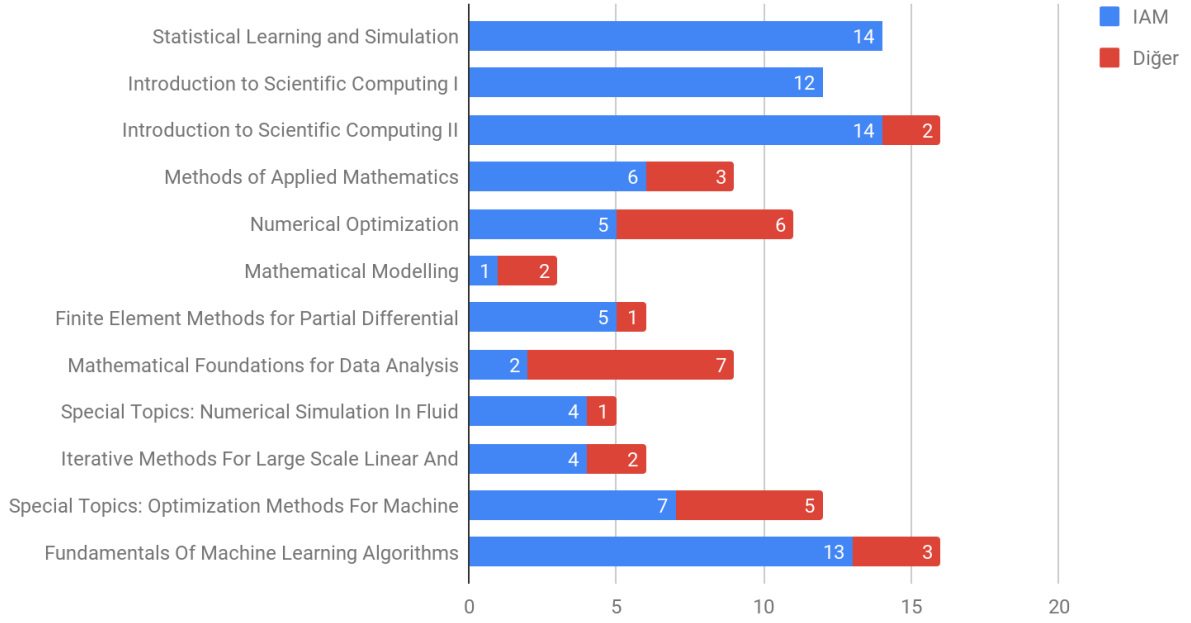
Enstitüdeki Dersler, Öğrenci Sayıları ve İstatistikler

Bu bölümde, Enstitümüzde 2023 yılı içerisinde açılan derslere ve bu derslere ilişkin istatistiklere yer verilmiştir. Aşağıdaki grafiklerde, her bir Anabilim Dalı için belirtilen derslerdeki enstitü ve enstitü-dışı öğrenci sayıları verilmektedir. Birçok dersimizin, birden fazla Anabilim Dalında listelenmiş olması programlar arası bilgi akışının sağlanması amacına yönelik olup, Enstitümüzün ve derslerimizin disiplinlerarası çalışmalara verdiği önemin bir göstergesidir.

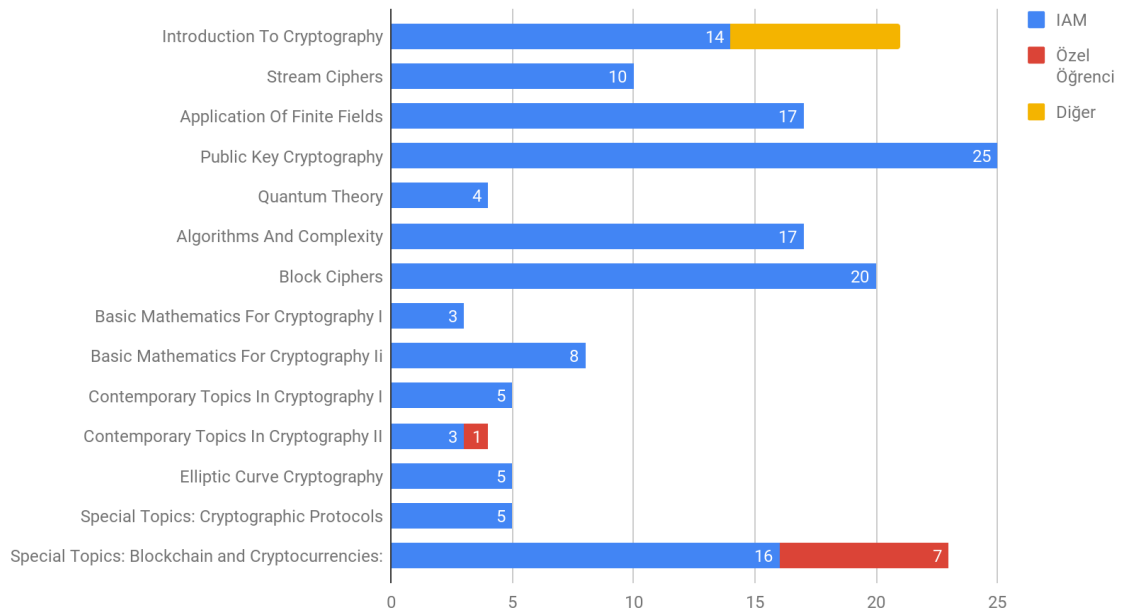
Aktüerya Bilimleri Dersleri Öğrenci Sayıları (2022-23 Bahar - 2023-24 Güz)



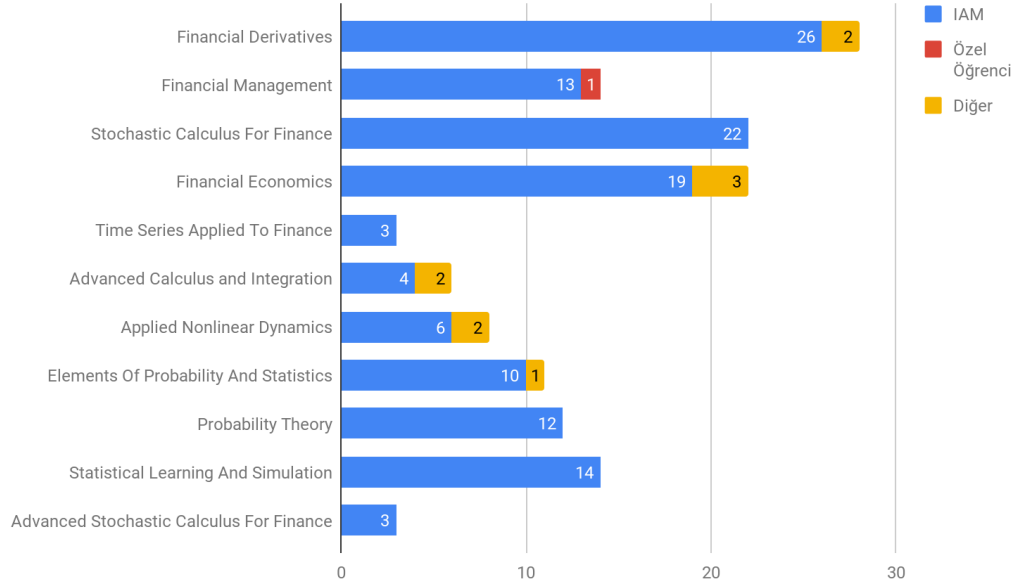
Bilimsel Hesaplama Dersleri Öğrenci Sayıları (2022-23 Bahar - 2023-24 Güz)



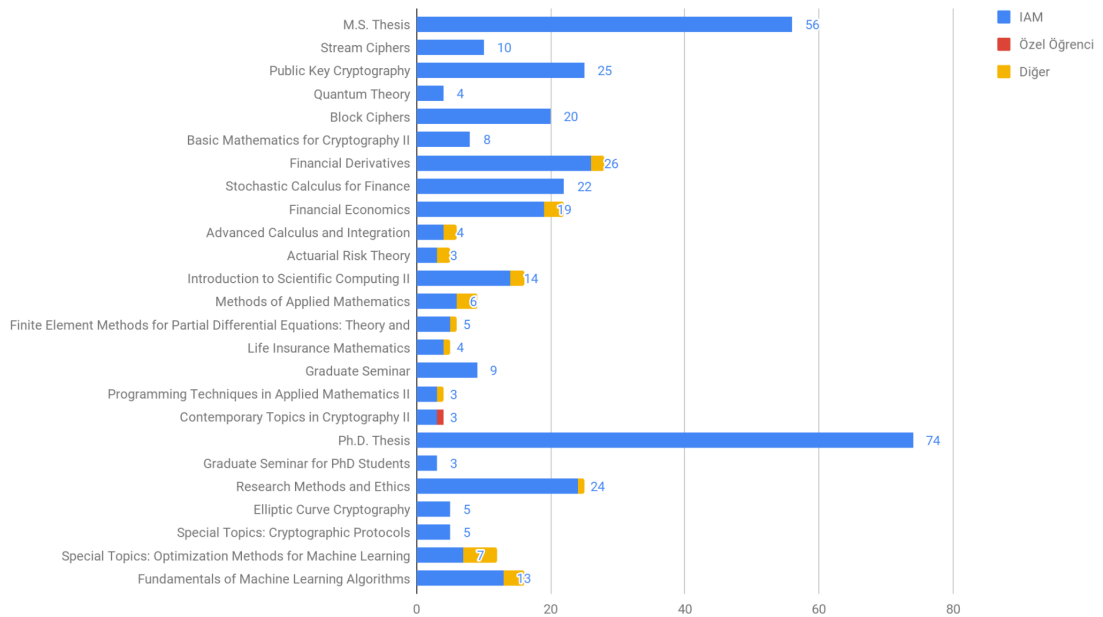
Kriptografi Dersleri Öğrenci Sayıları (2022-23 Bahar - 2023-24 Güz)



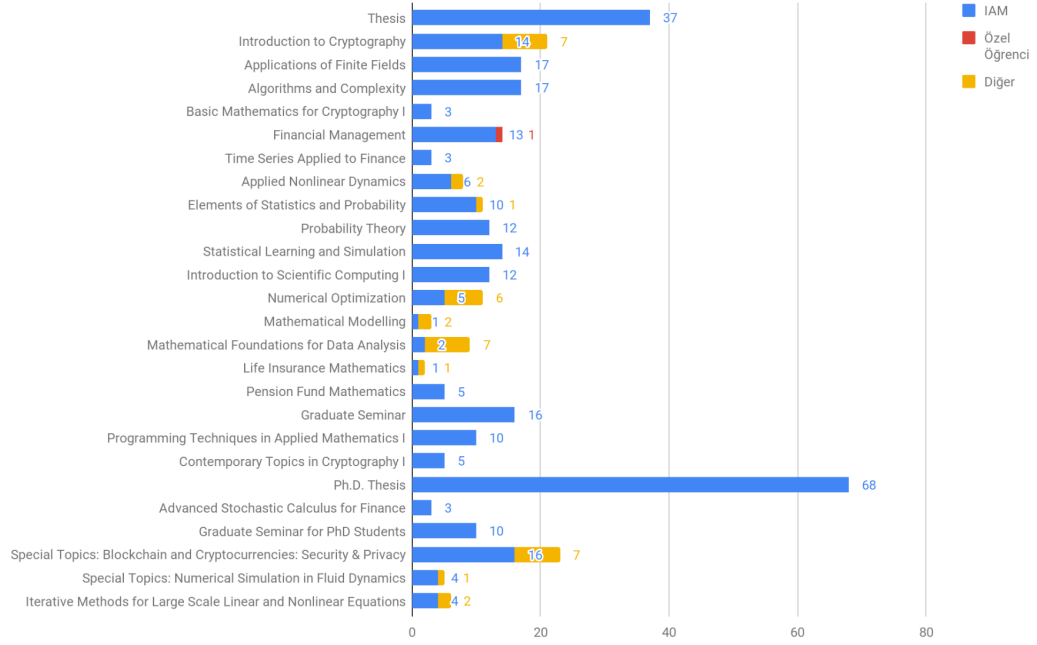
Finansal Matematik Dersleri Öğrenci Sayıları (2022-23 Bahar - 2023-24 Güz)



Derslerdeki Öğrenci Sayıları (2022-2023 Bahar)

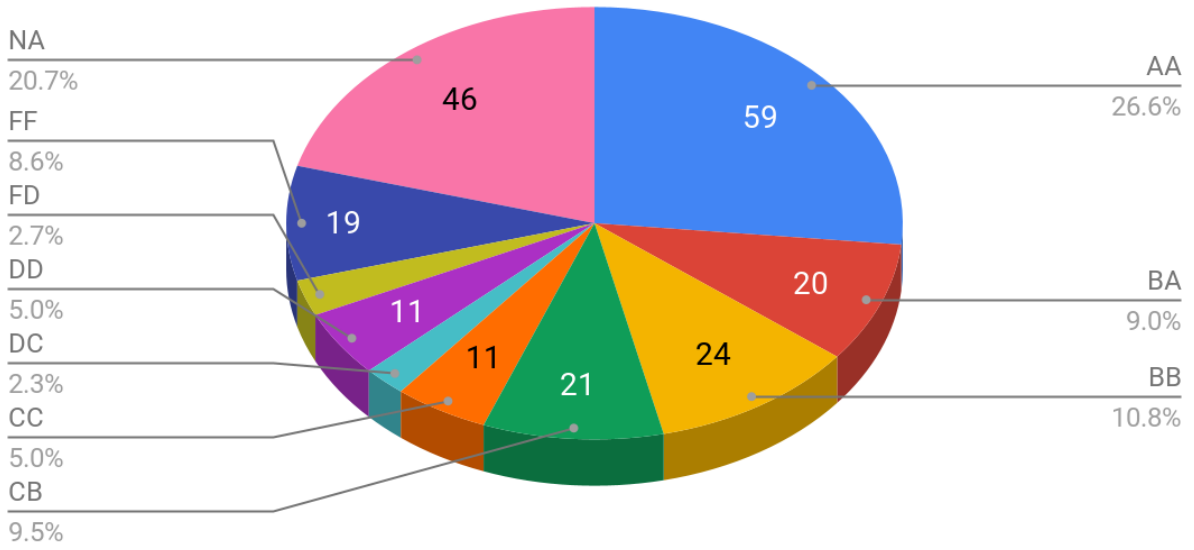


Derslerdeki Öğrenci Sayıları (2023-2024 Güz)

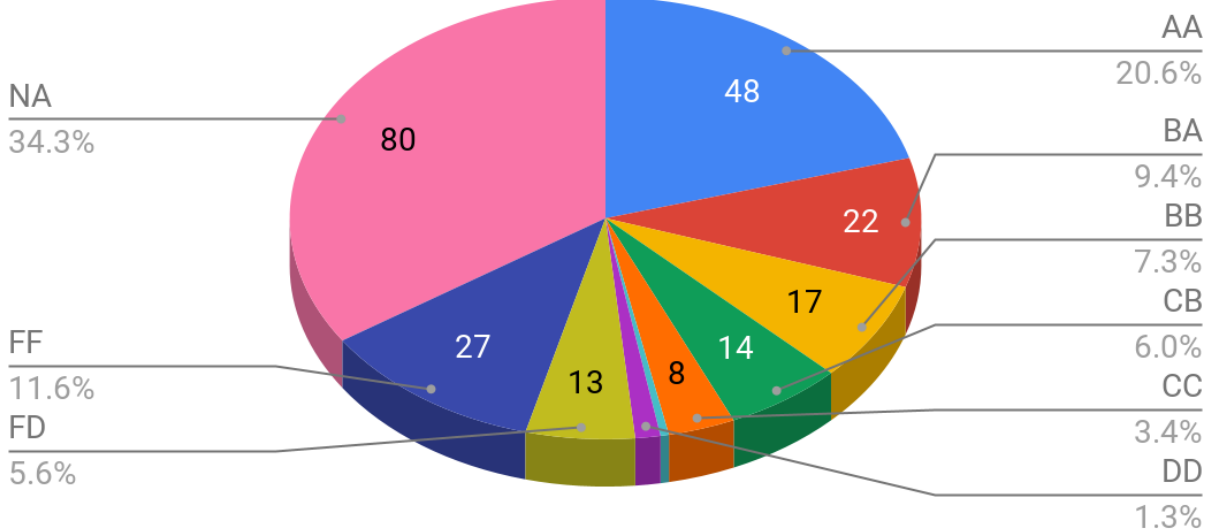


Aşağıdaki grafiklerde 2023 yılı içerisinde 2023-2024 Güz ve 2022-2023 Bahar dönemlerinde açılan tüm dersler, öğrenci sayıları ve not dağılımları verilmiştir. Özellikle not dağılımını gösteren grafiklerde %20-%30'lar seviyesinde olan “NA” notundaki artış sebeplerinden en önemlisi öğrencilerimizin eğitimlerinin yanı sıra çeşitli kurum ve kuruluşlarda çalışmaları olduğu düşünülmektedir.

2023-2024 Güz Dönemi Not Dağılımı

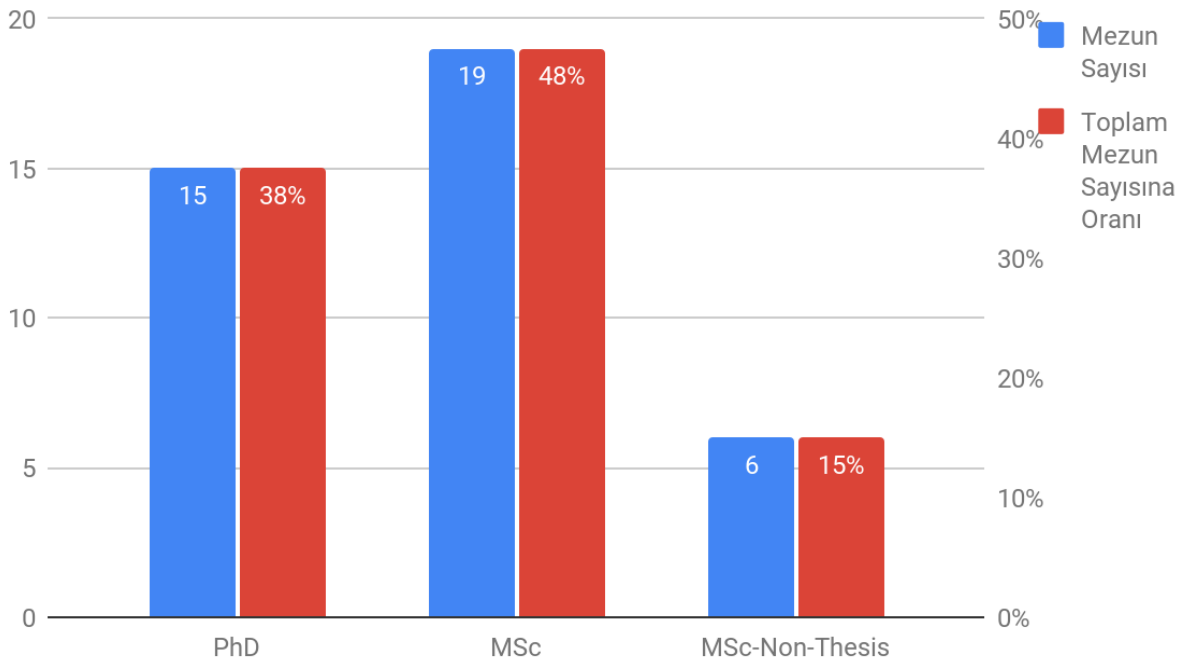


2022-2023 Bahar Dönemi Not Dağılımı



Enstitümüz Yüksek Lisans ve Doktora programlarından 2023 yılında mezun olan öğrencilerimizin sayıları ve oranları aşağıda yer almaktadır. 2023 yılındaki 15 doktora, 19 Tezli ve 6 Tezsiz Yüksek lisans mezunumuz akademik ve diğer kuruluşlarda çalışmaktadırlar.

Lisansüstü Programlara Göre Mezunlarımız



Doktora Programları

2023-2024 Güz ve 2022-2023 Bahar dönemlerinde Enstitümüz bünyesindeki Doktora programlarından aşağıda isimleri sıralanan öğrencilerimiz başarı ile mezun olmuştur. Doktora mezunlarına ve çalışmalarına ait detaylı bilgiler ise Faaliyet Raporu sonunda ayrıca sunulmaktadır. Mezunlarımızı tebrik eder, başarılarının devamını dileriz.

Doktora Mezunları

[1]	Özsoy, A. U., Option Pricing Via Reinforcement Learning: Extensions and Further Insights On the Qlbs Model PhD Thesis, Financial Mathematics, February 2023 (Danışman: Ömür Uğur)
[2]	Yerli, Ç., Markov-Chain Modulated Implied Liquidity: Modeling and Estimation, PhD Thesis, Financial Mathematics, June 2023 (Danışman: Sevtap Kestel; Ortak Danışman: Zehra Ekşi Altay)
[3]	Çiloğlu, P., Stochastic Discontinuous Galerkin Methods for PDE-Based Models with Random Coefficients, PhD Thesis, Scientific Computing, June 2023 (Danışmanı: Hamdullah Yücel)
[4]	Yaman, Y., Classification of Imbalanced Credit Data Sets with Borrower-Specific Cost-Sensitive Algorithms, PhD Thesis, Financial Mathematics, July 2023 (Danışman: Sevtap Kestel; Ortak Danışman: Ş. Kasırğa Yıldırak)
[5]	Kalaycı, B., Modelling Mutual Interaction of Finance and Human Factor Via Various Sorts of Indices, PhD Thesis, Financial Mathematics, July 2023 (Danışman: Vildapurutçuoğlu Gazi; Ortak Danışman: Gerhard Wilhelm Weber)
[6]	Güner, H. K., A Study on Space-Hard White-Box Cryptography, PhD Thesis, Cryptography, August 2023 (Danışmanı: Oğuz Yayla; Ortak Danışmanı: Ceyda Mangır)
[7]	Özden, D., Verifiable Timed Commitments Explored Timed Signature Schemes and an Application to Sealed-bid Auctions, PhD Thesis, Cryptography, September 2023; (Danışman: Oğuz Yayla)
[8]	Acunalp Erleblebici, İ., Some results on apn functions and weakly regular bent functions over finite fields, PhD Thesis, Cryptography, September 2023; (Danışman: Oğuz Yayla)
[9]	Öner Şimşek, D., Faster Secure Matrix Multiplication Using the Strassen Algorithm, PhD Thesis, Cryptography, September 2023; (Danışman: Ersan Akyıldız)
[10]	Solmaz, M. H., Flexible Hardware Design For Elliptic Curve Method of Integer Factorization, PhD Thesis, Cryptography, September 2023; (Danışman: Ersan Akyıldız)

[11]	Kaytancı, K., On Plateaued Functions, Linear Structures, Permutation Polynomials and c-Differential Uniformity, PhD Thesis, Cryptography, October 2023; (Danışman: Ferruh Özbudak)
[12]	Karakaş, Z., Classification of Distinct Maximal Flag Codes of a Prescribed Type and Related Results, PhD Thesis, Cryptography, October 2023; (Danışman: Ferruh Özbudak)
[13]	Hasgöl, E., A Hybrid Approach in Constructing an Internal Solvency Model, PhD Thesis, Financial Mathematics, October 2023 (Danışman: Sevtap Kestel)
[14]	İlter, M. B., Differential and Linear Cryptanalysis of Lightweight Block Ciphers With Milp Approach, PhD Thesis, Cryptography, October 2023; (Danışman: Ali Doğanaksoy; Ortak Danışman: Ali Aydın Selçuk)
[15]	Enginar, O., Deep Ensembles Approach For Energy Forecasting , PhD Thesis, Financial Mathematics, October 2023 (Danışman: Ömür Uğur)

Yüksek Lisans Programları

2023-2024 Güz ve 2022-2023 Bahar dönemlerinde Enstitümüz bünyesindeki Yüksek Lisans programlarından aşağıda isimleri listelenen öğrencilerimiz başarı ile mezun olmuştur. Mezunlarımızı tebrik eder, başarılarının devamını dileriz.

Tezli Yüksek Lisans Mezunları

[1]	Daş, İ., Bitcoin Price Forecasting Under the Influences of Network Metrics and Other Financial Assets, MSc Thesis, Financial Mathematics, January 2023 (Danışman: Sevtap Kestel)
[2]	Çelik, M., Loose Coupling of Su2 Multiphysics Code With Pato to Analyze the Surface Recession Effect On Surface Heat Flux, MSc Thesis, Scientific Computing, January 2023 (Danışman: Ömür Uğur; Ortak Danışman: Sinan Eyi)

[3]	Öztürk, Y., Trust in Banks: A Multi-Level Analysis, MSc Thesis, Financial Mathematics, February 2023 (Seza Danişoğlu)
[4]	Yıldırım, G., Routing Algorithms As An Application Of Graph Theory, MSc Thesis, Cryptography, February 2023 (Danışman: Ferruh Özbudak)
[5]	Kızıloğlu, İ. O., Clustering Influence On MTPL Premium Estimation Using Credibility Approach, MSc Thesis, Actuarial Science, February 2023 (Danışmanı: Sevtap Kestel; Ortak Danışman: Bukre Yıldırım Külekci)
[6]	Dağlı, T., Fem Approximation of Maxwell Equations: The Source Problem, Eigenproblem, and Electromagnetic Waves, MSc Thesis, Scientific Computing, February 2023 (Danışmanı: Önder Türk)
[7]	Rasoolzadeh, N., Solving The Inverse Problem of Electrocardiography for Spontaneous PVC Localization: Analysis of Clinical Electrocardiographic Data, MSc Thesis, Scientific Computing, March 2023 (Yeşim Serinağaoğlu Doğrusöz)
[8]	Yaşar, H. A., Comparison of Artificial Neural Network-Based and Adaptive Quadratic Neural Network-Based Multi-Fidelity Algorithms for Buckling Load Prediction of Stiffened Panels, MSc Thesis, Scientific Computing, May 2023 (Danışmanı: Ercan Gürses; Ortak Danışmanı: Hamdullah Yücel)
[9]	Malkoç, M., Balance Sheet Changes in The Turkish Banking Sector in The Face of FX Rate Volatility, MSc Thesis, Financial Mathematics, May 2023 (Danışmanı: İlkay Şendeniz Yüncü)
[10]	Çaylak, C., Investor Overconfidence: An Emerging Market Analysis, MSc Thesis, Financial Mathematics, May 2023 (Danışmanı: Seza Danişoğlu)
[11]	Tosun, İ., Seasonal Adjustment of High-Frequency Time Series, MSc Thesis, Financial Mathematics, May 2023 (Danışmanı: Ceylan Yozgatlıgil)
[12]	Doğan, C., A Comprehensive Study of Time Lock Puzzles and Timed Signatures in Cryptography, MSc Thesis, Cryptography, July 2023 (Danışmanı: Oğuz Yayla)
[13]	Seriner Gerenli, D. O., Secure Model Verification and Privacy Preservation with ZK-SNARKs and Neural Networks, MSc Thesis, Cryptography, September 2023 (Danışmanı: Ferruh Özbudak)
[14]	Gökçe., A. B., A New Efficient TMVP Algorithm and an Application for Post-Quantum Cryptography, MSc Thesis, Cryptography, September 2023 (Danışmanı: Oğuz Yayla)

[15]	Özeren, S., A Study on CRYSTALS-Kyber and its Masked Implementations, MSc Thesis, Cryptography, October 2023 (Danışmanı: Oğuz Yayla)
[16]	Girgin, Y., Modeling Exchange Rate Volatility Using ARMA-GARCH Approach with Non-Gaussian Distributions, MSc Thesis, Financial Mathematics, October 2023 (Danışmanı: Sevtap Kestel; Ortak Danışmanı: Özlem Türker Bayrak)
[17]	Tekin, E. N., Homomorphic Encryption: A Comprehensive Study of Types, Techniques, and Real-world Applications, MSc Thesis, Cryptography, October 2023 (Danışmanı: Ferruh Özbudak)
[18]	Özbek, İ., Extracting market expectations for monetary policy stance using overnight index swap: evidence from Türkiye, MSc Thesis, Financial Mathematics, October 2023 (Danışmanı: Esma Gaygısız)
[19]	Anapa, K., A Strategy Based on Statistical Modelling and Multi-Objective Optimization to Design a Dishwasher Cleaning Cycle, MSc Thesis, Scientific Computing December 2023 (Danışmanı: Hamdullah Yücel; Ortak Danışmanı: Songül Bayraktar)

Tezsiz Yüksek Lisans Mezunları

2023-2024 Güz ve 2022-2023 Bahar dönemlerinde Enstitümüz bünyesindeki Tezsiz Yüksek Lisans programlarından aşağıda isimleri listelenen öğrencilerimiz başarı ile mezun olmuştur. Mezunlarımızı tebrik eder, başarılarının devamını dileriz.

[1]	G, Derya., In The Context of COSO, Approach to the Risks Posed by Covid-19 in the Field of Banking within the COSO Internal Control-Integrated Framework, Financial Mathematics, February 2023 (Danışmanı: Ömür Uğur)
[2]	Kaya, A. E., Radix-2 and Radix-3 NTT Polynomial Multiplication, Cryptography, February 2023 (Danışmanı: Oğuz Yayla)
[3]	Küçükdemir, S., The Review of Design of Symmetric Primitives for Advanced Cryptographic Protocols, Cryptography, February 2023 (Danışmanı: Oğuz Yayla)
[4]	Aktaş, D., Liquidity Performance Measures on Bond Markets, Financial Mathematics, February 2023 (Danışmanı: Seza Danişoğlu)
[5]	Menekay, F. S., Single Server Private Information Retrieval and Simple PIR Protocol,

	Cryptography, July 2023 (Danışmanı: Oğuz Yayla)
[6]	Ceylan. C., Forecasting Gold Price Returns: A Time Series Analysis, Financial Mathematics, September 2023 (Danışmanı Esma Gaygısız)

Ödüller

2022-2023 Eğitim öğretim yılında ODTÜ Lisansüstü Tez Ödülü'nü Enstitümüzde;

- Bilimsel gelişmeye katkı kategorisinde, Finansal Matematik EABD'ndan Prof. Dr. Sevtap Kestel danışmanlığında ve Dr. Bilgi Yılmaz ortak danışmanlığında tamamladığı yüksek lisans tezi ile Umut Gölbaşı,
- Tezden kaynaklanan yayın kategorisinde, Bilimsel Hesaplama EABD'ndan Prof. Dr. Ömür Uğur danışmanlığında ve Prof. Dr. Tayfur E. Tezduyar ortak danışmanlığında tamamladığı doktora tezi ile Dr. Süleyman Cengizci,
- Tezden kaynaklanan yayın kategorisinde, Kriptografi EABD'ndan Prof. Dr. Murat Cenk danışmanlığında tamamladığı doktora tezi ile Dr. Esra Yeniaras

almıştır.

Mezunlarımızı ve danışmanlarını tebrik eder, başarılarının devamını dileriz. Ayrıca, Üniversitemiz Ders Performansı Ödülleri kapsamında başarılı bulunarak akademik çalışmalarından dolayı ödüllendirilen aşağıdaki listede isimleri yer alan belirtilen mezun ve öğrencilerimizi tebrik eder, başarılarının devamını dileriz.

[1]	Arda Buğra Özer (Kriptografi): Doktora Ders Performans Ödülü, 2023
-----	--



Ek Bilgiler

Yeni Açılan Dersler (2023 Yılı)

Enstitümüzün ders kataloğuna 2023-2024 Güz döneminde açılan aşağıdaki ders eklenmiştir.

2023 - 2024 Güz Dönemi

Course Code	9700574
Course Title	Mathematical Foundations for Data Analysis
Course Credit(s)	METU 3(3-0) ECTS 8
Instructor(s)	Doç. Dr. Önder Türk
Prerequisites	Consent to the Instructors
Course Catalog Description	Background in linear algebra: vector space, orthogonality, positive definiteness, eigenvalues and eigenvectors; Matrix decomposition: Cholesky decomposition, QR decomposition, singular-value decomposition; Least square problems: projectors; Best low rank approximation: Eckart-Young Theorem, principal component analysis; Vector Calculus: gradients, high order derivatives, chain rule;; Continuous optimization: convexity, gradient descent, Lagrange multipliers, stochastic gradient descent; Basics of probability and distribution: maximum likelihood estimation
Course Objectives	The goal of this course is to explain the mathematics on which data science depends: Linear algebra, vector calculus, and optimization. These concepts are considered as the mathematical pillars of data analysis. At the end of this course, the student will: - understand the basic mathematical tools and methods which will provide important background for understanding the mathematics involved in data science. - capture the state of the art of the interaction between linear algebra and data. understand the various numerical methods that underlie machine learning methods that have become so popular today in real-world applications.
Tentative (Weekly) Outline	1. Introduction and Motivation: basic problems in machine learning 2. Review of basic Linear Algebra: vectors, matrices, linear independence, basis 3. Orthogonal and Positive definite matrices: inner products, norm 4. Eigenvalues and Eigenvectors 5. Matrix decomposition: LU, Cholesky decomposition 6. Least squares problems: data fitting, projector, QR decomposition 7. Singular value decomposition 8. Best low rank approximation: Eckart-Young theorem, principal component analysis 9. Vector Calculus: gradient, high order derivatives 10. Backpropagation: chain rule, automatic differentiation 11. Nonlinear equations: Newton's method 12. Unconstrained optimization: convexity, gradient descent 13. Constrained optimization: projected gradient, Lagrange multipliers



	Basics of probability and distribution: maximum likelihood estimation
Course Textbook(s)	There will be no explicit textbook for the course; rather, the instructor will provide some hand-written lecture notes along with the progress of the course. However, the following books on this topic are recommended: • M. P. Deisenroth, A. A. Faisal, and C. S. Ong, Mathematics for Machine Learning, Cambridge University Press, 2020. • C. C. Aggarwal, Linear Algebra and Optimization for Machine Learning, Springer, 2020. • G. Strang, Linear Algebra and Learning from Data, Wellesley-Cambridge Press, 2019. • L. Trefethen and D. Bau, Numerical Linear Algebra, SIAM Press, 1997 I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, 2016.

2023 Yılı Doktora Mezunlarımız

Doktora derecesini alan mezunlarımıza ait kısa özgeçmişler, tez konusu özetleri ve tez çalışmalarından yaptıkları yayın listeleri mezun oldukları tarih sırasına göre bu kısımda verilmektedir.

Adı Soyadı: Kübra Kaytancı



Kübra Kaytancı 2015 yılında Boğaziçi Üniversitesi Matematik bölümünden mezun olmuş ve 2017 yılında aynı üniversitede Matematik bölümünde yüksek lisans çalışmalarını tamamlamıştır. Daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi Anabilim dalında doktora çalışmalarına devam etmiş ve Ağustos 2023 tarihinde Prof. Dr. Ferruh Özbudak danışmanlığında “On Plateaued Functions, Linear Structures, Permutation Polynomials and c-Differential Uniformity” başlıklı tezini tamamlamıştır. Araştırma konuları arasında Boole fonksiyonların inşası, Plateaued fonksiyonları, Doğrusal Yapılar, Permütasyon polinomları ve c-Diferansiyel Tekdüzelik bulunmaktadır. Kübra, 2015 ve 2017 yılları arasında Boğaziçi Üniversitesi Matematik bölümünde araştırma görevlisi olarak görev yapmış olup 2020 yılından bu yana ODTÜ Uygulamalı Matematik Enstitüsü bölümünde araştırma görevlisi olarak görev almaktadır.

Doktora Tezi Özeti :

İyi şifreleme sistemlerinin tasarlanmasında istenen bir amaç, yüksek doğrusal olmama, dengelilik, yüksek korelasyon bağımsızlığı ve yüksek cebirsel bağımsızlığa sahip olmak gibi iyi kriptografik özelliklere sahip boole fonksiyonları oluşturmaktır. Bu tezde, son zamanlarda 2017'de Cusick'te verilenden, doğrusal yapıları olmayan yüksek düzeyde doğrusal olmayan plateaued fonksiyonlar sınıfının cebirsel bağımsızlığına ilişkin somut üst sınırlar elde ediyoruz. Ayrıca, Cusick'in sınıfını çok daha büyük bir sınıfa genişletiyoruz ve bir örnekle sınıfımızın daha iyi cebirsel bağımsızlığa sahip olduğunu gösteriyoruz. Ayrıca 2018'de verilen Frobenius doğrusal çevirici, Cepak, Pasalic ve özel bir durum olarak Muratovic-Ribic içeren yeni bir doğrusal çevirici kavramı veriyoruz. Yeni doğrusal çevirici kavramının permütasyon polinomlarının inşasında bazı uygulamalarını buluyoruz. Ayrıca, F_q 'ın bazı özelliklerini ve 2011'in bazı koşullarını, Akbary, Ghioca ve Wang'ı kullanarak F_q^n üzerinde permütasyon polinomlarının sınıflarını veriyoruz. Ayrıca, son zamanlarda Ellingsen ve diğerleri diferansiyel kavramını genişleterek yeni bir kavram olan c-Fark Dağılım Tablosunu ve c-diferansiyel tekdüzeliği tanıttı. Bu yeni konseptin arkasındaki motivasyon, 2002'de Borisov ve diğerleri tarafından gösterilen bazı bilinen farklı saldırılara direnme yeteneğine sahip olmaya dayanmaktadır. 2002'de Hasan ve diğerleri Tr fonksiyonu aracılığıyla H ters fonksiyonla pertürbe edilen c-diferansiyel tekdüzeliğinin bir üst sınırını verdi. Çalışmalarında, H 'ın tam c-diferansiyel tekdüzeliği hakkında açık bir soru da sundular. Sonlu cisimler üzerinden cebirsel eğrilere dayalı yeni bir yöntem kullanarak, $c \in F_2^n \setminus \{0,1\}$ için $Tr(c)=1= Tr$ durumunda açık soruyu tamamen çözüyoruz ve H 'ın tam c-diferansiyel tekdüzeliğinin 8 olduğunu gösteriyoruz. Kalan durumda, sorunu neredeyse tamamen çözüyoruz ve H 'ın c-diferansiyel tekdüzeliğinin 8 veya 9 olduğunu gösteriyoruz.

Yayınlar:

- S. Mesnager, K. Kaytancı, F. Özbudak, On Plateaued Functions, Linear Structures, and Permutation Polynomials, in Codes, Cryptology and Information Security. C2SI 2019. Lecture Notes in Computer Science(), 11445. Springer (2019).
- K. Kaytancı, F. Özbudak, The c -Differential Uniformity of the Perturbed Inverse Function via a Trace Function Tr). (accepted 2023)

Adı Soyadı: Pelin Çiloğlu



Pelin Çiloğlu 2015 yılında Orta Doğu Teknik Üniversitesi Matematik bölümünden mezun olmuştur. Daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Bilimsel Hesaplama programında bütünleşik doktora çalışmalarına devam etmiş ve Haziran 2023 tarihinde Doç. Dr. Hamdullah Yücel danışmanlığında “Stochastic Discontinuous Galerkin Methods for PDE-Based Models with Random Coefficients” başlıklı tezini tamamlamıştır. Araştırma konuları arasında PDE-kısıtlı eniyileme, belirsizlik ölçümü, stokastik kesintili Galerkin, adaptif sonlu elemanlar yöntemleri, nümerik lineer cebir bulunmaktadır. Çiloğlu, 2018 ve 2023 yılları arasında ODTÜ Uygulamalı Matematik Enstitüsü’nde araştırma görevlisi olarak görev yapmış olup 2023 yılı

Ekim ayından itibaren Chemnitz Teknik Üniversitesi, Matematik Fakültesi, Bilimsel Hesaplama bölümünde doktora sonrası araştırmalarını yürütmektedir.

Doktora Tezi Özeti :

Belirsiz parametreler gibi belirsizlik, mühendislik ve bilimdeki birçok karmaşık fiziksel sistemden kaynaklanır; örneğin, akışkanlar dinamiği, ısı transferi, kimyasal olarak reaksiyona giren sistemler, sualtı kirliliği, radyasyon taşınımı ve petrol sahası rezervuarları. Bu sistemlerin rasgele girdi verileri ile kısmi diferansiyel denklemler ile modellenebileceği iyi bilinmektedir. Bununla birlikte, girdi verilerinde mevcut olan bilgiler çok sınırlıdır ve bu da bu problemlerin çözümüne yaklaşımda yüksek düzeyde belirsizliğe neden olur. Bu nedenle, belirsizlik ölçümü fikri, son on yılda bu tür fiziksel problemleri modellemek için güçlü bir araç haline geldi.

Bu tezde amaç, rastgele katsayılarla sahip kısmi diferansiyel denklem (PDE) tabanlı modeller için stokastik süreksiz Galerkin yönteminin geliştirilmesi, analizi ve uygulanmasıdır. Bir model olarak, önce belirsizlik içeren tek konveksiyon difüzyon denklemine odaklanıldı. Rastgele katsayıları belirlemek için iyi bilinen Karhunen Loève (KL) genişletme tekniğini kullanıldı. Belirsizlikler içeren orijinal problemi büyük bir deterministik problemler sistemine dönüştüren Stokastik Galerkin (SG) yaklaşımı, stokastik alanı ayırıklaştırmak için uygulanırken, konveksiyon ağırlıklı PDE'ler için daha iyi yakınsama davranışı nedeniyle uzaysal ayırıklaştırma için süreksiz bir Galerkin yöntemi tercih edilir. Priori ve posteriori hata tahminleri de türetilir. SG yöntemi genellikle, çözümünün standart çözümler kullanılarak hesaplanması zor olan büyük bir birleşik lineer denklem sistemiyle sonuçlanır. Bu sebeple, bu sistemlerin çözümlerine düşük kerteli yaklaşımlar hesaplayan bu tür çözümlerin verimli bir şekilde hesaplanması için düşük kerteli yinelemeli çözümler sağlandı. Ayrıca, sınır ve/veya iç katmanların, çözümün türevinin büyük olduğu yerel bölgelerin üstesinden gelmek için, parametrik konveksiyon difüzyon denklemlerinin sayısal çözümü için etkili bir uyarlamalı algoritma sunulmuştur. Öte yandan, istenen hedefe ulaşmak için bir modelin belirli parametrelerinin, örneğin yağın ortama eklendiği konum, bir eritme/ısıtma işleminin sıcaklığı veya uçak kanatlarının şekli gibi bazı parametrelerin optimize edilmesi gerekir. Bu nedenle, bulgular optimizasyon problemlerine genişletildi ve rastgele girdiler içeren konveksiyon difüzyon denklemleri tarafından yönetilen optimal kontrol problemlerini ele alındı.

Yayınlar:

- Çiloğlu, P., and Yücel, H., Stochastic Discontinuous Galerkin Methods for Robust Deterministic Control of Convection Diffusion Equations with Uncertain Coefficients, *Advances in Computational Mathematics*, 49, 16, 2023, doi: 10.1007/s10444-023-10015-5.
- Çiloğlu, P., and Yücel, H., Stochastic Discontinuous Galerkin Methods with Low-Rank Solvers for Convection Diffusion Equations, *Applied Numerical Mathematics* 172, 157-185, 2022, doi:10.1016/j.apnum.2021.10.007.
- Çiloğlu, P., and Yücel, An Adaptive Algorithm Based on Stochastic Discontinuous Galerkin for Convection Dominated Equations with Random Data, (İnceleme).

Adı Soyadı: Betül Kalaycı



Betül Kalaycı 2014 yılında Ankara Üniversitesi Matematik bölümünden mezun olmuş ve 2014 yılında ODTÜ Uygulamalı Matematik Enstitüsü, Finansal Matematik anabilim dalında yüksek lisans programına başlamıştır. 2017 yılında “Identification of Coupled Systems of Stochastic Differential Equations in Finance Including Investor Sentiment by Multivariate Adaptive Regression Splines” başlıklı tezini tamamladıktan sonra aynı yıl Finansal Matematik anabilim dalında doktora programına devam etmiş ve Haziran 2023 tarihinde de Prof.Dr.Vilda Purutçuoğlu ve Prof. Dr. Gerhard-Wilhelm Weber danışmanlığında “Modelling Mutual Interaction of Finance and Human Factor via Various Sorts of Indices” başlıklı tezini tamamlamıştır. Araştırma konuları arasında makine

öğrenmesi, veri madenciliği, markov modelleri, stokastik süreçler, volatilité modeller ve finansal karar verme süreçleri bulunmaktadır.

Doktora Tezi Özeti :

Bu tez, makine öğrenimi yaklaşımları ve parametrik olmayan modellerden parametrik volatilité modellerine kadar çeşitli modeller kullanılarak bazı finansal süreçler ve duyarlılık endeksleri arasındaki karşılıklı etkileri temsil etmektedir. Analizlerde, doğruluk ve hesaplama zamanındaki kazancı karşılaştırıyoruz. Ayrıca duyarlılık endeksi, tüketici güven endeksi, tüketici fiyat endeksi, işsizlik oranı ve döviz kurunun tahmin performansını da değerlendiriyoruz. Buna dayanarak, başlangıçta, tek çok değişkenli uyarlanabilir regresyon splinleri (MARS), sinir ağı (NN) ve rastgele orman (RF) modellerini kullanıyoruz. Ardından MARS-NN, MARS-RF, RF-MARS, RF-NN, NN-MARS ve NN-RF olmak üzere iki aşamalı hibrit modeller uyguluyoruz. Son olarak, duyarlılık endeksi ve tüketici güven endeksi için oynaklık modelleri uyguluyoruz ve tahmin performansını iyileştirmek için seçilen makroekonomik verilerle makul ilişkileri araştırıyoruz. Bulguların yorumlanmasında, altta yatan veri kümeleri önemli yapısal kırılmalar sergilemeye eğilimli olduğundan, Markov anahtarlama modelini uyguluyoruz, kırılmaların yerini tanımlıyoruz ve son olarak farklı zaman serisi oynaklık modelleri gerçekleştiriyoruz. Sonuçlar, alternatifler arasında Markov anahtarlama genelleştirilmiş otoregresif koşullu heterosketastik model, kısaca MSGARCH, altında daha iyi doğruluğu göstermektedir.

Yayınlar:

- Kalaycı, B., Özmen, A. and Weber, G.-W. Mutual relevance of investor sentiment and finance by modeling coupled stochastic systems with MARS, Annals of Operations Research, 295(173), pp. 1–24, 2020.
- Kalaycı, B., Purutçuoğlu, V. and Weber, G.-W. Operation Research in Neuroscience: A

Recent Perspective of Operation Research Application in Finance, Operations Research 1, CRC Press, 2022. 170-190.

- Kalaycı, B., Purutçuoğlu, V., Defterli, Ö., Uğur, Ö. and Weber, G.-W. Application of Various Modelling Techniques into Consumer Confidence Index: A Recent Perspective of Operation Research Application in Finance, Operations Research 2, CRC Press, 2023 (kabul edildi).
- Kalaycı, B., Purutçuoğlu, V. and Weber, G.-W. Optimal Model Description of Finance and Human Factor Indices, Central European Journal of Operations Research, 2023 (kabul edildi).

Adı Soyadı: Zeynelabidin Karakaş



Zeynelabidin Karakaş 2009 yılında Mimar Sinan Güzel Sanatlar Üniversitesi Matematik Bölümü'nden mezun olmuş ve Millî Eğitim Bakanlığı tarafından yurt dışında yüksek öğrenim imkanı sağlayan YLSY bursunu almaya hak kazanmıştır. Yüksek lisansını Birleşik Krallığa bağlı Royal Holloway Üniversitesi ve Bedford New College'da Uygulamalı Matematik alanında, Prof. Dr. Stefanie Gerke danışmanlığında yaptığı tez çalışmasıyla 2015 yılında tamamlamıştır. Zeynelabidin 2015-2019 yılları arasında mecburi hizmet yeri olan Kırklareli Üniversitesi – Matematik Bölümü'nde Araştırma Görevlisi olarak çalışmıştır. 2019 yılında ODTÜ Uygulamalı Matematik Enstitüsü – Kriptografi Anabilim Dalı'nda başlamış olduğu doktora öğrenimini Prof. Dr.

Ferruh Özbudak danışmanlığında “Belirli Bir Tipteki Farklı Maksimal Bayrak Kodlarının Sınıflandırılması ve İlgili Sonuçlar” başlıklı doktora tezi ve 120N932 nolu Uluslararası TÜBİTAK 1071 projesi desteği ile tamamlamıştır. 2019 yılından itibaren de Yüksek Öğrenim Kanunu'nun 35. Maddesi kapsamında ODTÜ – UME Kriptografi bölümünde Araştırma Görevlisi olarak çalışmaktadır.

Doktora Tezi Özeti:

Bu tezde, bayrak kodları için literatürde mevcut olan bazı sınırları geliştirmek ve belirli tipteki farklı kodların sayılarını vermekle birlikte bazı parametreler için onları karakterize etmeyi amaçlıyoruz.

Bayrak kodlarının ağ kodlamada önemli uygulamaları mevcuttur ve onların cebirsel ve kombinatorik yapıları son yıllarda aktif bir araştırma alanıdır. Verilen ambiyant uzay üzerinde belirli bir tipe ve uzaklığa sahip maksimal bayrak kodların karakterizasyonu çok zor bir problemidir. Bu tezde, biz bu problemi küçük parametreler için MAGMA kullanarak tamamen çözdük ve diğer tüm parametreler için çizge teorisindeki bazı yapılar üzerinden kombinatorik sonuçları da kullanarak birer alt sınır ve üst sınır belirledik. Verilen bir tipteki ve istenen bir uzaklığa sahip bayrak kodlarının sayısı için tam sonuçları bazı parametreler için belirledik, diğer değerler için de alt ve üst sınır verdik. Küme-bayrak-kodlarını tanımladık ve bu sayede Sascha Kurz'ub yayınında verilmiş olan bazı sınırların her q değeri için geçerli olmadığını gösterdik.

Yayınlar:

- Karakaş, Z., Özbudak F., On the Classification of Distinct Maximal Flag Codes of a Prescribed Type and Related Results, International Conference on Finite Fields and Their Applications 2023 (Fq15), Paris (FR), June 19-23, 2023.

Adı Soyadı: Onur Enginar



Onur Enginar 2013 yılında Hacettepe İşletme Bölümü'nden mezun olmuştur. Aynı bölümde 2018 yılında Parasal Daralma Süreci: Gelişmekte Olan Ülke Borsaları Performansları başlıklı tezi ile yüksek lisans eğitimini tamamlamıştır. Eylül 2023'te, Prof. Dr. Ömür Uğur danışmanlığında Deep Ensembles Approach for Energy Forecasting konulu tezini savunmuştur. Araştırma konuları derin öğrenme, derin topluluklar modeli, olasılıksal tahmin ve enerji tahminleme konuları üzerinedir. Onur, Hacettepe İşletme Bölümü'nde doktor araştırma görevlisi, Presify AI firmasında da kurucu ortak olarak çalışmaktadır.

Doktora Tezi Özeti:

Bu tez çalışmasında, model performansından ödün vermeden derin toplulukların (deep ensembles) zaman gereksinimini azaltmak için transfer öğrenmesini kullanarak yenilikçi derin topluluklar (deep ensembles) modeli geliştirilmiştir. Geliştirilen model açık veri setlerine uygulanmıştır. Ayrıca, bu çalışmada, derin topluluklar (deep ensembles) modeli, literatürde tabular öğrenmeye özel geliştirilmiş güncel modeller ile kıyaslanarak sonuçları raporlanmıştır. Son olarak, derin topluluklar (deep ensembles) tabanlı öz-nitelik seçim algoritması geliştirilerek, bu yöntem doğrusal öz-nitelik çıkarma modelleri ve ağaç tabanlı öz-nitelik çıkarma modelleri ile kıyaslanmıştır.

Yayınlar:

- Enginar, O., & Atici, K. B. (2022). Optimal forecast error as an unbiased estimator of abnormal return: A proposition. *Journal of Forecasting*, 41(1), 158-166.
- Büyükkara, G., Enginar, O., & Temiz, H. (2020). Volatility Spillovers Between Oil and Stock Market Returns in G7 Countries: A VAR-DCC-GARCH Model. *Regulations in the Energy Industry: Financial, Economic and Legal Implications*, 169-186.
- Enginar, O., Karan, M. B., & Büyükkara, G. (2018). Performances of emerging stock exchanges during the Fed's tapering announcements. *Global Approaches in Financial Economics, Banking, and Finance*, 415-443.
- Enginar, O., & KARAN, M. B., (2018). Using Neural Network in Event Study . Multinational Finance Society, Budapest, Hungary

Adı Soyadı: Dilek Öner Şimşek



Dilek Öner Şimşek 2005 yılında %100 burslu olarak girdiği Başkent Üniversitesi İstatistik ve Bilgisayar Bilimleri bölümünden 2009 yılında mezun olmuştur. Aynı yıl ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi anabilim dalında yüksek lisansa başlamıştır ve 2011 yılında mezun olmuştur. 2011 yılında aynı bölümde doktora çalışmalarına başlamıştır. 2012 yılında Sosyal Güvenlik Kurumu'nda sosyal güvenlik uzmanı olarak iş hayatına başlamıştır. 2023 yılında Danışmanı Prof. Dr. Ersan AKYILDIZ ve eş danışmanı Prof. Dr. Murat CENK ile Faster Secure Matrix Multiplication Using the Strassen Algorithm başlıklı tezini tamamlamıştır.

Doktora Tezi Özeti :

Bulutta, kişisel veriler güvenlik sorunlarına açıktır. Homomorfik şifreleme, şifrelenmiş veriler üzerinde hesaplamalara olanak sağlayarak gizlilik endişelerini gidermeye yönelik bir çözüm sunar. Bu hesaplamalar istatistiksel analiz veya makine öğrenme algoritmaları olabilir. Matris çarpımı şifrelenmiş verilere de uygulanabilir. Buna güvenli matris çarpımı denir. Güvenli matris çarpımı, istatistiksel analiz ve makine öğrenimi algoritmaları da dahil olmak üzere birçok uygulamadaki temel işlemlerden biridir. A ve B'nin iki kare matris olduğunu varsayalım; güvenli matris çarpım algoritması, her matris için sıkıştırılmış polinomlar oluşturur, bunları şifreler ve homomorfik olarak çarpır. Şifreyi çözdükten ve sıkıştırılmış polinomu açtıktan sonra $A \times B$ çarpım matrisini bulabiliriz. Büyük matrisler için homomorfik çarpım yapmak, sıkıştırılmış polinomların derecesinin ve şifreleme parametrelerinin artması nedeniyle zordur. Ayrıca büyük matrisler için homomorfik şifreleme işlemleri verimsiz hale gelir. Bu tezde, matrisleri alt bloklara böldükten sonra, güvenli matris çarpım algoritmasını uygulamaktayız ve iki matrisi güvenli bir şekilde çarpım için performansı artırmak amacıyla Strassen algoritmasını kullanmayı önermekteyiz. Strassen algoritması bir seviye özyineleme kullanıldığında homomorfik şifreleme sayısını sekizden yediye düşürmektedir. Ayrıca, homomorfik şifreleme ve çarpımlar polinomların derecesindeki azalmadan dolayı daha verimli uygulanmaktadır. Güvenli matris çarpımı için Fan ve Vercauteren (FV) ve Brakerski, Gentry ve Vaikuntanathan (BGV) homomorfik şifreleme algoritmalarını uygulamaktayız. 8 ile 128 arasındaki farklı matris ve alt matris boyutları için uygulama sonuçları önemli gelişmeler göstermektedir. Örneğin, FV homomorfik şifreleme kullanıldığında 128×128 boyutlu matris için alt matris boyutu iki olduğunda Strassen güvenli blok matris çarpımı algoritması standart blok matris çarpımına göre %47 daha hızlıdır. Ayrıca, benzer şekilde, BGV algoritması kullanıldığında alt matris boyutu iki olan 128×128 boyutlu bir matris düşünüldüğünde, algoritma standart güvenli matris çarpımına kıyasla %44 daha hızlıdır. Bu nedenle, uygulamamız homomorfik şifreleme çerçevesinde güvenli matris çarpımı için Strassen yöntemini kullanmanın faydalarının altını çizerek, özellikle daha büyük boyutlar için matrisleri alt bloklara böldükten sonra performansı artırma potansiyelini vurgulamaktadır. Ayrıca, bir uygulama olarak, Strassen güvenli blok matris algoritmasını kullanarak şifrelenmiş verilerin çoklu doğrusal regresyonunu hesaplamakta ve sonuçları standart blok matris yöntemiyle karşılaştırmaktayız. Elde edilen sonuçlara göre, matris boyutu 128 ve alt matris boyutu iki olduğunda, Strassen'in güvenli blok

matris çarpma algoritması ile çoklu doğrusal regresyon hesaplaması, standart güvenli blok matris çarpma algoritmasına göre %47 daha hızlıdır.

Yayınlar:

- Şimşek Öner D., Triaç Sistemlerine Genel Bakış ve Türkiye’de Acil Servis Başvurularını Etkileyen Faktörlerin Lojistik Regresyon ile Belirlenmesi, 2018, Sosyal Güvence Dergisi
- Cenk M., Şimşek Öner D., Faster Secure Matrix Multiplication with the BGV Algorithm, 16th International Conference on Security and Cryptology, 2023

Adı Soyadı: Duygu Özden



Duygu Özden 2014 yılında ODTÜ Matematik bölümünden mezun olmuş ve 2016 yılında ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi programında yüksek lisans çalışmalarını tamamlamıştır. Daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi programında doktora çalışmalarına devam etmiş ve Temmuz 2023 tarihinde Doç. Dr. Oğuz Yayla danışmanlığında “Verifiable Timed Commitments Explored: Timed Signature Schemes and an Application to Sealed-bid Auctions” başlıklı tezini tamamlamıştır. Duygu, aynı zamanda 2017 yılından bu yana Siber Güvenlik alanında çalışmaktadır. Araştırma konuları arasında dijital imzalar, zamanlanmış imzalar ve taahhütler, siber olay analizi, tehdit avcılığı, siber tehdit istihbaratı yer almaktadır.

Doktora Tezi Özeti :

Zamanlanmış taahhütler, bir tarafın bir değeri belirli bir süre için taahhüt etmesine ve o değerin varlığını ve bütünlüğünü kanıtlamasına olanak tanıyan protokollerdir. Bu tez, doğrulanabilir zamanlanmış taahhüt kavramını keşfeder ve zamanlanmış imza şemaları ve kapalı teklif müzayedeleri üzerindeki uygulamalarını araştırır. Çalışma, önerilen imza şemalarının güvenlik gereksinimlerini, yapım tekniklerini ve hesaplama karmaşıklığını ortaya koymaktadır. Ayrıca, hassas teklif verme ortamlarında yaygın olarak kullanılan kapalı teklif müzayedelerinde doğrulanabilir zamanlanmış taahhütlerin uygulamaları incelenmektedir. Kapalı teklif müzayedeleri, katılımcıların birbirlerinden habersiz olarak tekliflerini gizli bir şekilde sunmalarını ve aynı anda belirlenmiş bir zamanda ortaya çıkarmalarını gerektirir. Zamanlanmış taahhütlerin teklif gizliliği, bütünlüğü ve adilliği nasıl sağlayabileceği araştırılmıştır. Taahhüt oluşturma, taahhüt açma ve teklif doğrulama protokollerini ve gerekli güvenlik hususları da, bu tezde tartışılmaktadır. Araştırma, doğrulanabilir zamanlanmış taahhütler üzerine kurulu önerilen şemaların güvenliğini değerlendirmek için teorik analiz, algoritma tasarımı ve uygulamaları içeren çok disiplinli bir yaklaşım kullanmaktadır.

Yayınlar:

- Özden D., Yayla O., Verifiable Timed Commitments for Fair Sealed-bid Auctions, International Conference on Cryptography, Informatics and Cybersecurity, Bogor, Indonesia, 2023
- Özden D., Yayla O., Verifiable Timed Accountable Subgroup Multi-signatures, Ağustos 2023(incelemede).
- Özden D., Yayla O., Verifiable Timed Proxy Signatures and Multi-signatures, Temmuz 2023 (incelemede).

Adı Soyadı: Mustafa Hakan Solmaz



Mustafa Hakan Solmaz 1996 yılında Bilkent Üniversitesi Elektrik-Elektronik Mühendisliği Bölümünden mezun olmuştur. 1998 yılında aynı bölümde “İşlemsel olarak verimli sesle telefon çevirme sistemi” başlıklı tez ile yüksek lisans eğitimini tamamlamıştır. 2012 yılında ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi Anabilim Dalında doktora çalışmalarına başlamış, Temmuz 2023 tarihinde Prof. Dr. Ersan Akyıldız danışmanlığında “Flexible hardware design for elliptic curve method of integer factorization” başlıklı tezini tamamlamıştır. Araştırma konuları arasında kriptografik algoritmaların FPGA üzerinde gerçekleştirilmesi, matematiksel işlemler için donanım hızlandırıcıların tasarlanması ve gerçekleştirilmesi, kriptanaliz için

donanım tasarımı gibi konular bulunmaktadır. Doktora tezi kapsamında da bunların uygulaması olarak FPGA üzerinde esnek bir Montgomery modüler çarpıcı çözümü ve eliptik eğri yöntemi ile asal çarpanlara ayırma tasarımı üzerinde çalışmıştır. Çalışma hayatı boyunca özel sektör kuruluşlarında gömülü yazılım mühendisi, sayısal tasarım mühendisi ve ekip lideri olarak çalışan Mustafa Hakan Solmaz, STG Mühendislik firmasında sayısal tasarım ve doğrulama yöneticisi olarak çalışmaya devam etmektedir.

Doktora Tezi Özeti :

Çevremizi saran elektronik haberleşme cihazlarının çoğunda, gelişmiş kriptografik algoritma ihtiyaçları özel donanımlar üzerinde uygulanmaktadır. Bu özel donanımlar, uygulamaya özel tümleşik devre (ASIC) ve sahada programlanabilir kapı dizileri (FPGA) olmak üzere ikiye ayrılmıştır. Bu tez çalışmasında tamsayı çarpanlara ayırma için eliptik eğri yönteminde (ECM) kullanılan tüm aritmetik ilkeleri FPGA platformunda tasarladık ve uyguladık.

Bu alt modüller , yukarıdan aşağıya olmak üzere, eliptik eğri üzerindeki bir noktanın skaler çarpımı, nokta toplaması, nokta ikiye katlaması, modüler çarpma, toplama ve çıkarma işlemlerini içermektedir. Eliptik eğri ile çarpanlara ayırma yönteminde kullanılan eğriler asal alanlar üzerinde tanımlanır. En alt katmanda modüler aritmetik, modüler toplama, çıkarma ve çarpma işlemleri bulunur. En önemli ve zaman alıcı işlem olan modüler çarpma daha fazla incelenmiştir. Bir bellek ve donanımda-hazır çarpıcı tabanlı Montgomery modüler çarpıcısı tasarlanmıştır. Bu çarpıcı 4096-bite kadar bütün sonlu alanlarda , FPGA’i tekrar programlamaya gerek duymadan, parametrik olarak çalışabilecek bir yetenektir.

Bu düşük seviyeli ilkel öğeler, skaler nokta çarpma sonuçları elde etmek için yeni bir mikro komut denetleyicisi tarafından kontrol edilmiştir. ECM, paralel olarak uygulanabilen bir çarpanlara ayırma yöntemidir. Tüm yardımcı işlemcinin birden çok örneği, Xilinx FPGA ailesinden Zynq tabanlı bir işleme alt sisteminde çağırılmıştır. Bu sayede ECM çekirdeklerine bir uygulama ile kolayca erişilebilmektedir. Literatürdeki benzer çalışmalardan daha yüksek sentez frekansları elde edilmiştir. Elde edilen ölçeklenebilir tasarım sayesinde, ECM’yi farklı FPGA’lerde çalıştırmak ve FPGA kaynaklarının izin verdiği ölçüde verim elde etmek mümkündür.

Yayınlar:

- Mustafa Hakan Solmaz, H. Erdoğan, and R. Aykaç, A scalable platform for cryptanalysis of computationally intensive algorithms, in International Information Security and Cryptology Conference, ISCTURKEY, pp. 195–200, 2012.
- Mustafa Hakan Solmaz and Oğuz Yayla, Flexible FPGA Design for Elliptic Curve Method (hazırlanıyor).

Adı Soyadı: A. Umur Özsoy



Ahmet Umur Özsoy 2012’de TOBB Ekonomi ve Teknoloji Üniversitesi’nden Endüstri Mühendisliği bölümünden mezun olmuştur. 2016 yılında ise Orta Doğu Teknik Üniversitesi’nden Finansal Matematik alanında yüksek lisansını tamamlamıştır. *Option Pricing Via Reinforcement Learning: Extensions and Further Insights On The QLBS Model* başlıklı tez çalışmasını Prof. Dr. Ömür Uğur gözetimi altında tamamlamış ve Ocak 2023’te başarıyla savunmuştur. İlgi alanları arasında finans mühendisliği, finansa makine öğrenmesi ve hesaplamalı finans bulunmaktadır. 2021 yılından beri Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)’nda, Türkiye Sanayi Sevk ve İdare Enstitüsü (TÜSSİDE)’nde Araştırmacı olarak çalışmalarına devam etmekte; ulusal ve uluslararası

birçok projede yer almaktadır.

Doktora Tezi Özeti :

Çalışmamızda döviz kurları üzerine yazılan Avrupa tipi opsiyonlarını dikkate alarak pekiştirmeli öğrenmeden (reinforcement learning) faydalanılmıştır. Bu amaçla, QLBS modeli olarak adlandırılan ve köklerini pekiştirici öğrenmeden alan bir opsiyon fiyatlama modelini yeni bir varlık tipiyle sunup, daha sonra yeniden formüle etmekteyiz. İlk önce döviz kurlarında çalışması beklenen QLBS modelini tanıtmaktayız. Döviz kuru piyasalarına ilişkin sayısal gösterimlerin yanı sıra daha detaylı içgörü sunmaktayız. Farklı yapı (states) önermekteyiz ve daha sonra uzantımızı karşılaştırmalı olarak test etmekteyiz. Döviz kurlarında oluşabilecek sıçramaları da kullanmakta ve QLBS modelinin nasıl tepki verdiğini incelemekteyiz. Sonrasında, işlemleri döviz kuru piyasalarında kalıcı etki bırakan büyük bir yatırımcıyı modelleyerek, QLBS modelini piyasa etkileri altında yeniden formüle etmekteyiz. Piyasa etkileri altında opsiyon fiyatlamasında makine öğrenimini zenginleştirmek ve katkı sağlamak amacıyla bambaşka bir yaklaşım sunmaktayız. Tüm bölümlerde, gösterge (kıyaslama) fiyatlara yakınsama elde etmekte ve QLBS modeline dayalı katkımızın, geleneksel opsiyon fiyatlandırma modellerine bir alternatif olabileceğini tartışmaktayız.

Yayınlar:

- Özsoy A.U., Uğur Ö. “ The QLBS Model within the presence of feedback loops through the impacts of a large trader” (hazırlanmakta, çalışmanın working paper versiyonu için URL: <https://doi.org/10.48550/arXiv.2311.06790>)

Adı Soyadı: Murat Burhan İlter



Murat Burhan İlter 2014 yılında ODTÜ Matematik bölümünden mezun olmuş ve 2016 yılında ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi anabilim dalında yüksek lisansını tamamlamıştır. Daha sonra Kriptografi doktora programına devam etmiş ve Eylül 2023 tarihinde Doç. Dr. Ali Doğanaksoy ve Prof. Dr. Ali Aydın Selçuk danışmanlığında “Differential and Linear Cryptanalysis Of Lightweight Block Ciphers with MILP Approach” başlıklı tezini tamamlamıştır. Araştırma konuları arasında kaynak kısıtlı kriptografi, blok tipi şifreler ve kriptanaliz yer almaktadır. 2015-2019 yılları arasında ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi ana bilim dalında araştırma görevlisi olarak çalışmıştır. 2019 yılından itibaren ASELSAN'da çalışma hayatına devam

etmektedir.

Doktora Tezi Özeti :

Blok şifrelerin güvenliği kriptanaliz yöntemleri kullanılarak analiz edilebilir. Karma Tam sayılı lineer Programlamanın (KTLP) kullanımı, blok şifrelerin güvenlik yönlerini analiz etmede oldukça etkin olması nedeniyle önem kazanmıştır. Bu tezde, kapsamlı diferansiyel ve lineer kriptanaliz yöntemleri için KTLP tekniklerinin uygulanması araştırılmaktadır. Bu çalışma, özellikle diferansiyel ve lineer kriptanaliz alanındaki temel zorlukları ele almaktadır. Bu çalışmada şifrelerin diferansiyel ve lineer saldırılara karşı dayanıklı olması gerektiği dikkate alınarak bu saldırılara karşı şifre dirençleri incelenmektedir. Bu bağlamda bir blok şifrenin en iyi diferansiyel ve lineer karakteristiklerini bulmayı hedeflemek zor bir problemdir. Çalışmamızda bu problemin çözümüne yönelik olarak çoklu xor işlemlerini içeren denklemler için yenilikçi KTLP modelleme yöntemleri sunulmaktadır. Model 1 ve Model 2 olarak adlandırılan bu modeller sırasıyla daha az değişken ve kısıtlı alternatifler sunmaktadır. Model 1 ve Model 2 genellikle standart xor modeline göre daha kısa çözüm süreleri sağlar. Önerilen bu modeller, diferansiyel ve lineer kriptanalizin ötesinde geniş bir uygulanabilirliğe sahiptir ve çeşitli kriptanaliz yöntemlerindeki verimliliği artırır.

Bu tezde, KTLP ile KLEIN, PRINCE, FUTURE ve IVLBC gibi iyi bilinen şifreler modellenmektedir. Sunulan modeller, kesin minimum diferansiyel aktif S-kutularının sayısının ve en iyi diferansiyel ve lineer karakteristiklerin belirlenmesini sağlamaktadır. Geliştirilen KTLP modelleri, incelenen şifreler için literatürde yer alan en iyi tek anahtarlı diferansiyel ve lineer karakteristiklerde iyileştirmeler ortaya koymaktadır.

Yayınlar:

- Murat Burhan İlter, Ali Aydın Selçuk: Differential and Linear Cryptanalysis of IVLBC via MILP Modeling. 16th International Conference on Information Security and Cryptology (ISCTürkiye) 2023: 1-5
- Murat Burhan İlter, Ali Aydın Selçuk: MILP-Aided Cryptanalysis of the FUTURE Block Cipher. SecITC 2022: 153-167

- Murat Burhan İlter, Nese Koçak, Erkan Uslu, Oguz Yayla, Nergiz Yuca: On the Number of Arithmetic Operations in NTT-based Polynomial Multiplication in Kyber and Dilithium Cryptosystems. SIN 2021: 1-7
- Murat Burhan İlter, Ali Aydın Selçuk: A New MILP Model for Matrix Multiplications with Applications to KLEIN and PRINCE. SECUREPT 2021: 420-427
- Berkin Aksoy, Yusuf Alper Bilgin, Murat Cenk, Murat Burhan İlter, Nese Koçak, Yunus Emre Yılmaz. Analyzing NIST 2nd-round Lattice-based Post-quantum KEM Algorithms, Information Security and Cryptology Conference, Ankara, Turkey, 2019
- Murat Burhan İlter, Murat Cenk. Efficient Big Integer Multiplication in Cryptography, International Journal of Information Security Science 6.4 (2017): 70-78

Adı Soyadı: Etkin Hasgöl

Etkin Hasgöl 2012 yılında ODTÜ İstatistik bölümünden mezun olmuş ve 2015 yılında ODTÜ Aktüerya Bilimleri programında yüksek lisans çalışmalarını tamamlamıştır. Daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik bölümünde doktora çalışmalarına devam etmiş ve Ekim 2023 tarihinde Prof. Dr. A. Sevtap Kestel danışmanlığında “A Hybrid Approach in Constructing an Internal Solvency Model” başlıklı tezini tamamlamıştır. Araştırma konuları arasında zaman serileri, yapay sinir ağları, mortalite tabloları, Solvency II ve copula bağımlılık modelleri bulunmaktadır. Etkin, 2013 ve 2018 yılları arasında ODTÜ Afet Yönetim Merkezi ve Uygulamalı Matematik Enstitüsü’nde araştırma görevlisi olarak, 2019-2020 yıllarında Türkiye Sigorta Birliği’nde araştırmacı uzman olarak görev yapmış ve 2020 yılı Aralık ayından itibaren Marsh McLennan şirketler grubunda Analitik Çözümler Ülke Lideri olarak görev yapmaktadır.

Doktora Tezi Özeti :

Bu tez, çeşitli hayatdışı sigortalar branşlarında ele alınan Prim Riski için Solvency Sermaye Gerekliliğini (SCR) hesaplamak için Zaman Serisi, Yapay Sinir Ağı (YSA) ve Kopula modellerini birleştiren yeni bir hibrit yaklaşım sunmaktadır. Hasar prim oranı $Z_i = X_i + Y_i + \varepsilon_i$ formülü ile tanımlanmıştır. Bu formülde X_i zaman serisi bileşenini, Y_i ise YSA bileşenini temsil eder. İlk olarak, hasar prim oranları uygun zaman serisi modelleri kullanılarak modellenir ve modelin lineer bileşeni oluşturulur. Sonrasında, uygun otoregresif sinir ağı (NNAR) modeli, her bir branş için uyumlandırılan zaman serisi modellemesinin sonucunda oluşan artıklara uygulanarak, modelin doğrusal olmayan bileşenini tespit etmek için kullanılır. Son olarak, birleşik modelin artıkları R-vine yapısı kullanılarak modellenir. Zaman serisi, otoregresif sinir ağı ve kopula yapısı kullanılarak, seçilen branşlar için hasar prim oranı simülasyonları elde edilir ve Hayat Dışı Prim Riski analizi yapılabilir. Önerilen yaklaşımın etkinliğini değerlendirmek için Standart SCR modeli ve önerilen hibrit model sonucunda ortaya çıkan VaR ve TVaR değerleriyle karşılaştırma yapılır.

Yayınlar:

- Hasgöl, E., Sencuk-Kestel, A. S. (2023). A Hybrid Approach in Constructing an Internal Solvency Model (PhD thesis, Middle East Technical University).
- Hasgöl, E., Sencuk-Kestel, A. S. & Yolcu-Okur, Y. (2020). Forecasting mortality rates with a general stochastic mortality trend model . Communications. Faculty of Sciences University of Ankara Series A1 Mathematics and Statistics, 69 (1), 910-928. DOI: 10.31801/cfsuasmas.478265
- Hasgöl, E. (2015). Modeling future mortality rates using both deterministic and stochastic approaches (Master’s thesis, Middle East Technical University).

Adı Soyadı: Çiğdem Yerli



Çiğdem Yerli 2011 yılında Çankaya Üniversitesi İşletme bölümünden mezun olmuş ve YLSY bursu kapsamında 2013 yılında Durham İşletme Okulunda Finans ve Yatırım alanında yüksek lisans çalışmalarını tamamlamıştır. 2018 yılında ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik programında ikinci yüksek lisans derecesini almıştır. Daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik programında doktora çalışmalarına devam etmiş ve Nisan 2022-Nisan 2023 tarihleri arasında Avusturya Viyana Ekonomi Üniversitesi'nde TUBITAK 2214-A kapsamında doktora çalışmalarının bir kısmını yürütmüştür. Mayıs 2023 tarihinde Prof. Dr. Sevtap Kestel ve Doç. Dr. Zehra Eksi-Altay

danışmanlığında “Markov-Chain Modulated Implied Liquidity: Modeling and Estimation” başlıklı tezini tamamlamıştır. Araştırma konuları arasında stokastik modelleme ve tahmin, Markov süreçleri, piyasa likiditesi bulunmaktadır. Çiğdem, 2015 yılından itibaren Bartın Üniversitesi Meslek Yüksek Okulu Muhasebe ve Vergi Bölümünde öğretim görevlisi olarak görev yapmaktadır.

Doktora Tezi Özeti :

Bu tez, Konik Finans teorisi aracılığıyla tanıtılan ve piyasa likidite düzeyi için bir temsil olarak kabul edilen zımnî likiditeyi modellemek için bir metodoloji sunmaktadır. Gözlemlenemeyen gerçek piyasa likiditesine ilişkin gürültülü bilgileri temsil eden zımnî likidite dinamiklerinin, sürekli zamanlı Markov zinciri modülasyonlu üstel Ornstein-Uhlenbeck sürecini takip ettiği, bilginin kısmi olduğu bir çerçeve önerilmektedir. Model çıkarımı, gerçek piyasa likiditesinin gözlemlenmemiş durumlarının filtrelenmesini ve ayrıca bilinmeyen model parametrelerinin tahmin edilmesini gerektirir. Çıkarım problemi EM algoritması ile ele alınmaktadır. Algoritmanın beklenti adımı, olabilirlik fonksiyonunda bulunan nicelikler için sonlu boyutlu filtrelerin türetilmesini gerektirir. Bu amaçla, öncelikle OU süreci için mevcut EM algoritmasını incelenerek ayrıntılı ispatları sunulmaktadır. Algoritmanın pratik uygulaması sırasında, ortaya çıkan filtrelerin ayrıklaştırılması gerekmektedir. Sayısal sorunlardan kaçınmak ve algoritmanın çalışmasını sağlamak için gözlemlere sürekli bağlı olan filtreleri tanıtılmaktadır. Karşılık gelen filtreler sağlam (robust) filtreler olarak bilinir. Sürekli zaman filtrelerini doğrudan ayrıklaştırmak yerine, ayrık zaman ayarı altında çalışmamıza yardımcı olan ve aynı zamanda modelin varyans tahminini EM algoritması içinde elde etmemizi sağlayan sağlam filtreleri ayrıklaştırılmaktadır. Kapsamlı bir simülasyon çalışması kullanarak algoritmanın performansını değerlendiriyor ve literatürdeki mevcut alternatiflerle karşılaştırılmıştır. Performans değerlendirmesi, adım $\sim$ boyutu, sapma ve oynaklık parametrelerindeki değişikliklere olan duyarlılığı temel alır. Bu adım, yöntemleri geliştirmek ve teori ile pratik arasında bir bağlantı kurmak için çok önemlidir. Algoritma simüle edilmiş verilerle test edildikten sonra, önerdiğimiz modeli gerçek verilere uygulanmaktadır. Veri seti, 1 Ocak 2002 - 1 Ağustos 2022 dönemini kapsayan S&P500 opsiyon verilerinden alınan zımnî piyasa likidite serisinden oluşmaktadır. Uygulama sonuçları, üç likidite rejiminin piyasa likidite seviyesini tanımlayabildiğini göstermektedir: yüksek, orta ve düşük. Tahmin sonuçları, genel ekonomik ortamın piyasa likiditesi üzerindeki etkisini doğrulamaktadır.

Yayınlar:

- Yerli, C., Kestel, S. (2022). Risk Distribution Among Uncorrelated Risk Factors: Diversified Risk Parity. Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 40(2), 419-439.
- Yerli, C., Ekşi-Altay, Z., Kestel, S. (2023). The On the information content of implied liquidity measure: Evidence from the S&P 500 index options (incelemede).

Adı Soyadı: İlksen Acunalp Erleblebici



İlksen Acunalp Erleblebici, 2005 yılında ODTÜ Matematik Bölümü'nden mezun olmuştur. 2007 yılında ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi anabilim dalında Yüksek Lisansını tamamlamıştır. 2007-2019 yılları arasında TÜBİTAK/BİLGEM/UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) bünyesinde kriptografi alanında yapılan projeler başta olmak üzere yine TÜBİTAK/BİLGEM içerisinde farklı görevlerde bulunmuştur. 2019-2022 yılları arasında HAVELSAN'da Proje İzleme Mühendisi olarak çeşitli projelerde çalışmalarını sürdürmüş olup 2023 yılı itibari ile TÜBİTAK/BİLGEM/YTE (Yazılım Teknolojileri Araştırma Enstitüsü) Kalite ve Strateji Yönetimi Bölümü'nde göreve başlamıştır. Doktora çalışmalarına ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi programında devam etmiş, Doç. Dr. Oğuz Yayla danışmanlığında "Some Results On APN Functions And Weakly Regular Bent Functions Over Finite Fields" başlıklı tezini 2023 yılında tamamlamıştır.

Doktora Tezi Özeti:

Bu tezde, Carlet'in iki değişkenli neredeyse mükemmel lineer olmayan (APN) fonksiyonlarının ve APN kuvvet fonksiyonlarının üzerine yaptığımız çalışmalar sunulmaktadır. 2021'de Calderini ve arkadaşlarının, 2022'de Budaghyan ve arkadaşlarının verdiği yöntemlerden yararlanılarak sırasıyla bazı iki değişkenli APN ailelerinin inşası için gerekli ve yeterli koşullar ve APN kuvvet fonksiyonlarının gösterimi hakkındaki incelemelerimiz sunulmaktadır ve bu araştırma hakkında bazı hesaba dayalı sonuçlar verilmektedir. Diğer taraftan, kriptografik fonksiyonların kodlama teorisindeki uygulamasını çalışıyor ve tek karakteristikli sonlu cisimler üzerinde zayıf düzenli bükük fonksiyonları kullanarak iyi parametrelere sahip birçok doğrusal kod elde ediyoruz.

Yayınlar:

- İ. Acunalp Erleblebici, O. Yayla, A General Version of Carlet's Construction of APN Functions, 27th International Conference on Applications of Computer Algebra, 2022, Gebze, Türkiye.
- İ. Acunalp Erleblebici, A. Sınak, O. Yayla, On the Carlet's Bivariate APN Construction and Representations of Dobbertin Power Function, preprint
- İ. Acunalp Erleblebici, A. Sınak, O. Yayla, Few-weight linear codes based on weakly regular bent functions over finite fields, preprint

Adı Soyadı: Yasemin Yaman Kanmaz



Yasemin Yaman Kanmaz 2008 yılında ODTÜ İktisat bölümünden mezun olmuş ve 2012 yılında yine aynı bölümde yüksek lisans çalışmalarını tamamlamıştır. 2009 yılında Türkiye Cumhuriyet Merkez Bankası İstatistik Genel Müdürlüğü Ödemeler Dengesi Müdürlüğü'nde uzman yardımcısı olarak göreve başlamış ve hala aynı bölümde uzman olarak devam etmektedir. 2017 yılında ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik anabilim dalında doktora çalışmalarına başlamış ve Temmuz 2023 tarihinde Prof. Dr. A. Sevtap Selçuk-Kestel ve Prof. Dr. Ş. Kasırga Yıldırak danışmanlığında "Classification of Imbalanced Credit Data Sets with Borrower-Specific Cost-Sensitive Algorithms" başlıklı tezini tamamlamıştır. Çalışma konularında, Türkiye ve diğer gelişmekte olan ülkelerin ödemeler dengesi finansal hesap alt kalemleri, dış ticaret dengesi ve makro göstergeler arasındaki gecikmeli ve eş zamanlı ilişkilerini açıklayan ekonometrik modeller ve makine öğrenmesi kapsamında büyük verinin sınıflandırılma ve regresyon modelleri yer almaktadır.

Doktora Tezi Özeti :

Dengesiz kredi veri setlerinde eşit olmayan sınıf dağılımları farklı maliyetlere yol açan iki tür yanlış tahmin hatası ile sonuçlanmaktadır. Bunlar, yanlış sınıflandırılan batık krediler için parasal kayıp ve yanlış sınıflandırılan kredisini ödeyecekler için kaçırılan fırsat maliyeti olarak faiz geliridir. Bu çalışma, belirtilen sorunları ele alarak kredi veri setlerinde maliyete duyarlı öğrenme ve dengesiz veri sınıflandırması asimetrisine yönelik borçluya özgü maliyet/risk parametrelerini çözebilen yeni bir yaklaşım önermektedir.

Çalışmanın temel amacı, her kredi başvurusunun verilerinde saklı olan bilgileri ortaya çıkararak risk seviyesini gösteren bir ağırlık oluşturmak ve kayıp fonksiyonlarını bu ağırlık ile güçlendirmek ve çoğunluk sınıfının baskınlığını kırmaktır. Kredi almak için başvuruların temerrüt olasılıkları, risk seviyeleri hakkında değerli bilgiler sağlar. Bu çalışmayla, sınıfların veri büyüklük oranları yerine temerrüt risk seviyelerine dayalı her bir borçluya özgü maliyet /risk parametreleri önerilmektedir. Kredi ödememe olasılıkları, örneklenmiş alt veri kümeleriyle tahmin edilmekte ve bu aşamadan önce, Simüle Edilerek Kuvvetlendirilmiş (Annealing) stokastik süreciyle örneklenmiş alt veri kümelerinin en uygun sınıf oranı belirlenmektedir. Krediye başvuranların borçlarını ödememe olasılıklarını tahmin etmek için, lojistik regresyonlar ve derin öğrenmeye dayalı Grafik Sinir Ağları ve Grafik Dikkat Ağları gibi doğrusal olmayan karmaşık modeller kullanılmaktadır. Üç adet maliyet/risk parametresi, sınıf bazındaki kayıpları yine sınıf bazında toplam risk seviyelerine dayalı eşitleme hedefiyle oluşturulmaktadır.

AdaBoost, XGBoost ve ANN algoritmaları daha sonra bu yeni parametreleri içerecek şekilde değiştirilerek sekiz kredi veri seti üzerinde ampirik analiz gerçekleştirilmiştir. Bu algoritmaların başarısı, özellikle sınıf oranları giderek artan veri kümelerinin kategorizasyonunda daha belirgindir. Karşılaştırmalı analizler, yeni maliyet duyarlı algoritmalarla parasal kayıplardaki azalmanın verilmiş Özgüllük değerlerinde % 33.7'ye ulaşabildiğini göstermektedir.

Katıldığı Konferanslar:

- Imbalances in Foreign Trade and Characteristics of Net Capital Inflows Gaygısız E., Yaman Kanmaz Y. 83rd International Atlantic Economic Conference March 22-25, 2017 Berlin, Germany <https://iaes.confex.com/iaes/83am/webprogram/Paper13365.htm>

Adı Soyadı: Hatice Kübra Güner

Hatice Kübra Güner 2012 yılında Hacettepe Üniversitesi Matematik bölümünden mezun olmuştur. Yüksek lisansını 2015 yılında Prof. Dr. Murat Cenk danışmanlığında ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi programında yapmıştır. Aynı bölümde doktora programına başlamış ve “Uzay-Zor Beyaz Kutu Kriptografisi Üzerine Bir Çalışma” başlıklı teziyle Doç. Dr. Oğuz Yayla ve Dr. Ceyda Mangır danışmanlığında 2023 yılında tamamlamıştır. Araştırma konuları arasında açık anahtarlı kriptografi, beyaz kutu kriptografisi, kriptografik algoritmaların verimliliği ve tersine mühendislik yer almaktadır.

Doktora Tezi Özeti :

Gizli anahtarları kötü niyetli gözlemcilerden korumak, güvenilmeyen ortamlarda kriptografik algoritmalar için büyük bir sorundur. Beyaz kutu kriptografisi, beyaz kutu ayarında anahtarın çıkarılması imkansız hale gelecek şekilde uygun bir yöntemle şifre kodundaki anahtarın saklanması önerir. Anahtar genellikle uygun yöntemlerle karıştırma katmanına gömülür. Bunlardan biri kodlama teknikleri kullanmaktır. Bununla birlikte, birçok kodlama yöntemi cebirsel saldırılara ve yan kanal analizine karşı savunmasızdır. Bir diğeri, cihazdan kolayca çıkarılamayan büyük arama tabloları oluşturan alan sabitliği konseptidir. (M, Z) -uzay sabit algoritmalarında, gizli anahtar, uygun bir blok şifre ile bir ikame kutusu olarak oluşturulan büyük tablolara gömülür. Böylece, beyaz kutu ayarındaki anahtar çıkarma sorunu, kara kutu durumunda bir anahtar kurtarma sorununa dönüşür. (M, Z) -uzay sabit algoritmalarındaki ana sorunlardan biri, beyaz kutu/kara kutu uygulamasının çalışma zamanını hızlandırmaktır. Bu çalışmada, güvenlik boyutunu düşürmeden beyaz kutu algoritmalarının difüzyon katmanını hızlandırmak için hafif bileşenlerin etkinliğinin avantajını kullanmayı amaçlıyoruz. Bu nedenle, NIST Hafif Standardizasyon adaylarının doğrusal katmanını verimlilik ve mevcut uzay sabit şifrelerindeki beyaz kutu ayarlarına uygunluk açısından karşılaştırıyoruz. Algoritmaların performans sonuçları WARX ve SPNbox ile karşılaştırılmıştır. Sonuçlara göre, difüzyon katmanında hafif bileşenlerin kullanılması, beyaz kutu algoritmalarının performansını en az %16 hızlandırıyor. Ek olarak, yan kanal saldırılarına karşı bitslice uygulamasından yararlanmak için daha iyi çalışma zamanı performansına sahip LS tasarımı tabanlı bir beyaz kutu algoritması ve LS tasarımı tabanlı tablo oluşturma yöntemi öneriyoruz. Metodumuzun çalışma zamanı performansını SPNbox algoritması ile karşılaştırdığımızda, beyaz kutu uygulaması için %28 ve kara kutu uygulaması için %27 iyileştirme elde ediyoruz. Aynı zamanda, beyaz kutu ayarında, LS tasarımına dayalı yöntemi 256 bitlik blok boyutuna da uyguluyoruz.

Yayınlar:

- H.K. Güner, C. Mangır, O. Yayla, Performance Improvement of White-Box Algorithms Using Lightweight Components, Algebraic and Combinatorial Methods for Coding and Cryptography, ALCOCRYPT 2023.
- Güner, H.K., Mangır, C., Yayla, O. (2023). Improving Performance in Space Hard Algorithms. In: Dolev, S., Gudes, E., Paillier, P. (eds) Cyber Security, Cryptology, and

Machine Learning. CSCML 2023. Lecture Notes in Computer Science, vol 13914. Springer, Cham. https://doi.org/10.1007/978-3-031-34671-2_28.

- H.K. Güner, C. Mangır, and O. Yayla, White-Box Block Cipher Implementation Based on LS-Design, Cryptology ePrint Archive, Paper 2023/1096, 2023, <https://eprint.iacr.org/2023/1096>.