



ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

Uygulamalı Matematik Enstitüsü (UME)

Faaliyet Raporu 2020

Orta Doğu Teknik Üniversitesi
Uygulamalı Matematik Enstitüsü

<u>Önsöz</u>	3
<u>İnsan Kaynakları</u>	4
<u>Enstitü Yönetimi</u>	4
<u>Enstitü Personeli</u>	6
<u>Bağlantılı Öğretim Üyeleri - ODTÜ</u>	7
<u>Bağlantılı Öğretim Üyeleri - Diğer Üniversite ve Kurumlar</u>	8
<u>Araştırma</u>	10
<u>Yayınlar</u>	10
<u>SCI-E (A-Tipi) Dergilerde Makaleler</u>	11
<u>SCI-E (B-Tipi) Dergilerde Makaleler</u>	13
<u>Diğer Uluslararası Hakemli Dergilerde Makaleler</u>	14
<u>Kitaplarda Yayınlanan Bölümler</u>	16
<u>Konferans Makaleleri (Proceedings)</u>	16
<u>Kabul Edilmiş, Basım Aşamasındaki Makaleler</u>	17
<u>Basılan Kitaplar</u>	18
<u>Konferans ve Çalıştay Katılımları</u>	19
<u>Editörlükler</u>	20
<u>Bilimsel Etkinlikler</u>	21
<u>Genel Seminerler (Colloquia)</u>	21
<u>Özel Seminer ve Dersler</u>	22
<u>SIAM Student Chapter Seminerleri</u>	24
<u>Konferanslar / Çalıştaylar</u>	25
<u>Kısa Süreli Ziyaretler</u>	25
<u>Gelen Ziyaretçiler</u>	25
<u>Giden Mensuplarımız</u>	26
<u>Projeler</u>	27
<u>TÜBİTAK ve Döner Sermaye Projeleri</u>	28
<u>ODTÜ Bilimsel Araştırma Projeleri (BAP)</u>	30
<u>Eğitim</u>	31
<u>Başvurular, Kabul ve Kayıtlar</u>	31
<u>Enstitü Öğrencilerinin Programlara Göre Dağılımı ve İstatistikler</u>	33
<u>Enstitüdeki Dersler, Öğrenci Sayıları ve İstatistikler</u>	36
<u>Yeni Açılan Dersler</u>	43
<u>Doktora Programları</u>	44
<u>Doktora Mezunları</u>	44

<u>Yüksek Lisans Programları</u>	44
<u>Tezli Yüksek Lisans Mezunları</u>	44
<u>Tezsiz Yüksek Lisans Mezunları</u>	46
<u>Ödüller</u>	47
<u>Ek Bilgiler</u>	48
<u>Yeni Açılan Dersler (2020 Yılı)</u>	48
<u>2019 - 2020 Bahar Dönemi</u>	48
<u>2020 Yılı Doktora Mezunlarımız</u>	50

Önsöz

Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü (UME); kuruluşu olan 2002 yılından bu yana aşağıdaki misyonları gerçekleştirmeyi amaçlamaktadır:

- (i) Üniversitemizin araştırma potansiyeli ve ülkemizin ihtiyaçları göz önüne alınarak, matematik bazlı araştırma/uygulama alanlarında disiplinlerarası çalışma ortamı oluşturmak, bu alanlarda araştırmaya yönelik eğitimler, konferanslar/yaz okulları düzenlemek ve uluslararası işbirliği olanaklarını hayata geçirmek,
- (ii) ODTÜ-Sanayi/Kamu kuruluşları işbirliğini, gerek proje ve ürün geliştirerek gerekse kısa süreli eğitim/araştırma toplantıları düzenleyerek hayata geçirmek,
- (iii) Matematğin; doğayı, teknolojik ve ekonomik süreçleri daha iyi anlama yolunda bilim insanlarının ortak dili olduğundan hareketle yeni ve uygulanabilir Matematik konularında araştırmacıları bilgilendirmek ve bu amaca yönelik araştırmalar yapmak.

UME'nin vizyonu "lisansüstü programları ve araştırmaları ile uluslararası düzeyde saygın ve öncü bir araştırma enstitüsü" olmaktadır. Bu doğrultuda Enstitümüzde; Bilimsel Hesaplama, Finansal Matematik ve Kriptografi olmak üzere üç anabilim dalında yüksek lisans ve doktora eğitimi verilmektedir. Halihazırda yüksek lisans eğitimi verilmekte olan Aktüerya Bilimleri anabilim dalında doktora programının da açılması planlanmaktadır.

Bu raporda Enstitümüz ve Bağlantılı öğretim üyelerimiz ile yüksek eğitim öğrencilerimiz tarafından 2020 yılında gerçekleştirilen akademik etkinlikler ve performans göstergeleri sunulmaktadır. Enstitümüz, bu faaliyet yılında Bilimsel Hesaplama ve Kriptografi Anabilim dallarında olmak üzere iki yeni Dr. Öğretim Üyemizi ve Araştırma Görevlisi kadrosunda iki öğrencimizi kazanmıştır. Doktora programına kayıtlı 96 öğrencimizden %20'si kadarına Yüksek Öğretim Kurumu tarafından verilen YÖK 100/2000 bursları sağlanmaktadır. Kriptoloji, Hesaplamalı Bilişim ve Mühendislik, Yapay Zeka ve Makine Öğrenmesi, Siber Güvenlik kategorilerindeki öncelikli araştırma alanlarında burs almayı hak eden toplam 19 öğrencimiz bulunmaktadır. YÖK 100/2000 bursları aracılığıyla öncelikli araştırma alanlarının Enstitümüz görünürlüğünün artırılması hedeflenmektedir. Covid-19 küresel salgınının birçok akademik etkinliği ve uluslararası ziyaretleri engellemesine rağmen Enstitümüz yayın ve proje sayılarında artış gözlenmiştir. SCI-E kapsamındaki çalışmaların %44,2 kadarı SCI-A, %44,3 kadarı ise SCI-B ve diğer kategorisindeki dergilerde yayınlanmıştır. Kuruluşundan bugüne 94 doktora, 232 tezli yüksek lisans, 142 tezsiz yüksek lisans olmak üzere toplam 468 öğrenci mezun etmiş olan Enstitümüz, 2020 yılında 6 doktora, 7 tezli ve 3 tezsiz yüksek lisans öğrencisine diploma vermiştir.

Uygulamalı Matematik Enstitüsü'nün bugünkü başarısına ulaşmasında emeği olan tüm kadrolu ve bağlantılı öğretim üyeleri, eski yöneticileri ve yardımcıları, araştırma görevlileri ve öğrenci asistanları, idari personeli ve mezunlarımıza teşekkür ederiz.

Saygılarımla,

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

İnsan Kaynakları

Enstitü Yönetimi

Müdür
Prof. Dr. Ömür Uğur* (Uygulamalı Matematik Enstitüsü)
Müdür Yardımcıları
Doç. Dr. Murat Cenk* (Uygulamalı Matematik Enstitüsü)
Doç. Dr. Ceylan Yozgatlıgil* (İstatistik Bölümü)

*Prof. Dr. Ömür Uğur'un 20.11.2020 tarihinde görev süresi sona ermiş, yerine Prof. Dr. A. Sevtap Kestel Müdür olarak atanmıştır. Müdür Yardımcılığı görevlerine ise Prof. Dr. Ertan Onur (Bilgisayar Mühendisliği Bölümü) ve Dr. Öğretim Üyesi Önder Türk 30.11.2020 tarihi itibarıyla atanmışlardır.

Enstitü Kurulu	Enstitü Yönetim Kurulu
Prof. Dr. Ömür Uğur* (Uygulamalı Matematik Enstitüsü)	Prof. Dr. Ömür Uğur* (Uygulamalı Matematik Enstitüsü)
Doç. Dr. Murat Cenk* (Uygulamalı Matematik Enstitüsü)	Doç. Dr. Murat Cenk* (Uygulamalı Matematik Enstitüsü)
Doç. Dr. Ceylan Yozgatlıgil* (İstatistik)	Doç. Dr. Ceylan Yozgatlıgil* (İstatistik)
Prof. Dr. Ferruh Özbudak (Matematik, Kriptografi EABD Başkanı)	Doç. Dr. Seza Danışoğlu (İşletme)
Prof. Dr. A. Sevtap Kestel (Aktüerya Bilimleri ve Finansal Matematik EABD Başkanı)	Prof. Dr. Murat Manguoğlu (Bilgisayar Mühendisliği)
Doç. Dr. Hamdullah Yücel** (Bilimsel Hesaplama EABD Başkanı)	Dr. Öğr.Üyesi Nil İpek Şirikçi (İktisat)

*Prof. Dr. Ömür Uğur'un görev süresi 20.11.2020 tarihinde sona ermiş, yerine Prof. Dr. A. Sevtap Kestel Müdür olarak atanmıştır. Müdür Yardımcılığı görevine ise Prof. Dr. Ertan Onur (Bilgisayar Mühendisliği Bölümü) ve Dr. Öğretim Üyesi Önder Türk 30.11.2020 tarihi itibarıyla atanmışlardır.

**Doç. Dr. Hamdullah Yücel 28.04.2020 tarihinde görevinden ayrılmış olup, yerine 1 Aralık 2020 tarihine kadar Prof. Dr. Ömür Uğur atanmıştır.

Enstitü Personeli**Öğretim Üyeleri**

Murat Cenk, Doç. Dr.

A. Sevtap Kestel, Prof. Dr.

Ali Devin Sezer, Doç. Dr.

Önder Türk, Dr.

Ömür Uğur, Prof. Dr.

Oğuz Yayla, Dr.

Hamdullah Yücel, Doç. Dr.

Araştırma Görevlileri

Gülçin Akarsu

Pelin Çiloğlu

Esra Günsay

Zeynelabidin
Karakaş (35. madde)

Kübra Kaytancı

Mustafa Kütük

Oğuz Koç

Özenç Murat Mert

Meral Şimşek

Özge Tekin

Sıtkı Can Toraman

Bükre Yıldırım Külekci

Cem Yavrum

Hasan Bartu Yünüak

Öğretim Görevlisi

İrem Kesinkurt Paksoy

DOSAP

Maryam Sheikhi Garjan

İdari Personel

Nejla Erdoğan (Enstitü Sekreteri)

Serkan Demiröz (Sekreter)

Saffet Aykın (İdari Amir)

Cafer Topal (Görevli)

Ömer Ergüven (Bilgisayar İşletmeni)

Ebru Gündoğdu (Sekreter)

Muharrem Kayabel (Görevli)

Bağlantılı Öğretim Üyeleri - ODTÜ

Matematik	Ali Doğanaksoy, Doç. Dr. Songül Kaya Merdan, Prof. Dr. Ferruh Özbudak, Prof. Dr. Muhiddin Uğuz, Dr.
İstatistik	B. Burçak Başbuğ Erkan, Doç. Dr. Vilda Purutçuoğlu Gazi, Prof. Dr. Ceylan Yozgatlıgil, Doç. Dr.
Bilgisayar Mühendisliği	Emre Akbaş, Dr. Pelin Angın, Dr. Şeyda Ertekin Bolelli, Doç. Dr. Murat Manguoğlu, Prof. Dr. Ertan Onur, Prof. Dr.
Havacılık ve Uzay Mühendisliği	Ercan Gürses, Doç. Dr.
İktisat	Esmâ Gaygısız, Doç. Dr. Nil İpek Şirikçi, Dr.
İnşaat Mühendisliği	Serdar Göktepe, Doç. Dr.
İşletme	Seza Danışoğlu, Doç. Dr. Nuray Güner, Prof. Dr. Adil Oran, Doç. Dr.
Emekli Öğretim Üyeleri	Ersan Akyıldız, Prof. Dr. Aydın Aytuna, Prof. Dr. Selçuk Bayın, Prof. Dr. Cüneyt Bazlamaçcı, Prof. Dr. İ. Yurdahan Güler, Prof. Dr. Azize Hayfavi, Doç. Dr. Bülent Karasözen, Prof. Dr. Münevver Tezer-Sezgin, Prof. Dr. Abdurrahim Yılmaz, Prof. Dr.

Bağlantılı Öğretim Üyeleri - Diğer Üniversite ve Kurumlar

Ankara Üniversitesi	Furkan Başer, Doç. Dr. Fatih Tank, Prof. Dr.
Atılım Üniversitesi	Ümit Aksoy, Doç. Dr. Burcu Gülmez Temür, Doç. Dr. Fatih Sulak, Doç. Dr. Cansu Betin Onur, Dr.
Başkent Üniversitesi	Özge Sezgin-Alp, Doç. Dr.
Cumhurbaşkanlığı	Pınar Gürkan Balıkçioğlu, Dr. Mehmet Uzunkaya, Dr.
Bilkent Üniversitesi	Çağın Ararat, Dr. Firdevs Ulus, Dr.
Boğaziçi Üniversitesi	Könül Bayramoğlu Kavlak, Doç. Dr.
Çankaya Üniversitesi	A Nurdan Saran Buz, Dr. Özlem Türker Bayrak, Doç. Dr. Özlem Defterli, Dr.
Hacettepe Üniversitesi	Başak Bulut Karageyik, Dr. Uğur Karabey, Dr. Mehmet Baha Karan, Prof. Dr. Ş. Kasırğa Yıldırak, Prof. Dr.
Karabük Üniversitesi	Eda Tekin, Dr.
Katholieke Universiteit Leuven	Vincent Rijmen, Prof. Dr.
MICRA	Serdar Dalkır, Dr.
Necmettin Erbakan Üniversitesi	Ahmet Sınak, Dr.
Ondokuz Mayıs Üniversitesi	Sedat Akleylek, Doç. Dr. Erdem Alkım, Dr.
Poznan University of Technology	Gerhard-Wilhelm Weber, Prof. Dr.
Rice Üniversitesi (A.B.D.)	Tayfun E. Tezduyar, Prof. Dr.
Sinop Üniversitesi	Murat Uzunca, Doç. Dr.
Süleyman Demirel Üniversitesi	Barış Bülent Kırlar, Doç. Dr.
Technical University of Kaiserslautern	Ralf Korn, Prof. Dr.

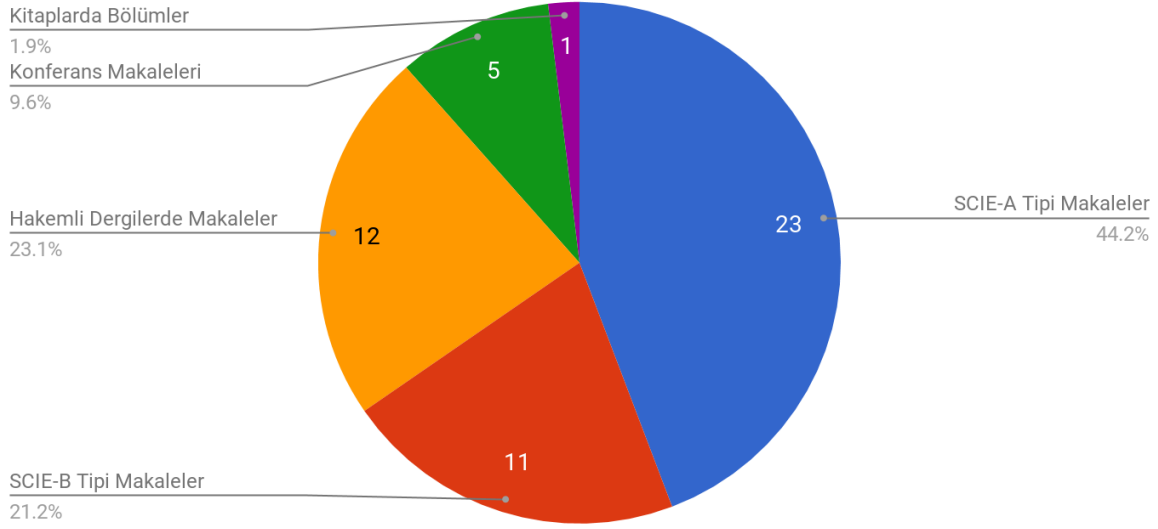
TOBB-ETÜ	Tahir Hanalioğlu, Prof. Dr. Zülfükar Saygı, Doç. Dr. Ali Aydın Selçuk, Prof. Dr.
TÜBİTAK	İsa Sertkaya, Dr.
Türk Hava Kurumu Üniversitesi	Tuğba Akman Yıldız, Dr.
Türk Standartları Enstitüsü	Ezgi Avcı, Dr.

Araştırma

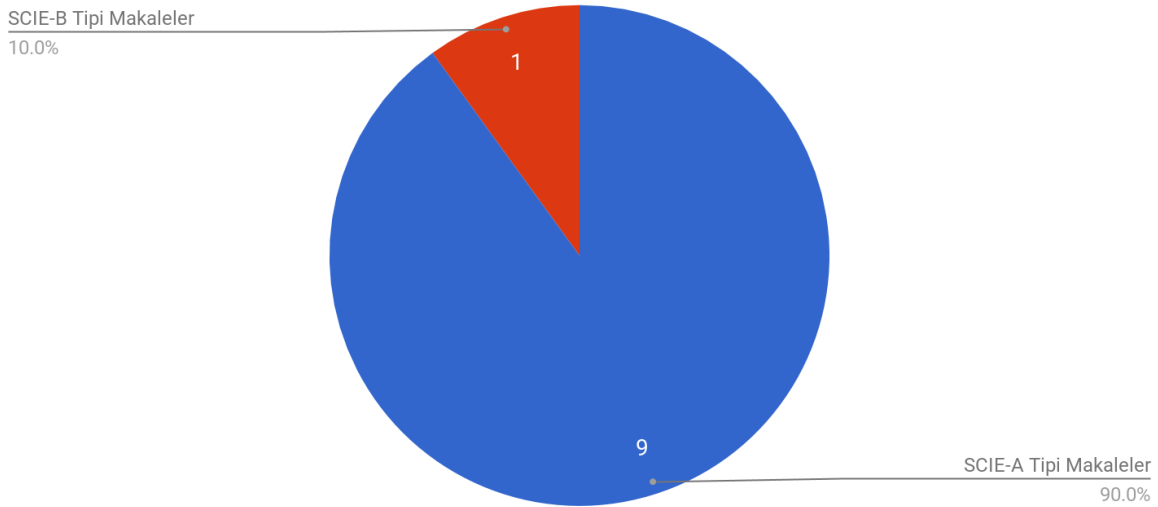
Yayınlar

Enstitümüz adresli yayınlarımızı genellikle SCI-E A, SCI-E B Tipi ve diğer Hakemli Dergilerdeki makaleler ve Konferans Bildirileri oluşturmaktadır. Bunun yanı sıra Kitaplarda Bölümler ve Editoryal Yayınlar da Enstitümüzün yayın portföyünde yer almaktadır. Yayınlarımıza ait istatistikler aşağıda belirtilmiştir.

Yayınlar (2020)



Basım Aşamasındaki Yayınlar (2021)



SCI-E (A-Tipi) Dergilerde Makaleler

Aşağıda SCI-E (A-Tipi) Dergilerdeki Uygulamalı Matematik Enstitüsü adresli yayınların listesine yer verilmiş olup, 2021 yılında basım aşamasında olan yayınlar yer almamaktadır.

[1]	Yıldız, H., Cenk, M., Onur, E., PLGAKD: A PUF-based lightweight group authentication and key distribution protocol, IEEE Internet of Things Journal, 14, pp. 1-14, 2020. DOI:10.1109/JIOT.2020.3032757
[2]	Kozpınar, S., Uzunca, M., Karasozen, B., Pricing European and American options under Heston model using discontinuous Galerkin finite elements, Mathematics and Computers in Simulation, 177, pp. 568-587, 2020. DOI:10.1016/j.matcom.2020.05.022
[3]	Karasozen, B., Uzunca, M., Kucukseyhan, T., Reduced order optimal control of the convective FitzHugh-Nagumo equations, Computers and Mathematics with Applications, 79(4), pp. 982-995, 2020. DOI:10.1016/j.camwa.2019.08.009
[4]	Elgindy, K. T., Karasozen, B., Distributed optimal control of viscous Burgers' equation via a high-order, linearization, integral, nodal discontinuous Gegenbauer-Galerkin method, Optimal Control Applications and Methods, 44(1), pp. 253-277, 2020. DOI: 10.1002/oca.2541
[5]	Özbudak, F., Pelen, R. M., Duals of non-weakly regular bent functions are not weakly regular and generalization to plateaued functions, Finite Fields and Their Applications, 64, pp. 101668, 2020. DOI:10.1016/j.ffa.2020.101668
[6]	Etzion, T., Kurz, S., Ota, K., Özbudak, F., Subspace packings: constructions and bounds, Design Codes and Cryptography, 88, pp. 1781-1810, 2020. DOI:10.1007/s10623-020-00732-z
[7]	Salagean, A., Özbudak, F., Counting Boolean functions with faster points, Design Codes and Cryptography, 88, pp. 1867-1883, 2020. DOI:10.1007/s10623-020-00738-7
[8]	Ünlü, K. D., Sezer, A. D., Excessive backlog probabilities of two parallel queues, Annals of Operations Research, 293(1), pp.141-174, 2020. DOI:10.1007/s10479-019-03324-w
[9]	Başoğlu-Kabran, F., Sezer, A.D., Approximation of the exit probability of a stable Markov modulated constrained random walk, Annals of Operations Research, 2020. DOI:10.1007/s10479-020-03693-7

[10]	Türk, Ö., Approximation of the Stokes eigenvalue problem on triangular domains using a stabilized finite element method, <i>Meccanica</i> , 55(10), pp. 2021–2031, 2020. DOI:10.1007/s11012-020-01243-w
[11]	Tirkolaee, E. B., Goli, A., Soltani, M., Weber, G. W., Multi-objective optimization for the reliable pollution-routing problem with cross-dock selection using Pareto-based algorithms, <i>Journal of Cleaner Production</i> , 276, pp. 122927, 2020. DOI:10.1016/j.jclepro.2020.122927
[12]	Tirkolaee, E. B., Aydin, N. S., Ranjbar-Bourani, M., Weber, G. W., A Robust bi-objective mathematical model for disaster rescue units allocation and scheduling with learning effect, <i>Computers and Industrial Engineering</i> , 149, pp. 106790, 2020. DOI:10.1016/j.cie.2020.106790
[13]	Das, S. K., Roy, S. K., Weber, G. W., Application of type-2 fuzzy logic to a multiobjective green solid transportation-location problem with Dwell time under carbon tax, cap, and offset policy: fuzzy versus Nonfuzzy techniques, <i>IEEE Transactions on Fuzzy Systems</i> , 28(11), pp. 2711-2725, 2020. DOI:10.1109/TFUZZ.2020.3011745
[14]	Tirkolaee, E. B., Goli, A., Weber, G. W., Fuzzy mathematical programming and self-adaptive artificial fish Swarm algorithm for just-in-time energy-aware flow shop scheduling problem with outsourcing option, <i>IEEE Transactions on Fuzzy Systems</i> , 28(11), pp. 2772-2783, 2020. DOI:10.1109/TFUZZ.2020.2998174
[15]	Kalaycı, B., Ozmen, A., Weber, G. W., Mutual relevance of investor sentiment and finance by modeling coupled stochastic systems with MARS, <i>Annals of Operations Research</i> , 295(1), pp. 183-206, 2020. DOI:10.1007/s10479-020-03757-8
[16]	Inc, M., Bouteraa, N., Akinlar, M. A., Benaicha, S., Chu, Y. M., Weber, G. W., Almohsen, B., New positive solutions of nonlinear elliptic PDEs, <i>Applied Sciences-Basel</i> , 10(14), pp. 4863, 2020.
[17]	No, F. G., Dogrusoz, Y. S., Onak, O. N., Weber, G. W., Reduced leadset selection and performance evaluation in the inverse problem of electrocardiography for reconstructing the ventricularly paced electrograms, <i>Journal of Electrocardiology</i> , 60, pp. 44-53, 2020. DOI: 10.1016/j.jelectrocard.2020.02.017
[18]	Tirkolaee, E. B., Mardani, A., Dashtian, Z., Soltani, M., Weber, G. W., A novel hybrid method using fuzzy decision making and multi-objective programming for sustainable-reliable supplier selection in two-echelon supply chain design, <i>Journal of Cleaner Productions</i> , 250, pp. 119517, 2020. DOI:10.1016/j.jclepro.2019.119517

[19]	Tirkolaei, E. B., Mahdavi, I., Esfahani, M. M. S., Weber, G. W., A robust green location-allocation-inventory problem to design an urban waste management system under uncertainty, Waste Management, 102, pp. 340-350, 2020. DOI:10.1016/j.wasman.2019.10.038
[20]	Akteke-Ozturk, B., Weber, G. W., Koksall, G., Generalized desirability functions: a structural and topological analysis of desirability functions, Optimization, 69(1), pp. 115-130, 2020. DOI:10.1080/02331934.2019.1570192
[21]	Grobelny, J., Michalski, R., Weber, G. W., Modeling human thinking about similarities by neuromatrices in the perspective of fuzzy logic, Neural Computing and Applications, 2020. DOI:10.1007/s00521-020-05363-y
[22]	Khalilpourazari, S., Khalilpourazary, S., Ciftcioglu, A. O., Weber, G. W., Designing energy-efficient high-precision multi-pass turning processes via robust optimization and artificial intelligence, Journal of Intelligent Manufacturing, 2020. DOI:10.1007/s10845-020-01648-0
[23]	Savku, E., Weber, G. W., Stochastic differential games for optimal investment problems in a Markov regime-switching jump-diffusion market, Annals of Operations Research, 2020. DOI:10.1007/s10479-020-03768-5
[24]	Türk, Ö., An MHD Stokes eigenvalue problem and its approximation by a spectral collocation method, Computers and Mathematics with Applications, 80(9), pp. 2045–2056, 2020. DOI:10.1016/j.camwa.2020.09.002

SCI-E (B-Tipi) Dergilerde Makaleler

Aşağıda SCI-E (B-Tipi) Dergilerdeki Uygulamalı Matematik Enstitüsü adresli yayınların listesine yer verilmiş olup, 2021 yılında basım aşamasında olan yayınlar yer almamaktadır.

[1]	Türkvatan, A., Hayfavi, A., Omay, T., A regime switching model for temperature modeling and applications to weather derivatives pricing, Mathematics and Financial Economics, 14(1), pp. 1-42, 2020. DOI:10.1007/s11579-019-00242-0
[2]	Kırlar, B. B., Efficient message transmission via twisted Edwards curves, Mathematica Slovaca, 70(6), pp. 1511-1520, 2020. DOI:10.1515/ms-2017-0444
[3]	Ergun, S., Kırlar, B. B., Gok, S. Z. A., Weber, G. W., An application of crypto cloud computing in social networks by cooperative game theory, Journal of Industrial and Management Optimization, 16(4), pp. 1927-1941, 2020. DOI:10.3934/jimo.2019036

[4]	Özbudak, F., Tekin, E., Correlation distribution of a sequence family generalizing some sequences of Trachtenberg, <i>Advances in Mathematics of Communications</i> , 14, 2020. DOI:10.3934/amc.2020087
[5]	Evcin, C., Uğur, Ö., Tezer-Sezgin, M., Controlling the power-law fluid flow and heat transfer under the external magnetic field using the flow index and the Hartmann number, <i>International Journal of Computational Methods</i> , 17(3), 2020. DOI:10.1142/S0219876218501438
[6]	Graczyk-Kucharska, M., Ozmen, A., Szafranski, M., Weber, G. W., Golinski, M., Spychala, M., Knowledge accelerator by transversal competences and multivariate adaptive regression splines, <i>Central European Journal of Operations Research</i> , 28(2), pp. 645-669, 2020. DOI:10.1007/s10100-019-00636-x
[7]	Bhaumik, A., Roy, S. K., Weber, G. W., Hesitant interval-valued intuitionistic fuzzy-linguistic term set approach in Prisoners' dilemma game theory using TOPSIS: a case study on Human-trafficking, <i>Central European Journal of Operations Research</i> , 28(2), pp. 797-716, 2020. DOI:10.1007/s10100-019-00638-9
[8]	Ali, S. S., Kaur, R., Ersoz, F., Altaf, B., Basu, A., Weber, G. W., Measuring carbon performance for sustainable green supply chain practices: a developing country scenario, <i>Central European Journal of Operations Research</i> , 28(4), pp. 1389-1416, 2020. DOI:10.1007/s10100-020-00673-x
[9]	Pervin, M., Roy, S. K., Weber, G. W., An integrated vendor-buyer model with quadratic demand under inspection policy and preservation technology, <i>Hacettepe Journal of Mathematics and Statistics</i> , 49(3), pp. 1168-1189, 2020. DOI:10.15672/hujms.476056
[10]	Evkaya, O. O., Yozgatigil, C. , Selcuk-Kestel, A. S., CD-vine model for capturing complex dependence, <i>Journal of Applied Statistics</i> , 2020. DOI:10.1080/02664763.2020.1834519
[11]	Taylan, P., Yerlikaya-Ozkurt, F., Ucak, B. B., Weber, G. W., A new outlier detection method based on convex optimization: application to diagnosis of Parkinson's disease, <i>Journal of Applied Statistics</i> , 2020. DOI:10.1016/j.scitotenv.2020.14360710.1080/02664763.2020.1864815

Diğer Uluslararası Hakemli Dergilerde Makaleler

Aşağıda diğer Uluslararası Hakemli Dergilerdeki Uygulamalı Matematik Enstitüsü adresli yayınların listesine yer verilmiş olup, 2021 yılında basım aşamasında olan yayınlar yer almamaktadır.

[1]	Alkım, E., Bilgin, Y. A., Cenk, M., Gérard, F., Cortex-M4 optimizations for {R, M} LWE schemes, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(3), pp. 336-357, 2020. DOI:10.13154/tches.v2020.i3.336-357
[2]	Evrin M. U., Cenk, M., A parallel gpu implementation of swifftx, Lecture Notes in Computer Science, 11989, 2020. DOI:10.1007/978-3-030-43120-4_16
[3]	Demircioğlu, M., Akleyek, S., Cenk, M., Efficient GeMSS based ring signature scheme, Malaysian Journal of Computing and Applied Mathematics, 3(1), pp. 35-39, 2020. DOI:10.37231/myjcam.2020.3.1.41
[4]	Karasan, A., Gaygısız, E., Volatility prediction and risk management: An SVR-GARCH approach, The Journal Financial Data Science, 2(4), pp. 85-104, 2020. DOI:10.3905/jfds.2020.1.046
[5]	Karasozen, E., Karasozen, B., Earthquake location methods, Gem-International Journal on Geomathematics, 11(1), pp. 13, 2020. DOI:10.1007/s13137-020-00149-9
[6]	Hasgül, E. , Selcuk-Kestel, A. S. , Yolcu-Okur, Y., Forecasting mortality rates with a general stochastic mortality trend model, Communications Faculty of Sciences University of Ankara Series A1 Mathematics and Statistics, 69(1), pp. 910-928, 2020. DOI:10.31801/cfsuasmas.478265
[7]	Carlet, C., Guilley, S., Güneri, C., Mesnager, S., Özbudak, F., Construction of efficient codes for high-order direct sum masking, Security and Privacy in the Internet of Things: Challenges and Solutions, 27, pp. 108-128, 2020. DOI:10.3233/AISE200008
[8]	Inc, M., Akinlar, M. A., Tchier, F., Bal, C., Bousbahi, F., Tawfiq, F. M. O., Weber, G. W., Solutions of fractional-stochastic Bao's system, Alexandria Engineering Journal, 59(6), pp. 4997-5006, 2020. DOI:10.1016/j.scitotenv.2020.14360710.1016/j.aej.2020.09.018
[9]	Tomaskova, H., Weber, G. W., Approaches combining methods of operational research with business process model and notation: A systematic review, PeerJ Computer Science, 6: e301, 2020.

[10]	Das, S. K., Roy, S. K., Weber, G. W., An exact and a heuristic approach for the transportation-p-facility location problem, Computational Management Science, 17(3), pp. 389-407, 2020. DOI:10.1007/s10287-020-00363-8
[11]	Mesnager S., Sınak A., Yayla O., Threshold-based post-quantum secure verifiable multi-secret sharing for distributed storage blockchain, Mathematics, 8(12), pp. 1-15, 2020. DOI:10.3390/math8122218
[12]	Yıldırım-Külekci, B., Büyükyazıcı, M., Effect of Turkish mortality developments on the expected lifetime and annuity using entropy measure, Journal of Statisticians: Statistics and Actuarial Sciences (JSSAS), 13(1), pp. 30-47, 2020.

Konferans Makaleleri (Proceedings)

Aşağıda Konferans Kitapçıklarında Uygulamalı Matematik Enstitüsü adresli yayınların listesine yer verilmiş olup, 2021 yılında basım aşamasında olan yayınlar yer almamaktadır.

[1]	Taşkın, H. K., Cenk. M., TMVP-friendly primes for efficient elliptic curve cryptography, 2020 International Conference on Information Security and Cryptology (ISCTURKEY), pp. 80-87, 2020. DOI:10.1109/ISCTURKEY51113.2020.9307999
[2]	Millidere M., Kurt, H. B., Balli H., Uğur, Ö., Kalman based neural network analysis with resampling methods for longitudinal aerodynamic coefficient estimation, AIAA AVIATION 2020 Forum, Virtual, Online, , ss. 1-25, 15 - 19 Haziran 2020. DOI:10.2514/6.2020-3197
[3]	Cengizci, S., Uğur, Ö., Srinivasan, N., A SUPG formulation for solving a class of singularly perturbed steady problems in 2D, The 20th Biennial Computational Techniques and Applications Conference (CTAC 2020 online edition), Sydney, NSW, Australia, 30th Aug–2nd Sep 2020
[4]	Cengizci, S., Uğur, Ö., Takizawa, K., Tezduyar, T., A Streamline-upwind/Petrov-Galerkin formulation for supersonic and hypersonic flow simulations, The 20th Biennial Computational Techniques and Applications Conference (CTAC 2020 online edition), Sydney, NSW, Australia, 30th Aug–2nd Sep 2020
[5]	Kurt, H. B., Millidere, M., Gomec, F. S., Uğur, Ö., Multi-fidelity aerodynamic dataset generation of a fighter aircraft, AIAA Scitech 2021 Forum, VIRTUAL EVENT, 19–21 January 2021. DOI:10.2514/6.2021-0544

Kabul Edilmiş, Basım Aşamasındaki Makaleler

Aşağıda Uygulamalı Matematik Enstitüsü adresli 2021 yılında basım aşamasında olan yayınlara yer verilmiştir.

[1]	Yücel, H., Goal-oriented a posteriori error estimation for Dirichlet boundary control problems, Journal of Computational and Applied Mathematics, 381, 2021. DOI:10.1016/j.cam.2020.113012
[2]	Eksert, L., Yücel, H., Onur, E., Intra- and inter-cluster link scheduling in CUPS-based ad hoc networks, Computer Networks, 185, 2021. DOI:10.1016/j.comnet.2020.107659
[3]	Ali, S. S., Ersoz, F., Kaur, R., Altaf, B., Weber, G. W., A quantitative analysis of low carbon performance in industrial sectors of developing world, Journal of Cleaner Production, 284, pp. 125268, 2021. DOI:10.1016/j.jclepro.2020.125268
[4]	Tirkolaee, E. B., Abbasian, P., Weber, G. W., Sustainable fuzzy multi-trip location-routing problem for medical waste management during the COVID-19 outbreak, Science of the Total Environment, 756, pp. 143607, 2021. DOI:10.1016/j.scitotenv.2020.143607
[5]	Türk, Ö., A DRBEM approximation of the Steklov eigenvalue problem, Engineering Analysis with Boundary Elements, 122, pp. 232–241, 2021. DOI:10.1016/j.enganabound.2020.11.003
[6]	Gurbuz, B., Mawengkang, H., Husein, I., Weber, G. W., Rumour propagation: an operational research approach by computational and information theory, Central European Journal of Operations Research, 2021. DOI:10.1016/j.scitotenv.2020.14360710.1007/s10100-020-00727-0
[7]	Lotfi, R., Mardani, N., Weber, G. W., Robust bi-level programming for renewable energy location, International Journal of Energy Research, 2021. DOI:10.1002/er.6332
[8]	Çıbık, A. B., Eroğlu, F. G., Kaya-Merdan, S., On the performance of curvature stabilization time stepping methods for double-diffusive natural convection flows in the presence of magnetic field, Numerical Algorithms, 2021. DOI:10.1007/s11075-020-01046-w
[9]	Cabuk, S., Mert, Ö. M., Selcuk-Kestel, A. S., Kalayci, E., Forecasting the Hydro Inflow and Optimization of Virtual Power Plant Pricing, CEVI Springer Book Chapter 2021
[10]	Özbudak, F., Salagean, A., New generalized almost perfect nonlinear functions, Finite Fields and Their Applications, 70, pp. 101796, 2021. DOI:10.1016/j.ffa.2020.101796

[11]	Mert, Ö. M., Selcuk-Kestel, A. S., Time dependent stop-loss reinsurance and exposure curves, Journal of Computational and Applied Mathematics, 389, 2021. DOI: 10.1016/j.cam.2020.113348
[12]	Karasozen, B., Yildiz, S., Uzunca, M., Structure preserving model order reduction of shallow water equations, Mathematical Methods in the Applied Sciences, 44(1), pp. 476-492, 2021. DOI:10.1002/mma.6751

Konferans ve Çalıştay Katılımları

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

[1]	Akcengiz, Z., Aslan, M., Karabayır, Ö., Doğanaksoy, A., Uğuz, M., Sulak, F., Statistical randomness tests of long sequences by dynamic partitioning, in: 2020 International Conference on Information Security and Cryptology (ISCTURKEY)
[2]	Yıldırım-Külekci, B., Selcuk-Kestel, A. S., Karabey, U., Backtesting in time varying extreme value copulas for dependent risks, in: Online International Conference in Actuarial Science (OICA).
[3]	Aksoy, Z., Kırklar, B. B., Planarity of a new class of Dembowski-Ostrom polynomials, in: 3rd International Conference on Mathematical Advances and Applications (ICOMAA 2020), İstanbul Turkey, 2020
[4]	Cengizci, S., Uğur, Ö., Srinivasan, N., A stabilized finite element formulation for numerical simulation of convection-dominated reactive models, in: International Conference on Advances in Differential Equations and Numerical Analysis (ADENA2020), Indian Institute of Technology Guwahati, October 12 - 15, 2020 (Online). DOI: 10.13140/RG.2.2.12131.78887
[5]	Çiloğlu, P., Yücel, H., Partial differential equations with random input data, in: COST Action Mat-Dyn-Net Meeting in Zagreb, Zagreb, Croatia, 24 - 27 February 2020

Bilimsel Etkinlikler

Enstitümüzün bilimsel etkinliklerini, dönem boyunca süren ve Salı günleri düzenlenen Genel Seminerler oluşturmaktadır. Ayrıca, farklı zamanlarda Özel Seminerler ve Dersler adıyla alana yönelik etkinlikler yapılmaktadır. Türkiye’de yalnızca 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 2020 yılında yapılan Bilimsel Etkinliklere yer verilmiştir.

Özel Seminer ve Dersler

[1]	Leila Miller, Some Results on Uniform Statistical Convergence, and New Results on Ideal Convergence, 11-12 Mart 2020 (Saraybosna Uluslararası Üniversitesi, Bosna)
-----	--

SIAM Student Chapter Seminerleri

[1]	Mehmet Alp Üreten, Scientific Computing Lecture Series: Introduction to MATLAB Programming, 17 February 2020 (Institute of Applied Mathematics, Middle East Technical University, Turkey)
[2]	Semih Tümen, Seeking Causality in Empirical Research, 18 February 2020 (Economics, TED University, Turkey)
[3]	Eda Oktay, Scientific Computing Lecture Series: Introduction to MATLAB Programming, 18 February 2020 (Institute of Applied Mathematics, Middle East Technical University, Turkey)
[4]	Sıtkı Can Toraman, Scientific Computing Lecture Series: Introduction to MATLAB Programming, 19 February 2020 (Institute of Applied Mathematics, Middle East Technical University, Turkey)

[5]	Elif Düşmez Tek, A Brief Overview of Turkish Electricity Market & Approaches for Market Modeling Studies, 25 February 2020 (Partner & Energy and Resources Industry Leader, Deloitte Turkey)
[6]	Selin Egehan, Are You Ready for Your First Job Interview?, 03 March 2020 (Consultant at Michael Page, Turkey)
[7]	Ömür Uğur, IAM & METU SIAM Student Chapter: Python Lecture Series, 09 March 2020 (Institute of Applied Mathematics, Middle East Technical University, Turkey)
[8]	Emrah Özdemir, SIAM TALKS, 10 March 2020 (Project Leader, Roketsan, Turkey)
[9]	Özge Tekin, IAM & METU SIAM Student Chapter: Python Lecture Series, 10 March 2020 (Institute of Applied Mathematics, Middle East Technical University, Turkey)
[10]	Onur Enginar, IAM & METU SIAM Student Chapter: Python Lecture Series, 11 March 2020 (Business Administration, Hacettepe University, Turkey)

Kısa Süreli Ziyaretler

Gelen Ziyaretçiler

[1]	Leila Miller, Erasmus Teaching Mobility, 9-13 Mart 2020 (Saraybosna Uluslararası Üniversitesi, Bosna)
-----	---

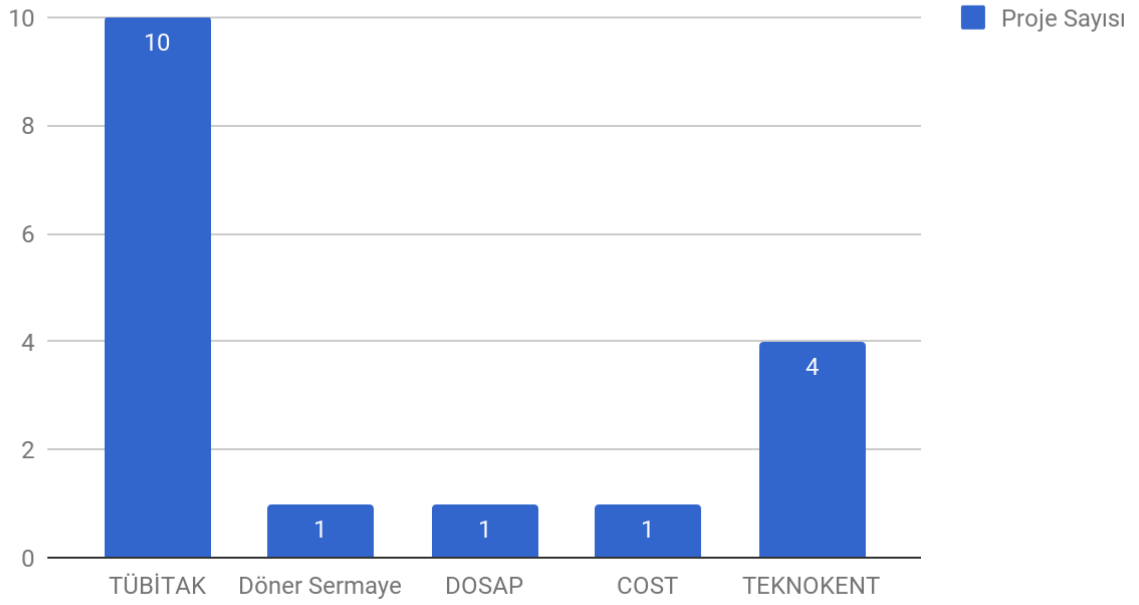
Giden Mensuplarımız

[1]	Meral Şimşek; 10 Ocak-20 Mart 2020 tarihleri arasında 'ERASMUS ve staj için Liverpool Üniversitesi, Birleşik Krallık'ta bulunmuştur.
[2]	Murat Cenk; 1 Temmuz-25 Eylül 2020 tarihleri arasında 'Waterloo University, Canada' ziyaretinde bulunmuş, 'Proje tabanlı Mevlana Değişim Programı kapsamında Kriptografik Hesaplamalar' üzerine araştırma yapmak için katılmıştır.
[3]	Murat Cenk; 20 Ocak-19 Şubat 2020 tarihleri arasında 'Waterloo University, Canada' ziyaretinde bulunmuş, 'Proje tabanlı Mevlana Değişim Programı kapsamında Kriptografik Hesaplamalar' üzerine araştırma yapmak için katılmıştır.
[4]	Tuğba Aru, Aktüerya Bilimleri/Finansal Matematik yüksek lisans programı öğrencisi 2019-2020 akademik yılı I ve II. Döneminde Ulm Üniversitesi, Almanya'da ERASMUS çerçevesinde bulunmuştur.

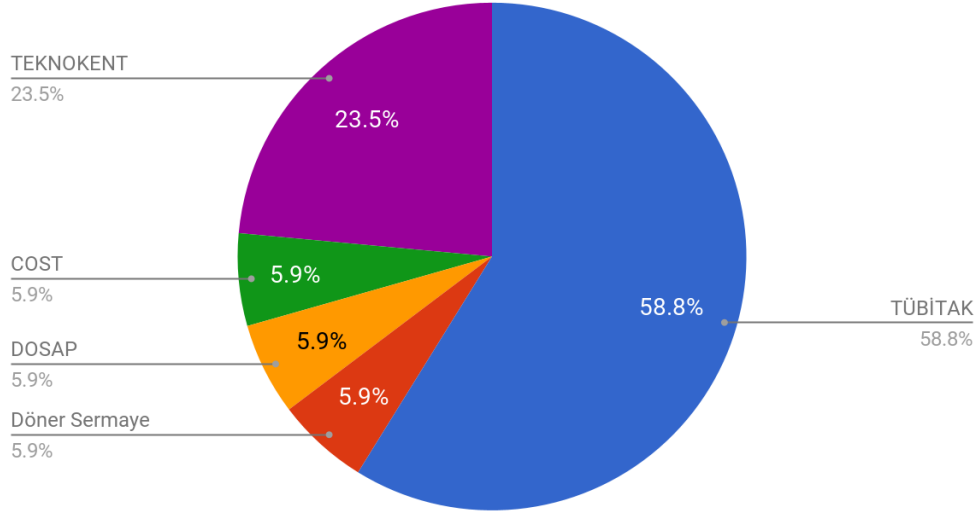
Projeler

Enstitümüzün çatısı altında yürütülen proje sayıları ve öğretim üyelerimizin araştırmacı olarak yer aldıkları proje bilgileri aşağıda verilmektedir. Aşağıdaki grafikte de görüldüğü gibi TÜBİTAK (%52,9) kaynaklı projelerin ağırlıklı olması sevindiricidir. Bunun yanı sıra, Teknokent projeleri de ikinci sırada yer almaktadır. Döner Sermaye, COST ve BAP projelerinin artırılması hedeflenmektedir.

Proje Sayıları



Proje Dağılımı (2020)



TÜBİTAK, Döner Sermaye ve Diğer Projeler

[1]	Proje Adı: Süpersingüler İzogen Tabanlı Kriptografik Protokollerin Geliştirilmesi (TÜBİTAK) Yürütücü: Murat Cenk Araştırmacılar: Sheikhi, M., Kılıç, N. G. O., Doğan, C. Başlangıç – Bitiş Tarihleri: 2020 – 2021 Bütçesi: 44 996 TL
[2]	Proje Adı: Kriptografik Algoritmaların Tasarımı, Gerçekleştirilmeleri ve Uygulamaları (TÜBİTAK) Yürütücü: Murat Cenk Araştırmacılar: Nazlı Deniz Türe, Sermin Çakın, Yaman, N., Kırçalı, M. Başlangıç – Bitiş Tarihleri: 2019 – 2025 Bütçesi: 2 352 480 TL
[3]	Proje Adı: Hızlı Polinom Çarpması (TÜBİTAK) Yürütücü: Murat Cenk, Ferruh Özbudak Araştırmacılar: Tülay Ayyıldız Akoğlu Başlangıç – Bitiş Tarihleri: 2020 – 2021 Bütçesi: 155 000 TL
[4]	Proje Adı: Hava Kuvvetleri Yardımlaşma Derneği Birikimlerinin Aktüeryal Değerlendirmesi 31.12.2019 (DÖNER SERMAYE) Yürütücü: Ayşe Sevtap Selcuk-Kestel Araştırmacılar: Bükre Yıldırım-Külekcı Başlangıç – Bitiş Tarihleri: Ocak 2020 – Mart 2020 Bütçesi: 8 500 TL

[5]	Proje Adı: Ntru Tabanlı Kriptosistemlerin Tasarımı ve Biçimsel Yöntemler İle Analizi (TÜBİTAK) Yürütücü: Sedat Akleylek UME Araştırmacı: Oğuz Yayla Başlangıç – Bitiş Tarihleri: 15 Şubat 2019 – 15 Şubat 2021 Bütçesi: 390 490 TL
[6]	Proje Adı: Kafes Tabanlı Güvenilir Kriptografik Protokol Tasarımı ve Verimli Uygulamaları (TÜBİTAK) Yürütücü: Sedat Akleylek UME Araştırmacı: Oğuz Yayla Başlangıç – Bitiş Tarihleri: 2018 – 2020 Bütçesi: 469 778 TL
[7]	Proje Adı: Kodlama Teorisi ve Uygulamaları Üzerine Araştırma (TÜBİTAK-Güney Kore Ulusal Araştırma Vakfı (NRF)) Yürütücü: Ferruh Özbudak Başlangıç – Bitiş Tarihleri: 19 Aralık 2020 – 1 Ocak 2022 Bütçesi: –
[8]	Proje Adı: Tekil Son Değerli, Geriye Doğru Stokastik Diferansiyel Denklemler ve Finansal Uygulamaları (TÜBİTAK 1001, 118F163) Yürütücü: Ali Devin Sezer Başlangıç – Bitiş Tarihleri: 1 Kasım 2018 – 1 Kasım 2020 Bütçesi: 225 650 TL
[9]	Proje Adı: Petrol ve Gaz Rezervuar Problemleri için Sayısal Çalışmalar (TÜBİTAK 1001: 119F022) Yürütücü: Hamdullah Yücel Araştırmacılar: Hamidullah Enes Ay, Pelin Çiloğlu, Sıtkı Can Toraman, Mehmet Alp Üreten, Başlangıç – Bitiş Tarihleri: 1 Ağustos 2019 – 1 Ağustos 2021 Bütçesi: 241 500 TL
[10]	Proje Adı: Kuantum Ertesi Kütüphanesi (TEKNOKENT) Yürütücü: Murat Cenk Araştırmacılar: Hasan Bartu Yünüak Başlangıç – Bitiş Tarihleri: 2020 – 2022 Bütçesi: 21 000 TL
[11]	Proje Adı: Kuantum Bilgisayarlar ve Kriptografi (TEKNOKENT) Yürütücü: Murat Cenk, Ferruh Özbudak Başlangıç – Bitiş Tarihleri: 2020 – 2021 Bütçesi: 174 519 TL

[12]	Proje Adı: Güvenli ve Mahremiyet Korumalı Blokzincir Tabanlı Sistem Geliştirme (TEKNOKENT) Yürütücü: Murat Cenk Araştırmacılar: Pelin Angın, Esra Günsay Başlangıç – Bitiş Tarihleri: 2020 – 2020 Bütçesi: 15 000 TL
[13]	Proje Adı: Kuantum Güvenli Özet Fonksiyon Tabanlı İmzalama (TEKNOKENT) Yürütücü: Murat Cenk Başlangıç – Bitiş Tarihleri: 2018 – 2020 Bütçesi: 577 041 TL
[14]	Proje Adı: Mathematical Models for Interacting Dynamics on networks, (Proje No: Cost Action CA18232) Katılımcı: Hamdullah Yücel Başlangıç – Bitiş Tarihleri: 4 Ekim 2019 – 3 Ekim 2023
[15]	Proje Adı: Bükülmüş Fonksiyonların Genellemeleri ve Permütasyon Polinomları (TÜBİTAK 1001, 120F309) Yürütücüsü: Nurdagül Anbar Meidl UME Araştırmacısı: Oğuz Yayla Başlangıç – Bitiş Tarihleri: 15 Mart 2021 – 15 Mart 2023 Bütçesi: 450 000 TL
[16]	Proje Adı: Simitli Cebirsel Geometri Ve Kodlama Teorisine Uygulamaları (TÜBİTAK 1001, 119F177) Yürütücüsü: Mesut Şahin UME Araştırmacısı: Oğuz Yayla Başlangıç – Bitiş Tarihleri: 15 Kasım 2019 – 15 Mayıs 2022 Bütçesi: 640 000 TL

ODTÜ Bilimsel Araştırma Projeleri (DOSAP)

[1]	Proje Adı: Süpersingüler İzogen Tabanlı Kriptografik Protokollerin Geliştirilmesi Yürütücü: Murat Cenk Araştırmacılar: Maryam Sheikhi Garjan Başlangıç – Bitiş Tarihleri: 2020 – 2021
-----	--

Eğitim

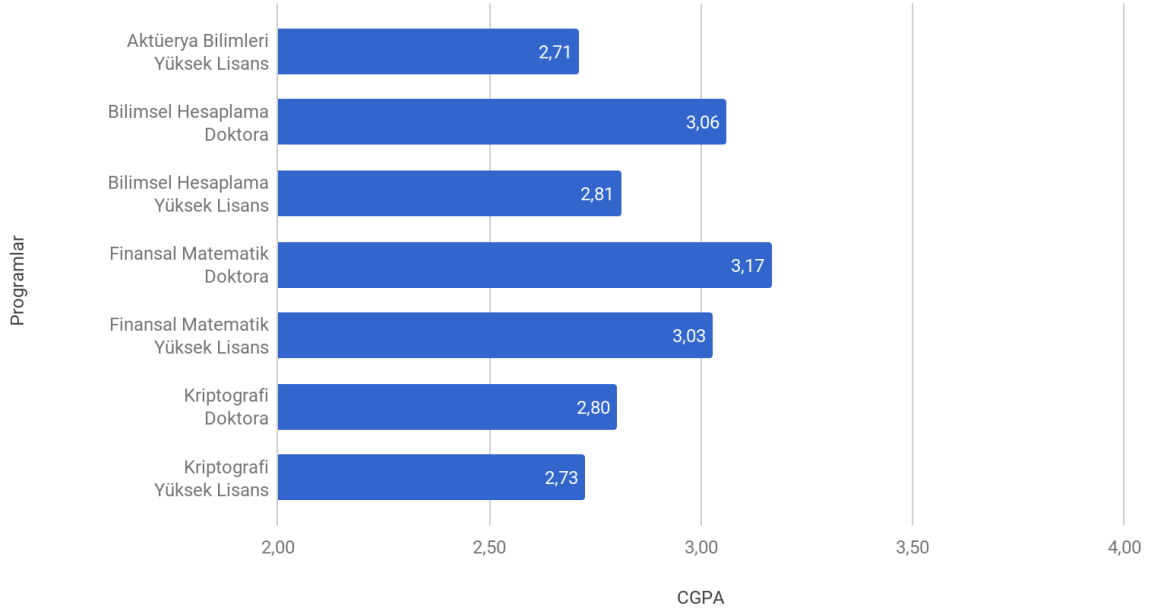
Başvurular, Kabul ve Kayıtlar

Enstitümüz 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.

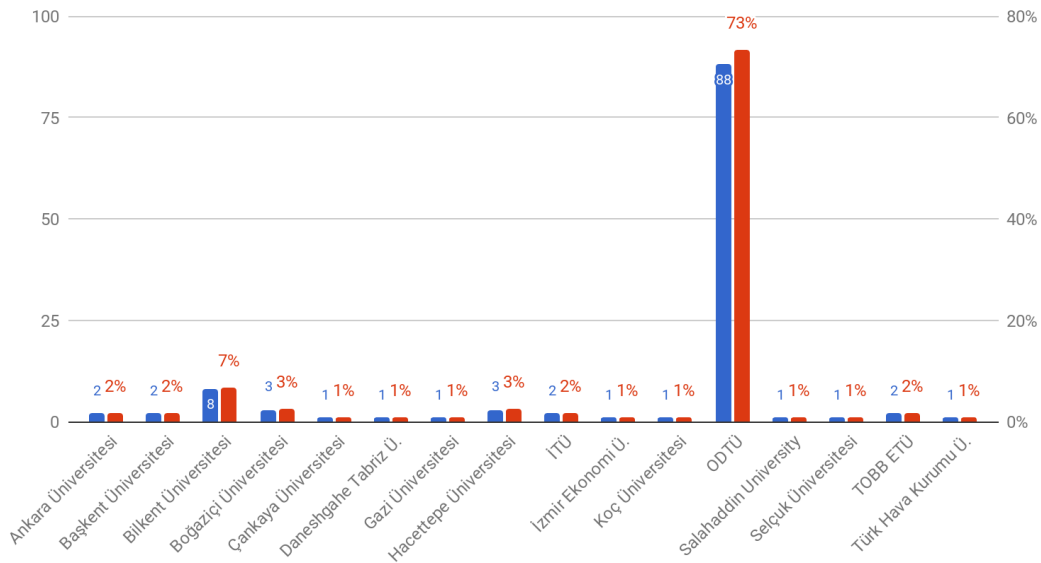
Enstitü Anabilim Dalları	BAŞVURULAR - 2020		
	Başvuru (%)	Kabul (%)	Kayıt (%)
Aktüerya Bilimleri	14 (% 7)	13 (% 8)	5 (% 4)
Bilimsel Hesaplama	71 (% 33)	39 (% 25)	29 (% 24)
Finansal Matematik	64 (% 30)	55 (% 35)	43 (% 36)
Kriptografi	65 (% 30)	48 (% 31)	43 (% 36)
Toplam	214	155	120

Enstitümüz programlarına kayıt yaptıran öğrencilerimiz hakkındaki diğer istatistiksel bilgiler (başarı ortalamaları, mezun oldukları üniversitelere ve bölümlerine göre dağılımları) aşağıda bilginize sunulmuştur.

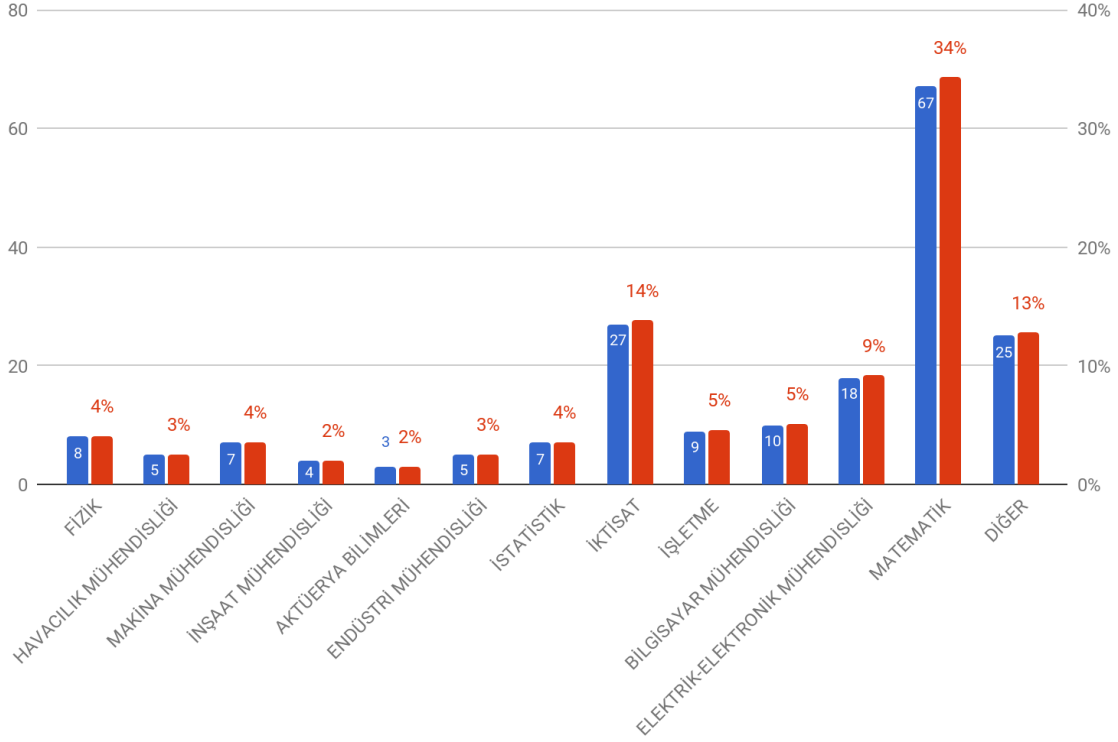
Kayıt Olan Öğrencilerin Lisans CGPA Ortalamaları



Kayıt Olan Öğrencilerin Mezun Oldukları Üniversitelere Göre Dağılımı



Kayıt Olan Öğrencilerin Mezun Oldukları Bölümlere Göre Dağılımı



Enstitü Öğrencilerinin Programlara Göre Dağılımı ve İstatistikler

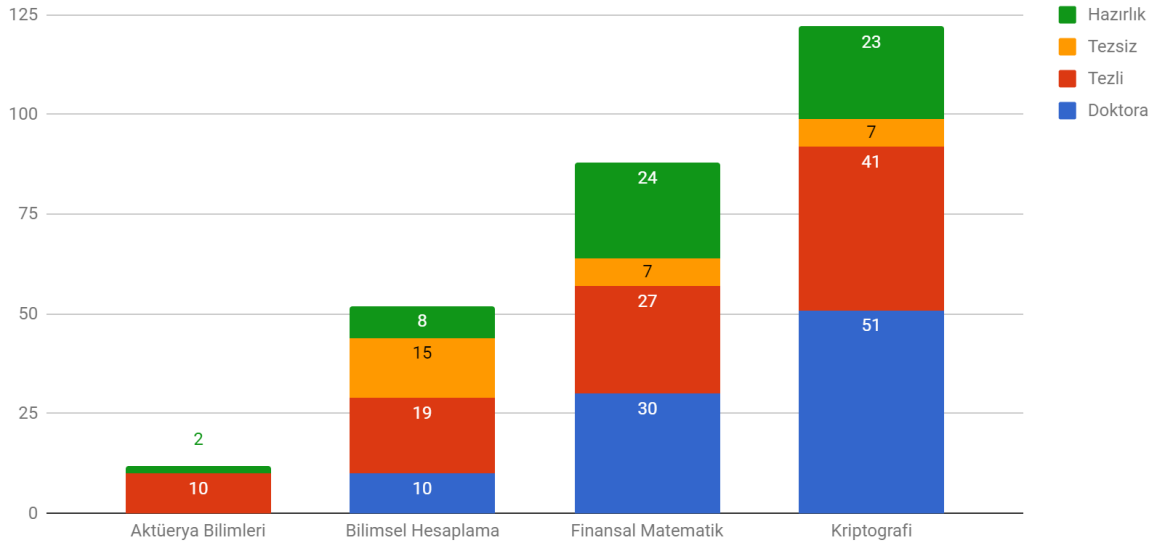
Enstitümüze yeni katılan öğrencilerimiz ile birlikte, mevcut öğrencilerimizin programlara göre dağılımı aşağıdaki “2020-2021 Güz” ve “2019-2020 Bahar” tablolarında belirtilmiştir.

2020-2021 Güz					
Anabilim Dalı	Doktora	Tezli	Tezsiz	Hazırlık	Toplam
Aktüerya Bilimleri		10		2	12
Bilimsel Hesaplama	10	19	15	8	52
Finansal Matematik	30	27	7	24	88
Kriptografi	51	41	7	23	122
Özel Öğrenci					5
	91	97	29	57	279

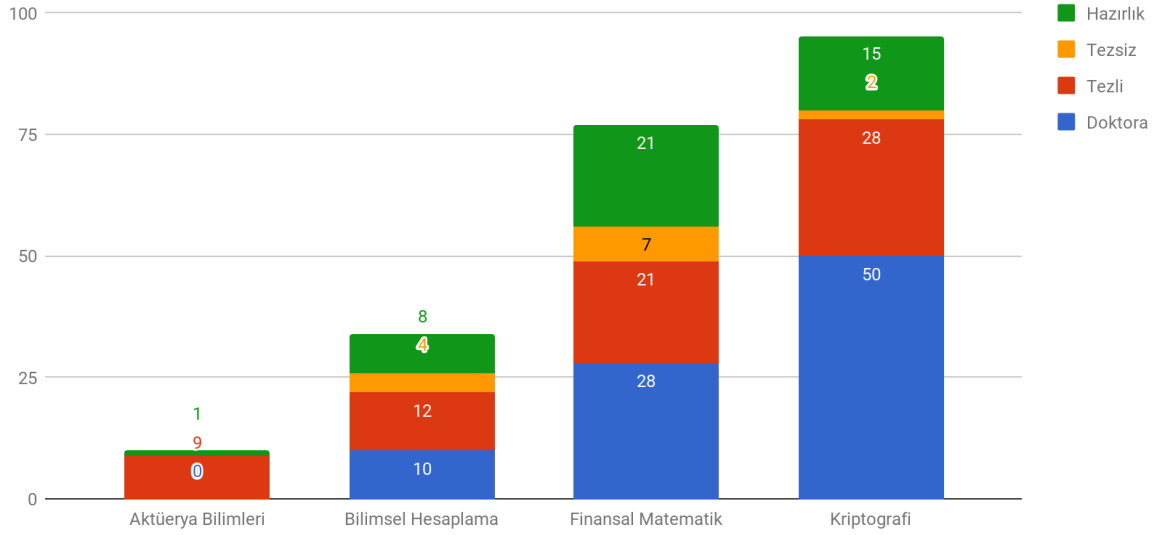
2019-2020 Bahar					
Anabilim Dalı	Doktora	Tezli	Tezsiz	Hazırlık	Toplam
Aktüerya Bilimleri		9		1	10
Bilimsel Hesaplama	10	12	4	8	34
Finansal Matematik	28	21	7	21	77
Kriptografi	50	28	2	15	95
Özel Öğrenci					14
	88	70	13	45	230

Tablolardaki veriler ışığında, programlara göre öğrenci (özel öğrencilerimiz hariç) dağılımları aşağıdaki grafiklerde belirtilmiştir.

Doktora, Tezli, Tezsiz Yüksek Lisans ve Hazırlık Öğrencileri Dağılımı (2020-21 Güz)

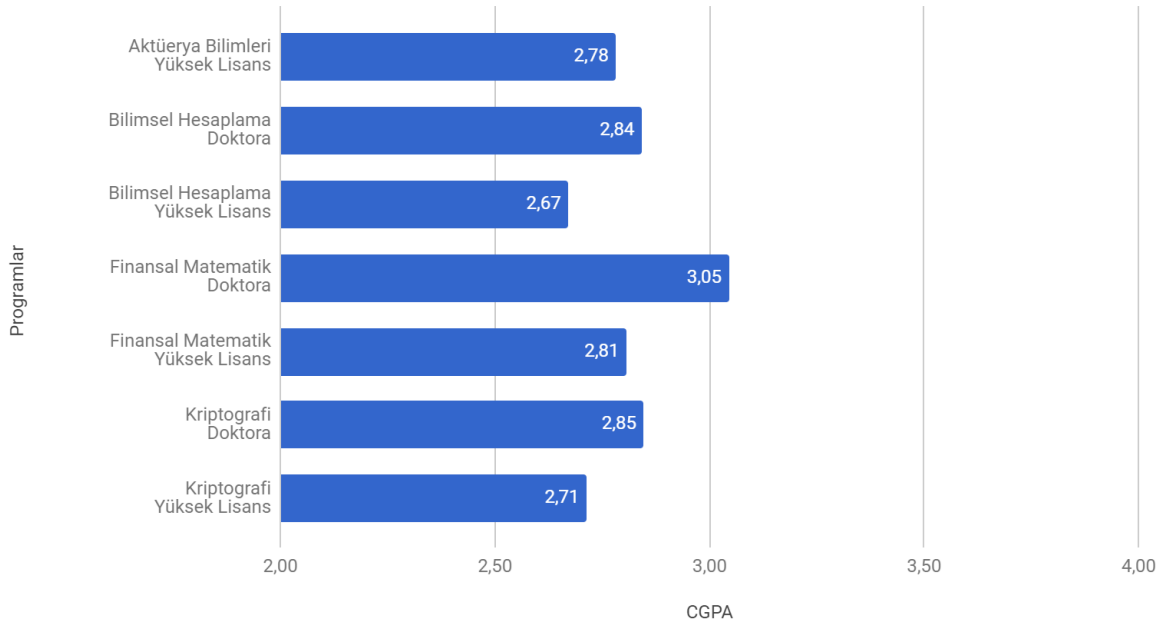


Doktora, Tezli, Tezsiz Yüksek Lisans ve Hazırlık Öğrencileri Dağılımı (2020- Bahar)



Son olarak, öğrencilerimizin Enstitü Anabilim Dalı bazında ve 2020 yılındaki akademik başarı performansları (CGPA ortalamaları) aşağıdaki gibi gerçekleşmiştir.

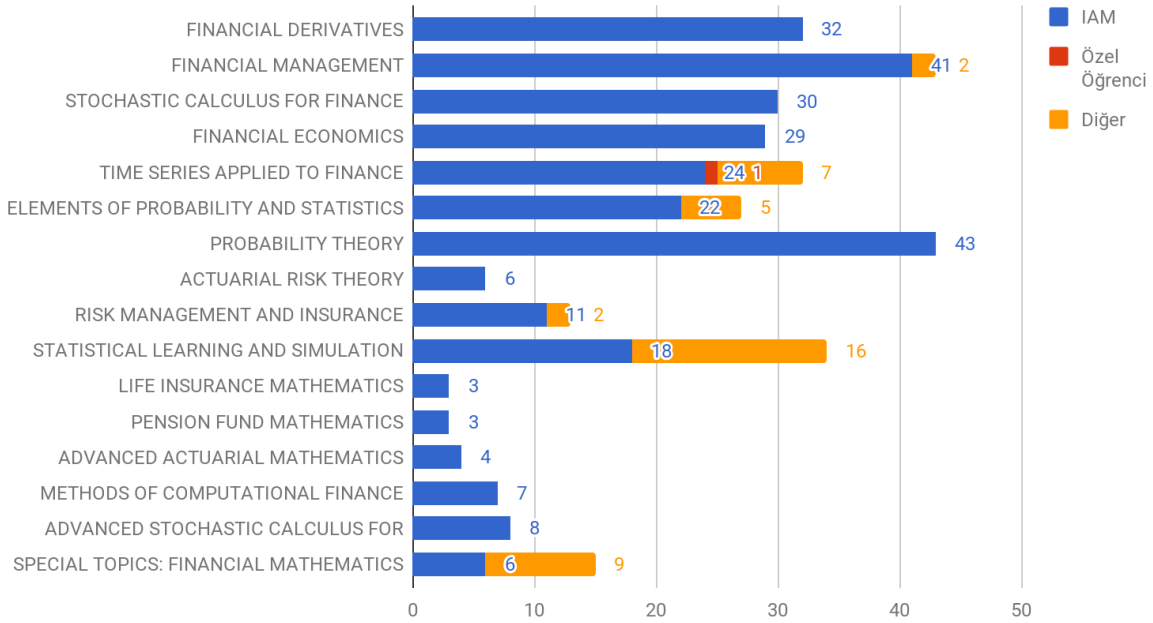
Kayıt Olan Öğrencilerin Lisans CGPA Ortalamaları



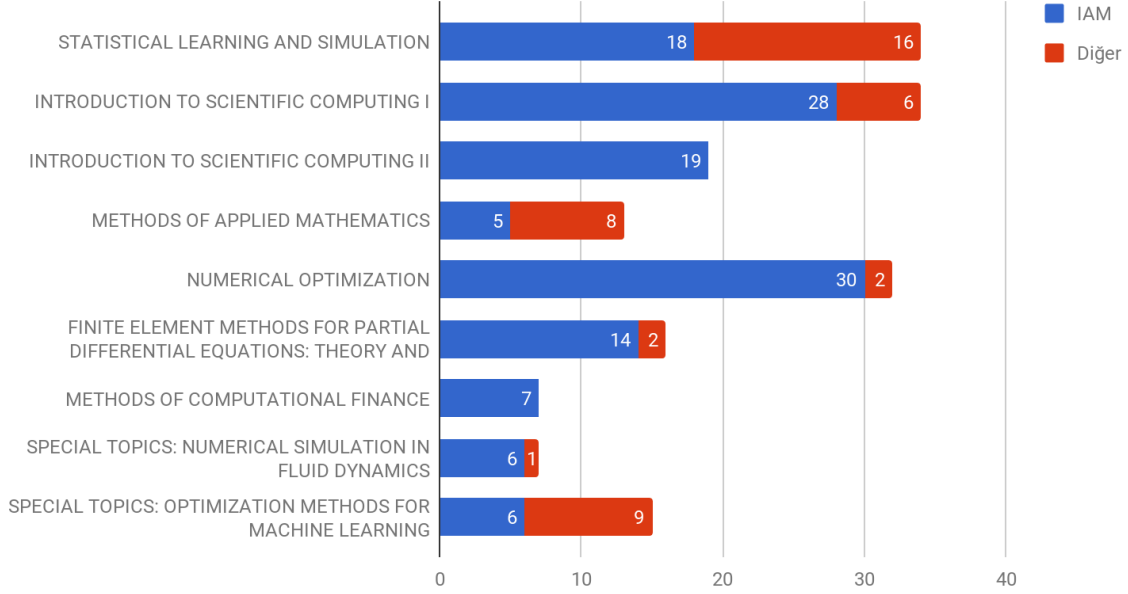
Enstitüdeki Dersler, Öğrenci Sayıları ve İstatistikler

Bu bölümde, Enstitümüzde 2020 yılı içerisinde açılan derslere ve bu derslere ilişkin istatistiklere yer verilmiştir. Aşağıdaki grafiklerde, her bir Anabilim Dalı için seçilmiş olan derslerdeki enstitü ve enstitü-dışı öğrenci sayıları verilmektedir. Birçok dersimizin birden fazla Anabilim Dalında listelenmiş olması Enstitümüzün ve derslerimizin disiplinlerarası çalışmalara verdiği önemin bir göstergesidir.

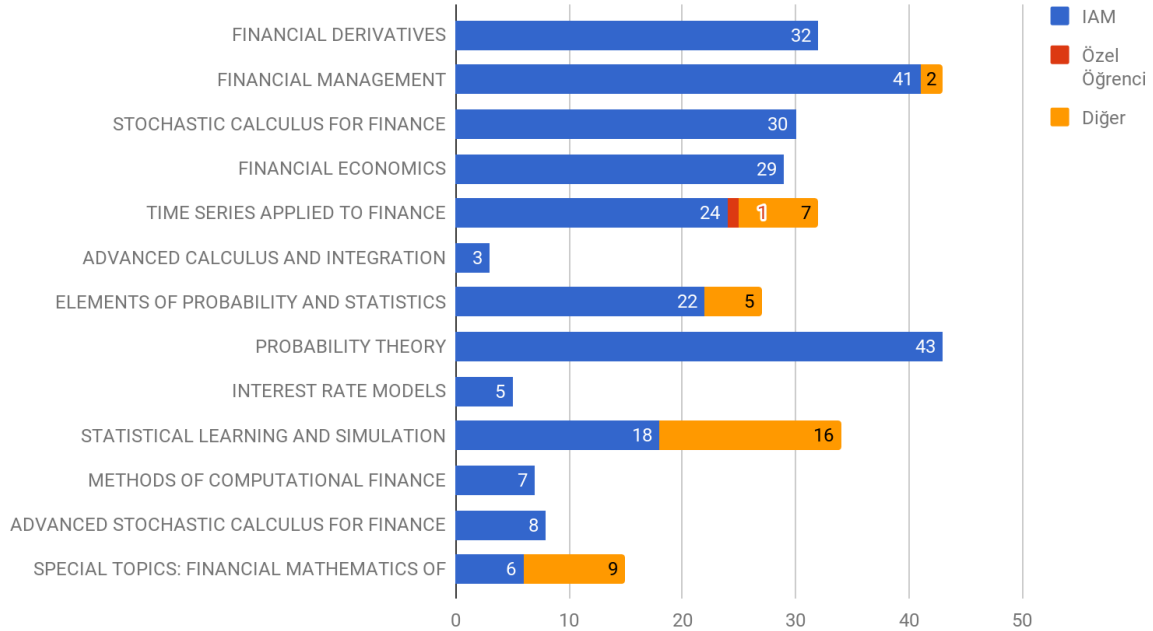
Aktüerya Bilimleri Dersleri Öğrenci Sayıları (2019-20 Bahar - 2020-21 Güz)



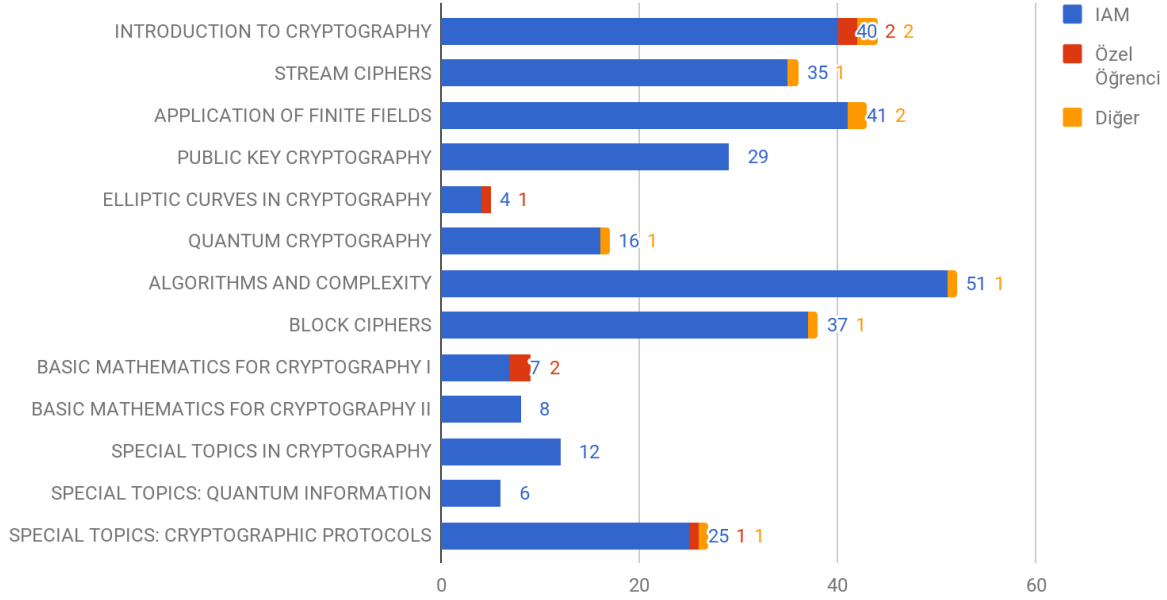
Bilimsel Hesaplama Dersleri Öğrenci Sayıları (2019-20 Bahar - 2020-21 Güz)



Finansal Matematik Dersleri Öğrenci Sayıları (2019-20 Bahar - 2020-21 Güz)



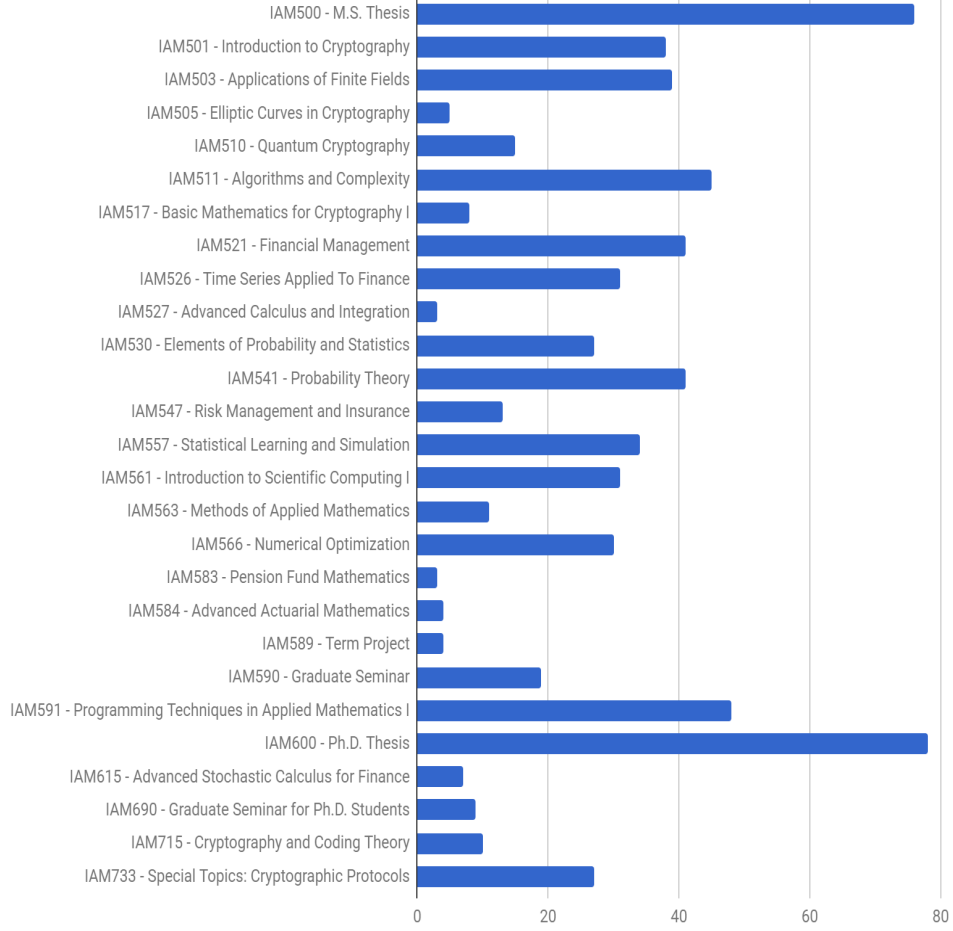
Kriptografi Dersleri Öğrenci Sayıları (2019-20 Bahar - 2020-21 Güz)



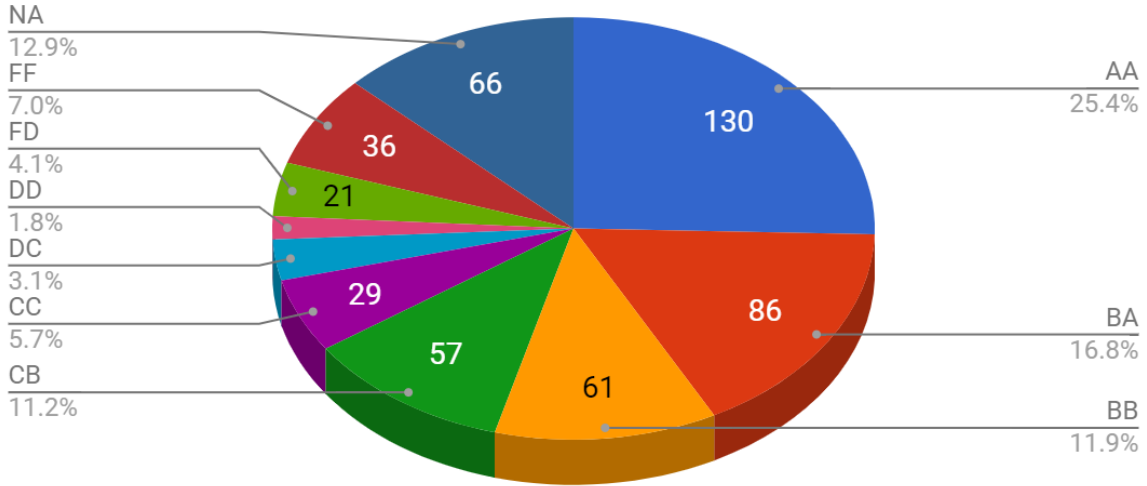
Aşağıdaki grafiklerde 2020 yılı içerisindeki 2020-2021 Güz ve 2019-2020 Bahar dönemlerinde açılan tüm dersler, öğrenci sayıları ve not dağılımları verilmiştir. Özellikle not dağılımını gösteren grafiklerde %10-%20’ler seviyesinde olan “NA” notundaki artışın sebeplerinden en önemlisinin öğrencilerimizin eğitimlerinin yanı sıra çeşitli kurum ve kuruluşlarda çalışmaları olduğu düşünülmektedir.



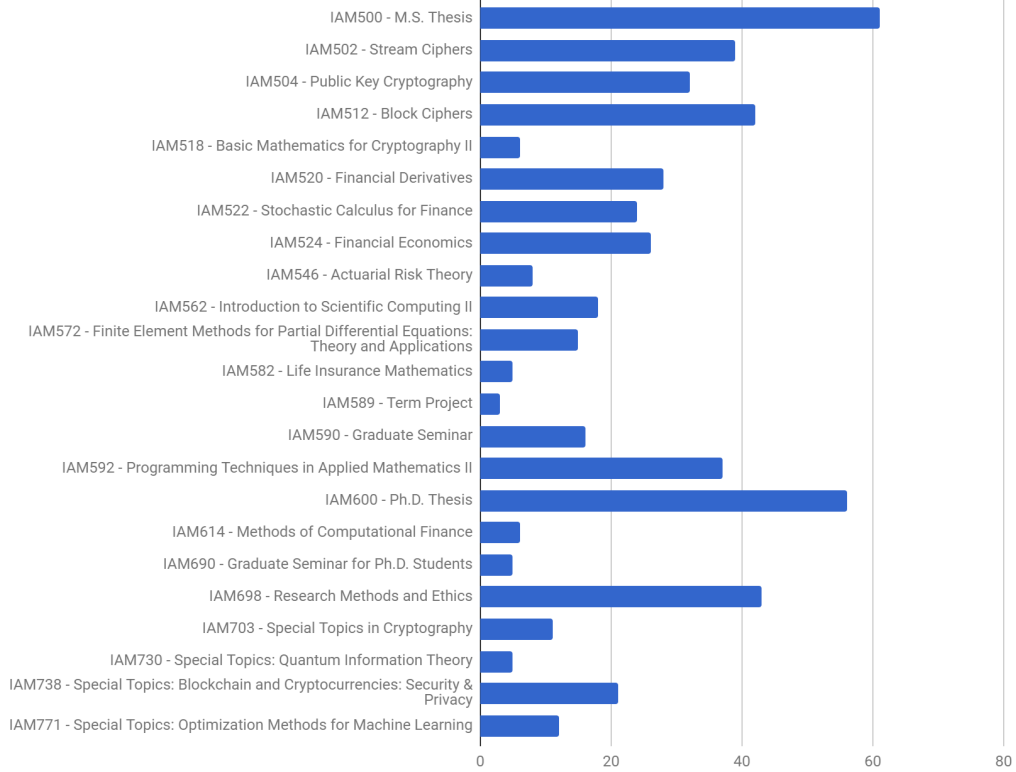
2020-2021 Güz Dönemi Dersleri ve Öğrenci Sayıları



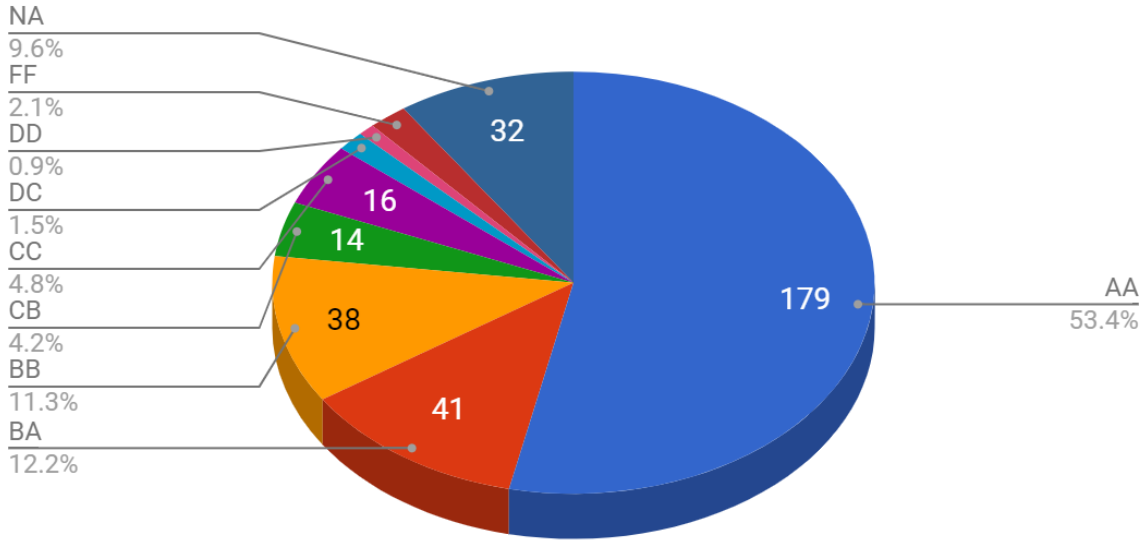
2020-2021 Güz Dönemi Not Dağılımı



2019-2020 Bahar Dönemi Dersleri ve Öğrenci Sayıları

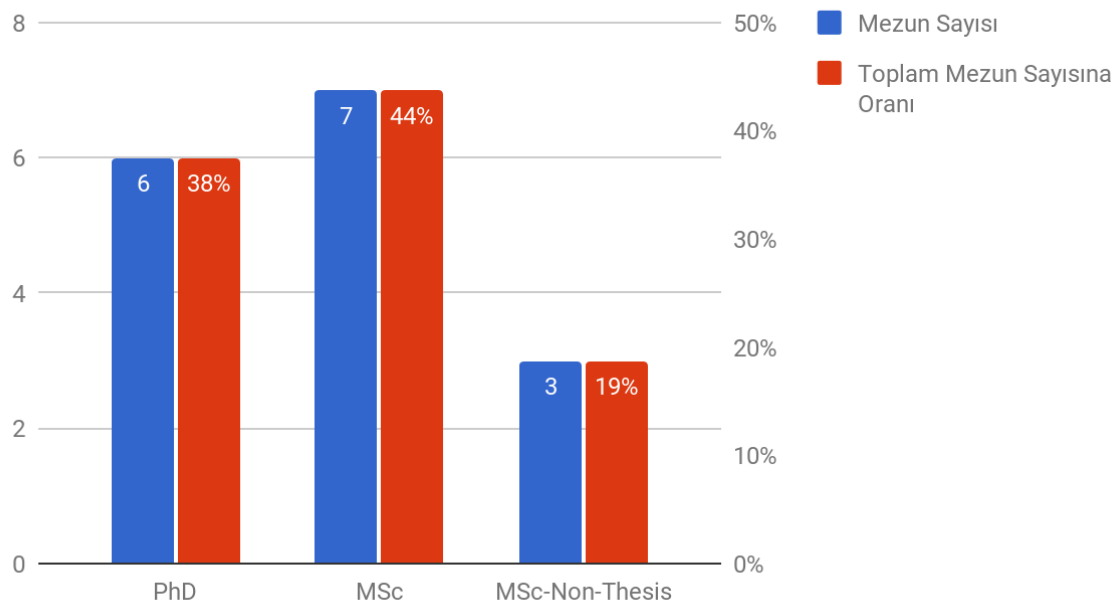


2019-2020 Bahar Dönemi Not Dağılımı



Son olarak, Enstitümüz Yüksek Lisans ve Doktora programlarından 2020 yılında mezun olan öğrencilerimizin sayıları ve oranları aşağıda verilmiştir.

Lisansüstü Programlara Göre Mezunlarımız



Doktora Programları

2020-2021 Güz ve 2019-2020 Bahar dönemlerinde Enstitümüz bünyesindeki Doktora programlarından aşağıdaki isimleri sıralanan öğrencilerimiz başarı ile mezun olmuştur. Doktora mezunlarına ait detaylı bilgiler ise rapor sonunda ayrıca sunulmaktadır. Kendilerini tebrik eder, başarılarının devamını dileriz.

Doktora Mezunları

[1]	Küçüksaraç, D., Option pricing in interest rate derivatives, PhD Thesis, Financial Mathematics, Middle East Technical University, January 2020 (Danışman: Seza Danışoğlu)
[2]	Ulu, M. E., High performance number theoretic transforms in cryptography, PhD Thesis, Cryptography, Middle East Technical University, January 2020 (Danışman: Murat Cenk)
[3]	Karasan, A., Analyses of factors of market microstructure: price impact, liquidity, and volatility, PhD Thesis, Financial Mathematics, Middle East Technical University, February 2020 (Danışman: Esma Gaygısız Lajunen)
[4]	Çomak, P., Mathematical countermeasures against implementation attacks, PhD Thesis, Cryptography, Middle East Technical University, April 2020 (Danışman: Ferruh Özbudak; Ortak Danışman: Rijmen Vincent)
[5]	Ahmadi, M., Backward stochastic differential equations and applications to liquidity risk, PhD Thesis, Financial Mathematics, Middle East Technical University, September 2020 (Danışman: Ali Devin Sezer)
[6]	Bilgin, Y. A., Efficient implementation of lattice-based schemes, PhD Thesis, Cryptography, Middle East Technical University, October 2020 (Danışman: Murat Cenk)

Yüksek Lisans Programları

2020-2021 Güz ve 2019-2020 Bahar dönemlerinde Enstitümüz bünyesindeki Yüksek Lisans programlarından aşağıda isimleri listelenen öğrencilerimiz başarı ile mezun olmuştur. Kendilerini tebrik eder, başarılarının devamını dileriz.

Tezli Yüksek Lisans Mezunları

[1]	Tonga, M., On password-based authenticated key exchange (PAKE) protocols, MSc Thesis, Cryptography, Middle East Technical University, July 2020 (Danışman: Ali Doğanaksoy; Ortak-Danışman: İsa Sertkaya)
[2]	Çamur, Z., A study of lightweight cryptography, MSc Thesis, Cryptography, Middle East Technical University, August 2020 (Danışman: Ali Doğanaksoy; Ortak-Danışman: Fatih Sulak)
[3]	Ertürk, E., Solution of the Almgren-Chriss model with quadratic market volume via special functions, MSc Thesis, Financial Mathematics, Middle East Technical University, October 2020 (Danışman: Ali Devin Sezer)
[4]	Bayram, B., Pricing inflation indexed bonds and embedded deflation floor options: An analysis on Turkish bond market, MSc Thesis, Financial Mathematics, Middle East Technical University, October 2020 (Danışman: Ali Devin Sezer)
[5]	Oktay, E., Reevaluating spectral partitioning for unsymmetric matrices, MSc Thesis, Scientific Computing, Middle East Technical University, October 2020 (Danışman: Murat Manguoğlu; Ortak Danışman: Hamdullah Yücel)
[6]	Öztürk, G., Identity/Attribute-based authentication protocols based on pairings, MSc Thesis, Cryptography, Middle East Technical University, October 2020 (Danışman: Ali Doğanaksoy; Ortak-Danışman: Ayşe Nurdan Saran Buz)
[7]	Yener, C., Cryptographic modules validation process according to the FIPS 140 and ISO/IEC 15408, MSc Thesis, Cryptography, Middle East Technical University, November 2020 (Danışman: Ali Doğanaksoy; Ortak-Danışman: Oğuz Yayla)

Tezsiz Yüksek Lisans Mezunları

[1]	Gevişen, İ., Optimal liquidation strategy using Almgren Chriss framework with affine trading volume, Financial Mathematics, Middle East Technical University, January 2020 (Danışman: Ali Devin Sezer)
[2]	Uyanık, S., Sovereign default probability estimation with logit model, Financial Mathematics, Middle East Technical University, January 2020 (Danışman: Seza Danişoğlu)
[3]	Atçeken, İ., Dynamics of the inventory process in the Avelenada-Stoikov market making model, Financial Mathematics, Middle East Technical University, August 2020 (Danışman: Ömür Uğur)

Ödüller

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

[1]	Ertuğrul Umut Yıldırım (Bilimsel Hesaplama): Yüksek Lisans Ders Performans Ödülü, 2020
[2]	Mustafa Kütük (Bilimsel Hesaplama): Doktora Ders Performans Ödülü, 2020
[3]	Gülçin Akarsu (Finansal Matematik): Doktora Ders Performans Ödülü, 2020
[4]	Melis Aslan (Kriptografi): Lisans Sonrası Doktora Ders Performans Ödülü, 2020
[5]	Hasan Bartu Yünüak (Kriptografi): Doktora Ders Performans Ödülü, 2020
[6]	Efe Giray (Kriptografi): Yüksek Lisans Ders Performans Ödülü, 2020

Ek Bilgiler

Yeni Açılan Dersler

Enstitümüzün ders kataloğuna 2020-2021 Güz ve 2019-2020 Bahar dönemlerinde açılan aşağıdaki ders(ler) eklenmiştir.

2019 - 2020 Bahar Dönemi

Course Code	9700771
Course Title	Special Topics: Optimization Methods for Machine Learning
Course Credit(s)	(3-0)3
Instructor(s)	Hamdullah Yücel (yucelh@metu.edu.tr)
Prerequisites	Consent to the Instructor
Course Catalog Description	Convexity; Gradient Descent; Stochastic Gradient Methods; Noise Reduction Methods; Second-Order Methods; Adaptive Methods; Methods for Regularized Models; Introduction to Machine Learning: support machine vector, neural network.
Course Objectives	The interplay between optimization and machine learning is one of the most important developments in modern computational science. Optimization formulations and methods are proving to be vital in designing algorithms to extract essential knowledge from huge volumes of data. Machine learning, however, is not simply a consumer of optimization technology but a rapidly evolving field that is itself generating new optimization ideas. Optimization approaches have enjoyed prominence in machine learning because of their wide applicability and attractive theoretical properties. The increasing complexity, size, and variety of today's machine learning models call for the reassessment of existing assumptions. 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 student will: • capture the state of the art of the interaction between optimization and machine learning. • understand the various optimization methods that underlie machine learning methods that have become so popular today in real-world applications. • use the computational tools available to solving optimization problems on computers once a mathematical formulation has been found.
Course Learning Outcomes	Upon successful completion of this course, the student will be able to • assess/evaluate the most important algorithms, function classes, and algorithm convergence guarantees • compose existing theoretical analysis with new aspects and algorithm variants. • formulate scalable and accurate implementations of the most important optimization algorithms for machine learning applications.

Tentative (Weekly) Outline	1. Background of machine learning 2. Convexity and nonsmooth calculus tools 3. Gradient descent 4. Projected gradient descent 5. Stochastic gradient methods 6. Variance reduction methods: SAG, SAGA, SVRG 7. Accelerated gradient descent 8. Mirror descent 9. Second-order methods 10. Second-order methods: stochastic quasi-Newton 11. Dual methods: stochastic dual coordinate ascent methods 12. Conditional gradient method 13. Adaptive methods 14. Methods for regularized models
Course Textbook(s)	There will be no explicit textbook for the course; rather, the instructor will provide some hand-written lecture notes along with the progress of the course. However, the following monographs on this topic are recommended: • S. Suvrit, S. Nowozin, and S. J. Wright, Optimization for Machine Learning, MIT Press, 2012. • J. Nocedal and S. J. Wright, Numerical Optimization, Second Edition, Springer, 2006. • S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004. • L. Bottou, F. E. Curtis, J. Nocedal: Optimization Methods for Large-Scale Machine Learning, arXiv:1606.04838v3 • W. Hu, Nonlinear Optimization in Machine Learning, Lecture Notes • E. Hazan, Optimization for Machine Learning, arXiv:1909.03550v1 • S. Bubeck, Convex Optimization: Algorithms and Complexity, arXiv:1405.4980v2 • M. Jaggi and B. Gärtner, Optimization for Machine Learning, Lecture Notes
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/

Doktora Mezunlarımız

Doktora derecesini alan mezunlarımıza ait kısa özgeçmişler, tez konusu özetleri ve yayın listeleri bu kısımda verilmektedir.

Adı Soyadı: Doruk Küçüksaraç

Doruk Küçüksaraç 2010 yılında Boğaziçi Üniversitesi İktisat ve İşletme bölümlerinden yüksek onur derecesiyle mezun olmuştur. 2010 yılında Türkiye Cumhuriyet Merkez Bankası Araştırma ve Para Politikası Genel Müdürlüğü'nde araştırmacı olarak göreve başlamıştır. 2014 yılında ODTÜ İktisadi ve İdari Bilimler Fakültesi İktisat bölümünde ve 2015 yılında London Business School'da Finans bölümünde yüksek lisanslarını yüksek onur dereceleriyle tamamlamıştır. 2020 yılında ise ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik anabilim dalında Doç. Dr. Seza Danışoğlu danışmanlığında "Option Pricing in Interest Rate Derivatives" başlıklı teziyle doktoraasını tamamlamıştır. Araştırma konuları arasında döviz ve faiz üzerine yazılan türev ürünler başta olmak üzere varlık fiyatlaması, getiri eğrisi modellenmesi ve tahmini, para politikası aktarım mekanizması gibi konular bulunmakta olup yurt içinde ve uluslararası alanlarda çeşitli çalışmaları bulunmaktadır. 2010 yılından itibaren TCMB'de çalışmakta olup mevcut durumda Piyasalar Genel Müdürü olarak görev almaktadır.



Doktora Tezi Özeti:

FAİZE DAYALI TÜREVLERDE OPSİYON FİYATLAMASI

Sabit getirili menkul kıymetlerdeki faize dayalı türev ürünlerin ve gömülü opsiyonların (embedded options) değerlemesi piyasa oyuncuları açısından önem arz etmektedir. Faize dayalı türev ürünlerini fiyatlandırmak için akademik yazında çok sayıda model geliştirilmiş olmasına rağmen, söz konusu modellerin varsayımları arasındaki tutarsızlık, özellikle faiz oranındaki değişimlere karşı risklerin birleştirilmesi kapsamında zorluk oluşturmaktadır. Ayrıca, modellerin belli durumlara yönelik olarak geliştirildiği ve genelleştirme kapsamında uygun olmadığı gözlenmektedir. Bu bağlamda, ürün bazlı olarak varsayım yapmadan genel bir metodolojinin kullanılarak faize dayalı türev ürünlerin fiyatlandırılması kritik önem taşımaktadır. Bu çalışmanın, Vasicek modeli altında düzenli veya düzensiz nakit akışları olan sabit getirili menkul kıymetlere uygulanabilecek genel bir yaklaşım sağlayarak literatüre katkı sağlaması beklenmektedir.

Uyarlanan yöntem temel olarak dört adımdan oluşmaktadır: (i) piyasada işlem gören faize dayalı türev ürünler için Vasicek modeli ile ilgili formülün türetilmesi, (ii) Vasicek model parametrelerinin tahmin edilmesi, (iii) fiyatlandırılması amaçlanan faize dayalı türev ürün için de Vasicek modeli altında formülasyon gerçekleştirilmesi ve (iv) tahmin edilmiş olan Vasicek model parametre tahminlerinin fiyatlama kapsamında kullanılması. Bu metodoloji,

düzenli veya düzensiz nakit akışlarına sahip tüm faize dayalı türev ürünlerine uygulanabilecek genel bir çözüm sunmaktadır. Ayrıca, faiz kaynaklı maruziyetlerin tutarlı bir şekilde hesaplanabilmesi ve faize dayalı opsiyon değerlerinin model parametrelerine olan duyarlılıklarının türetilmesi de sağlanmaktadır. Çalışmada yer alan sonuçlar Avrupa tipi opsiyonlar için bulunmuş olmakla beraber çalışmanın sonuçları Amerikan ve Bermudan tarzı opsiyon sözleşmelerine de uyarlanabilir. Ek olarak, metodolojinin gerekli özellikleri sağlayan diğer faiz modelleri ile de uygulanması mümkündür.

Yayınlar:

- Cepni, O., Küçüksaraç, D., Yılmaz, M., The sensitivity of CDS premium to the global risk factor: Evidence from emerging markets, Research Notes in Economics (No. 1704), Central Bank of the Republic of Turkey, 2017.
- Cepni, O., Küçüksaraç, D., Yılmaz, M., The sensitivity of credit default swap premium to global risk factor: Evidence from emerging markets, Economics Letters (No. 159), pp. 74-77, 2017.
- Küçüksaraç, D., A new approach for Turkish term structure: Cubic B-spline basis with variable roughness penalty, Research Notes in Economics (No. 1711), Central Bank of the Republic of Turkey, 2017.
- Guney, I., Kazdal, A., Küçüksaraç, D., Yılmaz, M., Estimation of currency swap yield curve, Research Notes in Economics (No. 1803), Central Bank of the Republic of Turkey, 2018.
- Cepni, O., Guney, I., Küçüksaraç, D., Yılmaz, M., The Interaction between yield curve and macroeconomic factors, Research Notes in Economics (No. 1802), Central Bank of the Republic of Turkey, 2018.
- Korkmaz, H., Küçüksaraç, D., Onay, Y., Senol, A., Estimation of FX option implied density functions: Nonparametric-Malz approach, Working Papers (No. 1903), Central Bank of the Republic of Turkey, 2019.
- Küçüksaraç, D., Okay, M., Yılmaz, M., The determinants of FX derivatives use: Empirical evidence from Turkish non-financial firms in BIST, Research Notes in Economics (No. 1908), Central Bank of the Republic of Turkey, 2019.
- Guney, I., Kazdal, A., Küçüksaraç, D., Yılmaz, M., Exchange rate sensitivity of firm value: Recent evidence from non-financial firms listed on Borsa Istanbul, Research Notes in Economics (No. 1911), Central Bank of the Republic of Turkey, 2019.
- Küçüksaraç, D., Ozbek, I., Talasli, I., A liquidity indicator for bond and foreign exchange swap markets, Research Notes in Economics (No. 2014), Central Bank of the Republic of Turkey, 2020.

Adı Soyadı: Pınar Çomak

Pınar Çomak 2010 yılında Orta Doğu Teknik Üniversitesi Matematik bölümünden mezun olmuş ve 2013 yılında ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi anabilim dalında yüksek lisansını tamamlamıştır. Aynı anabilim dalında doktora çalışmalarına devam etmiş ve Ocak 2020 tarihinde Prof Dr Ferruh Özbudak danışmanlığında “Mathematical Countermeasures Against Implementation Attacks” başlıklı tezini tamamlamıştır. Araştırma konuları arasında yan-kanal analizi, simetrik kriptografi, S-boxların ayrıştırılması, kriptografik protokoller bulunmaktadır. 2019 yılına kadar ODTÜ Matematik Bölümünde araştırma görevlisi olarak çalışmış, bu tarihten itibaren de telekomünikasyon güvenliği alanında çalışmalarına devam etmektedir. Halen Ericsson’da güvenlik araştırmacısı olarak 3GPP Güvenlik Standardizasyon ekibinde network automation, ve kriptografik profiller ve güvenlik protokolleri konularında Ericsson’u temsil etmektedir.



Doktora Tezi Özeti :

GERÇEKLEME ATAKLARINA KARŞI MATEMATİKSEL TEDBİRLER

Bağlantılı cihazların kullanımındaki hızlı gelişmeler, güvenliği sağlayan güçlü metotlara ihtiyaç doğurmuştur. Güvenilir bir iç dizayna sahip olan kara kutu modelinde, güvenilir kriptografik algoritmaların kullanımı, kriptografik anahtar depolayan cihazları koruyor gibi görünür. Ancak, bu cihazların fiziksel kaçaklarının, anahtarın ya da diğer hassas bilgilerin sızmasına sebep olduğu gösterilmiştir. Gri kutu denilen bu model, algoritmanın kendisinden ziyade kriptografik algoritmanın donanımdaki gerçekleşmesine odaklanır. Bu fiziksel sızıntılar bir programın çalışma süresi, harcadığı güç ya da yaydığı elektromanyetik radyasyon gibi yan-kanal bilgileri olabilir. Eğer bu sızıntı, cihaz içinde saklanan gizli bilginin tamamıyla veya bir parçasıyla ilişkili ise, yan-kanal bilgisi olarak adlandırılır. En başarılı şekilde kullanılan yan-kanallar, diferansiyel güç analizi (DPA) ile çözümlenebilen kripto sisteminin güç tüketimidir. Güç tüketimini kullanan bir DPA saldırısının amacı, kriptografik sistemdeki farklı düz metin ve anahtar girişlerinin farklı güç tüketiminin ölçümü ve analizleriyle, cihazdaki anahtarı veya diğer hassas bilgileri çıkarmaktır. Saldırgan, yan-kanaldan sızan bilgiler ile kriptografik algoritmanın ara sonuçları arasında bir korelasyon bulmaya çalışır. Son yirmi yılda saldırıların geniş çaplı etkisi nedeniyle, Yan-Kanal Analizi (SCA) saldırılarının önlenmesi büyük bir araştırma konusu olmuştur ve bu saldırıları engellemek için birçok önlem geliştirilmiştir. Yeniden anahtarlama, aynı anahtarı kullanarak bir algoritmanın yinleme sayısını sınırlar; gizleme, herhangi bir hassas bilgiden bağımsız olarak, her girdi için eşit miktarda güç tüketmesini sağlamak amacıyla algoritmadan ziyade aygıtın davranışını değiştirir; ve bizim çalıştığımız tedbir olan maskeleye ise bir yan-kanaldan sızan bilgiler ile hassas veriler arasındaki ilişkiyi önler veya azaltır, ki SCA saldırıları da bu korelasyona bağlıdır. Maskeleye, tüm hassas ara değerleri, iyi bilinen gizli paylaşım şemalarıyla rastgele hale getirerek gizler. Biri Eşik Gerçekleşmesi (TI) olan farklı

maskeleme şemaları önerilmiştir. Küçük teknik problemlerin varlığında bile DPA'ya karşı güvenli olduğu kanıtlanmıştır, aynı zamanda diğer güvenli maskeleme yöntemlerine kıyasla daha küçük bir alan gerektirir ve çok daha az rastgelelik kullanır. TI, hassas verilerin her bir bitinin eşit olasılıkla paylaşımlara ayrıldığı gizli paylaşım ve çok partili hesaplama dayandır, böylece herhangi bir paylaşım alt kümesi, verilerin kendisinden bağımsızdır. TI dört özelliğe, maskelenmemiş değişkenlerin tekdüzeliğine, doğruluğa, d. seviyeden tamsızlığa ve paylaşılan fonksiyonların tekdüzeliğine dayanır. TI'nin ilk çalışmaları, TI'nin afin dönüşüm altında değişmez olduğunu göstermiştir. Bu tezin katkılarını iki bölümde sunuyoruz. İlk bölümde, S-kutularının doğrusal olmayan bir dönüşüm altında TI paylaşımının davranışını inceledik ve S-kutularının bazı sınıfları haricinde TI'nin ters dönüşüm altında değişmez olmadığını gösterdik. Tezin ikinci bölümünde, yüksek dereceli S-kutularını paylaşmanın etkili yöntemlerinden biri olan ayrışma yöntemi çalışılmıştır. Yüksek dereceli S-kutularının hangi şartlar altında daha düşük dereceli olanlara ayrıştırılabileceği incelendi. Bu koşulları bulmak için, güç permütasyonları ve pariteleri dikkate alınarak, permütasyonların kuadratik veya kübik permütasyonlara ayrılması hedeflenmiştir. Son olarak, sonlu cisimler ve bunlara karşılık gelen düşük dereceli güç permütasyonları hakkındaki ayrışma sonuçlarını sunuyoruz.

Anahtar Kelimeler: Yan-kanal analizi, tedbirler, maskeleme, alt sınır gerçeklemeleri, Boolean fonksiyonlar, permütasyonlar, ayrışım.

Yayınlar:

- Bilgin, Z., Ersoy, M. A., Üstündağ-Soykan, E., Tomur, E., Çomak P., Karaçay, L., Vulnerability prediction from source code using machine learning, IEEE Access, 8, pp. 150672-150684, 2020.
- Çomak, P., Kim, J. L., Özbudak, F., New cubic self-dual codes of length 54, 60 and 66, Applicable Algebra in Engineering, Communication and Computing, 29(4), pp.303–312, 2018.
- Çomak, P., Nikova, S., Rijmen, V., On decomposition of permutations, Balkan CryptSec, Iasi, Romania, 20-21 Sep 2018.
- Çomak, P., Kim, J. L., Özbudak, F., Some new quasi-cyclic self-dual codes, 15th International Workshop on Algebraic and Combinatorial Coding Theory (ACCT), Albena, Bulgaria, 18-24 June 2016.

Adı Soyadı: Yusuf Alper Bilgin

Yusuf Alper Bilgin 2012 yılında ODTÜ Elektrik ve Elektronik Mühendisliği bölümünden mezun olmuş ve 2016 yılında aynı bölümde Yüksek Lisansını tamamlamıştır. Daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi anabilim dalında doktora çalışmalarına devam etmiş ve Eylül 2020 tarihinde Doç. Dr. Murat Cenk danışmanlığında “Efficient Implementation of Lattice-based Schemes” başlıklı tezini tamamlamıştır. Araştırma konuları arasında kuantum sonrası kriptografi, kriptografik algoritmaların etkin gerçekleştirilmesi, kriptografik protokoller, uygulama ve sistem güvenliği bulunmaktadır. 2012 yılından itibaren yazılım mühendisi olarak çalışmalarına devam etmektedir. Halen Aselsan’da Gömülü Yazılım Mühendisi olarak görev almaktadır.



Doktora Tezi Özeti :

KAFES TABANLI ALGORİTMALARIN VERİMLİ GERÇEKLENMESİ

Kuantum bilgisayarlar neredeyse otuz yıldır tartışılmasına rağmen bu konuda araştırmalar büyük ölçüde teoride kalmıştır. Son yıllarda, Google, IBM ve Microsoft gibi tanınmış şirketler büyük ölçekli bir kuantum bilgisayar yapabilmek için çaba sarf etmektedir. Bu bilgisayarlar ile çarpanlarına ayırma ve ayırık logaritma gibi zor bilinen problemler büyük ölçekli bir kuantum bilgisayar tarafından kırılabilir. Bu yüzden, dijital iletişimin gizliliği ve bütünlüğü ciddi biçimde tehlikeye girecektir. Büyük ölçekli kuantum bilgisayarların ne zaman yapılacağı sorusu hala açık bir sorudur. Önümüzdeki 10 yıl içinde, hâlihazırda kullanımda olan tüm açık anahtar algoritmalarını kırmak için yeterince büyük kuantum bilgisayarların inşa edileceği konusunda bazı tahminler vardır. Bu nedenle, NIST, bilgi güvenlik sistemlerimizi kuantum bilgisayarlarına karşı koruyabilmek için 2016 yılında bir standartlaştırma süreci başlatmıştır. Bu sürecin ilk iki turu tamamlanmıştır ve yedi tane aday algoritma, sekiz tane de alternatif algoritma seçilmiştir. Bu 15 algoritma içerisinde sekiz tanesi kafes tabanlıdır.

Bu tez kapsamında kafes tabanlı algoritmaların verimli bir şekilde gerçekleştirilmesi üzerine çalışılmıştır. İlk olarak, NIST kuantum sonrası standartlaştırma süreci ikinci tur adayı olan NewHope algoritmasının hızlı ve kompakt bir varyasyonu olan NewHope-Compact algoritması önerilmiştir. Önerilen bu algoritma sayı teorik dönüşümünde (NTT) olan son gelişmeleri yoğun bir şekilde kullanılmaktadır. Bunun için elemanlar arası çarpmada kullanılan her bir elemanın tanımı değiştirilmiştir. Güvenlik seviyesini değiştirmek için sadece polinom boyutunu ve eleman tanımını değiştirmenin yeterli olduğu gösterilmiştir. Daha sonra, NTT'yi kullanan kafes tabanlı algoritmalar için ARM Cortex-M4 üzerinde çeşitli optimizasyonlar sunulmuştur. Bu optimizasyonlar ile daha verimli modüler indirgeme, optimize edilmiş küçük terimli polinom çarpımı ve daha agresif NTT katmanı birleşimi kullanılarak daha hızlı bir uygulama sunulmuştur. Gerçekleştirilen bu performans

optimizasyonun yanında yığın bellek kullanımı da azaltılmıştır. Bu optimizasyonlar, NIST kuantum sonrası standartlaşma sürecinde üçüncü tur adayı olan Kyber, ikinci tur adayı olan ve üçüncü turda elenen NewHope ve kendi önerdiğimiz NewHope-Compact üzerinde test edilmiştir.

Yayınlar:

- Alkim, E., Bilgin, Y. A., Cenk, C., Gérard, F., Cortex-M4 optimizations for $\{R,M\}$ LWE schemes, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020(3), pp.336-357, 2020. <https://doi.org/10.13154/tches.v2020.i3.336-357>
- Alkim, E., Bilgin, Y. A., Cenk, M., Compact and simple RLWE based key encapsulation mechanism (LATINCRYPT 2019), *Lecture Notes in Computer Science*, Springer, 11774, pp. 237-256, 2019. DOI: 10.1007/978-3-030-30530-7_12
- Aksoy, B., Bilgin, Y. A., Cenk, M., İlter, M. B., Koçak, N., Yılmaz, Y. E., Analyzing NIST 2nd-round lattice-based post-quantum KEM algorithms, *Information Security and Cryptology Conference*, Ankara, Turkey, 2019.
- Bilgin Y. A., Yılmaz, A. Ö., Neighbor discovery in network with directional antennas, *21st Signal Processing and Communications Applications Conference (SIU)*, Haspolat, pp. 1-4, 2013. DOI: 10.1109/SIU.2013.6531286

Adı Soyadı: Mahdi Ahmadi

Mahdi Ahmadi 2011 yılında İran Urmia Üniversitesi Matematik Bölümünden mezun olmuş ve 2013 yılında Amirkabir Üniversitesi Matematik Fakültesinden Geometry Bölümünde Yüksek Lisansını tamamlamıştır. ODTÜ Uygulamalı Matematik Enstitüsünde doktora çalışmalarına devam etmiş ve Eylül 2020 tarihinde Prof. Dr. Ali Devin Sezer danışmanlığında “Continuity problem for BSDE equations with singular non-Markovian terminal condition and deterministic terminal times” başlıklı tezini tamamlamıştır. Araştırma konuları arasında Geriye Doğru Stokastik Diferansiyel Denklemler, Tekil son değerler, Markov olmayan son değer, Süreklilik Problemi bulunmaktadır. 2015 yılından itibaren Geriye Doğru Stokastik Diferansiyel Denklemler alanında çalışmalarına devam etmektedir.



Doktora Tezi Özeti : GERİYE STOKASTİK DİFERANSİYEL DENKLEMLER VE LİKİDİTE RİSKİNE UYGULAMALARI

$\mathbb{F} = \{\mathcal{F}_t, t \in [0, T]\}$ en azından d-boyutlu bir Brownian hareketi ve $\mathbb{R}^m \setminus \{0\}$ üzerinde bir Poisson rastgele-ölçümü kapsayan bir filtrasyon olsun. Bu tezde, deterministik $[0, T]$ zaman aralığında, $\mathbb{F}$ filtrasyonu ile uyumlu (adapted) süper-linear sürücü bir f sürecinin tanımladığı geriye doğru stokastik diferansiyel denklemler (Backward stochastic differential equations (BSDE)) çalışılmaktadır. f süreci süper-linear olduğu için bu BSDE1 değerini de alabilen son değer ξ değişkenleriyle de çözülebilir. ∞ değerini de alabilen son değerlere “tekil” denir. BSDE’nin son değeri bir Markov sürecin T anındaki pozisyonunun bir fonksiyonu ise bu son değere Markov denir. Bu tezin ilk amacı çalıştığımız BSDE’lerin Markov olmayan tekil son değerleri için çözümlerinin inşasıdır. Tezimiz iki sınıf son değeri çalışmaktadır: F, F_T ’ye göre ölçülebilir, mutlak değerinin yeterince yüksek kuvvetinin sonlu beklenen değeri olan, reel değerli bir rastgele değişken, $_1$, dağılımı T etrafında sınırlı yoğunluğu olan bir durma zamanı olsun. $\xi_1 = \infty \cdot \mathbf{1}_{\{\tau_1 \leq T\}} + F \cdot \mathbf{1}_{\{\tau_1 > T\}}$ olarak yazılabilen son değerler çalıştığımız ilk sınıfı oluşturmaktadır. $A_t, t \in [0, T], \mathbb{F}$ filtrasyonu ile uyumlu, azalan ve T anında olasılıksal olarak sürekli bir olaylar dizisi olsun. Çalıştığımız ikinci sınıf son değerler $\xi_2 = \infty \cdot \mathbf{1}_{A_T} + F \cdot \mathbf{1}_{A_T^c}$ şeklinde yazılabilen rastgele değişkenlerden oluşmaktadır. Tezimizde bu son değer sınıfları için çalıştığımız BSDE’lerin üst çözümlerinin çözüm olduğu, yani üst çözümlerin T anında sürekli oldukları ve denklemin son değerine tam olarak eriştikleri ispatlanmaktadır. X filtrasyonun Brownian hareketi tarafından sürülen ve kovaryans matrisi kesin olarak eliptik olan bir Markov difüzyon süreci olsun. Tezimizin ikinci amacı bu sürecin zamanla değişen sonlu ve açık bir kümeden ilk çıktığı anın dağılımının yoğunluğu olduğunu ispatlamıştır. Bu yoğunlukların varlığı, bu çıkış zamanları BSDE’nin son değerlerinde görülen τ_1 ve τ_2 zamanları olarak kullanabileceğini de gösterir. Tezimizde, elde ettiğimiz sonuçların stokastik optimal kontrol soruları açısından ne anlama geldiği de anlatılmıştır.

Anahtar Kelimeler: Geriye Doğru Stokastik Diferansiyel Denklemler, Tekil son değerler, Markov olmayan son değer, süreklilik problemi.

Adı Soyadı: Abdullah Karasan

Abdullah Karasan 2007 yılında Gazi Üniversitesi İktisat ve İşletme (Çift anadal) bölümlerinden mezun olmuş ve Hazine Müsteşarlığında Hazine Kontrolörü olarak göreve başlamıştır. 2012-2014 yılları arasında Michigan Üniversitesinde Uygulamalı Ekonomi alanında yüksek lisansını tamamlamıştır. 2015 yılında ise ODTÜ Uygulamalı Matematik Enstitüsü Finansal Matematik anabilim dalında doktorasına başlamış ve 2020 yılında doktorasını Doç. Dr. Esmâ Gaygısız danışmanlığında ‘Analyses of Factors of Market Microstructure: Price Impact, Liquidity, And Volatility’ isimli tez ile tamamlamıştır. Abdullah Karasan şu anda Veri Bilimi Takım lideri olarak Magnimind Academy’de ve eğitmen olarak O’Reilly ve Springboard şirketlerinde çalışmaktadır.



Doktora Tezi Özeti :

MARKET MİKRO YAPISININ FAKTÖRLERİNİN ANALİZİ: FİYAT ETKİSİ, LİKİDİTE VE OYNAKLIK

Bu tezin ilk bölümünde, Kyle tarafından önerilen modeli genişletilerek fiyat etkisini modellenmeye çalışılmıştır. Yeni denge fiyatına ulaşılması zaman aldığındaki pazarın tam etkin olmadığı varsayılmaktadır. Bu nedenle, fiyat etkisini modellemek için, iki yeni kavram olan piyasa esnekliği ve fiyatın bilgilendiriciliği kavramları tanımlanmıştır. Sonuç olarak, fiyatın bilgilendiriciliği arttıkça piyasa esnekliği ve fiyat etkisinin artma eğilimi göstermiştir. Bu bulgu ise, finansal piyasalarda bilginin hızının önemli olduğu ve piyasa esnekliğinin ihmal edilebilecek bir olgu olmadığını vurgulamaktadır.

İkinci bölümde finansal riskin ihmal edilen boyutu olarak kabul edilen likiditenin önemi vurgulanmaya çalışılmaktadır. Bunun için, Likidite Etkili Zıplamalı Stokastik Volatilité Modeli (LASVJ) modeli tanıtılmış ve stabilite ve performans açısından Zıplamalı Stokastik Volatilité Modeli (SVJ) modeli ile karşılaştırılmıştır. Simülasyon sonuçları, LASVJ modelinin düşük sapma ve kök ortalama kare hatasına sahip olduğu için SVJ modelinden daha iyi performans gösterdiğini ortaya koymuştur. Kalibrasyon bölümünde Dow-Jones 30’da listelenen on şirket kullanılmıştır ve LASVJ modeliyle tahmini temerrüt ve kredi marjı olasılığının SVJ modeline göre daha yüksek olduğu bulunmuştur. Kriz dönemi bu sonuçlar daha net bir şekilde ortaya çıkmaktadır. Bulgular, riskin likidite boyutu ihmal edilirse temerrüt olasılığı ve kredi marjının olması gerekenden daha düşük olduğunu ortaya koymaktadır ve bu da 2007-2008 finansal krizinin etkisinin tam olarak neden öngörülemediğini açıklamaktadır.

Üçüncü bölümde, oynaklık tahmin yöntemi geliştirilerek Riske Maruz Değer gibi finansal risk araçlarının daha etkin bir şekilde kullanılması amaçlanmaktadır. İyi performans gösteren bir oynaklık tahmini finansal piyasadaki belirsizliğe ışık tuttuğu için bunu modellemek önemli bir görevdir. Bu amaçla oynaklığı modellemek için GARCH tipi modeller ve bir

Makine Öğrenmesi modeli olan SVR-GARCH modeli kullanılmıştır ve sonuçlar performans ölçütlerine göre karşılaştırılmıştır. Ampirik analizde, S&P-500 endeksinde yer alan otuz hisse ile 01/01/2010-09/01/2019 dönemi kapsanmıştır. Bulgular, SVR-GARCH'ın oynaklığı tahmin etmede geleneksel modellerden daha iyi performans gösterdiğini ve ayrıca POF ve Basel Trafik Işığı Geri Test yaklaşımlarına dayanan VaR tahmininde daha güvenilir sonuç verdiğini göstermektedir.

Yayınlar:

- Karasan, A., Gaygisiz, E., Modeling volatility and revisiting risk management: An SVR-GARCH approach, Journal of Financial Data Science, 2020

Adı Soyadı: Metin Evrim Ulu

Metin Evrim Ulu, doktorasını Orta Doğu Teknik Üniversitesi Uygulamalı Matematik Enstitüsü Kriptografi anabilim dalından 2020 yılında aldı. Kriptografi çalışmaları sırasında, Bent Fonksiyonlar, PN/APN permütasyonlar gibi simetrik şifrelerde kullanılan matematiksel yapıları inceledikten sonra, post-quantum algoritmalar üzerine çalıştı. Bu algoritmaların GPGPU'lar ve FPGA'ler üzerinde hızlı ve verimli çalışmaları araştırma konuları arasında yer almaktadır. Ek olarak, fonksiyonel programlama konusundaki bilgilerini uygulamak için Japonya'da NTT Data Mathematical Systems şirketine 2014 yılında görev aldı. European Lisp Symposium komitesi üyesidir. Halen İstinye Üniversitesinde Öğretim Üyesi olarak görev almakta, Kuantum Hesaplama, Kuantum Bilgisayarlar ve Simulatörler üzerinde çalışmalarına devam etmektedir.

Doktora Tezi Özeti :**KRİPTOGRAFI'DE YÜKSEK PERFORMANSLI SAYI KURAMSAL DÖNÜŞÜMLER**

Son yıllarda meydana gelen fizikteki teorik gelişmeler, kuantum bilgisayarları üretmenin ve üzerinde hesaplama yapmanın olanaklı olduğunu gösterdi. Bu durum, var olan ve kullanılan kriptografik algoritmaları değişik seviyelerde güvensiz hale getirdi. Bunun sebebi ise, algoritmalarda kullanılan matematiksel çözümü zor olan problemlerin kuantum bilgisayarlarda verimli olarak çözülebilmesi. Örneğin Shor, tam sayıları asal çarpanlarına ayıran bir algoritmayı henüz kuantum bilgisayarlar var olmadan tasarlamıştı. Bu sayede, kuantum bilgisayarlar üzerinde, açık anahtar RSA kriptosistemi kırılabilir. Şubat 2016'da, NIST mevcut durumu incelemek, kuantum hesaplamanın var olan kriptosistemler üzerindeki etkisini çalışmak ve yeni nesil kuantum saldırılara dayanıklı sistemler geliştirebilmek için bir çalışma grubu kurdu. Kuantum ataklara karşı dayanıklı olan kriptografik sistemlerin bir çeşidi latis tabanlı sistemlerdir. Bu tür sistemlerde, performansı arttırmak için Sayı Kuramsal Dönüşümler kullanılmaktadır. Bu tezde, bu dönüşümlerin kriptografik uygulamalardaki performansları çalışılmıştır. Öncelikle, latis tabanlı Peikert şeması, O'nun gerçekleştirimi olan BCNS algoritması ve NewHope algoritması incelenmiştir. Ardından, bahsi geçen dönüşümleri kullanan SWIFFTX özet fonksiyonu sunulmuştur. Son olarak, bu fonksiyona ait verimli bir GPU uygulaması verilmiştir. Yapılan testlerde görülmüştür ki, bu yeni uygulama fonksiyona 10 kat hız kazandırmış, aynı zaman da 2¹⁶ girdi için 5 Watt güç tasarrufu sağlamıştır.

Yayınlar:

- Ulu, M. E., A common Lisp application server, International Lisp Conference (Core-server), Kyoto, Japan, October 2012.
- Ulu, M. E., Cenk, M. (2019) A parallel GPU implementation of SWIFFTX, MACIS, Gebze, Turkey, November 2019.

