ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

Uygulamalı Matematik Enstitüsü (UME)

Faaliyet Raporu 2022

Orta Doğu Teknik Üniversitesi
Uygulamalı Matematik Enstitüsü
Nisan 2023

https://iam.metu.edu.tr

Önsöz

Türkiye'deki Matematik alanında ilk disiplinlerarası araştırma kurumu olan Uygulamalı Matematik Enstitüsü (UME), 2022 yılı itibariyle kuruluşunun 20. yılını tamamlamış olmanın gururunu yaşamaktadır. 2022 Yılı Faaliyet Raporunda; Enstitümüz ve Bağlantılı öğretim üyelerimiz ile lisansüstü öğrencilerimiz tarafından gerçekleştirilen akademik etkinlikler ve performans göstergeleri sunulmaktadır.

Diğer üniversiteler ve kuruluşlarda, Orta Doğu Teknik Üniversitesi'nde görev yapan öğretim üyeleri ve uzmanların da katkısıyla eğitim ve araştırma faaliyetlerini gerçekleştiren UME, Matematik temelli araştırma/uygulama alanlarında disiplinlerarası çalışma ortamı oluşturmak, bu alanlarda araştırmaya yönelik aktiviteleri gerçekleştirmek, uluslararası işbirliği olanaklarını hayata geçirmek, ODTÜ-Sanayi/Kamu kuruluşları işbirliğini gerek proje ve ürün geliştirerek, gerekse kısa süreli eğitim/araştırma toplantıları düzenleyerek hayata geçirmek, matematiğin doğayı teknolojik ve ekonomik süreçleri daha iyi anlama yolunda bilim insanlarının ortak dili olduğundan hareketle, yeni uygulanabilir Matematik konularında araştırmacıları bilgilendirmek ve bu amaca yönelik araştırmalar yapmak misyonları çerçevesinde etkinliklerini sürdürerek yirmi yıllık birikim ve tecrübesini yeni alanlar ve açılımlar doğrultusunda geliştirmeyi hedeflemektedir.

Lisansüstü programları ve araştırmaları ile uluslararası düzeyde saygın ve öncü bir araştırma enstitüsü olmayı vizyon olarak belirleyen Uygulamalı Matematik Enstitüsü'nde Aktüerya Bilimleri, Bilimsel Hesaplama, Finansal Matematik ve Kriptografi olmak üzere dört anabilim dalında yüksek eğitim olanağı sunulmaktadır. Enstitümüz, bu faaliyet yılında Üniversitemiz çok disiplinli programları tarafından yönetilen Data and Decision Science lisansüstü eğitim programında Bilgisayar Mühendisliği, Elektrik-Elektronik Mühendisliği, Endüstri Mühendisliği ve İstatistik Bölümleri ile ortak paydaş olarak yer almıştır.

Enstitümüzün 20. Yıldönümünü kutlamak amacıyla, alanlarında uluslararası ve ulusal tanınırlığı olan davetli konuşmacıların yer aldığı bir çalıştay düzenlenmiştir (https://20years-iam.metu.edu.tr). Üniversitemiz yöneticileri, öğretim üyeleri ve öğrencilerimizin geniş bir katılımı ile gerçekleştirilen bu akademik etkinlikte güncel ve gelişmekte olan alanların matematiksel düşünce ve normları ile uygulamaları sunulmuştur. Bu sunumlara ait kayıtlar, konuşmacıların da onayları alınarak Enstitümüz sosyal medya kanalında yayınlanmıştır (@instituteofappliedmathematics).

Disiplinlerarası ve çoklu disiplinlerdeki alanlarda başarılı çalışmalar ve projeler gerçekleştiren UME, birçok araştırma grubuna ev sahipliği yapmaktadır. Applied Cryptography, Blockchain, Post-quantum Cryptography, Algorithmic Trading, Dependent Risks, Longevity & Pension, Uncertainty Quantification başlıkları altında toplanan bu araştırma-çalışma gruplarına ait

çalışma çıktıları Enstitü web sayfamızdaki Yayınlar ve Projeler bölümlerinde detaylı olarak yer almaktadır.

Enstitümüz bünyesinde doktora programına kayıtlı 94 öğrencimizden yaklaşık %14'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 %88,4'ü SCI-E, %2,3 kadarı ise diğer kategorisindeki dergilerde yayınlanmıştır. Uluslararası akademik veri tabanı platformlarından Enstitümüz öğretim ve bağlantılı öğretim üyeleri yayınlarına 2022 yılında yapılan toplam Web of Science (WoS) atıf sayısı 993 olarak gerçekleşmiştir.

Kuruluşundan bugüne 109 doktora, 275 tezli yüksek lisans, 149 tezsiz yüksek lisans olmak üzere toplam 533 mezunu olan Enstitümüz; 2022 yılında 9 doktora, 27 tezli ve 3 tezsiz yüksek lisans öğrencisine diploma vermiştir.

Bunların yanı sıra, 2021-2022 akademik yılı ODTÜ Tez, Yayın ve Ders Performans Ödülleri kapsamında mezunlarımızdan 3 doktora öğrencimiz Tez ayrıca 7 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 ederiz.

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*

* Özgür Ergül (Elektrik ve Elektronik Mühendisliği) yerine Müdür Yardımcısı olarak Doç. Dr. Oğuz Yayla (Uygulamalı Matematik Enstitüsü) 23.03.2022 tarihi itibariyle atanmıştır.

Enstitü Anabilim Dalı Başkanları	Enstitü Yönetim Kurulu
Prof. Dr. A. Sevtap Kestel (Aktüerya Bilimleri)	Prof. Dr. A. Sevtap Kestel (Uygulamalı Matematik Enstitüsü)
Doç. Dr. Önder Türk* (Bilimsel Hesaplama)	Doç. Dr. Önder Türk (Uygulamalı Matematik Enstitüsü)
Prof. Dr. A. Sevtap Kestel ** (Finansal Matematik)	Doç. Dr. Serdar Göktepe*** (İnşaat Mühendisliği)
Doç. Dr. Oğuz Yayla**** (Kriptografi)	Doç. Dr. Seza Danışoğlu (İşletme)
	Prof. Dr. Ferruh Özbudak**** (Matematik)
	Doç. Dr. Oğuz Yayla (Uygulamalı Matematik Enstitüsü)

* Doç. Dr. Hamdullah Yücel 04.02.2022 tarihine kadar Bilimsel Hesaplama EABD Başkanlığı görevini yürütmüştür.

** Prof. Dr. Ali Devin Sezer, 16.03.2022 tarihine kadar Finansal Matematik EABD Başkanlığı görevini yürütmüştür.

*** Dr. Öğr. Üyesi Nil İpek Şirikçi 23.03.2022 ve Prof. Dr. Özgür Ergül 29.08.2022 tarihine kadar Yönetim Kurulu üyeliği yapmışlardır.

**** Prof. Dr. Ferruh Özbudak 15.05.2022 tarihinde Kriptografi EABD Başkanlığı görevinden ayrılmış olup 24.08.2022 tarihinden itibaren yönetim kurulu üyesi olarak görev yapmıştır.

Enstitü Personeli

Öğretim Üyeleri	Araştırma Görevlileri	
Murat Cenk, Prof. Dr.	Gülçin Akarsu	Oğuz Koç
A. Sevtap Kestel, Prof. Dr.	Pelin Çiloğlu	Özenç Murat Mert
Ali Devin Sezer, Prof. Dr.	Tugay Dağlı	Meral Şimşek
Önder Türk, Doç. Dr.	Esra Günsay	Özge Tekin*
Ömür Uğur, Prof. Dr.	Burcu Ecem Karakaş	Sıtkı Can Toraman*
Oğuz Yayla, Doç. Dr.	Zeynelabidin Karakaş (35. madde)	Cem Yavrum
Hamdullah Yücel, Doç. Dr.	Kübra Kaytancı	
	Mustafa Kütük	Hasan Bartu Yünüak

Öğretim Görevlisi	DOSAP
İrem Keskinkurt Paksoy	Cansu Betin Onur*
	Buket Özkaya
	Hüsnü Yıldız*

İdari Personel	
Saffet Aykın (İdari Amir)	Ebru Gündoğdu (Sekreter)
Serkan Demiröz (Sekreter)	Muharrem Kayabel (Görevli)
Nejla Erdoğdu (Enstitü Sekreteri)	Cafer Topal (Görevli)

Ömer Ergüven (Bilgisayar İşletmeni)

*2022 yılı içinde Enstitüdeki görevinden ayrılmıştır.

Bağlantılı Öğretim Üyeleri - ODTÜ

Matematik	Songül Kaya Merdan, Prof. Dr. Ferruh Özbudak, Prof. Dr. Muhiddin Uğuz, Dr.
İstatistik	B. Burçak Başbuğ Erkan, Doç. Dr. Özlem İlk Dağ, Prof. Dr. Fulya Gökalp Yavuz, Dr Vilda Purutçuoğlu Gazi, Prof. Dr. Ceren Vardar Acar, Doç. Dr. Ceylan Yozgatlıgil, Prof. Dr.
Bilgisayar Mühendisliği	Emre Akbaş, Dr. Pelin Angın, Doç. Dr. Şeyda Ertekin Bolelli, Doç. Dr. Murat Manguoğlu, Prof. Dr. M. Halit S. Oğuztüzün, Prof. Dr. Ertan Onur, Prof. Dr.
Elektrik Elektronik Mühendisliği	Özgür Ergül, Prof. Dr. Yeşim Serinağaoğlu Doğrusöz, Doç. Dr.
Fizik	Emre Yüce, Doç. Dr.
Havacılık ve Uzay Mühendisliği	Sinan Eyi, Prof. Dr. Ercan Gürses, Doç. Dr.
İktisat	Esma Gaygısız-Lajunen, Doç. Dr. Nil İpek Şirikçi, Dr. Atak Alev, Dr.
İnşaat Mühendisliği	Serdar Göktepe, Doç. Dr.
İşletme	Hande Ayaydın Hacıömeroğlu, Dr. Seza Danışoğlu, Doç. Dr. Z. Nuray Güner, Prof. Dr. İlkay Şendeniz Yüncü, Dr. Adil Oran, Doç. Dr.
Emekli Öğretim Üyeleri	Ersan Akyıldız, Prof. Dr. Aydın Aytuna, Prof. Dr. Selçuk Bayın, Prof. Dr. Ali Doğanaksoy, Doç. Dr.

	İ. Yurdahan Güler, Prof. Dr. Azize Hayfavi, Doç. Dr. Bülent Karasözen, Prof. Dr. Münevver Tezer-Sezgin, Prof. Dr.

Bağlantılı Öğretim Üyeleri - Diğer Üniversite ve Kurumlar

Ankara Üniversitesi	Furkan Başer, Doç. Dr. Fatih Tank, Prof. Dr. Murat Osmanoğlu, Dr.
ARÇELİK A.Ş.	Songül Bayraktar, Dr.
Atılım Üniversitesi	Ümit Aksoy, Prof. Dr. Burcu Gülmez Temür, Doç. Dr. Fatih Sulak, Doç. Dr.
Başkent Üniversitesi	Özge Sezgin-Alp, Doç. Dr.
Cumhurbaşkanlığı	Mehmet Uzunkaya, Dr. Ceyda Mangır, Dr.
Başkent Üniversitesi	Sinem Kozpınar, Dr. Özge Sezgin Alp, Doç. Dr.
Bilkent Üniversitesi	Çağın Ararat, Dr. Firdevs Ulus, Dr.
Boğaziçi Üniversitesi	Könül Bayramoğlu Kavlak, Doç. Dr.
Çankaya Üniversitesi	Özlem Türker Bayrak, Doç. Dr. A. Nurdan Saran Buz, Dr. Özlem Defterli, Dr.
Dokuz Eylül Üniversitesi	Erdem Alkım, Dr.
Hacettepe Üniversitesi	Başak Bulut Karageyik, Dr. Uğur Karabey, 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 Balıkçıoğlu, Dr.
İzmir Yüksek Teknoloji Üniversitesi	Cüneyt Bazlamaçcı, Prof. Dr.
Karabük Üniversitesi	Eda Tekin, Dr.

	Oytun Haçarız, Dr.
Kahramanmaraş Sütçü İmam Üniversitesi	Bilgi Yılmaz, 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.
Silent Protocol	İsa Sertkaya, Dr.
Sinop Üniversitesi	Murat Uzunca, Doç. Dr.
Süleyman Demirel Üniversitesi	Barış Bülent Kırlar, Doç. Dr.
Technical University of Kaiserslautern	Ralf Korn, Prof. Dr. Bükre Yıldırım Külekci, Dr. Bilgi Yılmaz, 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.
Türk Standartları Enstitüsü	Ezgi Avcı, Dr.

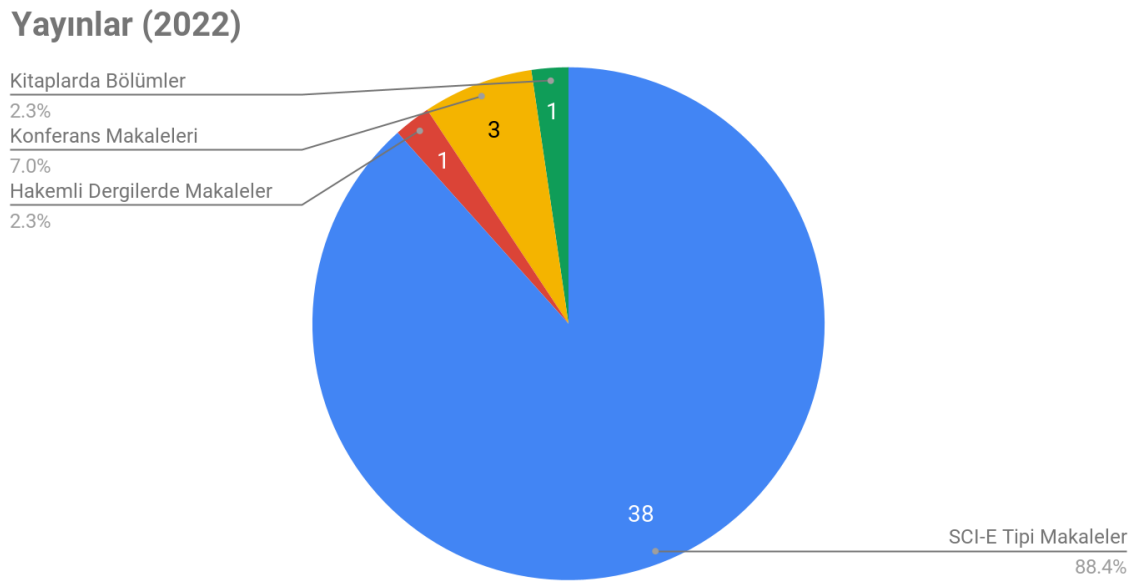
Vienna Uni. of Economics and Business	Zehra Ekşi-Altay, Doç. Dr.
Western University	Rogemar S. Mamon, Prof. Dr.
Diğer Kuruluşlar	Songül Bayraktar, Dr. Tayfun Çimen, Dr. Öznur Mut Sağdıçoğlu, Dr.

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.

SCI-E Tipi yayınların 2021 yılına göre artış gösterdiği belirlenerek, bu yayınların çoğunluğunun WoS tanımlı Q1 ve Q2 kategorisinde yer aldığı gözlemlenmiştir. 2022 yılında Enstitümüz öğretim ve bağlantılı üyeleri tarafından yapılan yayınların %60 kadarı tez öğrencileri ve mezunlarımızla ortak yapılan çalışmalardan oluşmaktadır.



Bunun yanı sıra, 2022 yılı ilk çeyreği yayın sayılarına bakıldığında %88,4 SCI-E tipi dergilerde yayınlanan çalışmaların ağırlıklı olarak tez öğrencileri ile yapılan araştırmalara ait olduğu belirlenmiştir.

SCI-E Dergilerde Makaleler

Aşağıda SCI-E (A ve B-Tipi) Dergilerdeki Uygulamalı Matematik Enstitüsü adresli yayınların listesine yer verilmiş olup, 2023 yılında basım aşamasında olan yayınlar ayrı bir bölümde yer almaktadır.

[1]	Allahmadi, A., AlKenani, A., Hijazi, R., Muthana, N., Özbudak, F., Sole, P., New constructions of entanglement-assisted quantum codes, Cryptography and Communications, 14 5–37, 2022, https://doi.org/10.29233/sdufeffd.1053097
[2]	Aydoğan, B., Uğur, Ö., Aksoy, Ü., Optimal Limit Order Book Trading Strategies with Stochastic Volatility in the Underlying Asset, Computational Economics, 1-36, 2022, https://doi.org/10.1007/s10614-022-10272-4
[3]	Basoglu-Kabran, F., Sezer, A. D., Approximation of the exit probability of a stable Markov modulated constrained random walk, Annals of Operations Research, 310(2) 431-475, 2022, 10.1007/s10479-020-03693-7
[4]	Bozkaya, C., Türk, Ö., Chebyshev spectral collocation method for MHD duct flow under slip condition, Progress in Computational Fluid Dynamics, 22(2) , 118-129, 2022, 10.1504/pcfd.2022.121863
[5]	Cengizci, S., Uğur, Ö., Natesan, S., SUPG-YZ beta computation of chemically reactive convection-dominated nonlinear models, International Journal of Computer Mathematics, 100(2) 283-303, 2022, 10.1080/00207160.2022.2114794
[6]	Cenk, M., Karakaş, B. E., Orhon Kılıç, N. G., Kuantum Sonrasına Eliptik Eğri Kriptografi ve Uygulamaları, Siber Güvenlik ve Savunma Kitap Serisi 6: Siber Güvenlik Ontolojisi, Tehditler ve Çözümler 395-456 2022
[7]	Choi, W. H., Güneri, C., Kim, J. L., Özbudak, F., Optimal Binary Linear Complementary Pairs of Codes, Cryptography and Communications, 2022, https://doi.org/10.1007/s12095-022-00612-4
[8]	Codina, R., Türk, Ö., Modal analysis of elastic vibrations of incompressible materials using a pressure-stabilized finite element method, Finite Elements in Analysis & Design, 206(103760), 2022, 10.1016/j.finel.2022.103760
[9]	Coşkun, B. N., Yayla, O., Yıldız, H., Application of blockchain technology and internet of things in uroflowmetry for clinical trials: A pilot test, European Urology, 81 S152-S154, 2022, 10.1016/s0302-2838(22)00190-7

[10]	Çakıroğlu, Y., Yayla, O., A new lower bound on the family complexity of Legendre sequences, Applicable Algebra in Engineering, Communication and Computing, 33 (2) 173-192, 2022, 0.1007/s00200-020-00442-y
[11]	Çakıroğlu, Y., Yayla, O., Yilmaz, E.S., The number of irreducible polynomials over finite fields with vanishing trace and reciprocal trace, Designs, Codes and Cryptography, 90 (10), 2407-2417, 2022, 10.1007/s10623-022-01088-2
[12]	Çiloğlu, P. , Yücel, H., Stochastic Discontinuous Galerkin Methods with Low-Rank Solvers for Convection Diffusion Equations, Applied Numerical Mathematics, 172 157-185, 2022, https://doi.org/10.1016/j.apnum.2021.10.007
[13]	Fellah, N., Guenda, K., Özbudak, F., Seneviratne, P., Construction of self dual codes from graphs, Applicable Algebra in Engineering, Communication and Computing, 2022, https://doi.org/10.1007/s00200-022-00567-2
[14]	Gaygisiz E., Karasan A., Hekimoglu A., Investigating the effects of illiquidity on credit risks via new liquidity augmented stochastic volatility jump diffusion model, Optimization, 71(8) 2421-2449, 2022, 10.1080/02331934.2021.2013842
[15]	Karasözen, B., Mülayim, G., Uzunca, M., Nonintrusive model order reduction for cross-diffusion systems, Communications in Nonlinear Science and Numerical Simulation, 115 106734, 2022, https://doi.org/10.1016/j.cnsns.2022.106734
[16]	Karasözen, B., Yıldız, S., Uzunca, M., Energy preserving reduced-order modeling of the rotating thermal shallow water equation, Physics of Fluids, 34(5) 056603, 2022, https://doi.org/10.1063/5.0091678
[17]	Karasözen, B., Yıldız, S., Uzunca, M., Intrusive and data-driven reduced order modelling of the rotating thermal shallow water equation, Applied Mathematics and Computation, 421 126924, 2022, https://doi.org/10.1016/j.amc.2022.126924
[18]	Köse, Ş., Özbudak, F., Factorization of some polynomials over finite local commutative rings and applications to certain self-dual and LCD codes, Cryptography and Communications, 14 933-948, 2022, https://doi.org/10.1007/s12095-022-00557-8
[19]	Mert, Ö.M., Selçuk-Kestel, A.S., Optimal premium allocation under stop-loss insurance using exposure curves, Hacettepe Journal of Mathematics and Statistics, 51(1), 288-307 2022, 10.15672/hujms.889619
[20]	Mesnager, S., Özbudak, F., Boomerang uniformity of power permutations and algebraic curves over F_2^n, Advances in Geometry, 23(1) 107-134, 2022, https://doi.org/10.1515/advgeom-2022-0026

[21]	Ozmen, A., Zinchenko, Y., Weber, G.W. Robust multivariate adaptive regression splines under cross-polytope uncertainty: an application in a natural gas market, Annals of Operations Research, Early Access, 2022, 10.1007/s10479-022-04993-w
[22]	Özbudak, F., Gülmez Temür, B., Classification of permutation polynomials of the form x^3g(x^(q−1)) of F_(q^2) where g(x)=x^3+bx+c and b,c∈ (F_q^)*, Designs, Codes and Cryptography, 90 1537–1556, 2022
[23]	Özbudak, F., Gülmez Temür, B. Classification of some quadrinomials over finite fields of odd characteristic, Finite Fields and Their Applications, 87 102158, 2022, https://doi.org/10.1016/j.ffa.2022.102158
[24]	Özbudak, F., Pelen, R. M., Two or Three Weight Linear Codes From Non-Weakly Regular Bent Functions, IEEE Transactions on Information Theory, 68 (5), 2022, 10.1109/TIT.2022.3145337
[25]	Özbudak, F., Pelen, R. M., Imprimitive symmetric association schemes of classes 5 and 6 arising from ternary non-weakly regular bent functions, Journal of Algebraic Combinatorics, 56 635-658, 2022, https://doi.org/10.1007/s10801-022-01126-1
[26]	Paksoy, İ., Cenk, M., Faster NTRU on ARM Cortex-M4 With TMVP-Based Multiplication, IEEE Transactions on Circuits and Systems I: Regular Papers, 69(10) 4083-4092, 2022, 10.1109/tcsi.2022.3191111
[27]	Samuel, S. A., Popier, A., Sezer, A. D., Continuity problem for singular BSDE with random ter-minal time, ALEA-Latin American Journal of Probability and Mathematical Statistics, 19 1185-1220, 2022, https://doi.org/10.30757/alea.v19-49
[28]	Shi, M., Helleseth, T., Özbudak, F., Sole, P., Covering Radius of Melas Codes, IEEE Transactions on Information Theory, 68(7), 2022, 10.1109/TIT.2022.3152092
[29]	Shi, M., Liu, N., Özbudak, F., Sole, P. Additive cyclic complementary dual codes over F_4, Finite Fields and Their Applications, 83, 102087, 2022, https://doi.org/10.1016/j.ffa.2022.102087
[30]	Yeniaras, E., Cenk, M. Faster characteristic three polynomial multiplication and its application to NTRU Prime decapsulation, Journal of Cryptographic Engineering, 12(3) 329-348, 2022, 10.1007/s13389-021-00282-7
[31]	Yılmaz, B., Hekimoglu, A., Selçuk-Kestel, A.S., Default and prepayment options pricing and default probability valuation under VG model Journal of Computational and Applied Mathematics, 399, 2022, 10.1016/j.cam.2021.113724
[32]	Yılmaz, B., Korn, R., Selçuk-Kestel, A.S., The Impact of Large Investors on the Portfolio Optimization of Single-Family Houses in Housing Markets, Computational Economics, 1(1) 1-

	20, 2022, 10.1007/s10614-022-10233-x
[33]	Zhu, H., Shi, M., Özbudak, F., Complete b-symbol weight distribution of some irreducible cyclic codes, Designs, Codes and Cryptography ,90 1113–1125, 2022

Diğer Uluslararası Hakemli Dergilerde Makaleler

Aşağıda diğer Uluslararası Hakemli Dergilerdeki Uygulamalı Matematik Enstitüsü adresli yayınların listesine yer verilmiş olup, 2023 yılında basım aşamasında olan yayınlar yer almamaktadır.

[1]	Gölbası, U., Yılmaz, B., Selçuk-Kestel, A.S., Optimal Capacity Allocation in accordance with Renewable Energy Sources: The US Electricity Market, International Journal of Ambient Energy, 1(1) 1-20, 2022, 10.1080/01430750.2022.2120912
[2]	Selcuk, M., Koç, O., Selçuk-Kestel, A.S., The prediction power of machine learning on estimating the sepsis mortality in the intensive care unit, Informatics in Medicine Unlocked, 28, 2022, 10.1016/j.imu.2022.100861
[3]	Yavrum, C., Selçuk-Kestel, A.S., Impact of Outlier-Adjusted Lee–Carter Model on the Valuation of Life Annuities, Contributions to Economics, 495-513, 2022, 10.1007/978-3-030-85254-2_30
[4]	Yerli, Ç., Selçuk-Kestel, A.S. Risk Distribution Among Uncorrelated Risk Factors: Diversified Risk Parity, Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 40(2) 419-439, 2022, 10.17065/huniibf.880072

Ulusal Kitap Bölümü

[1]	Cenk, M., Kılıç, N. G. O., Yılmaz, B. E., Kuantum Öncesinden Kuantum Sonrasına Eliptik Eğri Kriptografi ve Uygulamaları, BGD Siber Güvenlik ve Savunma Kitap Serisi 6, Nobel Akademik Yayincilik, 2022.

Kabul Edilmiş, Basım Aşamasındaki Makaleler

Aşağıda Uygulamalı Matematik Enstitüsü adresli 2021 yılında kabul edilip basım aşamasında olan ve 2022 yılı ilk çeyreğinde basılan yayınlara yer verilmiştir.

[1]	Çiloğlu, P., Yücel, H., Stochastic Discontinuous Galerkin Methods with Low–Rank Solvers for Convection Diffusion Equations, Applied Numerical Mathematics, 172, pp. 157-185, 2022. DOI:10.1016/j.apnum.2021.10.007
[2]	Mert, Ö.M., Selcuk-Kestel, A.S., Optimal premium allocation under stop-loss insurance using exposure curves, Hacettepe Journal of Mathematics and Statistics, 2022. DOI:10.15672/hujms.889619
[3]	Selcuk, M., Koc, O., Selcuk-Kestel, A. S., The prediction power of machine learning on estimating the sepsis mortality in the intensive care unit, Informatics in Medicine Unlocked, 2022. DOI:10.1016/j.imu.2022.100861
[4]	Yavrum, C. Selcuk-Kestel, A. S., Impact of Outlier-Adjusted Lee–Carter Model on the Valuation of Life Annuities, Advances in Econometrics, Operational Research, Data Science and Actuarial Studies. Springer, 2022. DOI:10.1007/978-3-030-85254-2_30
[5]	Yilmaz, B., Korn, R., Selcuk-Kestel A. S., The Impact of Large Investors on the Portfolio Optimization of Single-Family Houses in Housing Markets, Computational Economics, 2022. DOI:10.1007/s10614-022-10233-x

Konferans ve Çalıştay Katılımları

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

[1]	Aksoy B., Cenk, M., Analysis of Block Recombination and Lazy Interpolation Methods and Their Applications to Saber, 15th International Conference on Information Security and Cryptography, ISCTURKEY 2022, Ankara, Turkey, 19 - 20 Ekim 2022
[2]	Aydoğan, B., Uğur, Ö., Aksoy, Ü., Optimal Market Making with Mean-Reversion and Stochastic Volatility Price Process Stochastics Numerics and Statistical Learning: Theory and Applications Workshop, KAUST, Suudi Arabistan, 15-28 Mayıs, 2022

[3]	Boffi, D., Codina, R., Türk, Ö., Approximatıon of the Maxwell Eigenvalue Problem by a Residual Based Stabilized Finite Element Method, Computational Methods in Applied Mathematics (CMAM 2022), Viyana, Avusturya, 29 Ağustos - 2 Eylül, 2022
[4]	Boztaş, S., Özbudak, F., Tekin, E., New Correlations of m-sequences over the finite field F_4 compatible with a new bijection to Z_4, 10th International Workshop on Signal Design and Its Applications in Communications, Çevrim içi, 1-5 Ağustos 2022
[5]	Çelik, M., Uğur, Ö., Eyi, S., Numerical Modeling of Hypersonic Air and Carbon Dioxide Flows in Thermochemical Non-Equilibrium with SU2-NEMO Solver, The 2nd International Conference on Flight Vehicles, Aerothermodynamics and Re-entry Missions Engineering (FAR), Heilbronn, Almanya, 19-22 Haziran, 2022
[6]	Çiloğlu, P. , Yücel, H., Stochastic Discontinuous Galerkin Methods for Robust Deterministic Optimal Control, The SFB 1294 Spring School 2022, Schorfheide (Brandenburg), Almanya, 21-25 Mart, 2022
[7]	Çiloğlu, P. , Yücel, H., Solving Optimal Control Problems Containing Uncertain Coefficients with Stochastic Discontinuous Galerkin Methods, 17th Copper Mountain Conference On Iterative Methods, Çevrim içi, 4-8 Nisan, 2022
[8]	Çiloğlu, P. , Yücel, H., Stochastic Discontinuous Galerkin Methods for Robust Deterministic Control of Convection Diffusion Equations with Uncertain Coefficients, Hybrid: SIAM Conference on Uncertainty Quantification (UQ22), Atlanta, Georgia, ABD,12-15 Nisan, 2022
[9]	Çiloğlu, P. , Yücel, H., Solving Optimal Control Problems Containing Uncertainty, Computational Methods in Applied Mathematics (CMAM 2022), Viyana, Avusturya, 29 Ağustos - 2 Eylül, 2022
[10]	Güneri, C., Özbudak, F., Sayıcı, S., On Subfield Subcodes Obtained from Restricted Evaluation Codes, WCC 2022: The Twelfth International Workshop on Coding and Cryptography, Çevrim içi, 7-11 Mart 2022
[11]	İrimağzı, C., Özbudak, F., On Two Applications of Polynomials x^k−cx−d over Finite Fields and More, International Workshop on the Arithmetic Finite Fields, 29 Ağustos - 2 Eylül 2022
[12]	Kara, G., Yayla, O., Gröbner Basis Attack on STARK-Friendly Symmetric-Key Primitives: JARVIS, MiMC and GMiMCerf 15th International Conference on Information Security and Cryptography (ISCTURKEY), Ankara, Türkiye, 19-20 Ekim, 2022

[13]	Özbudak, F. , Kaytancı, K., The c-Differential Uniformity of the Perturbed Inverse Function via a Trace Function Tr$\big(\frac{x^2}{x+1}\big)$, The 7th International Workshop on Boolean Functions and their Applications (BFA), Balestrand, Norveç, 11-16 Eylül 2022
[14]	Yeniaras, E., Cenk, M., Improved Polynomial Multiplication Algorithms over Characteristic Three Fields and Applications to NTRU Prime, Innovative Security Solutions for Information Technology and Communications, SecITC2021, 13 Ekim 2022
[15]	Yıldırım Külekci, B., Korn, R., Selçuk-Kestel, A. S., Optimal Dynamic Ruin Probabilities for Heavy-Tailed Losses Under Reinsurance Strategies, 25th International Congress on Insurance: Mathematics and Economics (IME), Çevrim içi, 12–15 Temmuz, 2022
[16]	Yücel, H., Solving PDE–Constrained Optimization Problems Containing Random Coefficients Cost Action Mat-Dyn-Net WG3+WG5 Meeting, Namur, Belçika, 18-20 Mayıs, 2022

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 2022 yılında yapılan Bilimsel Etkinliklere yer verilmiştir.

Genel Seminer ve Kolokyum

[1]	Constantinescu, Corina (University of Liverpool-IFAM, UK); 15 Mart 2022 tarihinde 'Managing the Double-Debt Problem in the Mortgage Markets' başlıklı semineri vermiştir.
[2]	Zafeirakopoulos, Zafeirakis (Gebze Technical University, Institute of Information Technologies, Türkiye); 05 Nisan 2022 tarihinde 'Using Polyhedral Geometry for Integer Linear Programming' başlıklı semineri vermiştir.
[3]	Kaya, Kamer (Sabancı University, Computer Science and Engineering, Türkiye); 12 Nisan 2022 tarihinde 'Computing and Approximating Sparse Matrix Permanents in Parallel' başlıklı semineri vermiştir.
[4]	Rainer, Martin (Risk Consultant, Germany); 19 Nisan 2022 tarihinde 'Relative Pricing: From Interest-Based Discounting to Economy-Adapted Numeraires' başlıklı semineri vermiştir.

[5]	Süli, Endre (Mathematical Institute, University of Oxford, UK); 17 Mayıs 2022 tarihinde 'Discrete De Giorgi-Nash-Moser Theory and the Finite Element Approximation of Chemically Reacting Fluids' başlıklı semineri vermiştir.
[6]	Kolkiewicz, Adam (Department of Statistics and Actuarial Science University of Waterloo, Waterloo, Canada); 24 Mayıs 2022 tarihinde 'Efficient Methods of Hedging of Path-Dependent Options' başlıklı semineri vermiştir.
[7]	Chen, An (University of Ulm, Institute of Insurance Science, Germany); 31 Mayıs 2022 tarihinde 'Non-Concave Optimization Under Risk Constraints' başlıklı semineri vermiştir.
[8]	Potapov, Vladimir (Novosibirsk State University, Mechanics and Mathematics Department, Russia); 18 Ekim 2022 tarihinde 'Constructions of Bent Functions and Their Number' başlıklı semineri vermiştir.
[9]	Araya, Felipe Lepe (Department of Mathematics, Universidad del Bio-Bio, Concepcion, Chile); 25 Ekim 2022 tarihinde 'Mixed Formulations and FEM for Eigenvalue Problems in Fluid and Solid Mechanics' başlıklı semineri vermiştir.
[10]	Eryılmaz, Serkan (Atılım University, Department of Industrial Engineering); 15 Kasım 2022 tarihinde 'Optimal Age Replacement Policies for Single Unit and Parallel Systems with Discrete Lifetimes' başlıklı semineri vermiştir.
[11]	Sole, Patrick (CNRS, Aix-Marseille University, Centrale Marseille, Marseilles, France); 22 Kasım 2022 tarihinde 'Type IV Codes Over Non-Unitary Rings' başlıklı semineri vermiştir.
[12]	Ciğercioğlu, Ender (Department of Mechanical Engineering, METU); 20 Aralık 2022 tarihinde 'Periodic Forced Response Prediction of Nonlinear Structures' başlıklı semineri vermiştir.

SIAM Student Chapter Seminerleri

[1]	Halil Kolbaşı, Aktüerlik Üzerine, 07 Haziran 2022 (Actuary Country Manager, Milliman Türkiye)
[2]	Can Eriş, Blockchain Tabanlı Dijital Varlıkların Saklanması, 13 Aralık 2022 (Software Developer, XYZ Technology Türkiye)
[3]	Gerhard Wilhelm Weber, Applications of Regime Switching Models via Stochastic Optimal Control, 27 Aralık 2022 (Poznan University of Technology, Poland)

Kısa Süreli Ziyaretler

Gelen Ziyaretçiler

[1]	Codina, Ramon (Universitat Politecnica de Catalunya-Spain); 4 Kasım 2022 tarihinde 'Hybrid Intrusive/ML-based Reduced Order Model for the Optimisation of Aerodynamic Profiles' başlıklı semineri vermiştir.
[2]	Constantinescu, Corina (University of Liverpool-IFAM, UK); 4 Kasım 2022 tarihinde 'Subsidizing Inclusive Insurance to Reduce Impoverishment' başlıklı semineri vermiştir.
[3]	Ekşi-Altay, Zehra (Institute for Statistic and Mathematics, WU Vienna, Austria); 4 Kasım 2022 tarihinde 'Mean-Reversion and Momentum Trading under Partial Information' başlıklı semineri vermiştir.
[4]	Zajac, Michal (Nethermind); 4 Kasım 2022 tarihinde 'A Short Introduction to zkSNARKs: Recent Results and Open Problems' başlıklı semineri vermiştir.
[5]	Atak, Alev (METU, Department of Economics); 4 Kasım 2022 tarihinde 'Information Disclosure and Financial Sentiment Index using a Machine Learning Approach' başlıklı semineri vermiştir.
[6]	Sulak, Fatih (Atılım Üniversitesi, Department of Mathematics); 4 Kasım 2022 tarihinde 'Randomness in Cryptography' başlıklı semineri vermiştir.
[7]	Karasan, Abdullah (UMBC and TFI TAB); 4 Kasım 2022 tarihinde 'Factor Analysis through SEC Announcements: A Machine Learning Approach' başlıklı semineri vermiştir.
[8]	Gürkan Balıkçıoğlu, Pınar (INTERPROBE Information Technologies); 4 Kasım 2022 tarihinde 'Dealing with Real Life Use Cases of Cryptography' başlıklı semineri vermiştir.
[9]	Koçak, Neşe (ASELSAN A.Ş.); 4 Kasım 2022 tarihinde 'Challenges in Post-Quantum Cryptography' başlıklı semineri vermiştir.
[10]	Demir, Mert (Adendum Actuarial Consultancy, Managing Partner); 4 Kasım 2022 tarihinde 'An Alternative Approach to the Mean-Variance Markowitz Model' başlıklı semineri vermiştir.
[11]	Ölmez, Oktay (LEad Research Scientist, Algorithms, RED, Afiniti); 4 Kasım 2022 tarihinde 'Moving from Academia to Industry' başlıklı semineri vermiştir.

[12]	Çetinkaya, Şirzat (Director, Sompo Insurance, President of Turkish Actuarial Society); 4 Kasım 2022 tarihinde 'New Technology Age for Insurance Industry' başlıklı semineri vermiştir.

Giden Mensuplarımız

[1]	Murat Cenk; 'Kuantum Sonrası Kriptografi' üzerine araştırma yapmak üzere 25 Ocak-21 Mart 2022 tarihleri arasında 'Waterloo University, Canada' ziyaretinde bulunmuştur.
[2]	Oğuz Yayla; 'TÜBİTAK 2204A 53. Lise Öğrencileri Araştırma Projeleri Yarışması Jüri Üyeliği yapmak üzere 15 Mart 2022 tarihinde Samsun' ziyaretinde bulunmuştur.
[3]	Pelin Çiloğlu; 'The Annual SFB Spring School 2022 toplantısına katılmak ve poster sunumu yapmak üzere 20-26 Mart 2022 tarihleri arasında Döllnsee/Almanya' ziyaretinde bulunmuştur.
[4]	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.
[5]	Oğuz Yayla; 'Symbolic Computation Istanbul Meetings adlı toplantıya bildirili katılmak üzere 15 Nisan 2022 tarihinde İstanbul' ziyaretinde bulunmuştur.
[6]	A. Sevtap Kestel; 'Erasmus+ Mobility Agreement Staff Mobility for Teaching' adlı seminere katılmak üzere 8-14 Mayıs 2022 tarihleri arasında Kaiserslautern Technical University, Almanya ziyaretinde bulunmuştur.
[7]	Hamdullah Yücel; 'Mat-Dyn-Net WG3+WG5 Meeting - Cost Action CA18232 adlı toplantıya bildirili katılmak üzere 17-21 Mayıs 2022 tarihinde Namur/Belçika' ziyaretinde bulunmuştur.
[8]	Oğuz Yayla; 'SuSAAN-Summer School on Applied Arithmetic adlı yaz okuluna eğitim vermek üzere 6-17 Haziran 2022 tarihinde İzmir' ziyaretinde bulunmuştur.
[9]	Gülçin Akarsu Şengöz; '33rd International Summer School of the Swiss Association of Actuaries 2022 adlı yaz okuluna katılmak üzere 13-20 Ağustos 2022 tarihinde Lausanne/İsviçre' ziyaretinde bulunmuştur.
[10]	Hamdullah Yücel; '9th International Conference on Computational Methods in Applied Mathematics (CMAM 2022) adlı konferansa bildirili katılmak üzere 28

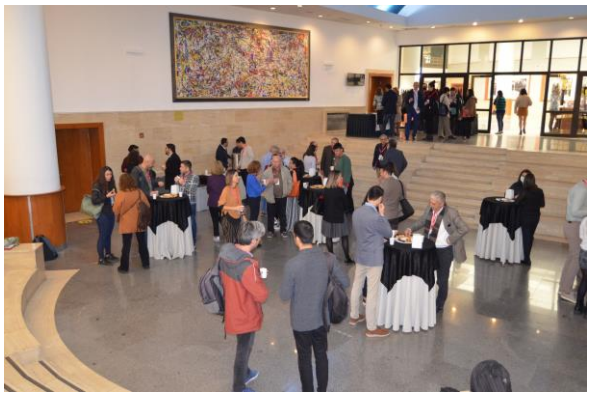
	Ağustos-2 Eylül 2022 tarihinde Viyana/Avusturya' ziyaretinde bulunmuştur.
[11]	Önder Türk; '9th International Conference on Computational Methods in Applied Mathematics (CMAM 2022) adlı konferansa bildirili katılmak üzere 28 Ağustos-3 Eylül 2022 tarihinde Viyana/Avusturya' ziyaretinde bulunmuştur.
[12]	Oğuz Yayla; 'Intermediate and Advanced Course on Post-Quantum Cryptography adlı etkinliğe bildirili katılmak üzere 6-11 Eylül 2022 tarihinde Bakü/Azerbaycan' ziyaretinde bulunmuştur.
[13]	Pelin Çiloğlu; 'Summer School-Uncertainty, Adaptivity, and Machine Learning adlı yaz okuluna katılmak üzere 11-15 Eylül 2022 tarihinde Augsburg/Almanya' ziyaretinde bulunmuştur.
[14]	Meral Şimşek; 'Markov Additive Processes konulu akademik çalışma yapmak üzere 14-23 Eylül 2022 tarihinde Wroclaw/Polonya' ziyaretinde bulunmuştur.
[15]	Murat Cenk; 'Kuantum Sonrası Kriptografi' üzerine araştırma yapmak üzere 5 Ağustos-4 Ekim 2022 tarihleri arasında 'Waterloo University, Canada' ziyaretinde bulunmuştur.
[16]	A. Sevtap Kestel; 'Aktüeryal Değerlendirme ve İş Akışı Konferansı' üzerine seminerler vermek üzere 17-18 Kasım 2022 tarihleri arasında 'Karabük Üniversitesi, Karabük' ziyaretinde bulunmuştur.
[17]	A. Sevtap Kestel; 'The LEAD2 Final Conference and Academic Leaders Forum' toplantısı & Avrupa ve Çin Halk Cumhuriyeti Üniversiteleri ile Erasmus+ İş Birlikleri görüşmeleri yapmak üzere 27-30 Kasım 2022 tarihleri arasında 'Vrije University, Brüksel,' ziyaretinde bulunmuştur.
[18]	A. Sevtap Kestel; 'Finansal Matematik ve Aktüerya Araştırma grubu-Matematik Bölümü'nde seminerler vermek ve ileriye dönük ortak araştırma planları yapmak üzere 14-17 Aralık 2022 tarihleri arasında Erasmus Teaching Mobility çerçevesinde 'Kaiserslautern Technical University, Almanya' ziyaretinde bulunmuştur.

UME 20. Yıl Çalıştayı

Orta Doğu Teknik Üniversitesi (ODTÜ) Uygulamalı Matematik Enstitüsü'nün (UME) kuruluşunun 20. yılı, 4 Kasım 2022 tarihinde ODTÜ Kültür Kongre Merkezi'nde gerçekleştirilen özel bir çalıştay ile kutlanmıştır. Çalıştay, Uygulamalı Matematik disiplinlerindeki güncel yönelimleri sunmak, diğer disiplinlerde ve endüstride uygulanabilirliğini göstermek için bir platform oluşturulmasına yardımcı olmuştur. UME'deki Aktüerya Bilimleri, Bilimsel Hesaplama, Finansal Matematik ve Kriptografi olmak üzere dört lisansüstü programın içeriği doğrultusunda, davetli konuşmacılar ve katılımcılar aracılığıyla deneyim, ihtiyaçlar ve geleceğe yönelik eğilimler tartışılmıştır. Disiplinlerarası alanlar ve geniş çerçevede katılımcı profili ile gerçekleşen çalıştayda Uygulamalı Matematik alanındaki son gelişmeler ve yeni açılımlar aktarılmıştır. Enstitü bünyesinde yer alan dört programı temsilen ulusal ve uluslararası tanınırlığı olan akademik ve endüstri uzmanları tarafından yapılan konuşmalar, etkileşimli tartışmalarla donatılarak izleyicilere sunulmuştur. Enstitü'nün kuruluşundan bu yana müdürlük yaparak emeği geçen yöneticilere "Teşekkür" plaketi verilerek katkılarının onurlandırılması amaçlanmıştır. Sıcak ve keyifli bir kapanış resepsiyonu ile sonlandırılan Çalıştay Enstitümüzün daha nice yirmi senelere erişmesi dilekleri ile sonlandırılmıştır.

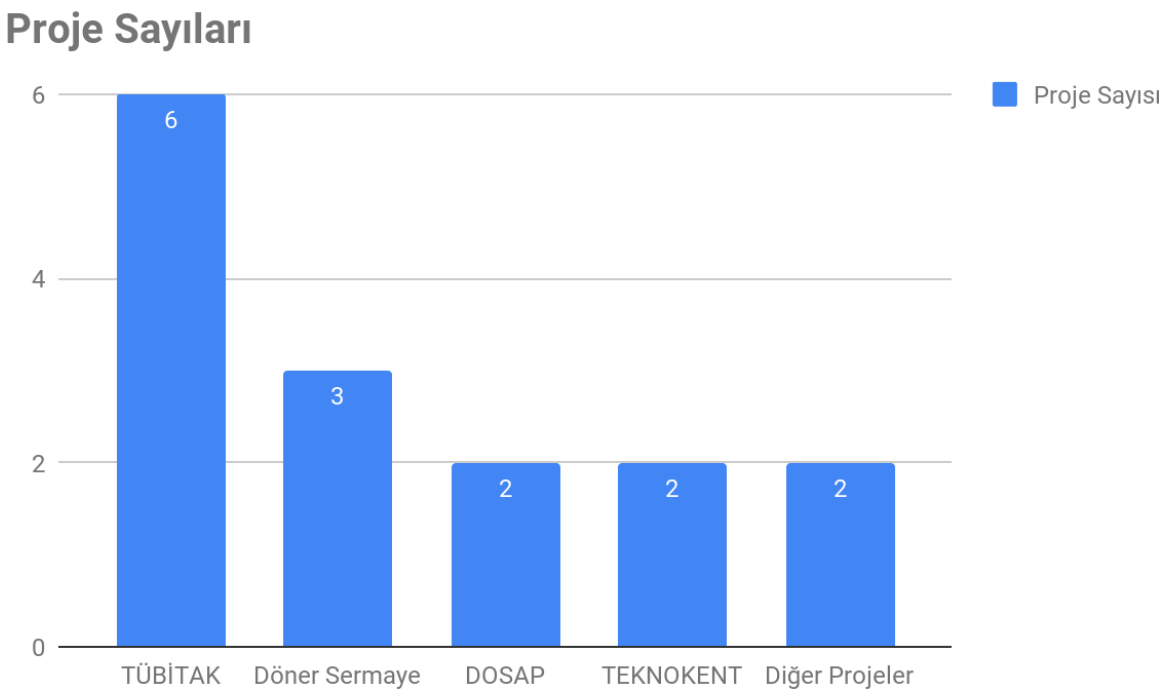

Workshop on
20th Anniversary of
Institute of
Applied Mathematics
November 4, 2022

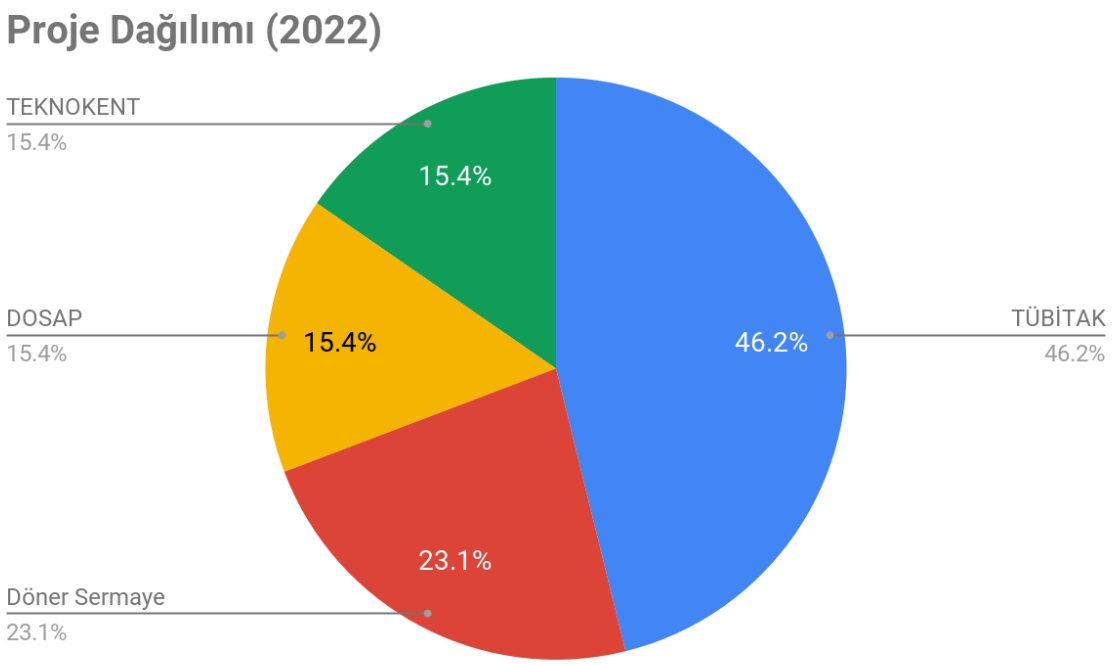

FINANCIAL
MATHEMATICS
ACTUARIAL
SCIENCES
Workshop on
SCIENTIFIC
COMPUTING



Projeler

Enstitümüzün çatısı altında yürütülen proje sayıları ve öğretim üyelerimizin araştırmacı olarak yer aldıkları proje bilgileri aşağıda verilmektedir. TÜBİTAK (%66,7) kaynaklı projeler ağırlıklı olmak üzere, Döner Sermaye, DOSAP, TEKNOKENT projeleri aracılığıyla hem Enstitümüz işbirliklerinin artırılması, hem de eğitim ve araştırmaya yönelik olanakların sağlanması sevindiricidir. TÜBİTAK projelerinin geçen seneye göre %26 civarında artışının olduğu da gözlenmiştir.





TÜBİTAK, Döner Sermaye ve Diğer Projeler

[1]	Proje Adı: Kriptografik Algoritmaların Tasarımı, Gerçekleştirilmeleri ve Uygulamaları (TÜBİTAK) Yürütücü: Murat Cenk* Araştırmacılar: Türe, N. D., Çakın, S., Yaman, N., Kırcalı, M. Başlangıç – Bitiş Tarihleri: 2019 – 2025 *22.09.2022 tarihi itibariyle Oğuz Yayla'ya devredilmiştir.
[2]	Proje Adı: Kodlama Teorisi ve Uygulamaları Üzerine Araştırma (TÜBİTAK-Güney Kore Ulusal Araştırma Vakfı (NRC)) Yürütücü: Ferruh Özbudak, Cem Güneri UME Araştırmacısı: Karakaş, Z., Özkaya, B. Başlangıç – Bitiş Tarihleri: 15 Nisan 2021 – 15 Nisan 2023
[3]	Proje Adı: Kuantum Ertesi Kütüphanesi (FAME CRYPT - TÜBİTAK) Yürütücü: Murat Cenk Araştırmacılar: Yünüak, H. B. Başlangıç – Bitiş Tarihleri: 2020 – 2022

[4]	Proje Adı: Bükülmüş Fonksiyonların Genellemeleri ve Permütasyon Polinomları (TÜBİTAK 1001, 120F309) Yürütücüsü: Nurdagül Anbar Meidl UME Araştırmacısı: Yayla, O. Başlangıç – Bitiş Tarihleri: 15 Mart 2021 – 15 Mart 2023
[5]	Proje Adı: Simitli Cebirsel Geometri Ve Kodlama Teorisine Uygulamaları (TÜBİTAK 1001, 119F177) Yürütücüsü: Mesut Şahin UME Araştırmacısı: Yayla, O. Başlangıç – Bitiş Tarihleri: 15 Kasım 2019 – 15 Mayıs 2022
[6]	Proje Adı: Siber Güvenlik Tasarım ve Test Çözümleri (TÜBİTAK 2244-Arçelik) Yürütücüsü: Pelin Angın UME Araştırmacısı: Yılmaz, B. E. Başlangıç – Bitiş Tarihleri: 2019 – 2023
[8]	Proje Adı: Mathematical Models for Interacting Dynamics on Networks, Proje No: Cost Action CA18232 (Cost European Cooperation in Science & Technology) Yürütücü: Hamdullah Yücel Araştırmacılar: Başlangıç – Bitiş Tarihleri: 4 Ekim 2019 - 3 Ekim 2023
[9]	Proje Adı: Sigortam.Net Ürün Skorlama ve Değerlendirme Projesi (ODTÜ Döner Sermaye) Yürütücü: A. Sevtap Kestel Araştırmacılar: Yavrum, C., Koç, O. Başlangıç – Bitiş Tarihleri: 1 Ocak-1 Şubat 2022
[10]	Proje Adı: HVKK 2021 Yılı Aktüeryal Değerlendirme (ODTÜ Döner Sermaye) Yürütücü: A. Sevtap Kestel Araştırmacılar: Külekci Yıldırım, B. Başlangıç – Bitiş Tarihleri: 1 Ocak- 30 Mart 2022
[11]	Proje Adı: TARSİM- Buğday Fiyatı Modellemeleri ve Senaryo Analizleri (ODTÜ Döner Sermaye) Yürütücü: A. Sevtap Kestel Araştırmacılar: Mert, O.M., Yavrum, C. Başlangıç – Bitiş Tarihleri: 1 Ekim-1 Kasım 2022

[12]	Proje Adı: Kriptografik Modül Sertifikasyonu (FAME CRYPT) Yürütücü: Oğuz Yayla Başlangıç – Bitiş Tarihleri: 05.2022 – 08.2022

ODTÜ Bilimsel Araştırma Projeleri (DOSAP)

[1]	Proje Adı: Post-Kuantum Kriptografi Tabanlı Anahtar Paylaşımı Yürütücü: Murat Cenk Araştırmacılar: Yıldız, H. Başlangıç - Bitiş Tarihleri: 2021 - 2022
[2]	Proje Adı: Kafes-tabanlı Sıfır-Bilgi Aralık İspatı Yürütücü: Murat Cenk Araştırmacılar: Betin Onur, C. Başlangıç - Bitiş Tarihleri: 2021 - 2023

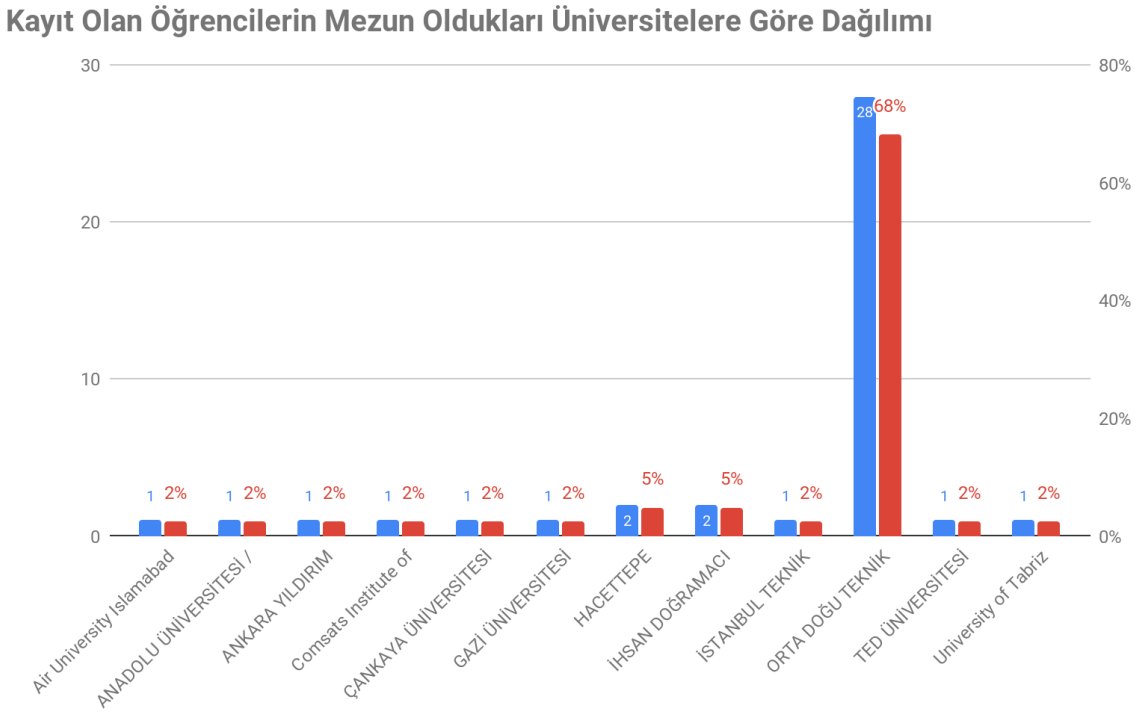
Eğitim

Başvurular, Kabul ve Kayıtlar

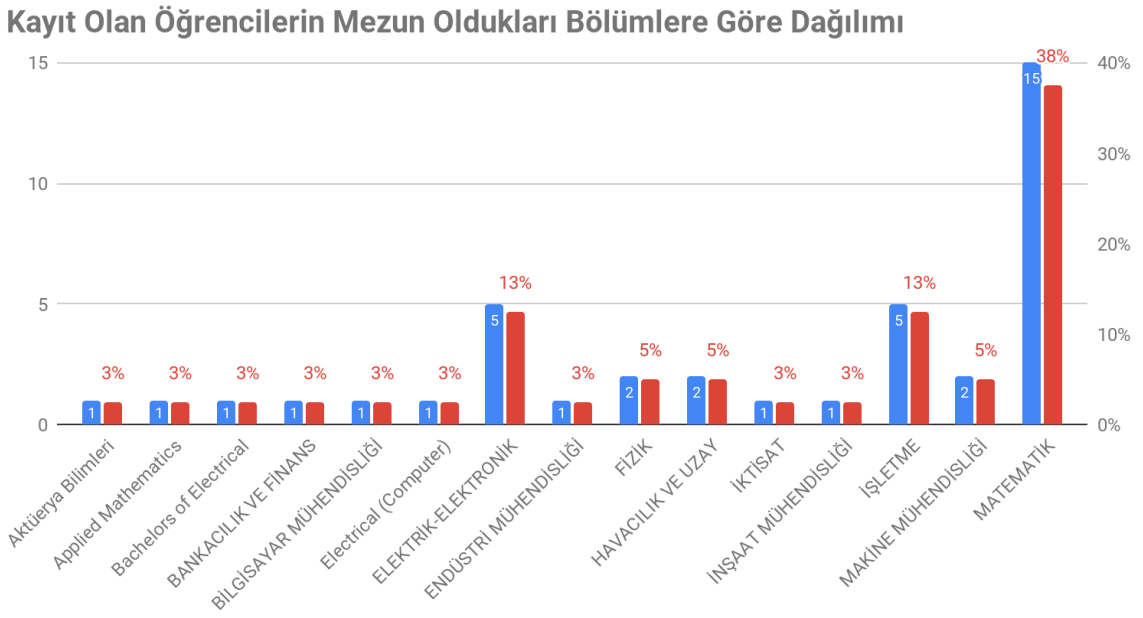
Enstitü Anabilim Dallarındaki programlara başvuru yapan ve kabul edilen öğrencilerin toplam başvuru sayılarına oranları aşağıdaki tabloda verilmiştir. Başvuru sayısının düşük olduğu programlar ile ilgili geniş çaplı tanıtım stratejilerinin belirlenmesi hedeflenmektedir.

Enstitü Anabilim Dalları	BAŞVURULAR - 2022		
	Başvuru (%)	Kabul (%)	Kayıt (%)
Aktüerya Bilimleri	3 (% 4)	3 (% 5)	3 (% 7)
Bilimsel Hesaplama	31 (% 36)	18 (% 30)	12 (% 29)
Finansal Matematik	23 (% 27)	16 (% 27)	10 (% 24)
Kriptografi	28 (% 33)	23 (% 38)	16 (% 39)
Toplam	85	60	41

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



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.



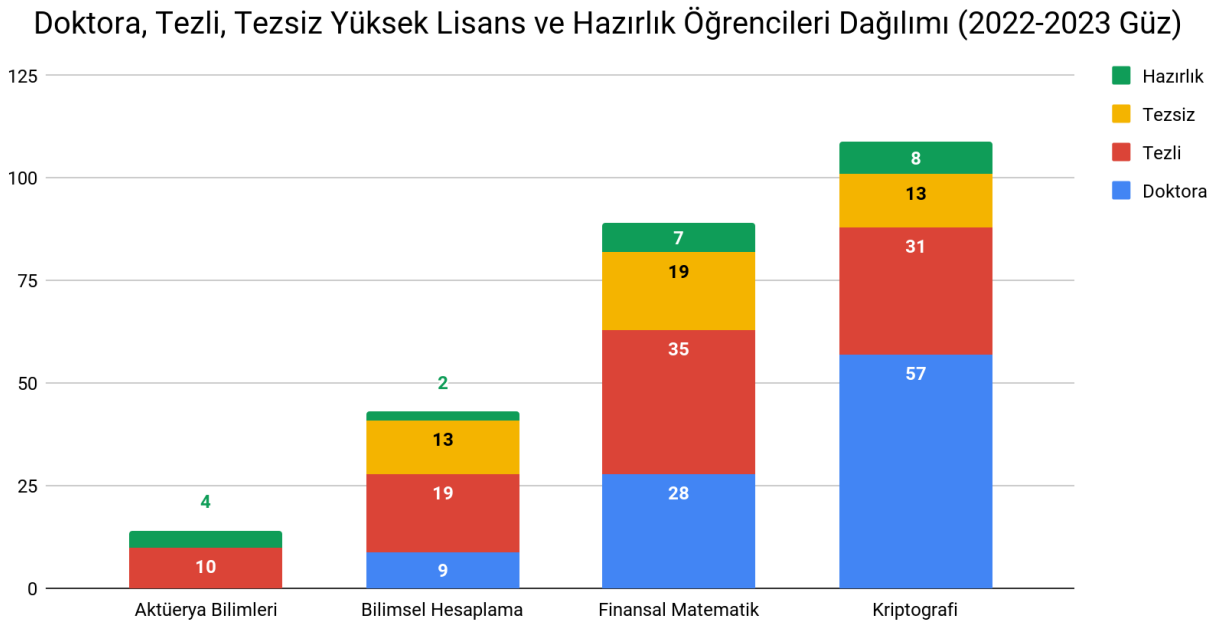
Enstitü Öğrencilerinin Programlara Göre Dağılımı ve İstatistikler

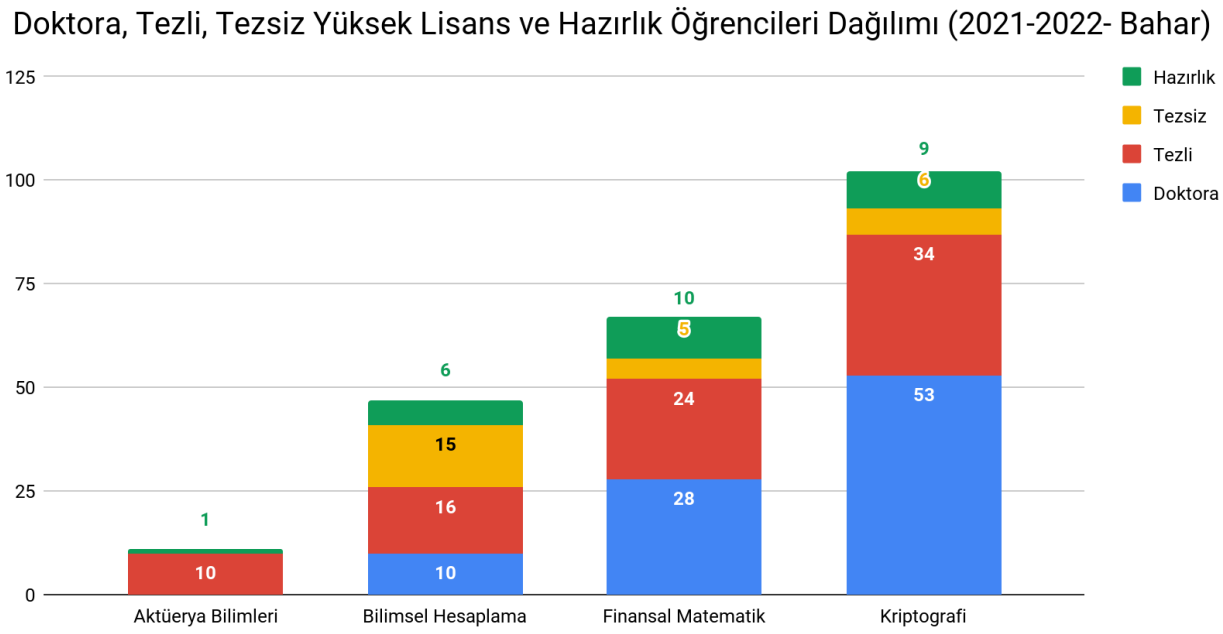
Enstitümüze yeni katılan öğrencilerimiz ile birlikte, mevcut öğrencilerimizin programlara göre dağılımı aşağıdaki "2022-2023 Güz" ve "2021-2022 Bahar" başlıklı tablolarda belirtilmiştir. Kriptografi programındaki öğrenci sayıları toplam kayıtlı öğrencilerin yaklaşık %42'sini, Finansal Matematik programı ise yaklaşık %30'unu oluşturmaktadır. Doktora programına kayıtlı öğrenciler ise %36'nın üzerindedir.

2022-2023 Güz					
Anabilim Dalı	**Doktora**	**Tezli**	**Tezsiz**	**Hazırlık**	**Toplam**
Aktüerya Bilimleri		8	2	1	**11**
Bilimsel Hesaplama	8	14	7	1	**30**
Finansal Matematik	24	31	15	5	**75**
Kriptografi	58	18	8	12	**96**
Özel Öğrenci					
	90	**71**	**32**	**19**	**212**

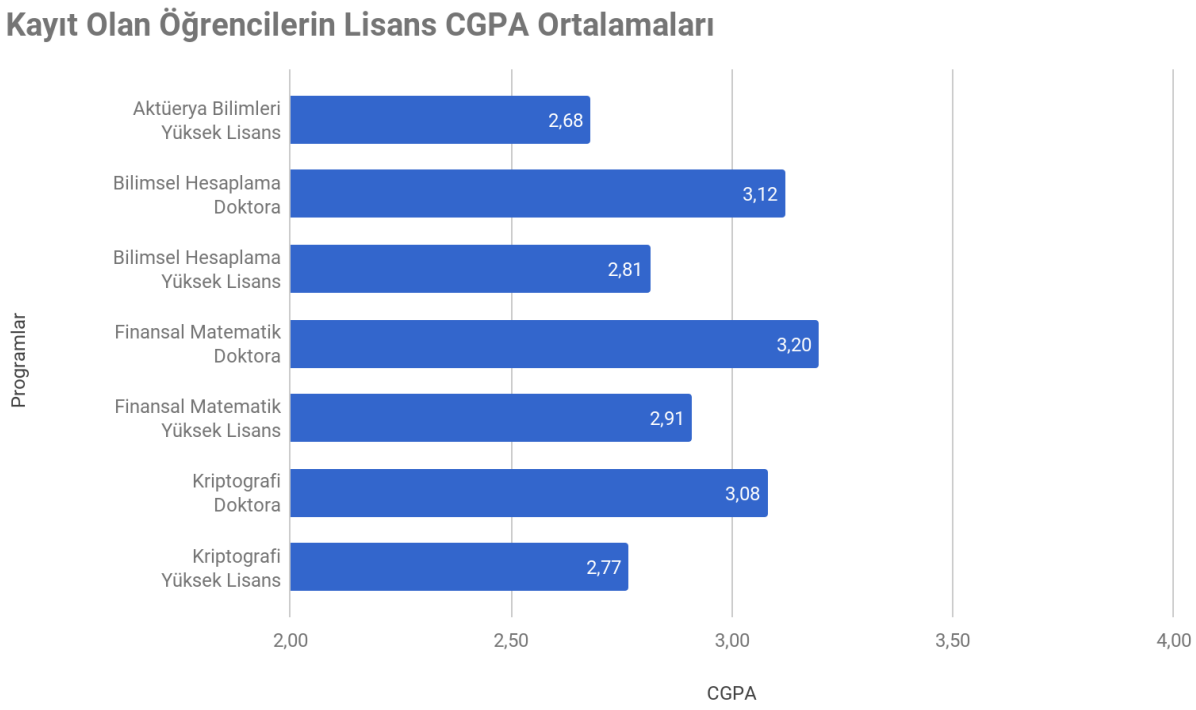
2021-2022 Bahar					
Anabilim Dalı	**Doktora**	**Tezli**	**Tezsiz**	**Hazırlık**	**Toplam**
Aktüerya Bilimleri		6			**6**
Bilimsel Hesaplama	7	8	8	1	**24**
Finansal Matematik	23	24	11	4	**62**
Kriptografi	53	14	5	4	**76**
	83	**52**	**24**	**9**	**168**

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



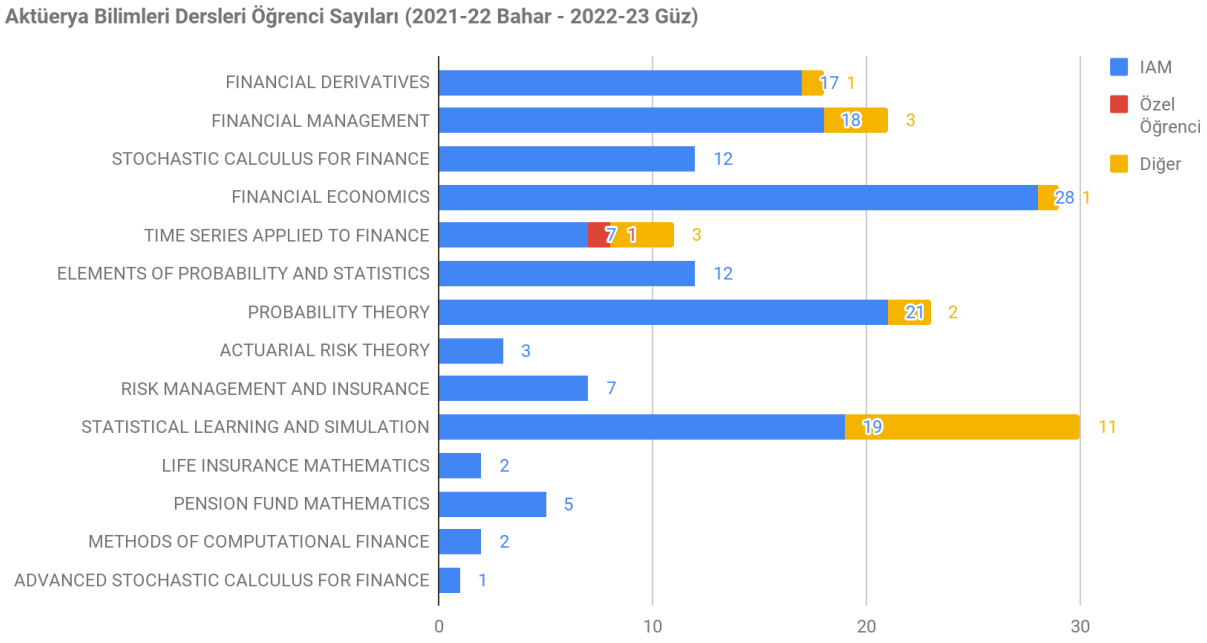


Enstitümüze kayıt yaptıran öğrencilerin Anabilim Dalı bazında lisans akademik başarı performansları (CGPA ortalamaları) aşağıdaki gibi gerçekleşmiştir.

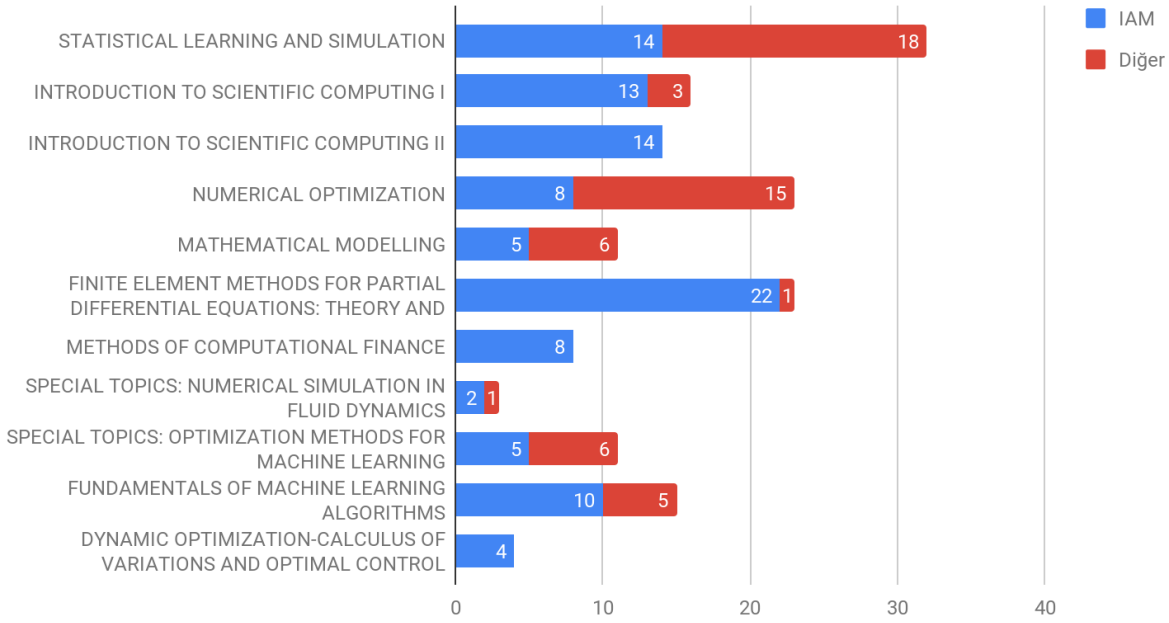


Enstitüdeki Dersler, Öğrenci Sayıları ve İstatistikler

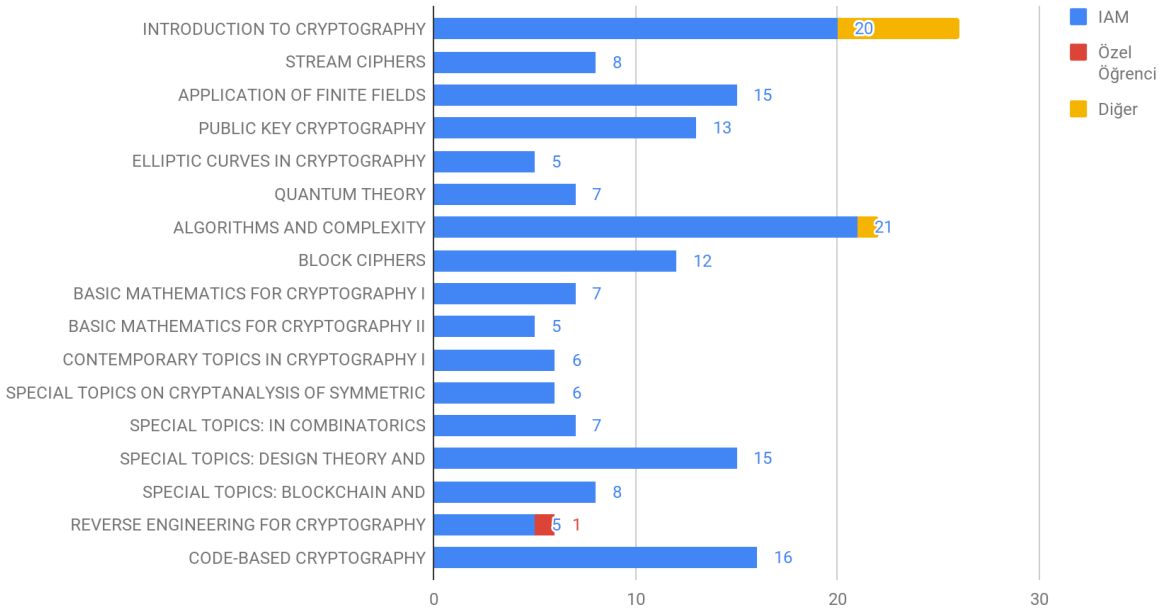
Bu bölümde, Enstitümüzde 2022 yılı içerisinde açılan derslere ve bu derslere ilişkin istatistiklere yer verilmiştir. Aşağıdaki grafiklerde, her bir Anabilim Dalı için belirtilen derslerdeki enstitü ve enstitü-dışı öğrenci sayıları verilmektedir. Birçok dersimizin, birden fazla Anabilim Dalında listelenmiş olması programlar arası bilgi akışının sağlanması amacına yönelik olup, Enstitümüzün ve derslerimizin disiplinlerarası çalışmalara verdiği önemin bir göstergesidir.



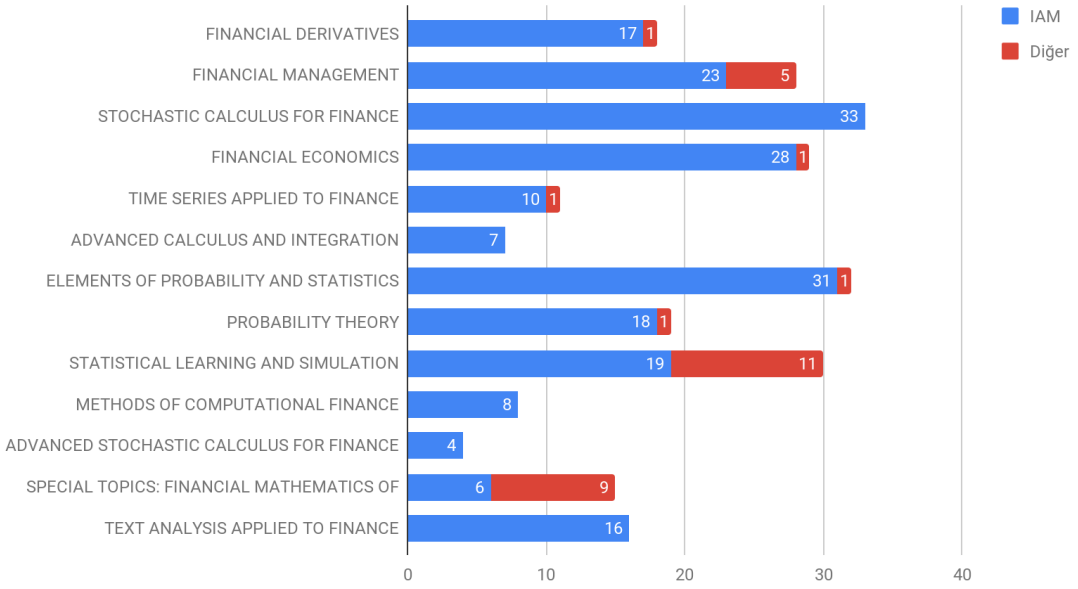
Bilimsel Hesaplama Dersleri Öğrenci Sayıları (2021-22 Bahar - 2022-23 Güz)



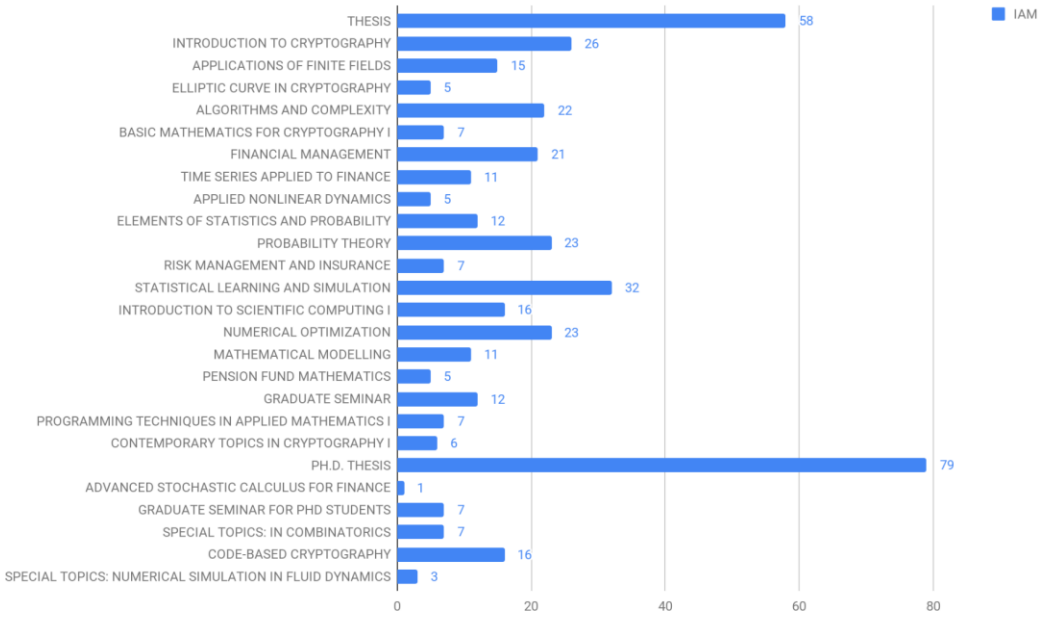
Kriptografi Dersleri Öğrenci Sayıları (2021-22 Bahar - 2022-23 Güz)

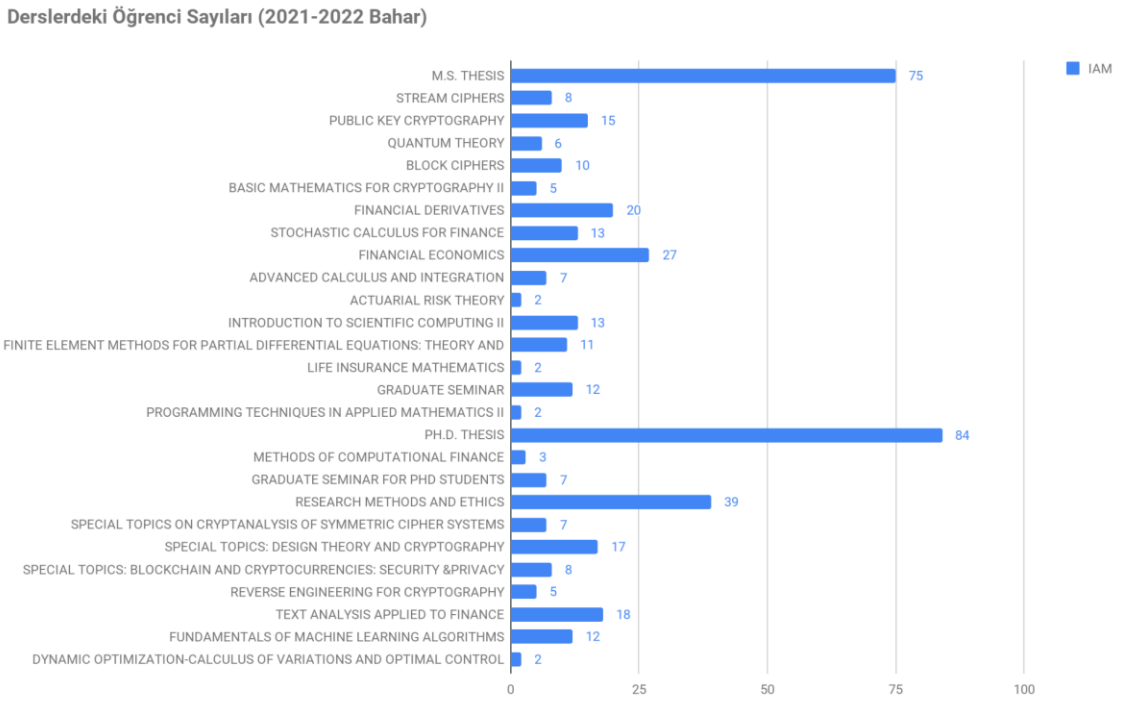


Finansal Matematik Dersleri Öğrenci Sayıları (2021-22 Bahar - 2022-23 Güz)



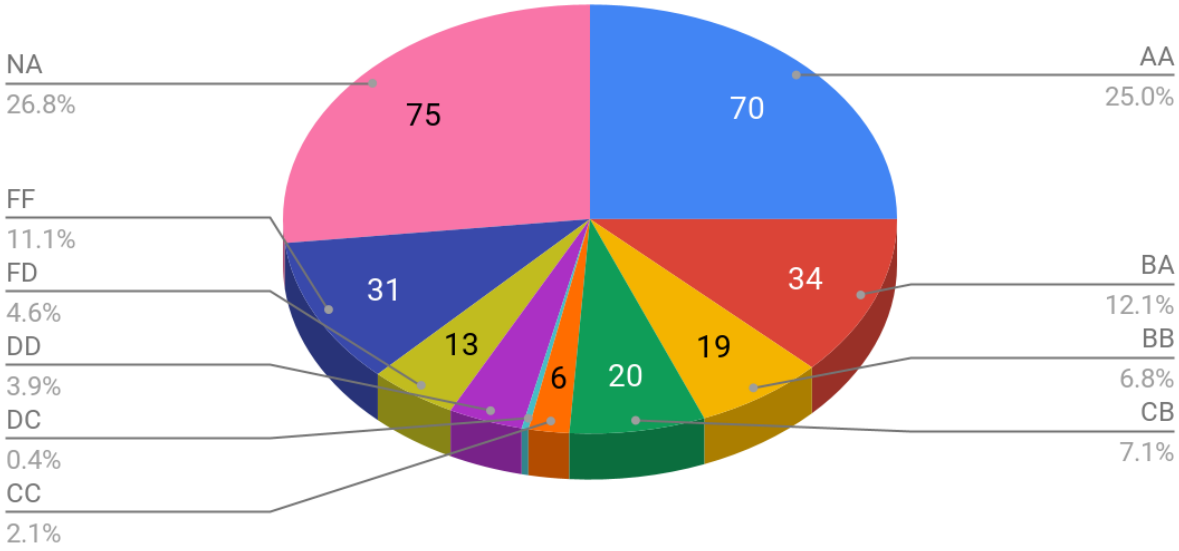
Derslerdeki Öğrenci Sayıları (2022-2023 Güz)



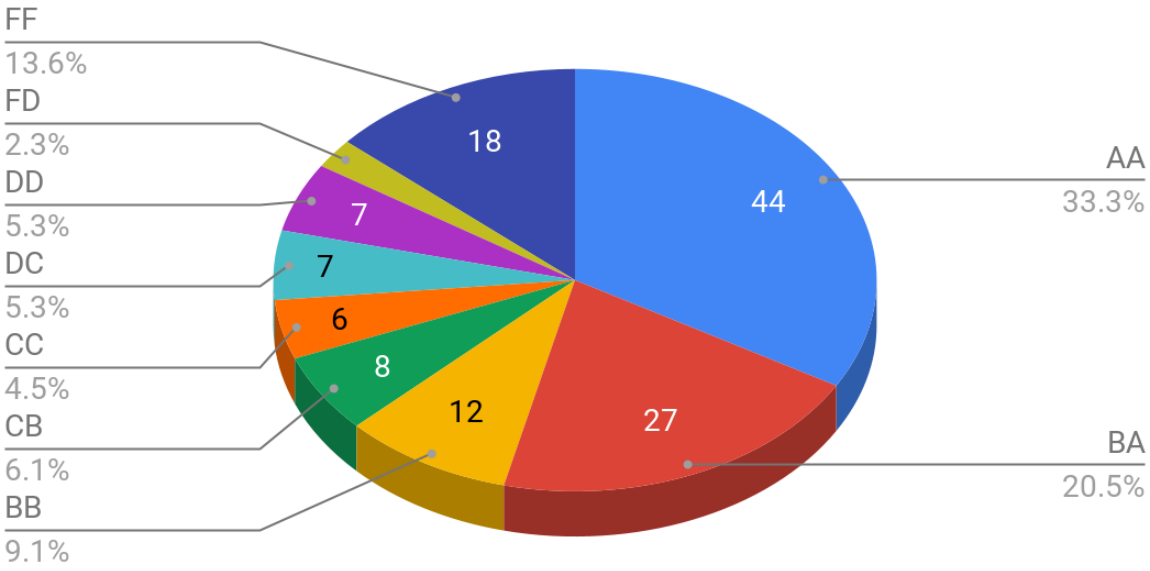


Aşağıdaki grafiklerde 2022 yılı içerisinde 2022-2023 Güz ve 2021-2022 Bahar dönemlerinde açılan tüm dersler, öğrenci sayıları ve not dağılımları verilmiştir. Özellikle not dağılımını gösteren grafiklerde %10-%20'ler seviyesinde olan "NA" notundaki artış sebeplerinden en önemlisinin öğrencilerimizin eğitimlerinin yanı sıra çeşitli kurum ve kuruluşlarda çalışmaları olduğu düşünülmektedir.

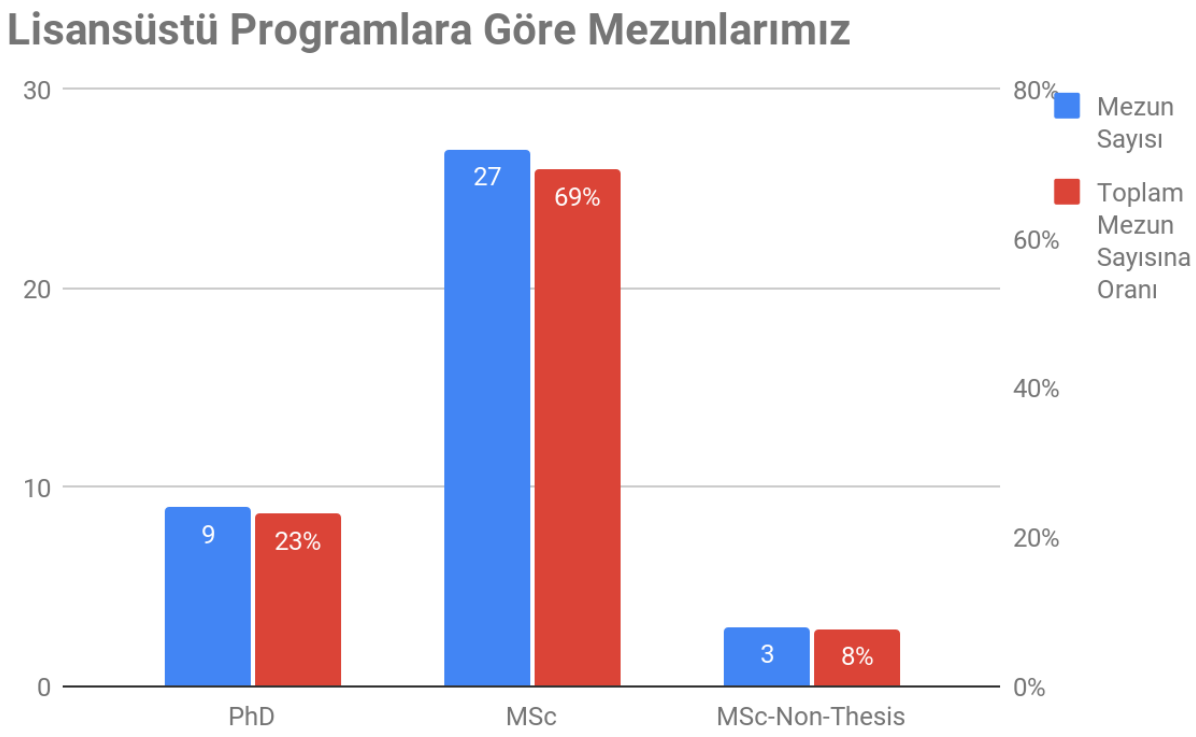
2022-2023 Güz Dönemi Not Dağılımı



2021-2022 Bahar Dönemi Not Dağılımı



Enstitümüz Yüksek Lisans ve Doktora programlarından 2022 yılında mezun olan öğrencilerimizin sayıları ve oranları aşağıda yer almaktadır. Toplam sayıda Yüksek lisans mezunlarının %63 oranı ile önde olduğu, 9 doktora mezunu, 27 Tezli ve 3 Tezsiz Yüksek lisans mezunu verdiği Enstitümüz mezunları akademik ve diğer kuruluşlarda çalışmaktadırlar.



Doktora Programları

2022-2023 Güz ve 2021-2022 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]	Yeniaras, E., New Efficient Characteristic Three Polynomial Multiplication Algorithms and Their Applications to NTRU Prime, PhD Thesis, Cryptography, January 2022 (Danışman: Murat Cenk)
[2]	Cengizci, S., Stabilized Finite Element Simulations of Multispecies Inviscid Hypersonic Flows in Thermochemical Nonequilibrium, PhD Thesis, Scientific Computing, March 2021 (Danışman: Ömür Uğur; Ortak Danışman: Tayfun E. Tezduyar)
[3]	Mülayim, G., Reduced-Order Modelling of Cross-Diffusion, PhD Thesis, Scientific Computing, July 2022 (Danışman: Bülent Karasözen)
[4]	Kılıç, D. A., Assessment of Artificial Neural Network to Improve Hidden Markov Model for Financial Data, PhD Thesis, Financial Mathematics, August 2022 (Danışman: A. Sevtap Kestel)
[5]	Paksoy, İ. K., New Tmvp-Based Multiplication Algorithms for Polynomial Quotient Rings and Application To Pqc, PhD Thesis, Cryptography, August 2022 (Danışman: Murat Cenk)
[6]	Demircioğlu, M. Efficient Multivariate-Based Ring Signature Schemes, PhD Thesis, Cryptography, September 2022 (Danışman: Murat Cenk; Ortak Danışman: Sedat Akleylek)
[7]	Tekin, Ö. Analytical Pricing Formula Under Three-State Regime-Switching Model, PhD Thesis, Financial Mathematics, September 2022 (Danışman: Ömür Uğur; Ortak Danışman: Rogemar S. Mamon)
[8]	Aksu, M. Optimal Liquidation with Conditions on Minimum Price, PhD Thesis, Financial Mathematics, October 2022 (Danışman: A. Devin Sezer)
[9]	Mert, Ö. M., Stochastic Modeling of Stop-Loss Reinsurance and Exposure Curves under Time-Dependent Structure, PhD Thesis, Financial Mathematics, December 2022 (Danışman: A. Sevtap Kestel)

Yüksek Lisans Programları

2022-2023 Güz ve 2021-2022 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]	Çalı, G., The effect of Focus Versus Diversification on Bank Performance: Does Ethical Structure Matter?, MSc Thesis, Financial Mathematics, January 2022 (Danışman: Seza Danışoğlu)
[2]	Toraman, S. C., Stochastic Momentum Methods for Optimal Control Problems Governed by Convection-Diffusion Equations with Uncertain Coefficients, MSc Thesis, Scientific Computing, January 2022 (Danışman: Hamdullah Yücel)
[3]	Bayrak, H. B., Competing Labels: A. Heuristic Approach to Pseudo-Labeling in Deep Semi-Supervised Learning, MSc Thesis, Scientific Computing, March 2021 (Danışman: Şeyda Ertekin; Ortak Danışman: Hamdullah Yücel)
[4]	Bozkurt, C., Analysis and Comparison of Fully Homomorphic Encryption Approaches Over Integers, MSc Thesis, Cryptography, February 2022 (Danışman: Murat Cenk; Ortak Danışman: Cansu Betin Onur)
[5]	Ceylan , Ö. A., Performance of Electrical Power Flow Solvers: Case Studies, MSc Thesis, Scientific Computing, February 2022 (Danışman: Ömür Uğur)
[6]	Aksoy, B., Analyzes of Block Recombination and Lazy Interpolation Methods and Their Applications to Saber, MSc Thesis, Cryptography, February 2022 (Danışman: Murat Cenk)
[7]	Efe, G., Hybrid Analysis of TMVP for Modular Polynomial Multiplication in Cryptography, MSc Thesis, Cryptography, February 2022 (Danışman: Murat Cenk)
[8]	Gül, A. E., Investor Attention and Stock Performance: A Search Engine Optimization Approach, MSc Thesis, Financial Mathematics, February 2022 (Danışman: Seza Danışoğlu)
[9]	Yıldırım, E. U., Quality Enhancement of Computed Tomography Images of Porous Media Using Convolutional Neural Networks, MSc Thesis, Scientific Computing, February 2022 (Danışman: Ömür Uğur; Ortak Danışman: Guenther Glatz)

[10]	Yıldırım, İ. E., Seismic First Arrival Traveltime Inversion Harnessing Physics Informed Neural Networks, MSc Thesis, Scientific Computing, February 2022 (Danışman: Ömür Uğur; Ortak Danışman: Umair bin Waheed)
[11]	Höçük, F., Incorporation of Foreign Exchange Risk to Fama-French Factor Model: A Study on Borsa İstanbul, MSc Thesis, Financial Mathematics, February 2022 (Danışman: Esma Gaygısız)
[12]	Orhan, S., Examination of Bond Risk Premia from a Banking Perspective: The Case of Turkey, MSc Thesis, Financial Mathematics, June 2022 (Danışman: Seza Danışoğlu)
[13]	Hassan, C. A., Radix-3 NTT-Based Polynomial Multiplication for Lattice-Based Cryptography, MSc Thesis, Cryptography, June 2022 (Danışman: Oğuz Yayla)
[14]	Jubeh, R. M. A., Modeling Cash Flows Under IFRS17: Türkiye Case, MSc Thesis, Actuarial Science, June 2022 (Danışman: Sevtap Kestel; Ortak Danışman: Oytun Haçarız)
[15]	İrge, A. K.., Forecasting Financial Performance Using the F Score, MSc Thesis, Financial Mathematics, July 2022 (Danışman: Seza Danışoğlu)
[16]	Özbaba, İ., Resilience in to Disaster Risk Management, MSc Thesis, Financial Mathematics, August 2022 (Danışman: B. Burçak Başbuğ Erkan; Ortak Danışman: A. Sevtap Kestel)
[17]	Özbaba, İ., Resilience in to Disaster Risk Management, MSc Thesis, Financial Mathematics, August 2022 (Danışman: B. Burçak Başbuğ Erkan; Ortak Danışman: A. Sevtap Kestel)
[18]	Kayapınar, İ., Determination of Spot Wheat Prices under Climate Impact using Copula Approach, MSc Thesis, Actuarial Science, August 2022 (Danışman: A. Sevtap Kestel; Ortak Danışman: Bükre Yıldırım Külekci)
[19]	Kahya, A., Machine Learning over Encrypted Data with Fully Homomorphic Encryption, MSc Thesis, Cryptography, September 2022 (Danışman: Murat Cenk)
[20]	Öznurlu, C., Data-Driven Model Discovery and Control of Lateral-Directional Fighter Aircraft Dynamics, MSc Thesis, Scientific Computing, October 2022 (Danışman: Ömür Uğur; Ortak Danışman: Tayfun Çimen)
[21]	Aru, T., The Impact of the 30th October Earthquake on the Covid-19 Pandemic in İzmir and its Vicinity, MSc Thesis, Financial Mathematics, October 2022 (Danışman: B. Burçak Başbuğ Erkan)

[22]	Topallar, S.T., Probabilistic Forecasting of Multiple Time Series with Single Recurrent Neural Network, MSc Thesis, Scientific Computing, October 2022 (Danışman: Ceylan Yozgatlıgil)
[23]	Dinçer, H., Cryptographic Protocols of Signal and Based Instant Messaging, MSc Thesis, Cryptography, October 2022 (Danışman: Ali Doğanaksoy; Ortak Danışman: Pınar Gürkan Balıkçıoğlu)
[24]	Gülşen, M. E.., Random Sequences in Vehicle Routing Problem, MSc Thesis, Cryptography, October 2022 (Danışman: Oğuz Yayla)
[25]	Çelik, K., Blockchain Based Solution for Electronic Healthcare Data Integrity, MSc Thesis, Cryptography, October 2022 (Danışman: Oğuz Yayla)
[26]	Batmaz, G., Studies on Almost Perfect Nonlinear Functions, MSc Thesis, Cryptography, October 2022 (Danışman: Ferruh Özbudak)
[27]	Hanikaz, B., Effects of Central Banks's Announcements on Financial Markets , MSc Thesis, Financial Mathematics, December 2022 (Danışman: Esma Gaygısız)

Tezsiz Yüksek Lisans Mezunları

2022-2023 Güz ve 2021-2022 Bahar dönemlerinde Enstitümüz bünyesindeki Tezsiz Yüksek Lisans programlarından aşağıda isimleri listelenen öğrencilerimiz başarı ile mezun olmuştur. Mezunlarımızı tebrik eder, başarılarının devamını dileriz.

[1]	Kuş, S. Ö., Monotonicity of Liquidity Sensitive Option Prices with Respect to Market Liquidity Parameters, Financial Mathematics, January 2022 (Danışman: A. Devin Sezer)
[2]	Demir, N. C., Quantum Key Distribution and Recent Advances, Cryptography, February 2022 (Danışman: Oğuz Yayla)
[3]	Özcan, B., Vayanos and Wang's (2012) Model for Liquidity and Asset Returns The Cases of Capital Gain Taxation and Dividend Payment Volatility, Financial Mathematics, August 2022 (Danışman: Esma Gaygısız)

Ödüller

2021-2022 Eğitim öğretim yılında ODTÜ Lisansüstü Tez Ödülü'nü Enstitümüzde;

- Bilimsel Hesaplama EABD'ndan Prof. Dr. Bülent Karasözen danışmanlığında tamamladığı doktora tezi ile Dr. Süleyman Yıldız,
- Finansal Matematik EABD'ndan Prof. Dr. Ömür Uğur danışmanlığında ve Prof. Dr. Ümit Aksoy ortak danışmanlığında tamamladığı doktora tezi ile Dr. Burcu Aydoğan,
- Kriptografi EABD'ndan Prof. Dr. Murat Cenk danışmanlığında tamamladığı doktora tezi ile Dr. Yusuf Alper Bilgin

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]	Rinad M. A. Jubeh (Aktüerya Bilimleri): Yüksek Lisans Ders Performans Ödülü, 2022
[2]	Kaan Çelik (Kriptografi): Yüksek Lisans Ders Performans Ödülü, 2022
[3]	Dursun Oylum Seriner (Kriptografi): Yüksek Lisans Ders Performans Ödülü, 2022
[4]	Veysel Ergenç (Finansal Matematik): Yüksek Lisans Ders Performans Ödülü, 2022
[5]	Can Deniz Çam (Bilimsel Hesaplama): Yüksek Lisans Ders Performans Ödülü, 2022
[6]	Bahri Tokmak (Bilimsel Hesaplama): Doktora Ders Performans Ödülü, 2022
[7]	Olha Khomlyak (Kriptografi): Doktora Ders Performans Ödülü, 2022

Ek Bilgiler

Yeni Açılan Dersler (2022 Yılı)

Enstitümüzün ders kataloğuna 2022-2023 Güz ve 2021-2022 Bahar dönemlerinde açılan aşağıdaki dersler eklenmiştir.

2022 - 2023 Güz Dönemi

Course Code	9700593
Course Title	Contemporary Topics in Cryptography I
Course Credit(s)	**METU 3(3-0) ECTS 8**
Instructor(s)	Ferruh Özbudak, Murat Cenk, Oğuz Yayla, Buket Özkaya
Prerequisites	None
Course Catalog Description	Introduction to Cryptography, Information Theory, Boolean Functions, Coding Theory, Quantum Codes, Quantum and Post-Quantum Cryptography, Hash Functions, Message Authentication Codes, Key management
Course Objectives	At the end of the course, the student will learn: ● Modern topics in Cryptography ● Key concepts and applications of Cryptography
Course Learning Outcomes	Student, who passed the course satisfactorily will be able to: · Follow regular courses of Cryptography program
Tentative (Weekly) Outline	1. Introduction to Cryptography 2. Cryptography and Complexity 3. Information Theory 4. Boolean Functions 5. Symmetric and Asymmetric ciphers 6. Coding Theory 7. Gröbner Bases and Applications 8. Finite Geometry and Cryptography 9. Computational aspects of Coding Theory and Cryptography 10. Quantum Codes 11. Quantum and Post-Quantum Cryptography 12. Hash Functions and Message Authentication Codes 13. Key Management

Course Textbook(s)	● C. Paar, J. Pelzl, "Understanding Cryptography", Springer, 2010. ● Nigel P. Smart, "Cryptography made simple", Springer. ● S. Ling, C. Xing, "Coding Theory: A First Course", Cambridge Press, 2004. ● M. B. Paterson, D. Stinson, "Cryptography. Theory and practice", CRC Press, 2019. ● W. Trappe, L. C. Washington, "Introduction to Cryptography with Coding Theory", Pearson, 2006.
Supplementary Materials and Resources	● D. J, Bernstein, J. Buchmann, E. Dahmen, "Post-Quantum Cryptography", Springer, 2009. ● W. Stallings, "Cryptography and Network Security: Principles and Practices", Pearson, 2006. ● J. Katz, Y. Lindell, "Introduction to Modern Cryptography", CRC Press, 2021. ● N. Ferguson, B. Schneier, T. Kohno, "Cryptography Engineering: Design Principles and Practical Applications", John Wiley and Sons, 2010. ● J.P. Aumasson, "Serious Cryptography: A Practical Introduction to Modern Encryption", 2017.

Course Code	9700594
Course Title	Contemporary Topics in Cryptography II
Course Credit(s)	**METU 3(3-0) ECTS 8**
Instructor(s)	Ferruh Özbudak, Murat Cenk, Oğuz Yayla, Buket Özkaya
Prerequisites	None
Course Catalog Description	Cryptography and Storage, Lightweight Cryptography, Side channel attacks, Cybersecurity, Cryptographic Protocols, Blockchain, Internet of Things, Big Data, Cryptography in everyday use
Course Objectives	At the end of the course, the student will learn: ● Modern topics in Cryptography ● Key concepts and applications of Cryptography
Course Learning Outcomes	Student, who passed the course satisfactorily will be able to: ● Follow regular courses of Cryptography program

Tentative (Weekly) Outline	1. Cryptography and Storage 2. Lightweight Cryptography 3. Information Security 4. Cryptanalysis 5. Side channel attacks 6. Cybersecurity and Cryptography 7. Cryptographic Implementations 8. Cryptographic Protocols 9. Blockchain 10. IoT Security 11. Big Data 12. Cryptography for home users 13. Cryptography for secure payment and identity cards 14. Cryptography for wireless communications
Course Textbook(s)	• C. Paar, J. Pelzl, "Understanding Cryptography", Springer, 2010. • Nigel P. Smart, "Cryptography made simple", Springer. • M. B. Paterson, D. Stinson, "Cryptography. Theory and practice", CRC Press, 2019. • Keith Martin, "Everyday Cryptography", Oxford, 2012.
Supplementary Materials and Resources	• D. J, Bernstein, J. Buchmann, E. Dahmen, "Post-Quantum Cryptography", Springer, 2009. • W. Stallings, "Cryptography and Network Security: Principles and Practices", Pearson, 2006. • J. Katz, Y. Lindell, "Introduction to Modern Cryptography", CRC Press, 2021. • N. Ferguson, B. Schneier, T. Kohno, "Cryptography Engineering: Design Principles and Practical Applications", John Wiley and Sons, 2010. • J.P. Aumasson, "Serious Cryptography: A Practical Introduction to Modern Encryption", 2017.

Course Code	9700740
Course Title	Code-Based Cryptography
Course Credit(s)	**METU 3(3-0) ECTS 8**
Instructor(s)	Ferruh Özbudak, Oğuz Yayla
Prerequisites	Consent of Instructors

Course Catalog Description	Introduction to Coding Theory and Public-Key Cryptography; McEilece and Niederreiter Cryptosystems; Information Set Decoding; NIST finalist schemes: McEilece, BIKE, HQC.
Course Objectives	Student, who passed the course satisfactorily will be able to: ● understand the basics of Coding Theory and Asymmetric Cryptography conduct research on Code-based Cryptography
Tentative (Weekly) Outline	● Background on Coding Theory (2 Weeks) ● Background on Public-key Cryptography (2 Weeks) ● McEilece and Niederreiter Cryptosystems (2 Weeks) ● Quasi-cyclic schemes (1 Week) ● Information Set Decoding (6 Weeks) ● Applications (1 Week)
Course Textbook(s)	● S. Ling, C. Xing, "Coding Theory: A First Course", Cambridge Press, 2004. ● R. Roth, "Introduction to Coding Theory", Cambridge Press, 2006. ● C. Paar, J. Pelzl, "Understanding Cryptography", Springer, 2010. ● D. J. Bernstein, J. Buchmann, E. Dahmen, "Post-Quantum Cryptography", Springer, 2009.
Supplementary Materials and Resources	● R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. Deep Space Network Progress Report, 44:114–116, Jan. 1978. ● H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory 15, 1(6):159–166, 1986. ● C. Aguilar-Melchor, O. Blazy, J.-C. Deneuville, P. Gaborit, and G. Z´emor. Efficient encryption from random quasi-cyclic codes. IEEE Transactions on Information Theory, 64(5):3927–3943, 2018. ● E. Prange. The use of information sets in decoding cyclic codes. IRE Transactions on Information Theory, 8(5):5–9, 1962.

2021 - 2022 Bahar Dönemi

Course Code	9700739
Course Title	Special Topics: Reverse Engineering for Cryptography
Course Credit(s)	**METU 3(3-0) ECTS 8**
Instructor(s)	Dr. Pınar Gürkan Balıkçıoğlu
Prerequisites	Basic programming knowledge

Course Catalog Description	Reverse Engineering Primer, Basic Static Analysis, PE format, Virtualization, Basic Dynamic Analysis, Traffic Capturing, Decrypting Traffic Content, x86 Crash Course, Dissassemblers, Debuggers, Recognizing C Constructs in Assembly, Windows APIs, Packing, Anti-debugging, Obfuscation
Course Objectives	The primary focus of this course is to give fundamental understanding of software reverse engineering and the applications in cryptography.
Course Learning Outcomes	Student, who passed the course satisfactorily will be able to: ● understand executable file format ● use traffic analysis tools ● understand C constructs in assembly ● use disassemblers ● use debuggers
Tentative (Weekly) Outline	1) Reverse Engineering Primer, 2) Basic Static Analysis, 3) PE format, 4) Virtualization, 5) Basic Dynamic Analysis, 6) Traffic Capturing, 7) Decrypting Traffic Content, 8) x86 Crash Course, 9) Dissassemblers, 10) Debuggers, 11) Recognizing C Constructs in Assembly, 12) Windows APIs, 13) Packing, 14) Anti-debugging, 15) Obfuscation
Course Textbook(s)	Reversing: Secrets of Reverse Engineering, ISBN-13: 978-0764574818. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation, ISBN-13: 978-1118787311.

Course Code	9700756
Course Title	Special Topics: Text Analysis Applied to Finance
Course Credit(s)	**METU 3(3-0) ECTS 8**
Instructor(s)	Pınar Karagöz; A. Devin Sezer; Halis Sak
Prerequisites	Consent of Instructors
Course Catalog Description	This course introduces basic text analytics models used in the finance industry to link unstructured text data to financial market data. The covered models and algorithms include the bag-of-words, term frequency-inverse document frequency, naive Bayes, BERT, k-means clustering, neural networks, and recurrent neural networks. These models are implemented on two sets of data: Financial Times and Xueqiu news articles. Applications will be done in Python. The first three weeks of the course consist of tutorials aimed at developing programming skills in Python- no prior experience is assumed.

Course Objectives	Recently, machine learning has become a core part of many financial products and services offered in the finance industry. This course aims to provide students with an understanding of some of the basic text analytics models and algorithms used in finance applications. The course gives an opportunity to the student to learn and implement (in Python) the covered models and algorithms.
Tentative (Weekly) Outline	Weeks 1-3 An intro to the course: ideas, goals; introduction to supervised learning/classification. Tutorial: Introduction to programming in Python (sets, lists, list comprehensions, tuples, zip, dictionaries, plotting, Numpy, and Pandas) Weeks 4-5 Introduction to Bayesian statistics and inference Weeks 6-8 ● Vector Space Modeling of Text: How to represent text as n-dimensional vector. Pre-processing steps. How to assign weights. Text embeddings. Similarity measurements. ● Text Processing with Neural Models: Introduction to neural models for text processing and Using Google BERT for text analytics. ● Introduction to clustering. k-means clustering and its application on text data (Devin Sezer) Week 9 Introduction to classical logistic regression Weeks 10-11 Lecture: Logistic regression and neural networks for classification Tutorial: Predicting next trading day's movement for China stock market using Xueqiu news articles with neural networks Weeks 12-13 Lecture: Recurrent neural networks for classification Tutorial: Predicting next trading day's movement for China stock market using Xueqiu news articles with recurrent neural networks
Course Textbook(s)	Notes will be provided.

Course Code	9700772
Course Title	**Special Topics: Fundamentals of Machine Learning Algorithms**
Course Credit(s)	**METU 3(3-0) ECTS 8**
Instructor(s)	Önder Türk (oturk@metu.edu.tr)
Prerequisites	Consent to the Instructors

Course Catalog Description	Matrix Decompositions: eigendecomposition and diagonalization, singular value decomposition, matrix approximations; Vector Calculus: gradients, backpropagation, automatic differentiation; Continuous Optimization: gradient descent, constrained optimization and Lagrange multipliers, convex optimization; Probability and Distributions: Bayes' theorem, discrete probabilities, Gaussian distribution; Data, Models, and Learning: model selection; Linear Regression: orthogonal projection; Dimensionality Reduction with Principal Component Analysis; Classification with Support Vector Machines; Decision Trees; Neural Networks, Machine Learning Applications: dynamical systems, data mining
Course Objectives	The automated identification of significant patterns in data has become an essential tool in many scientific processes that require an analysis of large data sets. Recently, a large number of statistical and algorithmic developments have been based on machine learning formalism. The primary objective of this course is to provide a solid mathematical foundation of the fundamental concepts applied within this developments. This course is designed for graduate students majoring in mathematics as well as mathematically inclined graduate engineering students. At the end of this course, the students will: ● Have a solid background in mathematical foundations of basic machine learning concepts. ● Gain a deep understanding of the basic items in machine learning and connect practical questions arising from the use of machine learning with fundamental choices in the mathematical model. ● Use the computational tools available to implement key machine learning algorithms.
Course Learning Outcomes	Upon successful completion of this course, the students will be able to: ● Design and analyze machine learning methodologies that extract significant patterns from data. ● Devise general purpose algorithms appropriate for large scale learning. ● Able to accurately implement the most widely used algorithms in machine learning applications.
Tentative (Weekly) Outline	1. Matrix Decompositions: Singular Value Decomposition 2. Matrix Approximations 3. Vector Calculus: Gradients, Backpropagation 4. Unconstrained optimization 5. Constrained optimization 6. Probability and Distributions: Bayes' Theorem, Discrete Probabilities, Gaussian Distribution 7. Data, Models, and Learning: Directed Graphical Models, Model Selection 8. Linear Regression: Dimensionality Reduction with Principal Component Analysis; Density Estimation with Gaussian Mixture 9. Decision Trees 10. Decision Tree Ensembles 11. Neural Networks 12. Deep Convolutional Networks 13. Machine Learning Applications: Dynamical systems

	14. Machine Learning Applications: Data mining
Course Textbook(s)	● Peter Deisenroth, A. Aldo Faisal, Cheng Soon Ong, Mathematics for Machine Learning, Cambridge University Press, 2020. ● Gareth James, Daniela Witten, Trevor Hastie, Robert Tibshirani, An Introduction to Statistical Learning, Springer, 2021. ● Steven L. Brunton, J. Nathan Kutz, Data-Driven Science and Engineering, Cambridge University Press, 2019.
Supplementary Materials and Resources	MATLAB Student Version is available to download on MathWorks website, http://www.mathworks.com, or METU FTP Servers (Licenced) Python: https://www.python.org/

Course Code	9700773
Course Title	Special Topics: Dynamic Optimization – Calculus of Variations and Optimal Control
Course Credit(s)	**METU 3(3-0) ECTS 8**
Instructor(s)	Ömür Uğur
Prerequisites	Consent of the Instructor
Course Catalog Description	First Variation: computing the first variation, Euler-Lagrange equation, extensions; Applications: brachistochrone, Lagrangian and Hamiltonian dynamics; Second Variation: computing the second variation, Ricatti equation, convexity and minimizers; Multivariable Variational Problems: eigenpairs, minimal surfaces, gradient flows; Optimal Control Theory: time-optimal linear control, Pontryagin maximum principle; Applications: linear-quadratic regulator, production-consumption, optimal harvesting; Dynamic Programming: Hamilton-Jacobi-Bellmann equation, general linear-quadratic regulator; Further Topics on Differential Games and Stochastic Control Theory

Course Objectives	At the end of the course, the student will learn: ● the basics of the calculus of variations and its applications; ● the theory of optimal controls and its applications; ● Pontryagin maximum principle, dynamic programming and Hamilton-Jacobi-Bellmann Equation.
Course Learning Outcomes	Student, who passed the course satisfactorily will be able to: ● how to calculate the first and second variations; ● how to approach and solve basic problems using calculus of variations; ● understand the basics of the theory of optimal control; ● how to approach and solve basic problems in optimal control;
Tentative (Weekly) Outline	1. First Variation and its Applications (1 – 3 weeks) 2. Second Variation and its Applications (4 – 5 weeks) 3. Multivariable Variational Problems (6 – 7 weeks) 4. Optimal Control Theory, Pontryagin Maximum Principle and Applications (8 – 10 weeks) 5. Dynamic Programming and Hamilton-Jacobi-Bellmann equation (11 – 12 weeks) 6. Further Topics on Differential Games, Stochastic Control Theory (13 – 14 weeks)
Course Textbook(s)	● L. C. Evans, Mathematical Methods for Optimization: Dynamic Optimization, 2021. ● M. Levi, Classical Mechanics with Calculus of Variations and Optimal Control: An Intuitive Introduction, 2014.
Supplementary Materials and Resources	● L. C. Evans, An Introduction to Mathematical Optimal Control Theory, Lecture Notes. ● M. I. Kamien and N. L. Schwartz, Dynamic Optimization – the Calculus of Variations and Optimal Control in Economics and Management, 2nd edition, 1991.

2022 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.

Dr. Esra Yeniaras

Esra Yeniaras 2004 yılında Ankara Üniversitesi Matematik Bölümünden mezun olmuş ve 2007 yılında aynı bölümde Topoloji alanında Yüksek Lisans eğitimini bitirdikten sonra 2010 yılında University of Wisconsin-Madison'da Hesaplamalı Matematik alanında Yüksek Lisans eğitimini tamamlamıştır. ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi anabilim dalında doktora çalışmalarına devam etmiş ve Ocak 2022 tarihinde Doç. Dr. Murat Cenk danışmanlığında "New Efficient Characteristic Three Polynomial Multiplication Algorithms and Their Applications to NTRU Prime" başlıklı tezini tamamlamıştır. Araştırma konuları arasında kuantum-sonrası kriptografi, kriptografik algoritmaların verimli gerçeklenmesi bulunmaktadır. Halen Milli Eğitim Bakanlığı Bilgi-İşlem Biriminde görev yapmaktadır.

Doktora Tezi Özeti:

Bazı kuantum-sonrası kriptografik protokoller karakteristik üç polinom çarpımı gerektirmektedir, dolayısıyla bu tarz çarpma algoritmalarının verimliliği son zamanlarda daha çok önem kazanmaya başlamıştır. Bu tezde karakteristik üç cisimlerinde dört yeni polinom çarpımı algoritması tasarlanmıştır ve bunların son zamanlardaki en son yöntemlerden daha verimli oldukları gösterilmiştir. Öncelikle iyi bilinen okulkitabı yöntemi, Karatsuba 2-yönlü ve 3-yönlü ayrılmalı metotları, Bernstein'ın 3-yönlü ayrılmalı metodu, Toom-Cook benzeri formüller ve son zamanlardaki diğer algoritmalar analiz edilmiştir. Çeşitli 4, 5, 6 veya fazla ayrılmalı algoritma versiyonlarına sahip olan ikili (karakteristik iki) cisimlerinden farklı olarak, karakteristik üç cisimlerinde hiç 4-yönlü veya 5-yönlü ayrılmalı çarpma algoritmalarının olmadığı fark edilmiştir. Sonrasında F_9'da interpolasyon tekniği kullanılarak geliştirilen üç farklı 4-yönlü ayrılmalı polinom çarpımı algoritması tasarlanmıştır. Dahası, yeni bir 5-yönlü ayrılmalı polinom çarpımı algoritması tasarlanmış ve sonrasında tüm bahsi geçen yöntemlerin aritmetik karmaşıklığı ve implementasyon sonuçları karşılaştırılmıştır. Yeni 4-yönlü ve 5-yönlü ayrılmalı algoritmaların, 1280 girdi boyutu için, F_9 üzerindeki çarpmaların aritmetik karmaşıklığında 48.6% ve F_3 üzerindeki çarpmaların aritmetik karmaşıklığında da 26.8% oranında düşüş sağladığı gösterilmiştir. Dahası, yeni 4-yönlü ve 5-yönlü ayrılmalı algoritmalar şu dönemdeki en son yöntemlere kıyasla daha hızlı implementasyon sonuçları sağlamıştır. Tasarlanan metotlar, bir anahtar kapsülleme mekanizması olarak Bernstein vd. tarafından NIST

PQC Standartlaştırma Süreci'ne sunulan ve kapsülden çıkarma aşamasında karakteristik üç polinom çarpımı gerektiren, NTRU Prime protokolüne uygulanmıştır. Yeni metotların C'de implementasyonu yapılmış ve NTRU Prime anahtar çıkarmasındaki karakteristik üç polinom çarpımı adımında strup653 için 26.85% 'lik bir hızlanma ve strup761 için de 35.52%'lik bir hızlanma gözlenmiştir.

Yayınlar:

- Esra Yeniaras, Murat Cenk. Faster characteristic three polynomial multiplication and its application to NTRU Prime decapsulation. *Journal of Cryptographic Engineering*, 2022. https://doi.org/10.1007/s13389-021-00282-7

Dr. Süleyman Cengizci

Süleyman Cengizci 2012 yılında Niğde Ömer Halisdemir Üniversitesi Matematik bölümünden mezun olmuş ve 2014 yılında ODTÜ Mühendislik Bilimleri bölümünden aldığı derslerle birlikte Nevşehir Hacı Bektaş Veli Üniversitesi Matematik bölümünde yüksek lisans çalışmalarını tamamlamıştır. Daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Bilimsel Hesaplama anabilim dalında doktora çalışmalarına devam etmiş ve Mart 2022 tarihinde Prof. Dr. Ömür Uğur ve Prof. Dr. Tayfun E. Tezduyar danışmanlığında "Stabilized Finite Element Simulations of Multispecies Inviscid Hypersonic Flows in Thermochemical Nonequilibrium" başlıklı tezini tamamlamıştır. Araştırma konuları arasında hesaplamalı akışkanlar dinamiği, stabilize sonlu elemanlar metotları, singüler pertürbasyon problemleri ve asimptotik yaklaşımlar bulunmaktadır. Süleyman Cengizci, 2014 ve 2017 yılları arasında Antalya Bilim Üniversitesi Ekonomi bölümünde araştırma görevlisi olarak görev yapmış olup 2017 yılından bu yana yine aynı üniversitenin Bilgisayar Programlama bölümünde öğretim görevlisi olarak görev almaktadır. 2022 yılı Mart ayı itibari ile Rice Üniversitesi Makine Mühendisliği bölümü TAFSM ekibinde doktora sonrası araştırmalarını yürütmektedir.

Doktora Tezi Özeti :

Hipersonik hızlarda hareket eden roketler, füzeler ve uzay araçları son yıllarda hem askeri hem de sivil havacılık amaçlarıyla kullanılmaktadırlar. Bu araçlar, ses hızının beş katı veya üzerindeki hızlarda hareket ederlerken, birçok şiddetli fiziksel ve kimyasal etkileşim tecrübe ederler. Bu tür yüksek hızlar, moleküler sürtünmeler nedeniyle çok yüksek sıcaklıklara, bu yüksek sıcaklıklar ise aracın içerisinde hareket ettiği gaz karışımının bileşenlerinin uyarılmasına neden olurlar. Bu durum, akış ortamında termokimyasal etkileşimlere neden olur ve aracın uçuş dinamiklerini etkiler. Hem uçuşun güvenliği hem de aracın doğru zamanda doğru hedefe ulaşabilmesi için bu etkileşimlerin hassas bir şekilde incelenmesi gerekmektedir.Rüzgar tüneli testleri hipersonik uçuşların yüksek sıcaklık ve şok etkileşimlerini oluşturmada hem yetersiz kalmaktadırlar hem de çok maliyetlidirler. Dahası, bu deneysel kurulumların tasarlanması, test edilmesi, ve nihayet deneysel verilerin elde edilmesi oldukça uzun zaman alabilmektedir. Bu nedenle, hipersonik araçların uçuş dinamiklerinin analizinde ve bu tür yüksek hızlara uygun araçların dizaynında hesaplamalı akışkanlar dinamiğinin (HAD) araçları büyük öneme sahiptirler. Standart ayrıklaştırma metotlarının, bu tür yüksek hızlı akışların simülasyonlarında sahte salınımlar ürettikleri için, stabilizasyon ve şok-yakalama teknikleri ile desteklemeleri gerekmektedir.Bu tezde, termokimyasal dengesizlikteki hipersonik akışlar hesaplamalı olarak incelenmektedir. Bu amaçla, 5-bileşenli (O, N, NO, O_2, N_2) bir gaz karışımının bir silindir etrafındaki hipersonik akışı 17-reaksiyonlu bir kimyasal modelle ele alınmaktadır. Gaz partikülleri hipersonik rejimlerdeki yüksek sıcaklıklar nedeni ile farklı enerji modlarında bulunabilirler: çizgisel, dönüşsel, titreşimsel, ve elektron-elektronik. Denge durumuna ulaşmada benzer zaman ölçeklerine sahip olduklarından, çizgisel ve dönüşsel

enerji modları aynı sıcaklıkla, titreşimsel ve elektron-elektronik enerji modları ise bir diğer sıcaklıkla ifade edebilirler. Bu nedenle, iki sıcaklıklı bir kimyasal kinetik model benimsenmektedir. Hesaplamalarda, sonlu elemanlar formülasyonunu stabilize etmek için sıkıştırılabilir-akış Streamline-Upwind/Petrov–Galerkin metodu kullanılmaktadır. Stabilize edilmiş formülasyon, şoklarda daha iyi çözüm profilleri elde etme amacıyla, YZβ şok-yakalama tekniği ile desteklenmektedir. Uzay ve zaman ayrıklaştırmaları sonucu elde edilen doğrusal olmayan denklem sistemleri Newton–Raphson lineer olmayan yinelemeli çözüm metodu ve ILU yöntemi ile ön koşullandırılmış genelleştirilmiş minimal kalıntı (GMRES) arama tekniği kullanılarak çözülmektedir. Çözücü kodlar FEniCS ortamında geliştirilmektedir.

Yayınlar:

· Cengizci S., Dursun Cengizci A., Uğur Ö., A mathematical model for human-to-human transmission of COVID-19: a case study for Turkey's data, Mathematical Biosciences and Engineering 18(6):9787-9805, 2021. doi: https://doi.org/10.3934/mbe.2021480

· Cengizci S., Ugur Ö., A stabilized finite element formulation with discontinuity-capturing for solving viscous Burgers'-type equations at high Reynolds numbers (incelemede).

Dr. Gülden Mülayim

Gülden Mülayim 2008 yılında Fırat Üniversitesi Matematik bölümünden mezun olmuş ve 2010 yılında Fırat Üniversitesi Matematik bölümünde Geometri alanında yüksek lisans çalışmalarını tamamlamıştır. Daha sonra MEB bursunu kazanarak Amerika'da University of Georgia Athens, Matematik bölümünde Geometri alanında ikinci yüksek lisans çalışmalarını tamamlamıştır. Son olarak ODTÜ Uygulamalı Matematik Enstitüsü Bilimsel Hesaplama anabilim dalında doktora çalışmalarına devam etmiş ve Ağustos 2022 tarihinde Prof. Dr. Bülent Karasözen ve Doç. Dr. Murat Uzunca danışmanlığında "Reduced-order modeling of cross-diffusion systems" başlıklı tezini tamamlamıştır. Araştırma konuları arasında reaksiyon-difüzyon sistemleri, çapraz-difüzyon sistemleri, desen oluşumu, sonlu-farklar metodu, uygun dik ayrıştırma metodu, radyal bazlı fonksiyonlar, tekil değer ayrışımı, tensörler bulunmaktadır. Gülden, 2015 yılından itibaren Adıyaman Üniversitesi Matematik bölümünde araştırma görevlisi olarak araştırmalarını yürütmektedir.

Doktora Tezi Özeti :

Bu tezde, çapraz-difüzyon sistemleri için müdahaleci ve müdahaleci olmayan düşük mertebeden modeller (ROMs) geliştirilmiştir. Birinci bölümde, lineer difüzyon ve çapraz-difüzyon terimleriyle parametre bağımlı sistemlerini ele alıyoruz. Tam mertebeli modeller (FOMs) uzayda sonlu farklar ile sistemi ayrıştırarak oluşturulmuştur. Sonuç olarak matris ve tensör formunda elde edilen adi diferansiyel denklemler (ODEs) zamanda açık-örtük Euler (IMEX) metodu ile entegre edilir. İndirgenmiş bazlar, iki kademeli uygun ortogonal ayrıştırma (POD) yaklaşımı ve tensör formundaki uzay-zaman anlık görüntülerine yüksek dereceli tekil değer ayrıştırma (HOSVD) uygulayarak oluşturulur. Yeni parametre değerleri için indirgenmiş katsayılar radyal bazlı fonksiyon (RBF) interpolasyonu kullanarak hesaplanır. Önerilen metodun verim oranı iki-boyutlu Schnakenberg, üç-boyutlu Brusselator çapraz-difüzyon denklemleri ve avcı-av problemleri için nümerik örneklerle gösterilmiştir. Tezin ikinci bölümünde, Lotka-Volterra kinetiği ile Shigesada-Kawasaki-Teramato (SKT) denklemi ve tümör büyüme modeli gibi lineer olmayan difüzyon ve çapraz difüzyon terimleri olan sistemleri ele alıyoruz. Bu sistemlerin uzayda sonlu fark ayrışımı doğrusal ikinci dereceden adi diferansiyel sistemleri (ODEs) ortaya çıkarır. Tam mertebeli modeller zamanda doğrusal olarak örtük Kahan metodu kullanarak entegrasyon yoluyla oluşturulur. İndirgenmiş mertebeli modeller ise müdahaleci olarak Galerkin projeksiyonu ile uygun ortogonal ayrıştırma metodu uygulanarak oluşturulur. İndirgenmiş mertebeli modellerin doğrusal ikinci dereceden yapısından yararlanarak, indirgenmiş modellerin çözümlerinin hesaplanması tensörel bir çerçevede uygun ortogonal ayrıştırma metodu kullanarak daha da hızlandırılır öyle ki indirgenmiş sistemdeki hesaplamalar tam mertebeli çözümlerden bağımsız olmaya başlar. İndirgenmiş modellerin uzun vadeli tahmin kabiliyetleri bir- ve iki- boyutlu SKT denklemi,

tümör büyüme problemi ve avcı-av problemleri için gösterilmiştir. Genel olarak, çapraz-difüzyon sistemlerinin uzay-zaman ,şekilleri iki ve üç dereceli hızlandırma faktörlerine sahip indirgenmiş modeller tarafından tam mertebeli modeller üzerine doğru bir şekilde yaklaştırılır.

Yayınlar:

· B. Karasözen, G. Mülayim, M. Uzunca, S. Yıldız, Reduced order modelling of nonlinear cross-diffusion systems, Applied Mathematics and Computation, 401, 126058, 2021.

· B. Karasözen, M. Uzunca, G. Mülayim, Nonintrusive model order reduction for cross-diffusion systems, Communications in Nonlinear Science and Numerical Simulation, 115, 106734, 2022 .

Dr. İrem Keskinkurt Paksoy

İrem Keskinkurt Paksoy 2005 yılında Hacettepe Üniversitesi Fen Fakültesi Matematik bölümünden mezun olmuştur. 2015 yılında ODTÜ UME Kriptografi anabilim dalında yüksek lisans eğitimine başlayana kadar matematik öğretmenliği yapmıştır. 2017 yılında yüksek lisansını tamamlayarak ODTÜ UME Kriptografi anabilim dalında doktora araştırmalarına başlamıştır. Prof. Dr. Murat Cenk danışmanlığında "New TMVP-based Multiplication Algorithms for Polynomial Quotient Rings and Application to Post-Quantum Cryptography" başlıklı tezi ile doktora derecesini almıştır. İlgi duyduğu araştırma alanları arasında kafes-tabanlı kriptografi, kuantum-sonrası kriptografi, aritmetik hesaplama karmaşıklığı, verimli algoritma geliştirme/gerçekleme, kriptanaliz gibi konular yer almaktadır. 2020 yılından bu yana ODTÜ UME Kriptoloji Laboratuvarında öğretim görevlisi olarak görev yapmaktadır.

Doktora Tezi Özeti :

Kuantum bilgisayarlara karşı güvenli kriptografi araştırma alanlarından biri kafes tabanlı kriptografidir. Kafes tabanlı sistemlerin birçoğu, polinom bölüm halkalarında çarpma için verimli algoritmalara ihtiyaç duyar. Çarpma için bilinen en hızlı algoritma, halkanın parametrelerinde modülün asal olması gibi belirli kısıtlamalar gerektiren Sayı Kuramsal Dönüşümdür (NTT). Bu kısıtlamalara uymayan bazı şemalar için doğrudan NTT uygulaması bir seçenek değildir; örneğin, ikinin kuvveti bir modül kullanan PQC standardizasyon yarışmasının iki finalisti Saber ve NTRU gibi. Toom-Cook ve Karatsuba, NTT direkt uygulanamadığında en yaygın kullanılan çarpma algoritmalarıdır. NTT'ye uygun olmayan halkalarda, modüler indirgeme gerektirmeyen daha büyük parametreler ile NTT kullanımına olanak veren bir yöntem önerilmiş olsa da NTT olmayan verimli çarpma algoritmaları geliştirmek de bu halkalardaki çarpma işlemini iyileştirebilir.Bu tezde, kuantum-sonrası kriptografik (PQC) sistemler için Toeplitz Matris-Vektör Çarpımı (TMVP) tabanlı çarpma algoritmaları geliştirmeye odaklanılmıştır. İlk olarak, beş ve yedi çarpma gerektiren yeni üçlü ve dörtlü TMVP formülleri önerilmiştir. Uygulama için Saber ve NTRU şemalarını seçilmiştir. Saber ve NTRU'nun tanımlandığı halkalar için yeni dörtlü formülü kullanarak TMVP tabanlı çarpma algoritmaları geliştirilmiş ve ayrıca, Saber için geliştirilen algoritmanın iyileştirilmiş bir versiyonunu sunulmuştur. Bunlara ek olarak NTRU şemasındaki çarpma işlemlerinde TMVP formüllerini kullanabilmek için bir doldurma yöntemi önerilmiştir.Ayrıca, önerilen algoritmaların, PQC adaylarının mikroişlemciler üzerinde değerlendirilmesi için NIST tarafından önerilen bir platform olan ARM Cortex-M4 üzerinde gerçeklemesi yapılmıştır. Performans ve hafıza kullanımı, literatürdeki tüm Toom gerçeklemelerine kıyasla iyileşme sağlanmıştır. Ayrıca, TMVP tabanlı algoritmaların, NTRU'nun üç parametre seti için NTT'den daha hızlı olduğu ve tümü için hafıza kullanımını azalttığı gözlemlenmiştir. Algoritmaların şemalar üzerindeki etkisini görmek için, yazılmış olan kodlar literatürdeki en gelişmiş Saber ve NTRU gerçeklemelerine entegre edilmiştir. Saber için önerilen algoritma, Toom yöntemine

kıyasla performansta %18,6'ya ve bellek tüketiminde %44,2'ye varan iyileştirmeler sağlamıştır. NTRU'nun tüm parametreleri için, hafıza kullanımı Toom'a kıyasla %5,9-%20,9 ve NTT'ye kıyasla %5,1-%19,3 arasında azaldığı görülmüştür. Ayrıca, tüm parametreler için Toom metoduna kıyasla %4,4-%17,5 arasında performans artışı gözlemlenmiştir. NTRU'nun bir tanesi dışındaki parametreleri için, algoritmalar NTT yönteminden daha iyi performans göstermiştir. Ayrıca, kare olmayan TMVP hesaplamaları için yeni formüller sunulmuş ve bu formülleri kullanarak yeni TMVP formülleri türetmek için bir yaklaşım önerilmiştir. Önerilen formüllerin aritmetik karmaşıklık hesaplamaları ve teorik verimlilik karşılaştırmaları da bu tezde sunulmaktadır.

Yayınlar:

· İrem Keskinkurt Paksoy, Murat Cenk, *TMVP-based Multiplication for Polynomial Quotient Rings and Application to Saber on ARM Cortex-M4*. (Hakemli bir dergide değerlendirmesi sürmektedir.)

· İrem Keskinkurt Paksoy, Murat Cenk, *Faster NTRU on ARM Cortex-M4 with TMVP-based multiplication*, accepted by IEEE Transactions on Circuits and Systems-I: Regular Papers. (Yayımlanmak üzere kabul edilmiştir.)

Dr. Özge Tekin

Özge Tekin 2012 yılında Hacettepe Üniversitesi Aktüerya Bilimleri bölümünden mezun olmuştur. 2015 yılında ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik programında yüksek lisansını Prof. Dr. Ömür Uğur ve Doç. Dr. Yeliz Yolcu Okur danışmanlığında "Object-oriented implementation of option pricing via Matlab: Monte Carlo approach" başlıklı tez ile tamamlamıştır. Doktora çalışmalarına aynı programda devam etmiş ve 2022 yılında Prof. Dr. Ömür Uğur ve Prof. Dr. Rogemar S. Mamon danışmanlığında "Analytical Pricing Formula Under Three-State Regime-Switching Model" başlıklı tezini tamamlamıştır. Araştırma konuları arasında saklı Markov modelleri ve yarı-saklı Markov modelleri altında türev ürünlerin fiyatlandırılması ve parametre tahmini bulunmaktadır. 2014-2022 yılları arasında ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik programında araştırma görevlisi olarak görev almıştır.

Doktora Tezi Özeti :

Ekonomik ve finansal veriler, dinamikleri ve stokastik yapıları nedeniyle farklı zaman aralıklarında farklı davranışlar sergilemektedir. Açıklayıcı modeller oluşturmak için benzer özelliklere sahip farklı zaman periyotları tek bir rejim altında gruplandırılabilir. Bu çalışmada, ekonominin durumlarının homojen bir birinci mertebeden, sürekli zamanlı, sonlu durumlu saklı Markov zinciri süreci izlediği varsayılmaktadır. Black-Scholes-Merton çerçevesinin üç durumlu Markov rejim değişimi modeline genişletilmesi durumunda Avrupa tipi opsiyonların değerlendirilmesi problemini ele alınmıştır. Bu bağlamda, faiz oranını, dayanak varlığın sapma ve oynaklık parametreleri altta yatan Markov zincirine bağlıdır ve parametre değerleri sonlu sayıda durumlar arasında geçiş yapmaktadır. Altta yatan Markov zincirinin sebep olduğu belirsizlik nedeniyle, piyasa eksiktir (incomplete). Eşdeğer martingale ölçüsünü belirlemek amacıyla Markov rejim değiştirme modeli için Esscher dönüşümü uygulanarak, bu ölçü altında, parametreleri altta yatan Markov zincirine bağlı olan Avrupa tipi opsiyonlar için analitik formül türetilmiştir. Bu model altındaki fiyatlama prosedürü, literatürde altta yatan Markov zincirinin iki durumlu olduğu model altında incelenmiştir. Bu tezde altta yatan Markov zincirinin üç durumlu olduğu model için analitik çözümü elde etmek amacıyla Falzon tarafından önerilen ortak olasılık yoğunluk fonksiyonunun kullanılması önerilmiştir. Önerilen yöntem kullanarak altta yatan Markov zincirine göre parametre değerleri değişen Avrupa tipi opsiyonlar için parametre hassasiyetlerinin hesaplamaları sunulmuştur. Egzotik opsiyonlardan bazıları Avrupa tipi opsiyonlar cinsinden ifade edilebilir. Bu ilişki bariyer opsiyonları açısından ele alınmıştır ve hem altta yatan Markov zincirine göre parametre değerleri değişen bariyer opsiyonları için hem de bu opsiyonların parametre hassasiyeti hesaplamaları için önerdiğimiz yöntemin nasıl genişletilebileceği gösterilmiştir. Yöntemin geçerliliği, çeşitli örnekler ile ve bu yöntem ile elde edilen sonuçların literatürde var olan sonuçlarla karşılaştırılması ile gösterilmiştir. Son olarak, vade sonunda minimum garanti ödemeli fayda opsiyonu değerlemesi

Markov rejim değişimi modeli altında ele alınmıştır. Değişken annüite sözleşmelerinin uzun ömürlü oldukları düşünüldüğünde sigorta sağlayıcılarının borsadaki dalgalanmalara ek olarak hem faiz oranı hem de ölümlülük oranlarındaki dalgalanmaları dikkate almaları gerekmektedir. Faiz oranı, ölümlülük oranı ve temel fon parametrelerinin altta yatan Markov zincirine bağlı olduğu modeli ele alınmaktadır ve ölümlülük bileşeni için bağımsız filtreleme varsayımı altında iki farklı model önerilmektedir. İlk model, hem finansal hem de ölümlülük parametrelerinin aynı temel Markov zinciri tarafından düzenlendiğini var sayarken, ikinci model, ölüm modelinin parametrelerinin ayrı bir ikinci Markov zincirine dayandığını varsayılmaktadır. Bu çalışma, Markov rejim değiştirme çerçevesi altında bu sözleşmelerin fiyatlandırılması konusundaki yaklaşımımızın etkisini göstermek için sayısal örneklerle tamamlanmıştır.

Dr. Mervan Aksu

Mervan Aksu 2011 yılında Fatih Üniversitesi İşletme bölümünden mezun olmuş ve 2015 yılında Galatasaray Üniversitesi İşletme yüksek lisans çalışmasını Muhasebe ve Finans alanında tamamlamıştır. Daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik anabilim dalında doktora çalışmalarına devam etmiş ve eylül 2022 tarihinde Prof. Dr. Ali Devin Sezer danışmanlığında "Optimal Liquidation with Conditions on Minimum Price" başlıklı tezini tamamlamıştır. Araştırma konuları arasında Risk Yönetimi, Portföy Optimizasyonu, Optimal likidasyon ve Finans problemlerinde makine öğrenimi ve yapay zeka uygulamaları bulunmaktadır. . Mervan, ilk olarak 2011 – 2012 yılları arasında Mardin Artuklu Üniversitesi İşletme Bölümünde Araştırma Görevlisi olarak çalışmaya başladı. Daha sonra 2012-2015 yılları arasında Galatasaray Üniversitesi İşletme bölümünde araştırma görevlisi olarak görev yapmıştır. 2016 2018 yılları arasında ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik alanında Araştırma Görevlisi olarak çalıştı. 2018 yılından bu yana Mardin Artuklu Üniversitesi İşletme bölümünde Araştırma Görevlisi olarak görev almaktadır.

Doktora Tezi Özeti :

Optimal likidasyon veya pozisyon kapatma, belirli bir [0,T] zaman aralığında finansal bir varlıkta bulunan bir q_0 pozisyonunun kapatılması sorusudur. Yatırımcının amacı bu zaman aralığında pozisyonu tam kapatarak işlemden gerçekleşecek kazancın beklenen faydasını maksimize etmektir. Likidasyon işlemleri stokastik ortamlarda gerçekleştiği için pozisyonu tam kapatma kısıtı çok bağlayıcı olabilir. Yatırımcı fiyattaki değişimleri baz alarak tam likidasyon kısıtını gevşetmek veya alım satım işlemlerini yavaşlatmak/durdurmak isteyebilir. Bu tezin amacı bu esnekliklere sahip optimal pozisyon kapatma emirlerinin formülasyonu ve bunların matematiksel olarak çalışılmasıdır. Bu esneklikte emirler üretmek için ilgili stokastik optimal kontrol problemine iki yeni parametre eklenmiştir: {0, 1} değerlerini alan bir I süreci ve ölçülebilir bir S olayı. I ne zaman işlem yapılabildiğini belirlerken S kümesi tam pozisyon kapatma işleminin koşullarını belirler. Fiyat süreci için yatırımcının belirleyeceği bir alt limiti baz alan dört farklı S ve I örneği verilmiştir. Önerilen yeni stokastik optimal kontrol sorusuna karşılık gelen geriye dönük stokastik denklemi (BSDE) belirlenmiş; bu denklemin minimal üstçözümlerinin stokastik optimal kontrol probleminin hem değer fonksiyonunu hem de optimal kontrolünü verdiği gösterilmiştir. Fiyat sürecini Markov olduğunda BSDE'ler kısmi diferansiyel denklemlere dönüşmektedirler (PDE). Stokastik volatiliteli Markovian fiyat süreçleri için bu PDE'lerin analizleri de verilmiştir. Önerilen algoritmanın finansal performansı, pozisyonun (kısmen) kapatıldığı ortalama fiyatın varlığın başlangıç fiyatından yüzde sapması ile ölçülmüştür. Bu sapma üç parçaya ayrılabilir: kalıcı fiyat etkisine bağlı bir parça (A_1), fiyattaki stokastik dalgalanmalarla ilgili bir parça (A_2) ve alış-satış fiyat farkı maliyeti ve işlem ücretleri ile ilgili bir parça (A_3). A_1, 1-q_T/q_0'nin doğrusal bir

fonksiyonu olduğu ve bu sebeple dağılımının tamamen q_T/q_0 (pozisyonun kapatılmayan kısmının başlangıçtaki büyüklüğüne oranı)'ın dağılımı tarafından belirlendiği gözlenmiştir. Fiyat sürecinin Brownian olduğu varsayımı altında I ve { S}'nin dört farklı değeri için q_T/q_0'ın dağılımı ve A_2 ve A_3'ün q_T/q_0'a göre şartlı dağılımları numerik olarak hesaplanmış ve bunların model parametreleriyle nasıl değiştiği numerik olarak gösterilmiştir.

Dr. Özenç Murat Mert

Özenç Murat Mert 2014 yılında ODTÜ Matematik bölümünden lisans mezunu olmuş ve 2016 yılında ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik anabilim dalında yüksek lisansını tamamlamıştır. Daha sonra Finansal Matematik doktora programına devam etmiş ve Aralık 2022 tarihinde Prof. Dr. Sevtap Selçuk-Kestel danışmanlığında "Stochastic Modeling of Stop-Loss Reinsurance and Exposure Curves under Time-Dependent Structure" başlıklı tezini tamamlamıştır. Araştırma konuları arasında veri odaklı stokastik modelleme, parametre tahmini ve kalibrasyonu, optimal reasürans sözleşmelerinde sigortacı ve reasürörün ortak fayda analizi, sigortacı ve reasürör risk eğri analizleri yaklaşımları bulunmaktadır. Özenç, 2015'ten bu yana ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik ana bilim dalında araştırma görevlisi olarak görev almaktadır.

Doktora Tezi Özeti :

Dünya ekonomisinde önemli bir rol oynayan sigorta piyasaları, nüfus artışı, katastrofik olaylar, politik ve ekonomik perspektifler nedeniyle reasürans politikalarını gerektirmektedir. Bu tezde, reasürans poliçe türlerinden biri olan zarar-durdur sözleşmeleri, (i) rehinli sözleşmeler ve (ii) hem reasüranslı hem de üst limitli (maksimum) sözleşmeler olmak üzere iki farklı sözleşme türü için ele alınmıştır. Bu tez, hasar modellemesinin analizi için hasar tutarlarının dağılımsal ve stokastik davranışları, sigortacı ve reasürör maliyetleri, adil prim payı elde etmek için riziko eğrileri olmak üzere iki farklı metodolojiyi kapsamaktadır. Reasürans politikaları üzerine yapılan çoğu çalışmanın aksine, tez, hasarların zamana bağlı yapısını vurgular ve hasar tutarlarını modellemek ve tarafların maliyetlerini ve riziko eğrilerini incelemek için kapsamlı çıkarımlar verir. Dağılım yaklaşımında, özellikle Pareto, Gamma ve Ters Gamma olmak üzere kalın kuyruklu dağılımlar kullanılır ve seçilen dağılımlar altında tarafların maliyetleri ve riziko eğrileri analitik olarak türetilir. Monte Carlo simülasyonları kullanılarak ve tarafların kayıp oranlarının ortak analizi göz önünde bulundurularak, VaR ve CVaR risk ölçütleri kapsamında optimal elde tutma ve maksimum seviyeler bulunur ve tarafların risklerini minimize eden değerler ile karşılaştırılır. Stokastik modelleme yaklaşımında, talep tutarlarının hem rastgele hem de zamana bağlı mekanizmasını ifade etmek için zamanla değişen parametrelerle Geometrik Brown Hareketi kullanılmış ve sözleşme sırasında geçen süre nedeniyle tarafların maliyetleri ve riziko eğrileri analitik olarak türetilmiştir. Zaman, hasar davranışında olduğu gibi maliyet, prim payı üzerinde de farklılıklar getirir. Ayrıca, olası aşırı kayıpları yakalamak için Pareto-Beta stokastik sıçrama difüzyon (PBJD) modeli ve arkasındaki teori uygulanmaktadır. Bu tez, maliyet türevlerini ve PBJD kapsamında riziko eğrilerini birleştirir. Stokastik yaklaşımlar için gerçek hayat verileri kullanılıp, özellikle Türkiye'nin zorunlu trafik sigortası hasar veri uygulamalarına vurgu yapılmıştır. Beklenen maliyetler için sonuçlar, riziko eğrileri sunulmaktadır. Kayıp miktarları, beklenen maliyetler ve riziko eğrilerinin tahmin değerlerini elde etmek için zamanla değişen parametreler zaman serisi olarak alınmış ve

stokastik yapıyı korumak için ARIMA ailesi modelleri ve bu serilere kübik spline ekstrapolasyonu uygulanmıştır.

Yayınlar:

· Mert, Ozenc Murat, and A. Sevtap Selcuk-Kestel. "Time dependent stop-loss reinsurance and exposure curves." Journal of Computational and Applied Mathematics, 389, 113348, 2021. https://doi.org/10.1016/j.cam.2020.113348

· Mert, Ö.M., Selcuk-Kestel, A.S., Optimal premium allocation under stop-loss insurance using exposure curves, Hacettepe Journal of Mathematics and Statistics, 2022. DOI:10.15672/hujms.889619

· Mert, Ozenc Murat, and A. Sevtap Selcuk-Kestel. "Time-Dependent Stop-Loss Reinsurance and Exposure Curves under Stochastic Jump Diffusion Influence." (incelemede).

Dr. Murat Demircioğlu

Murat Demircioğlu 2009 yılında ODTÜ Matematik bölümünden mezun olmuş ve 2011 yılında ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi anabilim dalında yüksek lisans çalışmalarını tamamlamıştır. Daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi anabilim dalında doktora çalışmalarına devam etmiş ve Ağustos 2022 tarihinde Prof. Dr. Murat Cenk ve Doç. Dr. Sedat Akleylek danışmanlığında "Efficient Multivariate-Based Ring Signature Schemes" başlıklı tezini tamamlamıştır. Araştırma konuları arasında açık anahtarlı kriptografik algoritmalar, post-quantum algoritmalar, kriptografik protokoller ve siber güvenlik bulunmaktadır. Murat, 2012 ve 2013 yılları arasında ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi anabilim dalında araştırma görevlisi olarak görev yapmış olup sonrasında 2017 yılına kadar özel sektörde çeşitli firmalarda siber güvenlik uzmanı olarak çalışmıştır. 2017-2022 yıllarında Türksat Uydu Haberleşme Kablo TV ve İşletme A.Ş.'de bilgi güvenliği uzmanı olarak çalıştıktan sonra ASELSAN'da çalışma hayatına devam etmektedir.

Doktora Tezi Özeti :

Halka imza şeması, açık anahtarlı kriptografide geniş bir kullanım alanına sahiptir. İmzalayanın kimliğini ifşa etmeden bir grup içinde bilgi sızdırma senaryosu bunlar içerisinden bir örnek olarak verilebilir. Öte yandan, kullanılan halka imza tekniklerinin çoğu, büyük ölçekli bir kuantum bilgisayarda Shor algoritmasına karşı savunmasız olduğu bilinen RSA ve ECDH gibi klasik kripto sistemlerine dayanmaktadır. Bu tezde, çok değişkenli imzalama algoritmaları olan GeMSS ve Gui algoritmalarına dayalı verimli ve kuantum dirençli halka imza şemaları önermekteyiz. GeMSS ve Gui, 2016 yılında NIST tarafından başlatılan Kuantum Sonrası Kriptografi Standardizasyon Projesi'nde yer almıştır. Projenin 1. turu sonrasında elenen Gui algoritmasının ardından 3. turuna GeMSS ile diğer çok değişken tabanlı imza algoritması Rainbow devam etmiştir. Önerilen GeMSS tabanlı halka imza şemamızı Rainbow tabanlı başka bir halka imza şemasıyla karşılaştırdığımızda, deneysel sonuçlar gösteriyor ki; gruptaki kullanıcı sayısı 50'ye yükseldikçe 300 kat daha hızlı imza doğrulama ve neredeyse 50 kat daha hızlı imza oluşturma süreleri elde etmekteyiz. Ayrıca, önerilen şema en az %20 daha küçük imza boyutu sağlamaktadır. Bu sayede, önerdiğimiz şemanın kullanılmak üzere daha etkili olduğu doğrulanmıştır.

Yayınlar:

· M. Demircioglu, S. Akleylek, and M. Cenk, Efficient GeMSS Based Ring Signature Scheme, Malaysian Journal of Computing and Applied Mathematics, 3(1), pp. 35–39, 2020. DOI: https://doi.org/10.37231/myjcam.2020.3.1.41

· M. Demircioglu, S. Akleylek, and M. Cenk, Efficient GeMSS Based Ring Signature Scheme:Revisited, (incelemede).