ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

Uygulamalı Matematik Enstitüsü (UME)

Faaliyet Raporu 2024

Orta Doğu Teknik Üniversitesi
Uygulamalı Matematik Enstitüsü
Nisan 2024

https://iam.metu.edu.tr

Önsöz

2022 yılında kuruluşunun 20. yılını tamamlayan Uygulamalı Matematik Enstitüsü (UME) Türkiye'deki Matematik alanında ilk disiplinler arası araştırma kurumudur. UME lisansüstü programları ve araştırmaları ile uluslararası düzeyde saygın ve öncü bir araştırma enstitüsü olmayı hedeflerken, öğrencilerine akademik norm ve etik kurallar çerçevesinde bilimsel çalışmalar yapmayı ve bu çalışmaların sonuçlarının yaygın kullanımının, sürdürülebilirliğinin sağlanacağı bir eğitim vermektedir. Aktüerya Bilimleri, Bilimsel Hesaplama, Finansal Matematik ve Kriptografi olmak üzere dört anabilim dalında yüksek eğitim olanağı sunulmakta olup, Kriptoloji Laboratuvarımızda bilgi güvenliği alanında ihtiyaç duyulan araştırma faaliyetleri ulusal ve uluslararası boyutta devam ettirilmektedir. Enstitümüz, ayrıca Üniversitemizde 2022 yılında kurulan Data and Decision Science (Veri ve Karar Bilimleri) lisansüstü eğitim programını Bilgisayar Mühendisliği, Elektrik-Elektronik Mühendisliği, Endüstri Mühendisliği ve İstatistik Bölümleri ile ortak yönetmektedir.

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

UME öğretim üyeleri tarafından gerçekleştirilen çalışmaların %66,7'sı SCI-E, %28 kadarı diğer kategorisindeki dergilerde ve konferans tam bildirisi kategorisinde, %5,3 kadarı ise kitapta bölüm ve kitap olarak yayımlanmıştır. Ayrıca, Enstitümüz bünyesinde yapılan TÜBİTAK, Teknokent ve Döner Sermaye projelerinde bursiyer olarak yer alan yüksek lisans ve doktora öğrencilerimizin araştırmada yer almalarına özen gösterilmektedir.

Kuruluşundan bugüne 131 doktora, 303 tezli yüksek lisans, 156 tezsiz yüksek lisans olmak üzere toplam 590 mezunu olan Enstitümüz; 2024 yılında 7 doktora, 10 tezli ve 1 tezsiz yüksek lisans öğrencisine diploma vermiştir. Bunların yanı sıra, 2023-2024 akademik yılı ODTÜ Tez, Yayın ve Ders Performans Ödülleri kapsamında mezunlarımızdan 1 doktora mezunumuz ODTÜ Tez ödülünü almaya hak kazanmıştır.

Uygulamalı Matematik Enstitüsünün 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 candan teşekkür ederim.

Saygılarımla,

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

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

Enstitü Anabilim Dalı Başkanları

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

Doç. Dr. Önder Türk
(Bilimsel Hesaplama)

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

Doç. Dr. Oğuz Yayla
(Kriptografi)

Enstitü Yönetim Kurulu

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

Doç. Dr. Önder Türk
(Uygulamalı Matematik Enstitüsü)

Prof. Dr. Serdar Göktepe
(İnşaat Mühendisliği)

Doç. Dr. Seza Danışoğlu
(İşletme)

Prof. Dr. Songül Kaya Merdan
(Matematik)

Doç. Dr. Oğuz Yayla
(Uygulamalı Matematik Enstitüsü)

Enstitü Personeli

Öğretim Üyeleri	Araştırma Görevlileri	
A. Sevtap Kestel, Prof. Dr.	Gülçin Akarsu*	Oğuz Koç
Ali Devin Sezer, Prof. Dr.	Beyza Avan	Özenç Murat Mert, Dr.
Ömür Uğur, Prof. Dr.	Burcu Ecem Karakaş	Meral Şimşek, Dr.
Hamdullah Yücel, Prof. Dr.	Zeynelabidin Karakaş, Dr.* (35. Madde)	Cem Yavrum
Önder Türk, Doç. Dr.	Handan İlhan Yüksel	Furkan Kerim Çabaş
Oğuz Yayla, Doç. Dr.	Kübra Kaytancı, Dr.	Gözde Cennet Bayraktar
Buket Özkaya, Dr. Öğr. Üyesi	Hasan Bartu Yünüak*	İlkyaz Aslanöz
Büşra Z. Temoçin, Dr. Öğr. Üyesi	Mustafa Kütük	Tegrid Fettuh

DOSAP

İsmail Güzel, Dr.

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)	

*2024 yılı içinde Enstitüdeki görevinden ayrılmıştır.

Bağlantılı Öğretim Üyeleri - ODTÜ

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

Bağlantılı Öğretim Üyeleri - Diğer Üniversite ve Kurumlar

Akdeniz Üniversitesi	Ahmet Sınak, Doç. Dr.
Ankara Üniversitesi	Furkan Başer, Prof. Dr. Murat Osmanoğlu, Dr. Fatih Tank, Prof. Dr.
ARÇELİK A.Ş.	Songül Bayraktar, Dr.
Atılım Üniversitesi	Ümit Aksoy, Prof. Dr. Burcu Gülmez Temür, Prof. Dr. Fatih Sulak, Doç. Dr. Emrah Sercan Yılmaz, Dr.
Cumhurbaşkanlığı	Ceyda Mangır, Dr. Mehmet Uzunkaya, Dr.
Başkent Üniversitesi	Sinem Kozpınar, Dr. Cansu Betin Onur, Dr. Özge Sezgin Alp, Prof. Dr.
Boğaziçi Üniversitesi	Ümit Işlak, Doç. Dr.
Çankaya Üniversitesi	Özlem Defterli, Doç. Dr. Nurgül Gökgöz Küçüksakallı, Dr. A. Nurdan Saran Buz, Dr.
Gazi Üniversitesi	Aytekin Bayram Çıbık, Prof. Dr.
Gebze Teknik Üniversitesi	Mansur İsgenderoğlu (İsmailov) Prof. Dr.
Hacettepe Üniversitesi	Talha Arıkan, Dr. Pınar Aydoğdu, Prof. Dr. Başak Bulut Karageyik, Dr. Uğur Karabey, Doç. Dr. Mesut Şahin, Prof. Dr. Könül Bayramoğlu Kavlak, Doç. Dr.
Hacı Bayram Veli Üniversitesi	Seher Nur Sülkü, Prof. Dr.
İstinye Üniversitesi	Sedat Akleylek, Prof. Dr.
Karabük Üniversitesi	Oytun Haçarız, Dr. Eda Tekin, Dr.

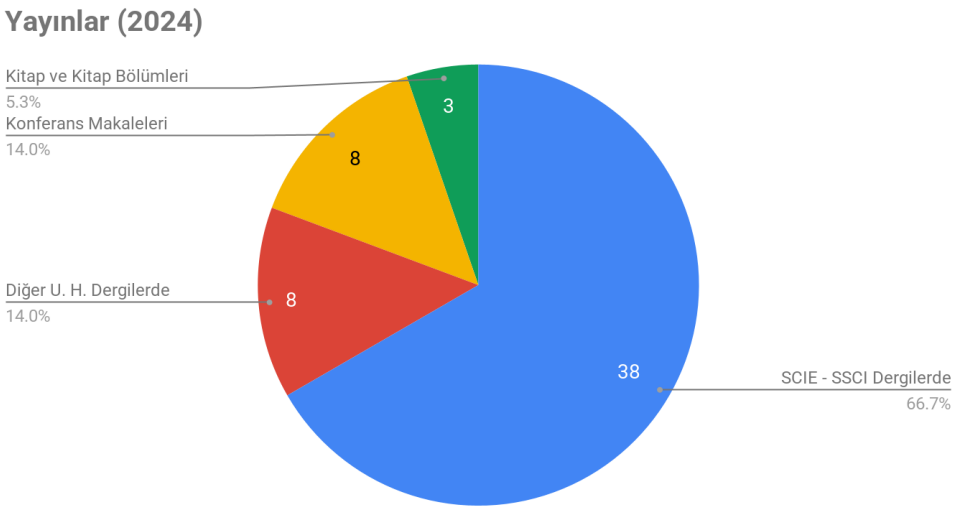
Kahramanmaraş Sütçü İmam Üniversitesi	Bilgi Yılmaz, Doç. Dr.
King Fahd University of Petroleum and Minerals (KFUPM)	Günther Glatz, Dr. Umair bin Waheed, Dr.
Koç Üniversitesi	Mine Çağlar, Prof. Dr.
Namık Kemal Üniversitesi	Cansu Evcin, Dr.
Poznan University of Technology	Gerhard-Wilhelm Weber, Prof. Dr.
Rawalpindi & Air University	Mansoor Ahmed Khan Dr.
Qatar University	Zarina Oflaz, Dr.
Rice Üniversitesi (A.B.D.)	Tayfun E. Tezduyar, Prof. Dr.
ROKETSAN	Tayfun Çimen, Doç. Dr.
Sabancı Üniversitesi	Ferruh Özbudak, Prof. Dr. Erkay Savaş, Prof. Dr.
Sinop Üniversitesi	Murat Uzunca, Prof. Dr.
Süleyman Demirel Üniversitesi	Barış Bülent Kırlar, Prof. Dr.
Technical University of Kaiserslautern	Ralf Korn, Prof. Dr.
TOBB-ETÜ	Tahir Hanalioğlu, Prof. Dr. Zülfükar Saygı, Prof. Dr. Ali Aydın Selçuk, Prof. Dr.
TÜBİTAK	Onur Koçak, Dr.
Vienna Uni. of Economics and Business	Zehra Ekşi-Altay, Doç. Dr.
Western University	Rogemar S. Mamon, Prof. Dr.
Diğer	Murat Cenk, Prof. Dr. Ahmet Ramazan Ağırtaş, Dr. Öznur Mut Sağdıçoğlu, Dr.

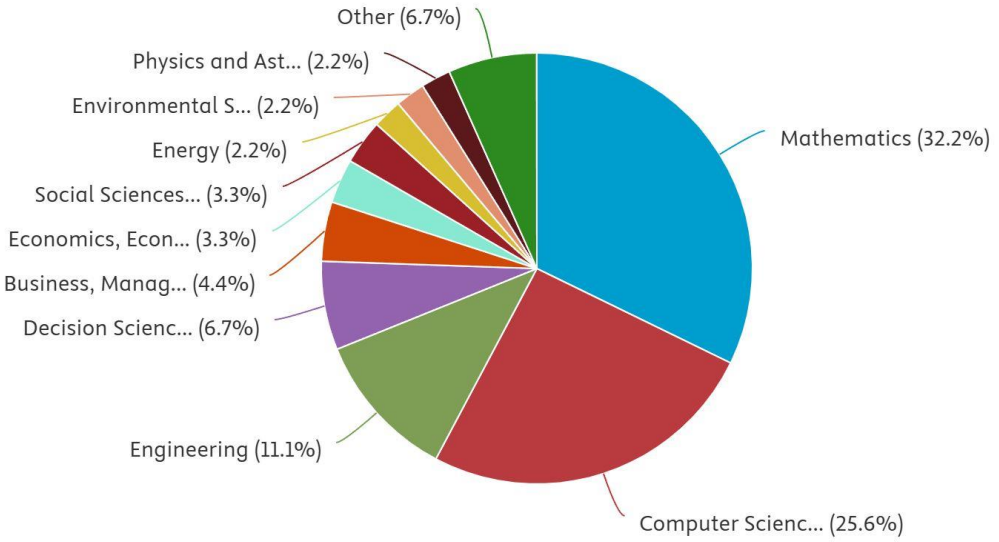
Araştırma

Yayınlar

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

SCIE Tipi yayınların 2023 yılına göre artış gösterdiği belirlenerek, bu yayınların çoğunluğunun WoS tanımlı Q1 ve Q2 kategorisinde yer aldığı gözlemlenmiştir. 2024 yılında Enstitümüz öğretim ve bağlantılı üyeleri tarafından yapılan yayınların çoğunluğunun tez öğrencileri ve mezunlarımızla ortak yapılan çalışmalardan oluşmaktadır.





Bunun yanı sıra, 2024 yılı yayın sayılarına bakıldığında %66,7 SCIE tipi dergilerde yayınlanan çalışmaların ağırlıklı olarak tez öğrencileri ile yapılan araştırmalara ait olduğu belirlenmiştir.

SCIE - SSCI Dergilerde Makaleler

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

[1]	A Computational Study for Pricing European- and American-Type Options Under Heston's Stochastic Volatility Model: Application of the SUPG-YZβ Formulation, Cengizci S., Uğur Ö., (2024) Computational Economics, Cited 1 times., DOI: 10.1007/s10614-024-10704-3
[2]	A computational study for simulating MHD duct flows at high Hartmann numbers using a stabilized finite element formulation with shock-capturing, Cengizci S., Uğur Ö., (2024) Journal of Computational Science, 81, art. no. 102381, Cited 1 times., DOI: 10.1016/j.jocs.2024.102381
[3]	A different base approach for better efficiency on range proofs, Günsay E., Betin Onur C., Cenk M., (2024) Journal of Information Security and Applications, 85, art. no. 103860, Cited 0 times., DOI: 10.1016/j.jisa.2024.103860

[4]	A fast NTRU software implementation based on 5-way TMVP, Yaman Gökce N., Gökce A.B., Cenk M., (2024) Journal of Information Security and Applications, 81, art. no. 103688, Cited 0 times., DOI: 10.1016/j.jisa.2023.103688
[5]	A novel Nash-based low-carbon implementation in agricultural supply chain management, Hamidoğlu A., Weber G.-W., (2024) Journal of Cleaner Production, 449, art. no. 141846, Cited 16 times., DOI: 10.1016/j.jclepro.2024.141846
[6]	A stabilized finite element formulation with shock-capturing for solving advection-dominated convection–diffusion equations having time-fractional derivatives, Cengizci S., Uğur Ö., Natesan S., (2024) Journal of Computational Science, 76, art. no. 102214, Cited 5 times., DOI: 10.1016/j.jocs.2024.102214
[7]	A strategy based on statistical modelling and multi-objective optimization to design a dishwasher cleaning cycle, Anapa K., Yücel H., (2024) Expert Systems with Applications, 249, art. no. 123703, Cited 0 times., DOI: 10.1016/j.eswa.2024.123703
[8]	Adaptive-Quadratic-Neural-Network-Based Multifidelity Modeling Approach for Buckling of Stiffened Panels, Avni Yaşar H., Gürses E., (2024) AIAA Journal, 62 (11), pp. 4207 - 4220, Cited 0 times., DOI: 10.2514/1.J064064
[9]	Characterization of Nearly Self-Orthogonal Quasi-Twisted Codes and Related Quantum Codes, Ezerman M.F., Grass M., Ling S., Ozbudak F., Ozkaya B., (2024) IEEE Transactions on Information Theory, Cited 0 times., DOI: 10.1109/TIT.2024.3503420
[10]	Circular Economy Practices in the Context of Emerging Economies, Ali S.S., Weber G.-W., Tirkolaee E.B., Goli A., (2024) Sustainability (Switzerland) , 16 (4), art. no. 1417, Cited 1 times., DOI: 10.3390/su16041417
[11]	Clustering Based Fuzzy Classification With a Noise Cluster in Detecting Fraud in Insurance, Koc O., Baser F., Selcuk-Kestel A.S., (2024) Applied Soft Computing, 167, art. no. 112430, Cited 0 times., DOI: 10.1016/j.asoc.2024.112430
[12]	Codes on Subgroups of Weighted Projective Tori, Şahin M., Yayla O., (2024) Designs, Codes, and Cryptography, 92 (5), pp. 1201 - 1218, Cited 0 times., DOI: 10.1007/s10623-023-01337-y
[13]	Complete Characterization of a Class of Permutation Trinomials in Characteristic Five, Grassl M., Özbudak F., Özkaya B., Temür B.G., (2024) Cryptography and Communications, 16 (4), pp. 825 - 841, Cited 1 times., DOI: 10.1007/s12095-024-00705-2
[14]	Construction of self dual codes from graphs, Fellah N., Guenda K., Özbudak F., Seneviratne P., (2024) Applicable Algebra in Engineering, Communications and Computing, 35 (4), pp. 545 - 556, Cited 2 times., DOI: 10.1007/s00200-022-00567-2

[15]	Disruption, panic buying, and pricing: A comprehensive game-theoretic exploration, Soltanzadeh S., Rafiee M., Weber G.-W., (2024) Journal of Retailing and Consumer Services, 78, art. no. 103733, Cited 5 times., DOI: 10.1016/j.jretconser.2024.103733
[16]	Finite Element Formulations for Maxwell's Eigenvalue Problem Using Continuous Lagrangian Interpolations, Boffi D., Codina R., Türk O., (2024) Computational Methods in Applied Mathematics, Cited 0 times., DOI: 10.1515/cmam-2023-0081
[17]	Fluctuations of an omega-type killed process in discrete time, Şimşek M., Ramsden L., Papaioannou A.D., (2024) Modern Stochastics: Theory and Applications, 11 (4), pp. 459 - 478, Cited 0 times., DOI: 10.15559/24-VMSTA257
[18]	Improved Spectral Bound for Quasi-Cyclic Codes, Luo G., Ezerman M.F., Ling S., Ozkaya B., (2024) IEEE Transactions on Information Theory, 70 (6), pp. 4002 - 4015, Cited 0 times., DOI: 10.1109/TIT.2024.3364489
[19]	Long-Term Wind Power And Global Warming Prediction Using Mars, Ann, Cart, Lr, And Rf, Yılmaz Y., Nalçacı G., Kańczurzewska M., Weber G.W., (2024) Journal of Industrial and Management Optimization, 20 (6), pp. 2193 - 2216, Cited 3 times., DOI: 10.3934/jimo.2023162
[20]	Metaheuristic-driven extended exergy accounting for sustainable closed-loop food supply chain management, Shokouhifar M., Naderi R., Goli A., Gultom P., Shafiei Nikabadi M., Weber G.-W., (2024) Computers and Industrial Engineering, 191, art. no. 110148, Cited 4 times., DOI: 10.1016/j.cie.2024.110148
[21]	New distance bounds for quasi-cyclic codes, Özbudak F., Özkaya B., (2024) Designs, Codes and Cryptography, 92 (12), pp. 3981 - 4009, Cited 0 times., DOI: 10.1007/s10623-024-01464-0
[22]	New q-ary quantum MDS codes of length strictly larger than q+1, Kırcalı M., Özbudak F., (2024) Quantum Information Processing, 23 (12), art. no. 387, Cited 0 times., DOI: 10.1007/s11128-024-04598-1
[23]	On a class of permutation trinomials over finite fields, Temür B.G., Özkaya B., (2024) Turkish Journal of Mathematics, 48 (4), art. no. 11, pp. 778 - 792, Cited 0 times., DOI: 10.55730/1300-0098.3540
[24]	On a group under which symmetric Reed–Muller codes are invariant, Toplu S.K., Arıkan T., Aydoğdu P., Yayla O., (2024) Journal of Algebra and its Applications, art. no. 2550295, Cited 0 times., DOI: 10.1142/S0219498825502950
[25]	On subfield subcodes obtained from restricted evaluation codes, Güneri C., Özbudak F., Sayıcı S., (2024) Designs, Codes, and Cryptography, 92 (3), pp. 667 - 680, Cited 0 times., DOI: 10.1007/s10623-023-01261-1

[26]	On some permutation Trinomials in Characteristic Three, Özkaya B., Gülmez Temür B. Hacettepe Journal of Mathematics and Statistics, accepted. https://doi.org/10.15672/hujms.1443686
[27]	On technical bases and surplus in life insurance, Haçarız O., Kleinow T., Macdonald A.S., (2024) Scandinavian Actuarial Journal, 2024 (9), pp. 881 - 909, Cited 1 times., DOI: 10.1080/03461238.2024.2363183
[28]	Optimal model description of finance and human factor indices, Kalaycı B., Purutçuoğlu V., Weber G.W., (2024) Central European Journal of Operations Research, Cited 5 times., DOI: 10.1007/s10100-023-00897-7
[29]	PATS: Let Parties Have a Say in Threshold Group Key Sharing, Kılıç A., Onur C.B., Onur E., (2024), IET Information Security, 2024, Cited 0 times., DOI: 10.1049/2024/7557514
[30]	Peer Group Situations And Games With Fuzzy Uncertainty, Özcan İ., Gök S.Z.A., Weber G.-W., (2024) Journal of Industrial and Management Optimization, 20 (1), pp. 428 - 438, Cited 24 times., DOI: 10.3934/jimo.2023084
[31]	Quasi-Twisted Codes As Contractions Of Quasi-Cyclic Codes, Özbudak F., Özkaya B., (2024) Advances in Mathematics of Communications, 18 (2), pp. 394 - 409, Cited 0 times., DOI: 10.3934/amc.2023041
[32]	Reduced-Order modeling for Heston stochastic volatility model. Kozpınar, S., Uzunca, M., Karasözen, B., (2024) Hacettepe Journal of Mathematics and Statistics, 53(6), pp. 1515-1528, Cited 0 times, DOI: 10.15672/hujms.1066143
[33]	Ruin probability for heavy-tailed and dependent losses under reinsurance strategies, Yıldırım Külekci B., Korn R., Selcuk-Kestel A.S., (2024) Mathematics and Computers in Simulation, 226, pp. 118 - 138, Cited 0 times., DOI: 10.1016/j.matcom.2024.06.018
[34]	SUPG-based stabilized finite element computations of convection-dominated 3D elliptic PDEs using shock-capturing, Cengizci S., Uğur Ö., Natesan S., (2024) Journal of Computational and Applied Mathematics, 451, art. no. 116022, Cited 1 times., DOI: 10.1016/j.cam.2024.116022
[35]	The c-differential uniformity of the perturbed inverse function via a trace function Tr(x2x+1), Kaytancı K., Özbudak F., (2024) Periodica Mathematica Hungarica, 88 (2), pp. 384 - 395, Cited 1 times., DOI: 10.1007/s10998-023-00561-2
[36]	The use of machine learning techniques for assessing the potential of organizational resilience, Ewertowski T., Güldoğuş B.Ç., Kuter S., Akyüz S., Weber G.-W., Sadłowska-Wrzesińska J., Racek E., (2024) Central European Journal of Operations Research, 32 (3), pp. 685 - 710, Cited 12 times., DOI: 10.1007/s10100-023-00875-z

[37]	Time dependent magnetic field effects on the MHD flow and heat transfer in a rectangular duct, Tezer-Sezgin M., Türk Ö., (2024) ZAMM Zeitschrift fur Angewandte Mathematik und Mechanik, 104 (5), art. no. e202300411, Cited 0 times., DOI: 10.1002/zamm.202300411
[38]	Vine Copula Approach to Understand the Financial Dependence of the Istanbul Stock Exchange Index, Evkaya O., Gür İ., Yıldırım Külekci B., Poyraz G., (2024) Computational Economics, 64 (5), pp. 2935 - 2980, Cited 0 times., DOI: 10.1007/s10614-023-10544-7

Diğer Uluslararası Hakemli Dergilerde Makaleler

[1]	A comparative and illustrative study for solving singularly perturbed problems with two parameters, Cengizci S., Uğur Ö., Turkish World Mathematical Society Journal of Applied and Engineering Mathematics, 2024, 14 (2), pp. 520-536, Cited 0 times.
[2]	Dependence analysis of the ISE100 banking sector using vine copula. Yıldırım Külekci, B., Poyraz, G., Gür, İ., Evkaya, O., Istanbul Journal of Economics, 73(1), 55-82, 2023. http://dx.doi.org/10.26650/ISTJECON2022-1229039
[3]	Dssa: Direct Simplified Symbolic Analysis Using Metaheuristic-Driven Circuit Modelling, Shokouhifar M., Yazdanjouei H., Weber G.-W., (2024) Journal of Dynamics and Games, 11 (3), pp. 232 - 248, Cited 0 times., DOI: 10.3934/JDG.2023023
[4]	Dynamics of a Newly Established Agricultural Commodities Market: Financialization, Hedging and Portfolio Diversification in Turkey. Acikgoz T., Alp O.S., Alkan N.B., Annals of Financial Economics, 2023. https://doi.org/10.1142/S2010495223500057
[5]	Protecting the Future of Information: LOCO Coding with Error Detection for DNA Data Storage, Irimagzi C., Uslan Y., Hareedy A., (2024) IEEE Transactions on Molecular, Biological, and Multi-Scale Communications, 10 (2), pp. 317 - 333, Cited 0 times., DOI: 10.1109/TMBMC.2024.3400794
[6]	Solving Matrix Game Using Rough Interval Payoffs, Ghosh P., Bhaumik A., Weber G.W., Roy S.K., (2024) Journal of Dynamics and Games, 11 (4), pp. 399 - 421, Cited 0 times., DOI: 10.3934/jdg.2024010
[7]	The assessment of early warning for insurance company using machine learning methods, Koçer, G.B., Selcuk-Kestel, A.S., Gazi University Journal of Science, 2024 (ESCI M.Sc. Thesis)

[8]	The prediction power of machine learning on estimating the sepsis mortality in the intensive care unit. Selcuk, M., Koc, O., Selcuk-Kestel, A.S., Informatics in Medicine Unlocked, Volume 28, 100861. Elseiver, 2023. https://doi.org/10.1016/j.imu.2022.100861

Konferans Makaleleri (Proceedings)

[1]	Compartment-Based and Hierarchical Threshold Delegated Verifiable Accountable Subgroup Multi-signatures. Ağırtaş, A.R., Yayla, O. (2025). In: Dąbrowski, A., Pieprzyk, J., Pomykała, J. (eds) Number-Theoretic Methods in Cryptology. NuTMiC 2024. Lecture Notes in Computer Science, vol 14966. Springer, Cham. https://doi.org/10.1007/978-3-031-82380-0_10
[2]	Design and Implementation of a Fast, Platform-Adaptive, AIS-20/31 Compliant PLL-Based True Random Number Generator on a Zynq 7020 SoC FPGA, Yayla O., Yılmaz Y.E., (2024) Lecture Notes in Networks and Systems, 957 LNNS, pp. 45 - 55, Cited 0 times., DOI: 10.1007/978-3-031-75016-8_5
[3]	Distributed Verifiable Random Function with Compact Proof, Ağırtaş A. R., Özer A. B., Saygı Z., Yayla O., (2024), In: Dolev, S., Elhadad, M., Kutyłowski, M., Persiano, G. (eds) Cyber Security, Cryptology, and Machine Learning. CSCML 2024. Lecture Notes in Computer Science, vol 15349. Springer, Cham. https://doi.org/10.1007/978-3-031-76934-4_8
[4]	Effects of Torso Inhomogeneities on Spontaneous PVC Localization in Potential and Dipole-Based Methods. Rasoolzadeh N., Ondrusova B., Dogrusoz Y.S., Svehlikov J., Proceedings of the 14th International Conference on Measurement, MEASUREMENT 2023, 2-5, 2023. https://doi.org/10.23919/MEASUREMENT59122.2023.10164347
[5]	Single Secret Leader Election in Proof-of-Stake Blockchains: A Concise Review, Fettuh T., Yayla O., Proceedings of the 2024 17th International Conference on Information Security and Cryptology (ISCTürkiye), Ankara, Turkiye, 2024, pp. 1-6, doi: 10.1109/ISCTrkiye64784.2024.10779312.
[6]	Probabilistic Design of Multi-Dimensional Spatially-Coupled Codes, Irimağzi C., Tanrikulu A., Hareedy A., (2024) IEEE International Symposium on Information Theory - Proceedings, pp. 653 - 658, Cited 0 times., DOI: 10.1109/ISIT57864.2024.10619442

Kitap ve Kitap Bölümleri

[1]	Analysis of the Systemic Risk in the Turkish Banking Sector. Malkoç, M. and Şendeniz-Yüncü, İ., Banking Resilience and the Global Financial Stability; Editors Elnahass, M. and Boubaker, S., World Scientific Publishing, 191-210, 2024, Cited 0 times., https://doi.org/10.1142/q0422.
[2]	Modelling Natural Gas Future Prices via Hybrid Stochastic Diffusion Processes, Ozenc M.M, Koc O., Selcuk-Kestel, A.S., Energy Entrepreneurship, Sustainability, Innovation and Financing: Practical Applications & Future Directions" (EESIF), Springer.
[3]	The Impact of Renewable Energy Incentives on Carbon Prices in the USA. Coşkun, E. H., Selcuk-Kestel, A.S., Dalkir, S., The ESG Framework and the Energy Industry Demand and Supply, Market Policies and Value Creation; Editors Thewissen, J., Arslan-Ayaydin, O., Westerman,W., Dorsman, A., Springer, pp: 113-136, 2024. DOI: 10.1007/978-3-031-48457-5_7

Konferans ve Çalıştay Katılımları

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

[1]	A. Sevtap Kestel; 'Aktüerya Bilimlerinde Güncel Gelişmeler adlı seminere konuşmacı olarak katılmak üzere 16 Aralık 2024 tarihinde Kırıkkale, Türkiye' ziyaretinde bulunmuştur.
[2]	A. Sevtap Kestel; 'European Actuarial Journal Conference 2024 (EAJC) adlı konferansa bildirili katılmak üzere 8-12 Eylül 2024 tarihinde Lizbon, Portekiz' ziyaretinde bulunmuştur.
[3]	A. Sevtap Kestel; 'Katastrofik Risk Modelleme ve İklim Etkileri adlı seminere bildirili katılmak üzere 21-23 Ekim 2024 tarihinde İstanbul, Türkiye' ziyaretinde bulunmuştur.
[4]	Buket Özkaya; '36. Ulusal Matematik Sempozyumu (UMS 2024) adlı sempozyuma bildirili katılmak üzere 8-13 Eylül 2024 tarihinde Amasya, Türkiye' ziyaretinde bulunmuştur.
[5]	Buket Özkaya; 'Kadın ve Bilim X Çalıştayı adlı çalıştaya bildirili katılmak üzere 29 Kasım 2024 tarihinde Yozgat, Türkiye' ziyaretinde bulunmuştur.
[6]	Buket Özkaya, "SU Matematik Seminerleri", Sabancı Üniversitesi, 25 Aralık 2024

	tarihinde İstanbul, Türkiye' ziyaretinde bulunmuştur.
[7]	Cem Yavrum; 'Climate Change and Insurance (CCI 2024) adlı çalıştaya bildirili katılmak üzere 3-7 Eylül 2024 tarihleri arasında Avusturya,Viyana' ziyaretinde bulunmuştur.
[8]	Eylem Bahadır; 'The Third International Conference on Applied Mathematics in Engineering 2024 (ICAME'24) adlı kongreye bildirili katılmak üzere 26-28 Haziran 2024 tarihleri arasında Balıkesir, Türkiye' ziyaretinde bulunmuştur.
[9]	Hamdullah Yücel; 'Mat-Dyn-Net Final Conference (COST Action:CA18232) adlı konferansa bildirili katılmak üzere 5-9 Şubat 2024 tarihleri arasında Braga, Portekiz' ziyaretinde bulunmuştur.
[10]	Oğuz Koç; 'Insurance Fraud Detection via Clustering-Based Fuzzy Classification On Noisy Unbalanced Datasets, European Actuarial Journal Conference 2024 (EAJC) adlı konferansa bildirili katılmak üzere 8-12 Eylül 2024 tarihinde Lizbon, Portekiz' ziyaretinde bulunmuştur.
[11]	Oğuz Yayla; '17th International Conference on Information Technology and Communications Security (SecITC 2024) adlı konferansa bildirili katılmak üzere 20-24 Kasım 2024 tarihinde Bükreş, Romanya' ziyaretinde bulunmuştur.
[12]	Oğuz Yayla; 'Number-Theoretic Methods in Cryptology (NuTMİC 2024) adlı konferansa bildirili katılmak üzere 24-27 Haziran 2024 tarihleri arasında Szczecin, Polonya' ziyaretinde bulunmuştur.
[13]	Oğuz Yayla; 'TÜBİTAK 18. 2204B Ortaokul Öğrencileri Araştırma Proje Yarışması jüri üyeliğine katılmak üzere 22-23 Nisan 2024 tarihleri arasında Samsun,Türkiye' ziyaretinde bulunmuştur.
[14]	Oğuz Yayla; 'TÜBİTAK 55. 2204A Lise Öğrencileri Araştırma Proje Yarışması jüri üyeliğine katılmak üzere 5 Mart 2024 tarihleri arasında Samsun,Türkiye' ziyaretinde bulunmuştur.
[15]	Önder Türk; '10th International Conference on Computational Methods in Applied Mathematics (CMAM-10) adlı konferansa bildirili katılmak üzere 9-15 Haziran 2024 tarihleri arasında Bonn, Almanya' ziyaretinde bulunmuştur.
[16]	Önder Türk; '9th European Congress on Computational Methods in applied Sciences and Engineering (ECCOMAS CONGRESS) 2024 adlı kongreye bildirili katılmak üzere 2-8 Haziran 2024 tarihleri arasında Lizbon, Portekiz' ziyaretinde bulunmuştur.
[17]	Önder Türk; 'Chemnitz Finite Element Symposium 2024 adlı sempozyuma bildirili katılmak üzere 8-12 Eylül 2024 tarihleri arasında Chemnitz, Almanya' ziyaretinde bulunmuştur.

[18]	Önder Türk; 'Photonics and Electromagnetics Research Symposium (PIERS 2024) adlı sempozyuma bildirili katılmak üzere 19-27 Nisan 2024 tarihleri arasında Chengdu, Çin' ziyaretinde bulunmuştur.
[19]	Önder Türk; 'Seventh Chilean Workshop on Numerical Analysis of Partial Differential Equations (WONAPDE 2024) adlı konferansa katılmak üzere 13-21 Ocak 2024 tarihleri arasında Concepcion, Şili' ziyaretinde bulunmuştur.
[20]	Özenç Murat Mert, 'Optimal Risk Diversification For A Reinsurance Company Under A Stochastic Claim Approach, European Actuarial Journal Conference 2024 (EAJC) adlı konferansa bildirili katılmak üzere 8-12 Eylül 2024 tarihinde Lizbon, Portekiz' ziyaretinde bulunmuştur.
[21]	Ümit Işlak, Bükre Yıldırım Külekci; Analysis of the threshold dependence of degree related indices in weighted random graphs and complex networks, The 3rd International Conference on Applied Mathematics in Engineering (ICAME'24), Ayvalık-Balıkesir, Türkiye, 26-28 June 2024.

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 2024 yılında yapılan Bilimsel Etkinliklere yer verilmiştir.

Genel Seminer ve Kolokyum

[1]	Winkler, Max (Department of Mathematics, Technische Universitat Chemnitz, Germany); 07 Mart 2024 tarihinde 'Agent-Based Optimization of Pedestrian Dynamics via Local Attraction' başlıklı semineri vermiştir.
[2]	Tuğluk, Ozan; 04 Nisan 2024 tarihinde 'Analysis Driven Compression of Scientific Data with MGARD' başlıklı semineri vermiştir.
[3]	Uğurlu, Kerem (Nazarbayev University, Kazakhstan); 25 Nisan 2024 tarihinde 'A New Coherent Multivariate Average-Value-at-Risk' başlıklı semineri vermiştir.
[4]	Yıldırım Külekçi, Bükre (Institute of Applied Mathematics, METU); 09 Mayıs 2024 tarihinde 'Ruin Probability for Heavy-tailed and Dependent Losses Under Reinsurance Strategies' başlıklı semineri vermiştir.
[5]	Miroiu, Maria (Department of Mathematics and Informatics, National University of Science and Technology Politehnica Bucharest, Piteşti University Center, Romania); 25 Eylül 2024 tarihinde 'Solving Problems Using MATLAB Mathematical Software' başlıklı semineri vermiştir.

[6]	Bâlilescu, Loredana (Department of Mathematics and Informatics, National University of Science and Technology Politehnica Bucharest, Piteşti University Center, Romania); 26 Eylül 2024 tarihinde 'Bloch Waves Homogenization in The Graphene ' başlıklı semineri vermiştir.

Özel Seminer

[1]	Bülent Karasözen, Kernels and RKHS, 5 Mart 2024 (Emeritus, Affiliated Faculty at the Institute of Applied Mathematics, METU)
[2]	Ömür Uğur, Vectors, Matrices, Maps and the finite-dimensional RKHS-Part I, 12 Mart 2024 (Institute of Applied Mathematics, METU)
[3]	Ömür Uğur, Vectors, Matrices, Maps and the finite-dimensional RKHS-Part II, 14 Mart 2024 (Institute of Applied Mathematics, METU)
[4]	Aydın Aytuna, A Brief Introduction to Hilbert Space Theory with RKHS in Mind-Part I, 19 Mart 2024 (Emeritus, Affiliated Faculty at the Institute of Applied Mathematics, METU)
[5]	Ömür Uğur, Vectors, Matrices, Maps and the finite-dimensional RKHS-Part III, 26 Mart 2024 (Institute of Applied Mathematics, METU)
[6]	Baver Okutmuştur, Fundamental Properties of Reproducing Kernels and RKHS, 25 Nisan 2024 (Department of Mathematics, METU)
[7]	Azize Hayfavi, Stochastic Processes and the RKHS, 30 Mayıs 2024 (Emeritus, Affiliated Faculty at the Institute of Applied Mathematics, METU)
[8]	Jean-Marc Mercier, Kernel Methods: applications, promises and open issues, 25 Haziran 2024 (Dr., Head of R&D of MPG Partners)
[9]	Boumediene Hamzi, Machine Learning and Dynamical Systems meet in Reproducing Kernel Hilbert Spaces: Part I, 12 Kasım 2024 (Dr., Department of Computing and Mathematical Sciences, Caltech)
[10]	Boumediene Hamzi, Bridging Machine Learning, Dynamical Systems, and Algorithmic Information Theory: Insights from Sparse Kernel Flows, Poincaré Normal Forms and PDE Simplification, 3 Aralık 2024 (Department of Computing and Mathematical Sciences, Caltech, CA and The Alan Turing Institute, London)

[11]	Boumediene Hamzi, Machine Learning and Dynamical Systems meet in Reproducing Kernel Hilbert Spaces: Part I, 12 Kasım 2024 (Dr., Department of Computing and Mathematical Sciences, Caltech)
[12]	Aurelian Gheondea, Probability Error Bounds for Approximation of Functions in Reproducing Kernel Hilbert Spaces, 10 Aralık 2024 (Institute of Mathematics of the Romanian Academy, Bucharest, and Bilkent University, Ankara)

SIAM Student Chapter Seminerleri

[1]	Bağçe, Samet (Department of Philosophy/METU), 12 Aralık 2024 'Sanremo'lu bir Cizvit Giovanni Girolamo Saccheri (1667-1733) ve Euclides' başlıklı semineri vermiştir.

Konferans ve Çalıştay

[1]	WEB3 Workshop, 16 Mayıs 2024 (Institute of Applied Mathematics, METU, Ankara)
[2]	İbrahim Doğa Sarı, Hafıza Teknikleri Semineri, 30 Mayıs 2024 (Institute of Applied Mathematics,METU, Ankara)
[3]	Ankara-Istanbul Workshop on Stochastics Processes, Workshop, 6-7 Haziran 2024 (Institute of Applied Mathematics, METU, Ankara)
[4]	Recent Developments in Actuarial Science Workshop, 25 Haziran 2024 (Institute of Applied Mathematics, METU, Ankara)
[5]	İbrahim Doğa Sarı, Hafıza Teknikleri ve Hızlı Öğrenme Semineri, 19 Aralık 2024 (Institute of Applied Mathematics, METU, Ankara)

Kısa Süreli Ziyaretler Gelen Ziyaretçiler

[1]	Miroiu, Maria (Department of Mathematics and Informatics, National University of Science and Technology Politehnica Bucharest, Piteşti University Center, Romania); 24-27 Eylül 2024 tarihleri arasında 'Solving Problems using MATLAB Mathematical Software' başlıklı semineri vermiştir. The framework of the program Erasmus+ International Credit Mobility (KA171 Partner Countries – non-Europe Exchange)
[2]	Bâlilescu, Loredana (Department of Mathematics and Informatics, National University of Science and Technology Politehnica Bucharest, Piteşti University Center, Romania); 24-27 Eylül 2024 tarihleri arasında 'Bloch Waves Homogenization in The Graphene' başlıklı semineri vermiştir. The framework of the program Erasmus+ International Credit Mobility (KA171 Partner Countries – non-Europe Exchange)

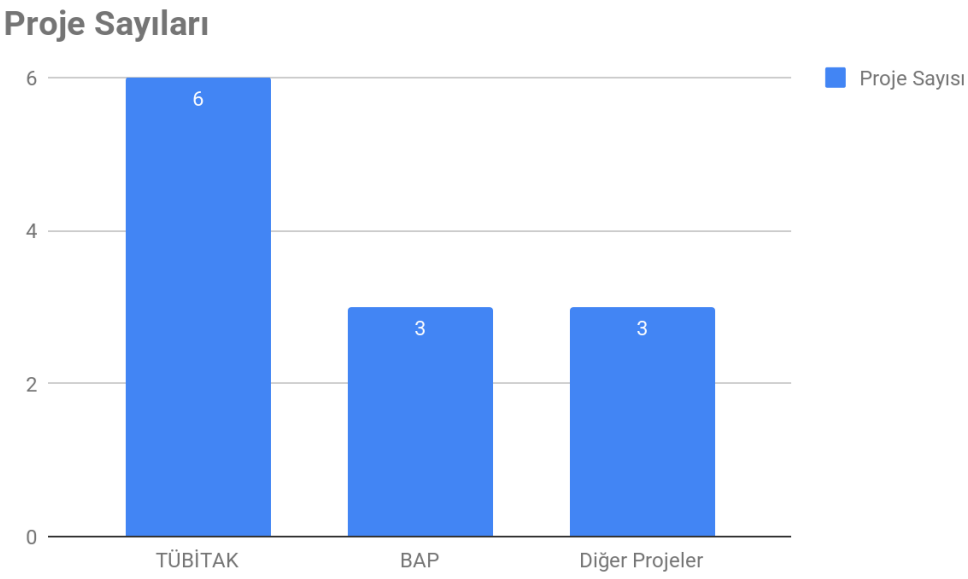
Giden Mensuplarımız

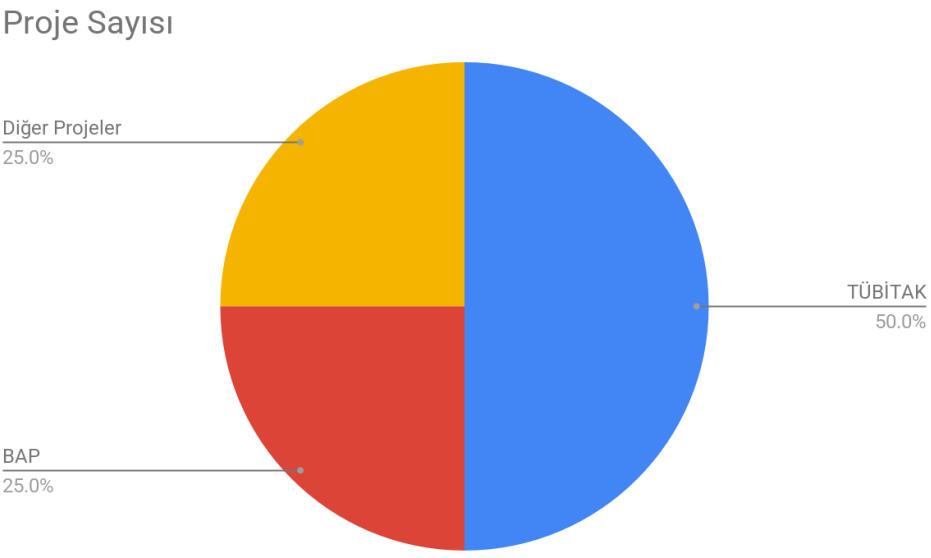
[1]	A. Sevtap Kestel; 'Albert Ludwigs University Freiburg-Institute for Economic Research Enstitüsünde seminer vermek ve işbirliği oluşturmak amacıyla 14-20 Ocak 2024 tarihleri arasında Freiburg, Almanya' ziyaretinde bulunmuştur.
[2]	Özenç Murat Mert; 'TÜBİTAK BİDEB 2219 Yurt Dışı Doktora Sonrası Araştırma Bursu çerçevesinde araştırmalar yapmak üzere 1 Şubat 2024-31 Ocak 2025 tarihleri arasında Technical University Kaiserslautern, Almanya' ziyaretinde bulunmuştur.
[3]	Meral Şimşek; 'Liverpool üniversitesinde seminer vermek üzere 27 Mart-5 Nisan 2024 tarihleri arasında Liverpool, Birleşik Krallık' ziyaretinde bulunmuştur.
[4]	Oğuz Koç; 'İstanbul Galatasaray Üniversitesi Matematik Festivalinde Enstitümüzün tanıtımını yapmak üzere 10-13 Mayıs 2024 tarihleri arasında İstanbul' ziyaretinde bulunmuştur.
[5]	Gözde Cennet Bayraktar; 'İstanbul Galatasaray Üniversitesi Matematik Festivalinde Enstitümüzün tanıtımını yapmak üzere 10-13 Mayıs 2024 tarihleri arasında İstanbul' ziyaretinde bulunmuştur.
[6]	A.Sevtap Kestel; 'RPTU Kaiserslautern (Technical University Kaiserslautern) ile akademik işbirliği yapmak üzere 29 Mayıs-1 Haziran 2024 tarihleri arasında Kaiserslautern, Almanya' ziyaretinde bulunmuştur.

[7]	Hamdullah Yücel; 'Max Planck Institute for Dynamics of Complex Technical Systems Enstitüsünde 7. Yıl İzni kapsamında araştırmalar yapmak üzere 1 Temmuz 2024-30 Haziran 2025 tarihleri arasında Magdeburg, Almanya' ziyaretinde bulunmuştur.
[8]	A.Sevtap Kestel; 'RPTU-Kaiserslautern Finans Matematiği Araştırma grubu ile devam eden çalışmaların ara raporlarının oluşturulması ve sonuçların değerlendirilmesini yapmak üzere 5-8 Ağustos 2024 tarihleri arasında Kaiserslautern, Almanya' ziyaretinde bulunmuştur.
[9]	Meral Şimşek; 'ERASMUS+ KA131 Projesi kapsamında Liverpool Üniversitesi'nde yaz stajı yapmak üzere 27 Temmuz-29 Eylül 2024 tarihleri arasında Liverpool, Birleşik Krallık' ziyaretinde bulunmuştur.
[10]	Gözde Cennet Bayraktar; 'Haluk Memili Lise Matematik Yaz Kampları kapsamında araştırma gruplarına katılmak ve ders vermek üzere 5 -31 Ağustos 2024 tarihleri arasında İzmir' ziyaretinde bulunmuştur.

Projeler

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


Proje Sayıları
6
4
2
0
6
3
3
TÜBİTAK
BAP
Diğer Projeler
Proje Sayısı


Proje Sayısı
Diğer Projeler
25.0%
TÜBİTAK
50.0%
BAP
25.0%

TÜBİTAK, Döner Sermaye ve Diğer Projeler

[1]	Proje Adı: Kriptografik Algoritmaların Tasarımı, Gerçekleştirilmeleri ve Uygulamaları (TÜBİTAK) Yürütücüsü : Oğuz Yayla Araştırmacılar: Nazlı Deniz Türe, Sermin Çakın, Yaman, N., Kırcalı, M. Başlangıç – Bitiş Tarihleri: 2019 – 2025 *22.09.2022 tarihine kadar Murat Cenk tarafından yürütülmüştür.
[2]	Proje Adı: Türkiye'deki Emeklilik Sisteminin Geliştirilmesi, Bütçe Açığı Minimizasyonu ve Özgün Emeklilik Planlarının Tasarlanması (TÜBİTAK 124F133) Yürütücü: Büşra Temoçin Araştırmacılar: A. Sevtap Kestel; Bükre Yıldırım Külekci Başlangıç - Bitiş Tarihleri: 2025 - 2028
[3]	Proje Adı: Zaman Gecikmeli Ve Stokastik Faktörlerle Entegreli Finansal Modelleri Temsil Eden Stokastik Optimal Kontrol Problemleri İçin Runge-Kutta Metoduna Dayalı Verimli Ve Kolay Hesaplamalı Algoritmaların Geliştirilmesi (TÜBİTAK 124F035) Başlangıç ve Bitiş Tarihleri 2024 - 2027
[4]	Proje Adı: Ortogonal Kodlar, Kaplama Yarıçapı, LCD Kodlar, Bayrak Kodları ve İlgili Alanlar Üzerine Araştırma (TÜBİTAK 1071) Yürütücüsü: Ferruh Özbudak Araştırmacılar: Buket Özkaya, C. Güneri, Z. Karakaş Başlangıç - Bitiş Tarihleri: 2024 - 2026
[5]	Proje Adı: Finansal Şokların Etkisine Bağlı Enflasyonun Dinamik Stokastik Diferansiyel Modellerle Tahmini (TÜBİTAK 1005 123F243) Yürütücüsü: A. Sevtap Kestel Araştırmacılar: Oğuz Koç Başlangıç - Bitiş Tarihleri: 2023 - 2025
[6]	Proje Adı: Levy Süreçlerinde En Büyük Artış/Düşüş Değerleri İle Sürelerinin Birlikte Dağılımları Ve Varlık/Sigorta Fiyatlarına Uygulama (TÜBİTAK 1001 124F094) Yürütücüsü: Ceren Vardar Acar Araştırmacılar: Başlangıç - Bitiş Tarihleri: 2024-2026

[7]	Proje Adı: Deprem Hasarlarının Finansal Risk Yönetiminde Katastrofik Bonoların CatBond Katkısının Enflasyon Etkisi Altında Değerlendirilmesi (GAP-705-2023-11376) Yürütücü: Sevtap Kestel Araştırmacılar: Özenç Murat Mert, Gülçin Akarsu Şengöz, Cem Yavrum Başlangıç - Bitiş Tarihleri: 2023 - 2024
[8]	Proje Adı: Enflasyon Etkisi Altında Katastrofi Bonolarının (CatBobds) Fiyatlandırılması (GAP-705-2023-11376) Yürütücü: A. Sevtap Kestel Araştırmacılar: Özenç Murat Mert, Cem Yavrum, Gülçin Akarsu Şengöz Başlangıç - Bitiş Tarihleri: 2023 - 2025
[9]	Proje Adı: Borsa Hisse Senedi Fiyat Tahmininde Stokastik Diferansiyel Denklem Modellerinin Yapay Zeka Metotları Yoluyla İstiflendirilmesi (ADEP-705-2024-11514) Yürütücü: A. Sevtap Kestel Araştırmacılar: Özenç Murat Mert, Oğuz Koç, Kerem Zengin Başlangıç - Bitiş Tarihleri: 2024 - 2025
[10]	Proje Adı: Laplace-Steklov Özdeğer Problemlerinin Sınır-Sonlu Elemanları Yöntemleriyle Analizi (AGEP-705-2023-11411) Yürütücü: Önder Türk Araştırmacılar: Eylem Bahadır Başlangıç - Bitiş Tarihleri: 2023 - 2025
[11]	Proje Adı: Silik Hedef Tespiti ve Konvoy Takibi Algoritmaları Tedariki (SİLİ-KON) Yürütücüsü: Prof. Dr. A. Aydın Alatan Araştırmacılar: Aybora Köksal, Furkan Aykut Sarıkamış, Önder Tuzcuoğlu, Haktan Yalçın, Mustafa Kütük* Başlangıç-Bitiş Tarihleri: Ocak 2024-Ocak 2025 (Ekim 2024-Ocak 2025)*
[12]	Proje Adı: Hava Kuvvetleri Komutanlığı Yardımlaşma Derneği 2023 Yılı Aktüeryal Değerlendirme (Döner Sermaye: 2024-15-00-2-00-001) Yürütücüsü: A. Sevtap Kestel, Bükre Yıldırım-Külekci Başlangıç - Bitiş Tarihleri: 2024 - 2024

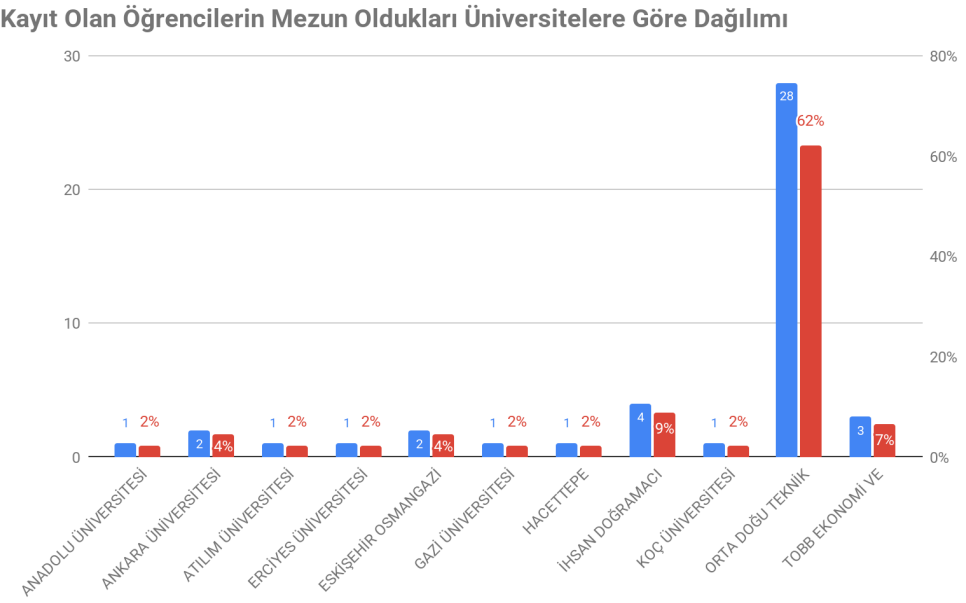
Eğitim

Başvurular, Kabul ve Kayıtlar

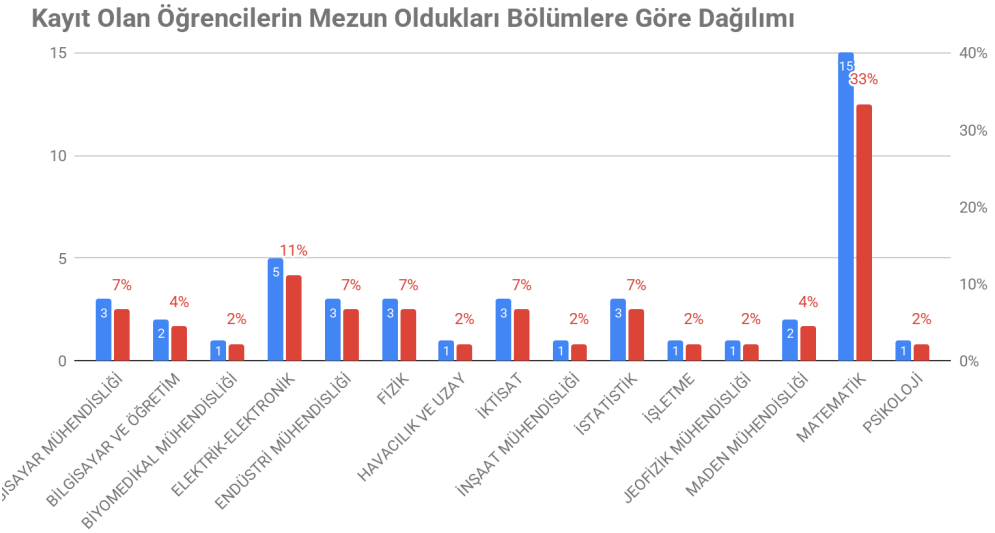
Enstitü Anabilim Dallarındaki programlara başvuru yapan ve kabul edilen öğrencilerin toplam başvuru sayılarına oranları aşağıdaki tabloda verilmiştir. Başvuru sayısının düşük olduğu programlar ile ilgili geniş çaplı tanıtım stratejilerinin belirlenmesi hedeflenmektedir.

Enstitü Anabilim Dalları	BAŞVURULAR - 2024		
	Başvuru (%)	Kabul (%)	Kayıt (%)
Aktüerya Bilimleri	11 (% 11)	10 (% 14)	6 (% 13)
Bilimsel Hesaplama	41 (% 40)	23 (% 33)	14 (% 31)
Finansal Matematik	22 (% 22)	14 (% 20)	11 (% 24)
Kriptografi	28 (% 27)	22 (% 32)	14 (% 31)
Toplam	102	69	45

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



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.



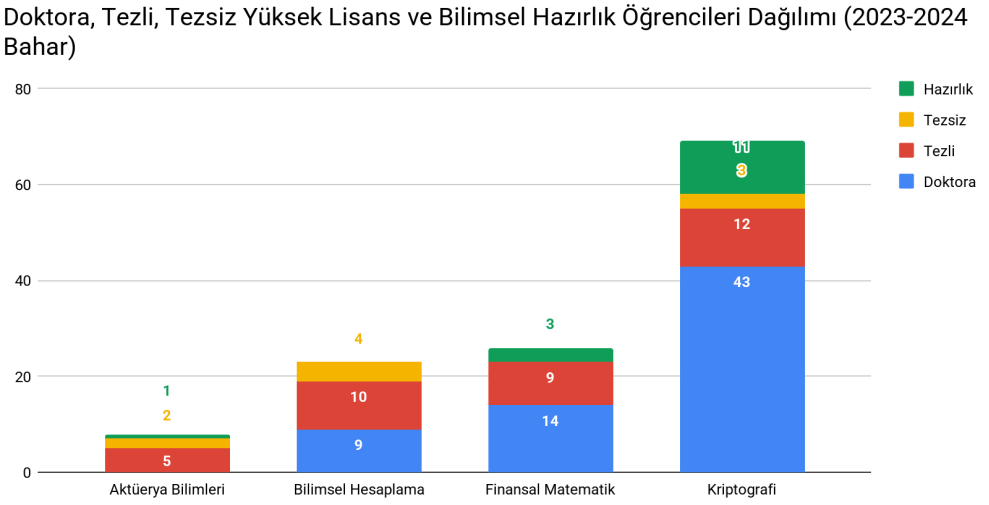
Enstitü Öğrencilerinin Programlara Göre Dağılımı ve İstatistikler

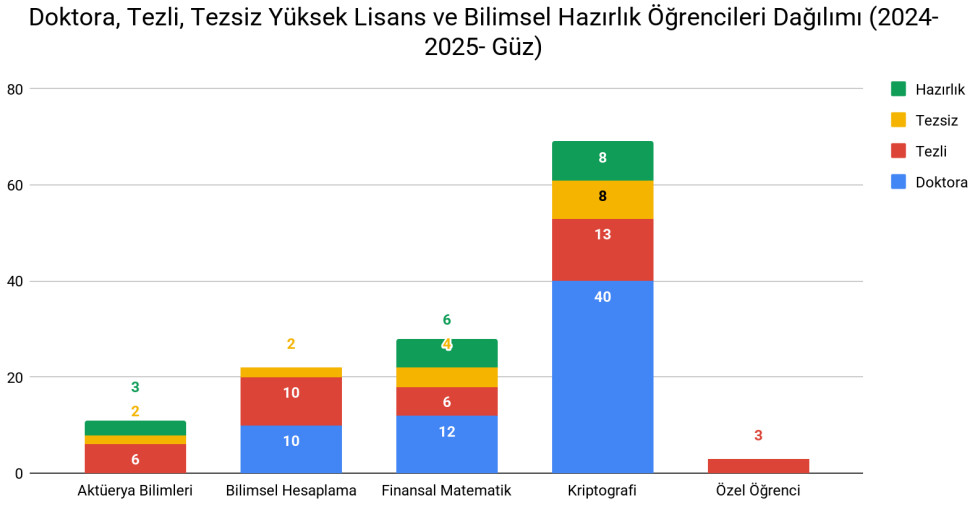
Enstitümüze yeni katılan öğrencilerimiz ile birlikte, mevcut öğrencilerimizin programlara göre dağılımı aşağıdaki “2024-2025 Güz” ve “2023-2024 Bahar” başlıklı tablolarda belirtilmiştir.

2023-2024 Bahar					
Anabilim Dalı	**Doktora**	**Tezli**	**Tezsiz**	**Hazırlık**	**Toplam**
Aktüerya Bilimleri		5	2	1	**8**
Bilimsel Hesaplama	9	10	4		**23**
Finansal Matematik	14	9		3	**26**
Kriptografi	43	12	3	11	**69**
Özel Öğrenci					**0**
	66	**36**	**9**	**15**	**126**

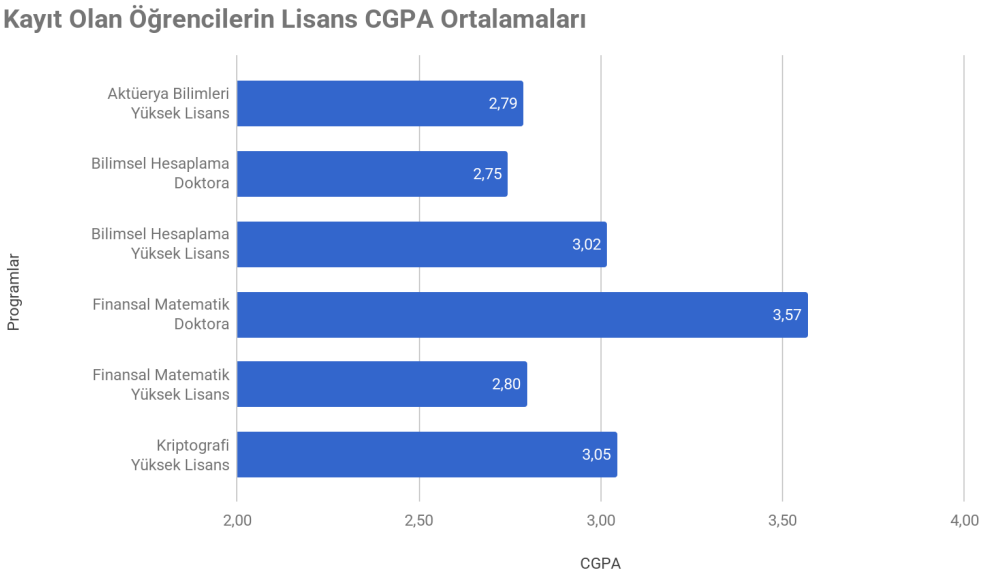
2024-2025 Güz					
Anabilim Dalı	**Doktora**	**Tezli**	**Tezsiz**	**Hazırlık**	**Toplam**
Aktüerya Bilimleri		6	2	3	**11**
Bilimsel Hesaplama	10	10	2		**22**
Finansal Matematik	12	6	4	6	**28**
Kriptografi	40	13	8	8	**69**
Özel Öğrenci		3			**3**
	62	**38**	**16**	**17**	**133**

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



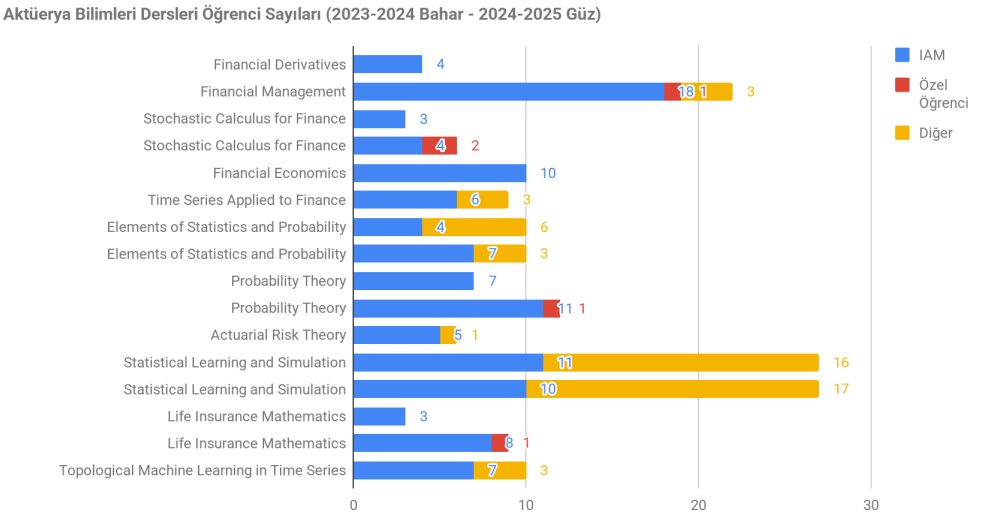


Enstitümüze kayıt yaptıran öğrencilerin Anabilim Dalı bazında lisans akademik başarı performansları (CGPA ortalamaları) aşağıdaki gibi gerçekleşmiştir.

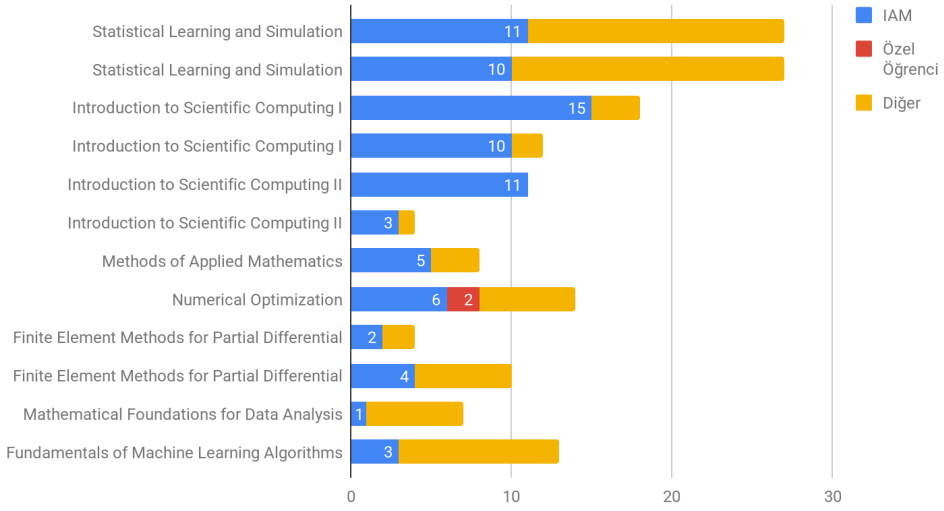


Enstitüdeki Dersler, Öğrenci Sayıları ve İstatistikler

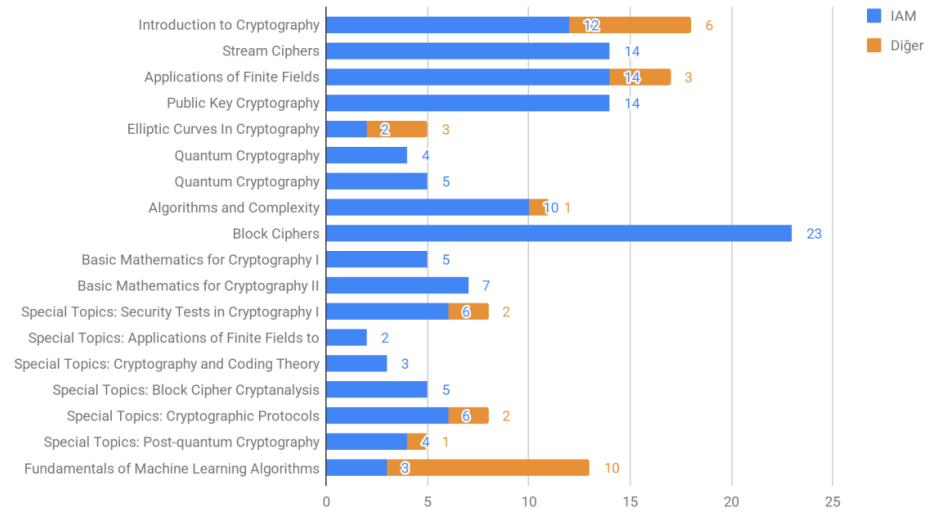
Bu bölümde, Enstitümüzde 2024 yılı içerisinde açılan derslere ve bu derslere ilişkin istatistiklere yer verilmiştir. Aşağıdaki grafiklerde, her bir Anabilim Dalı için belirtilen derslerdeki enstitü ve enstitü-dışı öğrenci sayıları verilmektedir. Birçok dersimizin, birden fazla Anabilim Dalında listelenmiş olması programlar arası bilgi akışının sağlanması amacına yönelik olup, Enstitümüzün ve derslerimizin disiplinlerarası çalışmalara verdiği önemin bir göstergesidir.



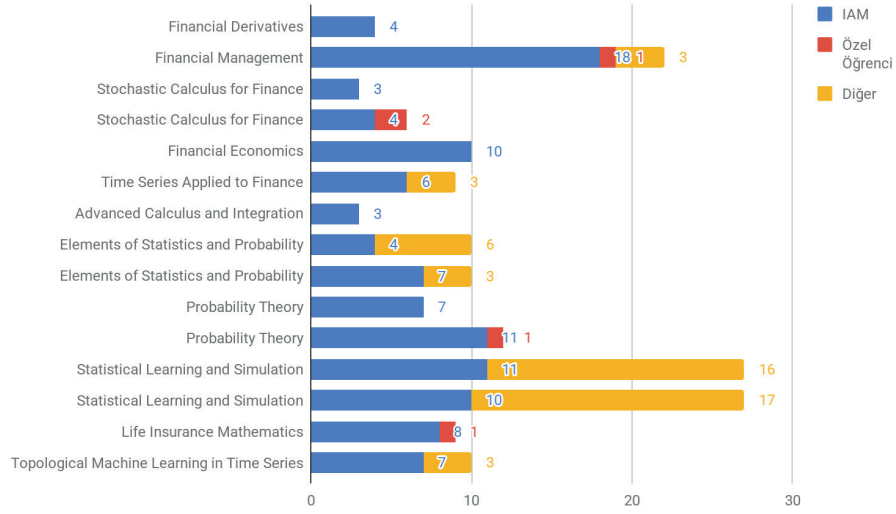
Bilimsel Hesaplama Dersleri Öğrenci Sayıları (2023-2024 Bahar - 2024-2025 Güz)



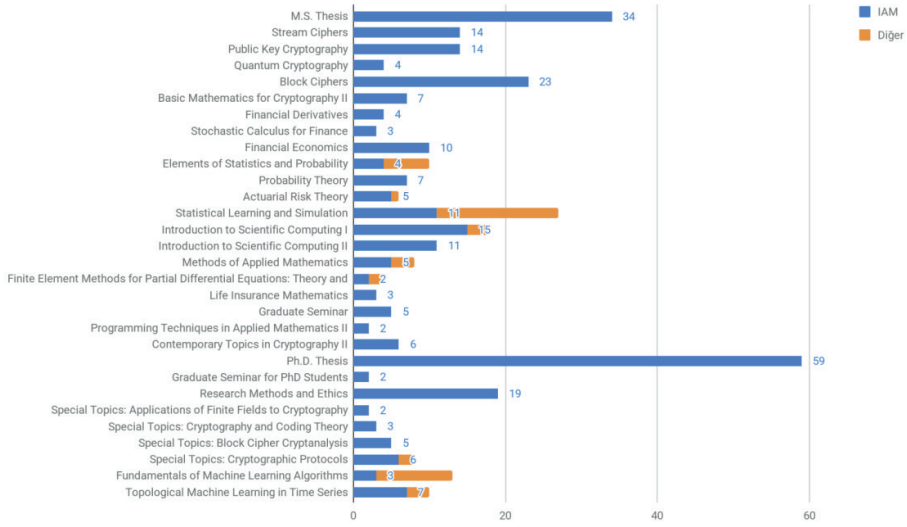
Kriptografi Dersleri Öğrenci Sayıları (2023-2024 Bahar - 2024-2025 Güz)

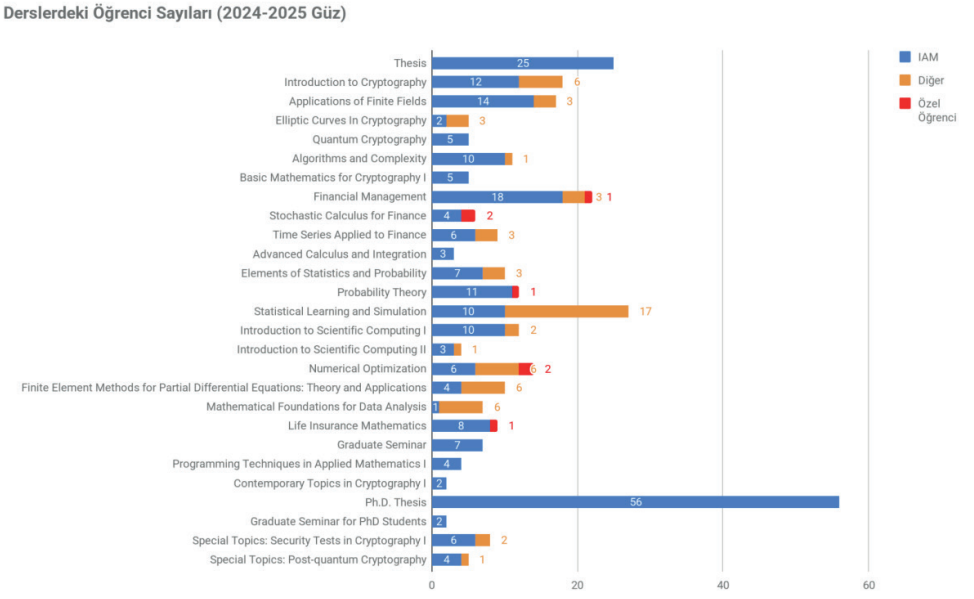


Finansal Matematik Dersleri Öğrenci Sayıları (2023-2024 Bahar - 2024-2025 Güz)



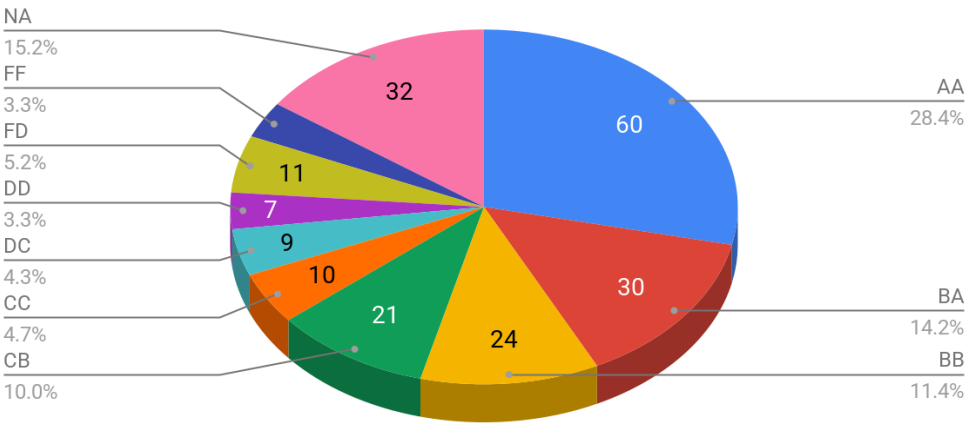
Derslerdeki Öğrenci Sayıları (2023-2024 Bahar)



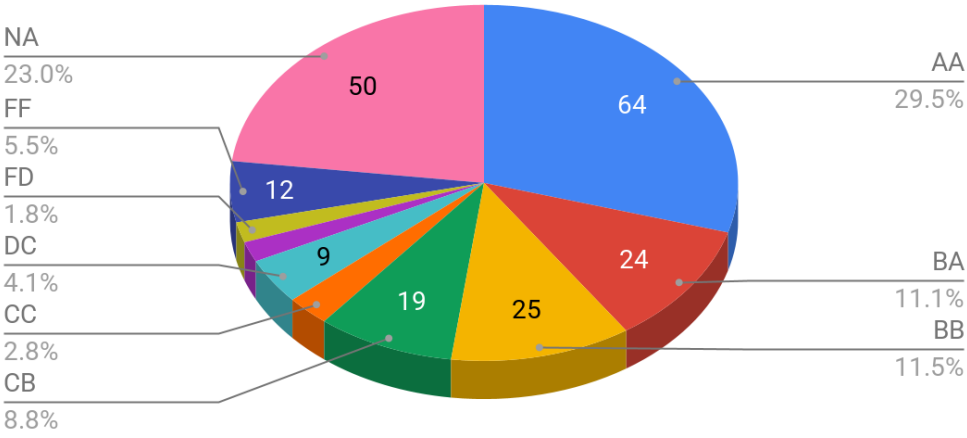


Aşağıdaki grafiklerde 2024 yılı içerisinde 2024-2025 Güz ve 2023-2024 Bahar dönemlerinde açılan tüm dersler, öğrenci sayıları ve not dağılımları verilmiştir. Özellikle not dağılımını gösteren grafiklerde %20-%30'lar seviyesinde olan "NA" notundaki artış sebeplerinden en önemlisi öğrencilerimizin eğitimlerinin yanı sıra çeşitli kurum ve kuruluşlarda çalışmaları olduğu düşünülmektedir.

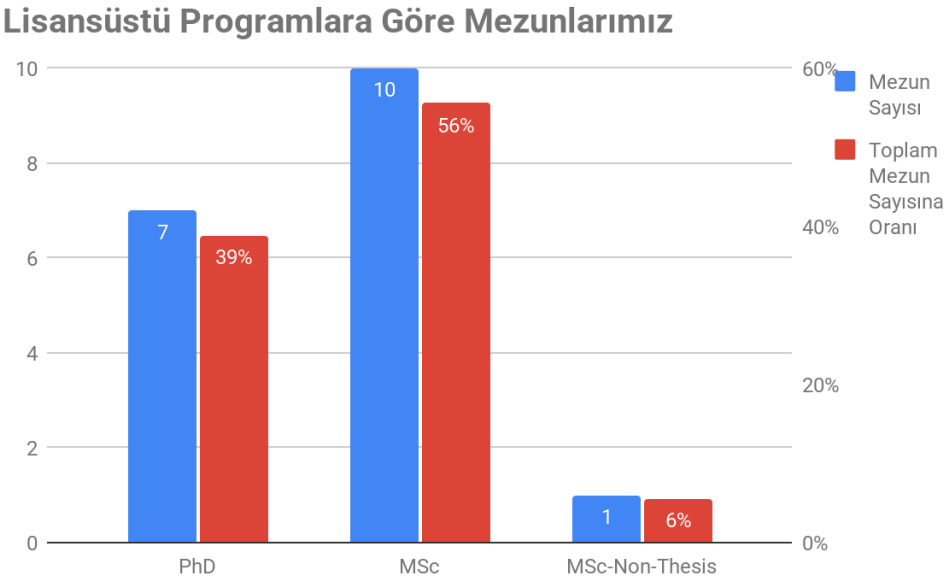
2024-2025 Güz Dönemi Not Dağılımı



2023-2024 Bahar Dönemi Not Dağılımı



Enstitümüz Yüksek Lisans ve Doktora programlarından 2024 yılında mezun olan öğrencilerimizin sayıları ve oranları aşağıda yer almaktadır. 2024 yılındaki 7 doktora, 10 Tezli ve 1 Tezsiz Yüksek lisans mezunumuz akademik ve diğer kuruluşlarda çalışmaktadırlar.



Doktora Programları

2024-2025 Güz ve 2023-2024 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]	Kocaman, S., Proba: Privacy-Preserving, Robust and Accessible Blockchain-Powered Helios, PhD Thesis, Cryptography, February 2024 (Danışmanı: Ali Doğanaksoy; Ortak Danışmanı: Fatih Sulak)
[2]	Ağırtaş, A. R., Verifiable Accountable Subgroup Multi-Signatures, PhD Thesis, Cryptography, February 2024 (Danışmanı: Oğuz Yayla)
[3]	Yılmaz Y. E., On An Efficient Implementation of Combined True Random Number Generator and Physically Unclonable Function on A Soc Fpga, PhD Thesis, Cryptography, September 2024 (Danışmanı: Oğuz Yayla)
[4]	Gülveren, A., Influence Of Expected Premium on Optimal Reinsurance and İnvestment strategy, PhD Thesis, Financial Mathematics, September 2024 (Danışmanı: A. Sevtap Kestel; Ortak Danışmanı: Başak Bulut Karageyik)
[5]	Aslan, M., Entropy Estimation Methods and Health Tests for Cryptographic Random Number Generators, PhD Thesis, Cryptography, September 2024 (Danışmanı: Ali Doğanaksoy)
[6]	Alptekin, E. E., Option Pricing Under Delay Effect, PhD Thesis, Financial Mathematics, October 2024 (Danışmanı: Ömür Uğur)
[7]	Türe, N. D., Efficient Batch Algorithms For The Post-Quantum Crystals Dilithium Signature Scheme And Crystals Kyber Encryption Scheme, PhD Thesis, Cryptography, November 2024 (Danışmanı: Oğuz Yayla; Ortak Danışmanı: Murat Cenk)

Yüksek Lisans Programları

2024-2025 Güz ve 2023-2024 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]	Çam, C. D., Multiple Connectivity Approach to Network Formation Games, M.Sc. Thesis, Scientific Computing, January 2024 (Danışmanı: Esma Gaygısız Lajunen; Ortak Danışmanı: Hamdullah Yücel)
[2]	Aykurt, F., Analysis of Two Versatile Mpc Frameworks Mp-Spdz and Mpyc, M.Sc. Thesis, Cryptography, January 2024 (Danışmanı: Oğuz Yayla)
[3]	Elmas, G., Some Constructions of Mutually Unbiased Bases Over Finite Fields, M.Sc. Thesis, Cryptography, February 2024 (Danışmanı: Buket Özkaya; Ortak Danışmanı: Ferruh Özbudak)
[4]	Kahveci , S., İnvestigation of the Greenium in Commercial Mortgage-Backed Securities, M.Sc. Thesis, Financial Mathematics, May 2024 (Danışmanı: Zehra Nuray Güner)
[5]	Yakut, Ş. K., Estimation of A Stochastic Volatility And Jumps Model Using Generalized Method of Moments With Ordinary Moment Conditions, M.Sc. Thesis, Financial Mathematics, May 2024 (Danışmanı: Ali Devin Sezer)
[6]	Karasu, N., Future Price İndex of Farm Products Based on Climate Factors, M.Sc. Thesis, Financial Mathematics, July 2024 (Danışmanı: Erkan Erdil; Ortak Danışmanı: Şahap Kasırga Yıldırak)
[7]	Aslanöz, İ., The İmpact of Dependence Between Claim Frequency and Severity on Expected Loss Using Glm: Mtpl Application, M.Sc. Thesis, Actuarial Science, August 2024 (Danışmanı: A. Sevtap Kestel; Ortak Danışmanı: Bükre Yıldırım Külekci)
[8]	Açıkgöz, T., Optimal Portfolio Allocation Under Fractal Theory, M.Sc. Thesis, Financial Mathematics, August 2024 (Danışmanı: Büşra Zeynep Temoçin)
[9]	Ateşağaoğlu, Alan, G. D., İmpact of Risk Liquidity Premium on İnventory Process in A Market Making Model, M.Sc. Thesis, Financial Mathematics, September 2024 (Danışmanı: Ali Devin Sezer)

[10]	Uykun, F. N., Machine Learning Applications in Portfolio Optimization, M.Sc. Thesis, Financial Mathematics, October 2024 (Danışmanı: Büşra Zeynep Temoçin)

Tezsiz Yüksek Lisans Mezunları

2024-2025 Güz ve 2023-2024 Bahar dönemlerinde Enstitümüz bünyesindeki Tezsiz Yüksek Lisans programlarından aşağıda ismi listelenen öğrencimiz başarı ile mezun olmuştur. Mezunumuzu tebrik eder, başarılarının devamını dileriz.

[1]	Gökcan, Ö., Contingent Convertible Bonds and An Analysis About Their Pricing, Financial Mathematics, February 2024 (Danışmanı: Esma Gaygısız Lajunen)

Ödüller

2023-2024 Eğitim öğretim yılında ODTÜ Lisansüstü Tez Ödülü'nü Enstitümüzde;

- Tezden kaynaklanan yayın kategorisinde, Finansal Matematik EABD'ndan Prof. Dr. Sevtap Kestel danışmanlığında ve Doç. Dr. Zehra Ekşi-Altay ortak danışmanlığında tamamladığı doktora tezi ile Çiğdem Yerli, almıştır.

Mezunumuzu ve danışmanlarını tebrik eder, başarılarının devamını dileriz.

Ek Bilgiler

Yeni Açılan Dersler (2024 Yılı)

Enstitümüzün ders kataloğuna 2024-2025 Sonbahar döneminde açılan aşağıdaki ders eklenmiştir.

Course Code	**9700788**
Course Title	**Topological Machine Learning in Time Series**
Course Credit(s)	**METU 3(3-0) ECTS 8**
Instructor(s)	**Ceylan Yozgatlıgil, A. Sevtap Kestel, İsmail Güzel**
Prerequisites	None
Course Catalog Description	This course provides students with time series modeling, and Topological Data Analysis (TDA) that are recently used to examine the shape of the data in data science field. The topics include the fundamentals of many disparate fields such as algebraic topology, linear algebra, machine learning algorithms, statistics, and time series modeling in order to understand recent results in the TDA and time series field besides using the efficient software for the computation of things discussed in class, such as persistent homology. Real world cases will be presented throughout the course and students will get experience in data science platforms using Python or R programming language and High Performance Computing.
Course Objectives	At the end of the course, the student will learn: ● Statistical methods in time series ● Data management: cleaning, curation and preparation ● Deep learning (machine learning methods) ● Simulation methods ● Topological background and implementation ● Gain knowledge about machine learning concepts in TDA ● Topological approach in predicting time series data ● Application of proposed material in real and simulated data

Tentative (Weekly) Outline	**1.** Basics in statistical modeling **2.** Time series modeling **3.** Data management **4.** Machine learning models **5.** Parameter estimation approaches in ML **6.** Fitting conditions in ML models **7.** Base in algebraic topology **8.** Persistent homology **9.** Topological mapping in time series data **10.** Data application and or simulation
Course Textbook(s)	**1.** Shumway R.H., Stoffer, D.S., Time Series Analysis and Its Applications: with R examples, Springer, 2017. **2.** Tamal K. Dey and Yusu Wang. Computational Topology for Data Analysis, 2021. **3.** Carlsson, Gunnar, and Mikael Vejdemo-Johansson. Topological data analysis wi*h applications. **4.** Cambridge University Press, 2021.

2024 Yılı Doktora Mezunlarımız

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

Adı Soyadı: Ahmet Ramazan Ağırtaş

Ahmet Ramazan Ağırtaş 2003 yılında Kara Harp Okulu'ndan mezun olmuştur. Daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi bölümünde lisans sonrası doktora çalışmalarına devam etmiş ve Ocak 2024 tarihinde Doç. Dr. Oğuz Yayla danışmanlığında "Verifiable Accountable Subgroup Multi-signatures" başlıklı tezini tamamlamıştır. Araştırma konuları arasında dijital imzalar, çoklu imzalar, doğrulanabilir rastgele fonksiyonlar, eşleme ve kafes tabanlı kriptografi, blok zincir uygulamaları, sıfır bilgi ispatları ve yapay zeka uygulamaları bulunmaktadır. Ahmet Ramazan Ağırtaş, 2003 ve 2021 yılları arasında Jandarma Genel Komutanlığı bünyesinde çeşitli görevlerde bulunmuş olup 2022 yılından bu yana Londra merkezli blok zincir teknoloji şirketi olan Nethermind'da blok zincir ve kriptografi araştırmacısı olarak görev almaktadır. Ayrıca kurucu ortağı olduğu AYWARE Bilişim Çözümleri Ltd. Şti'nde müdür olarak görev yapmakta ve blok zincir / kriptografi alanında projeler yürütmektedir.

Doktora Tezi Özeti :

Bu tezde, hesap verilebilir bir altgrup çoklu imza (ASM) çerçevesi tanıtıyoruz. Çerçeve, her biri seçilmiş mesaj saldırılarına karşı güvenli ve hesaplamalı co-Diffie-Hellman / ψ-co-Diffie-Hellman varsayımına dayanan üç yeni eşleme tabanlı ASM şemasını, yani vASM, ASMwSA ve ASMwCA şemalarını içermektedir. İmza üretimi sırasında imzacı altgrubunun bilinmediği yeni ASM şemaları önererek bir açık problemi ele alıyoruz. Şemalarımız, imza üretimi, birleştirme ve doğrulama aşamalarında hesaplama verimliliği açısından mevcut yöntemleri geride bırakmaktır. Ek olarak, vASM imza yetkisinin kısmi ve hiyerarşik eşik delegasyonu için yeni metotlar öneriyoruz. Şemanın bir vekil imza olarak işlev görebileceğini, bir yetkili kullanıcının imza haklarını yetkisiz bir kullanıcıya veya gruba devretmesine izin verebileceğini gösteriyoruz. Özyinelemeli vASM uygulaması, Shamir'in sır paylaşım şeması, iç içe sır paylaşımı ve hiyerarşik eşik sır paylaşımı kullanarak dört yeni yapı sunuyor ve bunların verimlilik ve güvenlik açısından kar¸sıla¸stırmasını yapıyoruz. Ayrıca, vASM'nin grup kurulum yöntemi ile Damgård ve diğerlerinin kafes tabanlı MS2 çoklu imza şemasını birleştirerek yeni bir kafes tabanlı ASM şeması (vMS2) öneriyoruz. Anahtar üretim, imza üretim ve doğrulama aşamalarının MS2 şemasıyla eşdeğer olduğunu gösteriyoruz. Önerdiğimiz vMS2 şeması, grup kurulumu sırasında müşterek doğrulanabilir gizli paylaşım şeması kullanarak hesap verilebilirliği altta yatan MS2 şemasının biraz üzerinde bir maliyetle gerçekleştirmektedir.

Yayınlar:

- Ağırtaş, A.R., Yayla, O. (2023). Delegated Verifiable Accountable Subgroup Multi-signatures. ALgebraic and combinatorial methods for COding and CRYPTography. ALCOCRYPT 2023. CIRM. Luminy.
- Ağırtaş, A.R., Yayla, O. (2025). Compartment-Based and Hierarchical Threshold Delegated Verifiable Accountable Subgroup Multi-signatures. In: Dąbrowski, A., Pieprzyk, J., Pomykała, J. (eds) Number-Theoretic Methods in Cryptology. NuTMiC 2024. Lecture Notes in Computer Science, vol 14966. Springer, Cham. https://doi.org/10.1007/978-3-031-82380-0_10
- Ağırtaş, A.R., Özer, A.B., Saygı, Z., Yayla, O. (2025). Distributed Verifiable Random Function with Compact Proof. In: Dolev, S., Elhadad, M., Kutyłowski, M., Persiano, G. (eds) Cyber Security, Cryptology, and Machine Learning. CSCML 2024. Lecture Notes in Computer Science, vol 15349. Springer, Cham. https://doi.org/10.1007/978-3-031-76934-4_8
- Ağırtaş, A.R., Yaman Gökçe, N., Yayla, O. (2025). Enhancing Local Verification: Aggregate and Multi-Signature Schemes. International Conference on Security for Information Technology and Communications. SECICT 2024. Bucharest.
- Ağırtaş, A.R., Yayla, O.: Pairing-based accountable subgroup multi-signatures with verifiable group setup. Cryptology ePrint Archive, Report 2022/018 (2022), https://ia.cr/2022/018
- Ağırtaş, A. R., Yayla, O. (2024). A Lattice-based Accountable Subgroup Multi-signature Scheme with Verifiable Group Setup. Cryptology ePrint Archive, Report 2024/14 (2024), https://eprint.iacr.org/2024/014.pdf

Adı Soyadı: E. Ezgi Aladağlı

E.Ezgi Alptekin 2013 yılında ODTÜ Matematik bölümünden mezun olmuştur. 2014 yılında ODTÜ Uygulamalı Matematik Enstitüsünde Finansal Matematik Anabilim dalında başlamış olduğu yüksek linans çalışmalarını ise 2017 yılında tamamlamıştır. ODTÜ Uygulamalı Matematik Enstitüsünde Finansal Matematik Anabilim dalında doktora çalışmalarına devam etmiş ve Eylül 2024 tarihinde Prof. Dr. Ömür Uğur danışmanlığında "Option Pricing Under Delay Effect" başlıklı tezini tamamlamıştır. Araştırma konuları arasında rassal olmayan diferansiyel denklemler, opsiyon fiyatlamaları ve gecikmenin opsiyon fiyatlamasına etkileri vardır. E.Ezgi Alptekin, 2014 yılında ODTÜ matematik bölümünde araştırma görevlisi olarak göreve başlamış ve bu görevine devam etmektedir.

Doktora Tezi Özeti :

Fizik, ekoloji, biyoloji, ekonomi, mühendislik, finansal matematik gibi birçok alanda olaylar genellikle anında etki göstermez. Bunun yerine, gelecekteki durumları etkilerler. Bu sistemlerin nasıl çalıştığını ve davrandığını anlamak için, stokastik diferansiyel denklemlere (SDE) geçmiş olaylardan gelen bilgileri ekleyerek elde edilen stokastik gecikmeli diferansiyel denklemler (SDDE) kullanılır. Bu nedenle, SDDE'ler gerçek hayatı daha iyi yansıtabildikleri için giderek daha fazla ilgi çekmektedir. Stokastik kalkülüs kullanılarak tam çözümler bulmak genellikle çok zor ve bazen imkansız olduğundan, SDDE'ler için bazı sayısal yöntemler geliştirilmiştir. En bilinen yöntemler Euler Maruyama ve Milstein yöntemleridir. Son zamanlarda, ekonomi ve finans alanında, zaman gecikmelerinin rastgele ya da sabit olabileceği sistemler için opsiyon fiyatlandırması üzerine araştırmalar yapılmaktadır. Bu tez, sabit bir gecikme süresi olduğunda SDDE'lerin genel formlarını anlamayı, bu denklemleri çözmeyi ve daha sonra bu denklemleri opsiyon fiyatlandırması için kullanmayı amaçlamaktadır. Gecikmeli geometrik Brown hareketini (GBM) takip eden dinamikler altında Avrupa tipi vanilla, Amerikan tipi vanilla, Avrupa tipi döviz, Avrupa tipi takas opsiyonlarının ve varlık fiyatının gecikmeli Heston modelini takip ettiği Avrupa tipi vanilla opsiyonlarının fiyatlandırılması ele alınmıştır. Ardından gecikme teriminin fiyatlandırma sürecine etkisini görmek için bazı sayısal uygulamalar yapılmıştır.

Adı Soyadı: Melis Aslan

2024 yılında Orta Doğu Teknik Üniversitesi (ODTÜ) Uygulamalı Matematik Enstitüsü'nde Kriptografi alanında bütünleşik doktora programını tamamlayan Melis Aslan, aynı üniversiteden 2015 yılında Matematik bölümünden lisans derecesiyle mezun olmuştur. Ayrıca, 2012-2015 yılları arasında ODTÜ İşletme Bölümü'nde Finans üzerine yandal programını tamamlamıştır. 2017 yılından itibaren FAME CRYPT bünyesinde Kriptosistem Tasarımı ve Analizi alanında araştırmacı ve akademik danışman olarak görev yapmıştır. 2022 yılından bu yana aynı şirkette direktör ve kıdemli araştırmacı olarak görev yapmaktadır. Bunun yanı sıra, 2018 yılından itibaren ODTÜ Matematik Bölümü'nde araştırma görevlisi olarak çalışmaktadır.

Doktora Tezi Özeti :

Rastgele sayılar kriptografide önemli bir rol oynar, kriptografik protokollerin güvenliği gizli anahtarlar, parolalar, başlatma vektörleri, gürültü, maskeleme vektörleri gibi dizileri üretmek için düzgün dağılıma sahip ve öngörülemeyen rastgele sayıların kullanılabilirliği varsayımına dayanır. Gerçek Rastgele Sayı Üreteçleri (GRSÜ'ler), çeşitli fiziksel olgulardan (radyoaktif bozunma, termal gürültü ve atmosferik gürültü gibi) rastgele sayılar üretirler ve bu üretim doğası gereği rastgele olarak kabul edilir. fakat pratik uygulamalarda, rastgele sayı üreteçleri bazen başarısız olur ve düşük entropili çıktılar üretir, bu da güvenlik açıklarına yol açar. Genel olarak gözlemlendiği üzere, Gerçek Rastgele Sayı Üreteçleri (GRSÜ) çıktılarında istatistiksel sapma ve bağımlılıklar bulunmaktadır ve bu nedenle doğrudan kriptografik amaçlar için kullanılmaya uygun değildirler. Kriptografik uygulamalar için uygun rastgele sayı üretme ve test metotları konusunda standartlar ve kılavuzlar mevcuttur.

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Özel Yayını (SP) 800-90 serisi, kriptografik uygulamalar için rastgele sayı üretme konusunda kılavuzlar ve öneriler sunmakta, istatistiksel rastgelelik testleri ve 10 kara kutu entropi tahmin yöntemi tanımlamaktadır. Bu tezde, NIST SP 800-90B entropi tahmin yöntemlerinin etkinliğini ve sınırlamalarını, bilinen entropili simüle edilmiş rastgele sayılar kullanarak deneysel olarak değerlendirmekte, bu tahmin edicilerin doğruluğu, entropi tahminleri arasındaki korelasyon ve deterministik dönüşümlerin tahmin ediciler üzerindeki etkileri üzerine gözlemler yapılmaktadır.

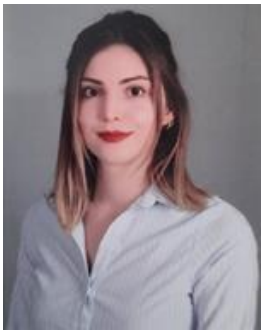
Çıktıların öngörülemezliğini anlamak için entropilerini doğru bir şekilde tahmin etmek önemlidir. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Özel Yayını (SP) 800-90B, basit frekans tabanlı tahmin edicilerden daha gelişmiş yaklaşımlara kadar uzanan on adet minimum entropi tahmin edicisini belirlemektedir. Her tahmin edicinin belirli varsayımları vardır ve bu da onları farklı kaynak türlerini değerlendirmeye uygun hale getirir. Bu tahminlerin minimumunun, GRSÜ'nin minimum entropisi olduğu varsayılır. Bu tezde, bazı bağımlılıklar içerebilecek çıktıları değerlendirmek için uygun olduğu öngörülen indeks-değer çakışması tahmini adı verilen yeni bir entropi tahmin yöntemi tanımlanmaktadır ve yöntemin etkinliğini gösteren bazı deneysel sonuçlar sunulmaktadır.

Ek olarak, GRSÜ'leri çalışmaları sırasında sıcaklık, nem vb. gibi dış koşullardan etkilenebilir. Sağlık testleri, çalışma sürecindeki beklenmedik değişiklikleri ve gürültü kaynağı tarafından üretilen entropi miktarındaki dramatik değişiklikleri tespit etmek için tanımlanan GRSÜ'nin gürültü kaynağının bileşeni olarak tanımlanmaktadır. Çalışmalar kapsamında literatürde bulunan sağlık testi paketleri incelenmiş ve ağırlık, öbek , 1-uzunluğunda öbekler ve örtüşen kalıplar rastgele değişkenlerini kullanarak kriptografik GRSÜ'leri için bir sağlık testi paketi tanımlanmıştır, test paketi için önerilen parametreler ve deneysel sonuçlar sunulmaktadır

Yayınlar:

- Z. Akcengiz, M. Aslan, A. Doğanaksoy, F. Sulak, and M. Uğuz, "LS-14 test suite for long sequences," Hacettepe Journal of Mathematics and Statistics, 2024. DOI: 10.15672/hujms.1190807.
- M. Aslan, A. Doğanaksoy, Z. Saygı, M. Sönmez Turan, and F. Sulak, "Observations on NIST SP 800-90B Entropy Estimators," in Sequences and Their Applications, 2024.
- Z. Akcengiz, M. Aslan, Ö. Karabayır, A. Doğanaksoy, M. Uğuz, and F. Sulak, "Statistical Randomness Test of Long Sequences by Dynamic Partitioning," in International Conference on Information Security and Cryptology, 2020.
- M. Aslan, A. Doğanaksoy, Z. Saygı, and F. Sulak, "Kriptografik Rastgele Sayı Üreteçleri için Sağlık Testleri," in 15. Ankara Mathematics Days, 2024.
- M. Aslan, A. Doğanaksoy, F. Sulak, and Z. Saygı, "Health Tests for Cryptographic Random Number Generators," in Recent Developments in Mathematics, Fatih Yılmaz, Metin Orbay, Vildan Öztürk, Umut Selvi, and Samet Arpacı, Eds., Turkey: Pegem Akademi Yayıncılık, 2024, pp. 134–146. ISBN: 9786256140486.

Adı Soyadı: Sermin Kocaman



Sermin Kocaman 2019 yılında ODTÜ Matematik bölümünden mezun olmuş ve daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi bölümünde bütünleşik doktora çalışmalarına devam etmiştir. Ocak 2024 tarihinde Doç. Dr. Ali Doğanaksoy ve Doç. Dr. Fatih Sulak danışmanlığında "PROBA: Privacy-Preserving, Robust and Accesible Blockchain-powered Helios" başlıklı tezini tamamlamıştır. Araştırma konuları arasında elektronik oylama sistemleri, çok partili imzalamalar ve hiyerarşik eşik imzalamalar bulunmaktadır. Sermin, 2019 ve 2024 yılları arasında Tübitak 2244 bursiyeri olarak çalışmalarını yapmıştır. 2024 yılı Ocak ayı itibari ile FAME Crypt şirketinde araştırma-geliştirme faaliyetlerini yürütmektedir.

Doktora Tezi Özeti :

Helios, ilk web tabanlı ve açık denetimli oylama sistemidir. Açık denetim özelliği, herkesin oylama sürecini takip etmesine olanak tanımaktadır ve böylece seçimlerin tüm aşamalarında kolay doğrulama sağlamaktadır. Helios'un birçok avantajına rağmen, merkezi bir sunucuya bağımlı olması nedeniyle yetkisiz erişim yoluyla verileri değiştirmek veya sunucuyu erişilemez kılmak gibi birkaç zayıflığı mevcuttur. Bu zayıflıkların üstesinden gelmek için blokzincir destekli Helios adlı sonraki bir çalışma önerilmiştir. Bu sistem, merkezileştirilmiş sunucuyu, blokzincir ve merkezi olmayan bir depolama protokolü kullanarak merkezi olmayan sunucularla değiştirmiştir. Bu yenilik Helios'un merkezileştirilmiş zayıflıklarını ortadan kaldırsa da, bazı yeni sorunlar oluşturmakta ve bu nedenle güvenlik zayıflıklarına neden olmaktadır. Bunlar, cüzdan kayıt prosedüründeki hatalı davranış, cüzdan yetkilendirme prosedüründeki bağlantı ve işlem maliyetinin yüksek olmasıdır. Bu tezde, blokzincir destekli Helios'un geliştirilmiş bir versiyonu, Proba, sunulmaktadır. Seçimde gizliliğin korunması, sağlamlık ve erişilebilirlik sağlamak için sistem yeniden tasarlanmıştır. Proba, seçmenler ve cüzdanları arasındaki bağlantıyı kesen yeni bir eşik verme-anonim kimlik bilgisi kullanmaktadır. Ayrıca, eşik sürümü, seçim yetkililerinin cüzdan kaydındaki uygunsuz davranışlarını azaltmaktadır. Bunlara ek olarak Proba, uygun fiyatlı seçim maliyetleri sağlayan konsorsiyum blokzinciri kullanmaktadır. Proba'nın performans analizi, eşik veren anonim kimlik bilgilerinin kullanımının seçim aşaması için kritik bir maliyeti olmadığını göstermektedir; aksine, akıllı sözleşme depolama maliyetini azalttığı görülmektedir.

Proba tasarımına ek bir çalışma olarak bu tez, iki taraflı eliptik eğri dijital imza algoritmasını hızlandırarak seçmenin cüzdan imzalama anahtarının korunmasına katkıda bulunmaktadır. Blokzincirde işlemlerin cüzdan imzalama anahtarı kullanılarak imzalanması gerekmektedir. Bu nedenle, seçmenin blokzincir üzerinde işlem gönderme hakkı, bu tek anahtarın güvenliğine bağlı olmaktadır. Seçmen, cüzdan imzalama anahtarını korumak için bu anahtarı akıllı telefon ve dizüstü bilgisayar gibi iki farklı yerde saklamayı seçebilmektedir. Bu senaryoda saldırganın aynı anda her iki yere de erişim sağlaması gerekmektedir ancak bu gerçekçi bir senaryo değildir. Bu nedenle bu tezde seçmenlere, azaltılmış bant genişliğine sahip iki taraf imzalama protokolü aracılığıyla cüzdan imzalama anahtarlarını koruması için iki farklı yere ayırmaları önerilmiştir. Bu protokol, bu kadar verimli bir

çevrimiçi aşamaya sahip iki taraflı bir ECDSA protokolü için en verimli çevrimdışı aşamayı sunmaktadır.

Ayrıca bu tez, anahtar koruması için seçmenin imzalama anahtarlarının hiyerarşik bir yapıda kullanılmasına olanak sağlamaktadır. Akıllı telefonların, bir kişinin kimliğini doğrulamada önemli cihazlar olarak kabul edildiği göz önüne alındığında, seçmen imzalama anahtarını akıllı telefonuna ve diğer cihazlara bölme seçeneğine sahiptir. Bu senaryoda imza aşamasında en üst hiyerarşide yer alan akıllı telefonun kullanılması zorunlu olmaktadır. Ancak diğer cihazlarla paylaşılan imzalama anahtarları sistemde belirlenen eşik değerine göre kullanılabilir. Mevcut hiyerarşik eşik şemaları, her bir hiyerarşik seviyede belirli sıralama kuralları ve sınırlamaları içerdiğinden bunların uyarlanabilirliğini kısıtlamaktadır. Ancak önerilen FlexHi şeması, bu kısıtlamalardan kurtulan esnek bir mimari sunmaktadır.

Yayınlar:

- Kocaman, S., & Talibi Alaoui, Y. Efficient Secure Two Party ECDSA. In IMA International Conference on Cryptography and Coding (pp. 161-180). Cham: Springer Nature Switzerland. (2023, December).
- Bingol, M.A., Kocaman, S., Dogan, A., & Kurt Toplu, S. FlexHi: A Flexible Hierarchical Threshold Signature Scheme. In Computing Conference 2024. https://eprint.iacr.org/2024/024.
- Doröz, Y., Kocaman, S., Muş, K., Sulak, F., & Yayla, O. Proba: Privacy-preserving, Robust and Accessible Blockchain-powered Helios. Journal of Information Security and Applications (incelemede)

Adı Soyadı: Nazlı Deniz Türe

Nazlı Deniz TÜRE, 2018 yılında Orta Doğu Teknik Üniversitesi (ODTÜ) Matematik bölümünden mezun olmuş ve aynı yılda ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi bölümünde yüksek lisansına başlamıştır. Yüksek lisans eğitiminin birinci yılının sonunda TÜBİTAK 2244 Sanayi Doktora Programı desteğini almaya hak kazanarak aynı bölümde bütünleşik doktora programına geçiş yapmış ve bu alanda doktora çalışmalarına devam etmiştir. Kasım 2024 tarihinde Prof. Dr. Murat CENK ve Doç. Dr. Oğuz YAYLA danışmanlığında "Efficient Batch Algorithms for the Post-Quantum Crystals Dilithium Signature Scheme and Crystals Kyber Encryption Scheme" başlıklı tezini tamamlamıştır. Araştırma konuları arasında; kafes tabanlı kuantum sonrası şifreleme ve imzalama algoritmaları, aritmetik karmaşıklık, verimli matris ve polinom çarpım yöntemleri, algoritmaların verimli gerçeklenmesi, çoklu imzalama ve şifreleme yöntemleri yer almaktadır. Tezinde de yer alan çalışmaların bir kısmının açıklandığı "Efficient Batch Post-Quantum Signatures with Crystals Dilithium" isimli makalesi International Workshop on the Arithmetic of Finite Fields 2024 (WAIFI 2024) isimli konferansta sunulmuştur. Doktora eğitimi boyunca FAME CRYPT isimli firmada araştırmacı olarak çalışmış ve alanıyla ilgili birçok projede yer almıştır. Günümüzde aynı firmada hem akademik çalışmalarına devam etmekte hem de kriptografi alanındaki projelerde başuzman araştırmacı olarak görev almaktadır.

Doktora Tezi Özeti :

Dijital imzalar kimlik doğrulama ve veri bütünlüğü sağlarlar ve bilgi teknolojileri, finans, eğitim, hukuk gibi birçok alanda yaygın olarak kullanılırlar. Kullanıcı ile sunucu arasındaki iletişimlerde kimlik doğrulama amaçlı kullanılarak sunucuların siber saldırılara karşı güvenliklerinin sağlanması konusunda da oldukça önemlidirler. Diğer bir yandan şifreleme ise veri güvenliğini sağlamak amacıyla güvenli iletişim, bulut ve veritabanı güvenliği gibi birçok alanda kullanılmaktadır. Dijital imzalar ve şifreleme mekanizmalarında sıklıkla açık anahtarlı kriptosistemler kullanılır. Açık anahtarlı kriptosistemlerin güvenliği ise tam sayılarda çarpanlara ayırma ve ayrık logaritma problemi gibi çözümü zor matematiksel problemlere dayanmaktadır. P. Shor (1999), güvenlikleri ayrık logaritma ve tam sayılarda çarpanlara ayırma problemlerine dayanan kriptosistemlerin, gelişmiş kuantum bilgisayarlar kullanılarak kırılabileceğini göstermiştir. Güvenliklerini kaybedecek olan algoritmaların, yeni nesil kuantum güvenli algoritmalar ile değiştirilmesi için NIST (Ulusal Standartlar ve Teknoloji Enstitüsü, ABD) tarafından kuantum sonrası standartlaşma süreci düzenlenmiştir. Bunun sonucunda Crystals Dilithium, Falcon ve SPHINCS+ dijital imza standartları, Crystals Kyber ise şifreleme/anahtar kapsülleme standardı olarak seçilmiştir. Bu çalışmada, NIST'in (Ulusal Standartlar ve Teknoloji Enstitüsü, ABD) kuantum ertesi kriptografi dijital imza standardı olarak belirlemiş olduğu Crystals Dilithium algoritması ile toplu imza üretimi ve bir kullanıcıdan gelen imzaların doğrulaması, kuantum ertesi şifreleme standardı olarak belirlenmiş olan Crystals Kyber ile bir kullanıcı için toplu şifreleme üzerine yoğunlaşılmıştır. Dilithium ve Kyber'ın barındırdığı en önemli işlemlerden biri de; girdileri polinom olan matris ve vektörlerin çarpımıdır. m>1 olmak üzere m adet imza klasik Dilithium yöntemi ile üretildiğinde ya da doğrulandığında (m adet mesaj klasik Kyber ile şifrelendiğinde) m adet benzer çarpım gerekmektedir. Bu tezde, Dilithium ile m imzayı üretmek/doğrulamak için üçten büyük matrislerde ve Kyber ile m mesajı şifrelemek için ikiden büyük boyutlu matrislerde verimli matris

çarpımlarının kullanılabileceği gösterilmiştir. Bu sebeple, Dilithium imza üretimi, doğrulama ve Kyber şifreleme algoritmaları analiz edilmiştir. Bu çalışmada, birden fazla mesaj veya imza için ayrı ayrı gerçekleştirilen işlemlerin, toplu şekilde yapılabilmesi için yeni algoritmalar tasarlanmıştır. Bu amaçla, bu algoritmalardaki matris-vektör çarpımları, matris-matris çarpımlarına dönüştürülmüş ve yeni toplu Dilithium imza üretimi/doğrulama ve toplu Kyber şifreleme algoritmaları tasarlanmıştır. Ayrıca, verimli toplu Dilithium imza üretim algoritmasının tek bir imzanın üretilmesinde kullanılabileceği de gösterilmiştir. Bu, olasılık ve verimlilik analizleri ile doğrulanmıştır. Yeni toplu algoritmalar, orijinal Dilithium ve Kyber'in güvenliğini sağlayan bileşenlere sahiptir ve güvenlik açıklarına neden olmadan toplu imzalama/doğrulama ve şifrelemeye olanak sağlar. Matris-vektör çarpımlarını matris-matris çarpımlarına dönüştürerek, bu sistemlerde verimli değişmeli veya değişmeli olmayan matris-matris çarpım algoritmalarının kullanılmasına imkân tanır. Elde edilen verimlilik, belirli bir mimari, cihaz veya platformdan bağımsızdır ve matematiksel iyileştirmelere dayanmaktadır. Tasarlanan toplu algoritmalar, herhangi bir toplu işlem boyutunun seçilmesine ve uygun matris-matris çarpım tekniğinin uygulanmasına olanak sağlar. Bu bağlamda, farklı toplu işlem boyutlarına göre hem toplu hem de tekli imzalar için Dilithium imza algoritmasının kullanımı üzerine olasılık hesaplamaları yapılmış ve seçilen matris-matris çarpım tekniklerine dayalı olarak verimlilik yüzdeleri elde edilmiştir. Ayrıca, değişen toplu işlem boyutları için uygun matris-matris çarpım yöntemleri aracılığıyla toplu Kyber şifrelemesi ve Dilithium doğrulamasının sağladığı iyileştirme yüzdeleri hesaplanmıştır. Teorik hesaplamaları örneklemek amacıyla, örnek toplu işlem değerleri seçilmiş ve uygun matris-matris çarpım yöntemleri belirlenmiştir. Matrislerin boyutlarına göre, Dilithium ve Kyber'ın üç güvenlik seviyesi için çarpım formülleri elde edilmiştir. Hesaplamaları test etmek amacıyla, bu çalışmada tasarlanan toplu Dilithium imzalama, doğrulama ve Kyber şifreleme algoritmaları C programlama dilinde gerçeklenmiştir. Türetilen matris-matris çarpım formülleri de, Kyber ve Dilithium'un altyapısına uyacak şekilde C dilinde gerçeklenmiş ve yeni toplu algoritmalara entegre edilmiştir. Yeni algoritmalar ile referans algoritmalar arasında verimlilik karşılaştırmaları yapılmıştır. Sonuç olarak, Dilithium'un imzasının üç farklı güvenlik seviyesinde aritmetik karmaşıklıkta sırasıyla %28.1, %33.3 ve %31.5 oranında iyileşmeler gözlemlenmiştir. Verimli matris çarpım yöntemi kullanılan toplu Dilithium imza algoritması, üç güvenlik seviyesi için CPU döngü sayılarında sırasıyla %34.22, %17.40 ve %10.15 iyileştirmeler sağlamıştır. Toplu Dilithium imza üretimi için kullanılan çarpım formülleri, aynı zamanda toplu Dilithium doğrulaması için de kullanılmıştır. Üç farklı güvenlik seviyesi için aritmetik karmaşıklıkta sırasıyla %28.13, %33.33 ve %31.25 oranında iyileşmeler gözlemlenmiştir. Ayrıca, üç güvenlik seviyesi için CPU döngü sayıları açısından sırasıyla %49.88, %56.60 ve %61.08 iyileşmeler elde edilmiştir. Verimli çarpım algoritmaları kullanılan toplu Kyber şifrelemesi uygulandığında, aritmetik karmaşıklıkta %12.50, %22.22 ve %28.13 oranında iyileşmeler ile birlikte, üç güvenlik seviyesi için CPU döngü sayılarında %22.34, %24.07 ve %30.83 oranında iyileşmeler gözlemlenmiştir.

Yayınlar:

- Türe, N. D. & Cenk, M. (2024). Efficient Batch Post-Quantum Signatures with Crystals Dilithium. In Proceedings of the International Workshop on the Arithmetic of Finite Fields (WAIFI 2024). Lecture Notes in Computer Science (LNCS). Cham: Springer.

Adı Soyadı: Yunus Emre Yılmaz

Yunus Emre Yılmaz 2011 yılında ODTÜ Elektrik-Elektronik Mühendisliği Bölümünden mezun olmuş ve aynı bölümde 2016 yılında yüksek lisansını tamamlamıştır. Daha sonra ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi anabilim dalında doktora çalışmalarına başlamış ve Doç. Dr. Oğuz Yayla danışmanlığında "On an Efficient Implementation of Combined True Random Number Generator and Physically Unclonable Function on a SoC FPGA" başlıklı tezini Eylül 2024'te tamamlamıştır. Araştırma konuları arasında gerçek rastgele sayı üreteçleri (TRNG'ler) ve fiziksel olarak klonlanamayan fonksiyonlar (PUF'lar) ile bu kriptografik primitiflerin yüksek performanslı ve verimli bir şekilde FPGA'ler veya SoC'ler üzerinde donanımsal olarak gerçeklenmesi yer almaktadır.

2011 yılından beri sayısal donanım tasarımı mühendisi olarak çalışmaktadır. Haberleşme cihazları için FPGA ve SoC tabanlı sayısal donanım çözümlerinin tasarımını içeren bu görevini ASELSAN'da sürdürmektedir.

Doktora Tezi Özeti :

Gerçek Rastgele Sayı Üreteçleri (TRNG'ler) ve Fiziksel Olarak Klonlanamayan Fonksiyonlar (PUF'lar) kriptografik sistemlerin tasarlanmasında kullanılan iki temel ve kullanışlı ilkel araçtır. TRNG'ler değişmez şekilde rastgele olmalıdır, PUF'lar ise tekrarlayan sonuçlara ve örneğe özgü rastgeleliğe sahip olmalıdır. Bu çalışmada, bu ilkeller bir Çip Üzerinde Sistem Alan Programlanabilir Kapı Dizisinde (SoC FPGA) veya kısaca SoC'de uygulanmıştır. Faz Kilitli Döngüler (PLL'ler) hem FPGA'lerde hem de SoC'lerde çeşitli işlevler için yaygın olarak uygulanan temel bileşenlerdir. Bu cihazlarda PLL'ler rastgele sayılar üretmek için umut verici bir yöntem sunar. Önceki araştırmalarla doğrulandığı üzere, izole çalışmaları, geniş kullanımları ve güçlü entropi üretimleri nedeniyle, FPGA'lara veya SoC'lere entegre edilen PLL'ler, PLL tabanlı gerçek rastgele sayı üreteçleri (PLL-TRNG'ler) için oldukça etkili temeller olarak hizmet eder. Bu da PLL-TRNG'leri bu tür mimarilerde güvenli rastgele sayılar üretmek için özellikle uygun bir çözüm hâline getirmektedir. PLL-TRNG'de parametre seçimi, hem yeterli bir entropi oranı hem de yeterli bir çıkış bit oranı sağlamayı gerektirdiğinden çok kritik bir süreçtir. Bu nedenle, bu çalışmada, literatürdeki geri izleme (backtracking) yöntemine dayalı bir parametre seçim algoritması seçilmiş ve seçilen SoC'ye uyarlanmıştır. Bunlara ek olarak, entropi özelliklerini korurken belirli bir ara bağlantıya sahip ekstra PLL'ler kullanarak PLL-TRNG'nin rastgele veri biti üretme oranını artırmak için yeni bir metodoloji önerilmiştir. Performans ölçütleri, Alman Federal Bilgi Güvenliği Ofisi (BSI) AIS-20/31 Testleri tarafından belirlenen kriterlere göre titizlikle değerlendirilmiş ve literatürdeki çalışmalarla karşılaştırılmıştır.

İlk silikon PUF olarak kabul edilen hakem (Arbiter) PUF, hafif tasarımını korurken, girdiye bağlı olarak anında önemli sayıda gizli anahtar üretebilmektedir. Bu avantajlı özellik, özellikle Nesnelerin İnterneti (IoT) cihazları gibi kısıtlı kaynaklara sahip uygulamalarda cihaz kimlik doğrulaması için çok uygundur. Bu avantajlara rağmen, hakem PUF'lar makine öğrenimi saldırılarına karşı savunmasızdır. Bu nedenle, bu tür saldırılara karşı daha fazla direnç elde etmek için bu hakem PUF tasarımları geliştirilmiştir. Bu iyileştirmeler, IoT uygulamaları için kullanışlılığı ve verimliliği korurken makine öğrenmesi

saldırılarına karşı dayanıklılığı artırmayı amaçlamaktadır. Bu çalışmada, literatürde bulunan bir tasarıma dayalı olarak makine öğrenmesine dirençli 32 bit ve 64 bit bileşen farklılaştırmalı XOR Hakem PUF (CDC-XPUF) gerçeklenmiştir. 32-bit ve 64-bit 7 akışlı CDC-7-XPUF'ler, literatürdeki PUF ölçütleri olan kararlılık, doğruluk, dağınıklık, tekdüzelik ve benzersizlik kullanılarak değerlendirilmiştir. Ek olarak, hem TRNG hem de PUF uygulamaları için kullanım oranları sunulmuştur.

Bu çalışmanın son bölümünde, dört PLL'li PLL-TRNG (4-PLL-TRNG) ve 64-bit 7 akışlı CDC-XPUF (CDC-7-XPUF) birlikte çalışabilecek şekilde birleştirilmiştir. 4-PLL-TRNG tarafından üretilen rastgele sayılar CDC-7-XPUF tarafından ana PUF girdisinden (challenge) diğer PUF girdilerini üretmek için kullanılır. TRNG ve PUF'a uygulanan tüm testler bu birleşik tasarıma da uygulanmış ve bu birleşik tasarımın bir IoT sisteminde kullanılmak için uygun bir aday olduğu gösterilmiştir. Sonuç olarak, ikisi PLL-TRNG ve CDC-XPUF'un ayrık uygulamaları ve biri de bu PLL-TRNG ve CDC-XPUF'un birleşik uygulaması olmak üzere toplam üç farklı konfigürasyon gerçeklenmiştir. Tüm testler, Xilinx Zynq 7020 SoC içeren ZC702 Rev1.1 Değerlendirme Kartı kullanılarak uygulanmış ve deneysel doğrulama için üç kart içeren bir yapılandırma kullanılmıştır.

Yayınlar:

- Yayla, O., Y. E. Yılmaz, A Combined Design of 4-PLL-TRNG and 64-bit CDC-7-XPUF on a Zynq-7020 SoC, Cryptology ePrint Archive, Paper 2024/1457, 2024, https://eprint.iacr.org/2024/1457. (Hakemli bir dergide değerlendirmesi sürmektedir.)

- Yayla, O., Y. E. Yılmaz, 32-bit and 64-bit CDC-7-XPUF Implementations on a Zynq-7020 SoC, Cryptology ePrint Archive, Paper 2024/1443, 2024, https://eprint.iacr.org/2024/1443. (SecITC 2024 tarafından kabul edilmiştir ve "SECITC 2024 – Springer as LNCS" cildi içerisinde yakında yayınlanacaktır.)

- Yayla, O., Yılmaz, Y.E. (2024). Design and Implementation of a Fast, Platform-Adaptive, AIS-20/31 Compliant PLL-Based True Random Number Generator on a Zynq 7020 SoC FPGA. In: Quintián, H., et al. International Joint Conferences. ICEUTE CISIS 2024 2024. Lecture Notes in Networks and Systems, vol 957. Springer, Cham. https://doi.org/10.1007/978-3-031-75016-8_5. Extended version available at: https://eprint.iacr.org/2024/1442.

- 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, in Proceedings of the 12th International Conference on Information Security and Cryptology (ISCTURKEY 2019), Ankara, Turkey, pp. 59-64, Oct. 2019. Avaliable: Link to Proceedings.