ORTA DOĞU TEKNİK ÜNİVERSİTESİ
UYGULAMALI MATEMATİK ENSTİTÜSÜ

RAPOR
2006

INSTITUTE OF APPLIED MATHEMATICS
MIDDLE EAST TECHNICAL UNIVERSITY
ODTÜ ANKARA 06531
Tel: +90 (312) 210 29 87
Fax: +90 (312) 210 29 85
http: //www.iam.metu.edu.tr
E-mail: wwwiam@metu.edu.tr

İÇİNDEKİLER

ÖNSÖZ.....2
ÖZET BİLGİLER.....4
ENSTİTÜNÜN PROGRAMLARI.....5
İNSAN KAYNAKLARI.....5
PROTOKOLLER.....7
ÖĞRENCİ BİLGİLERİ.....7
ARAŞTIRMA FAALİYETLERİ.....10
YAYINLAR/TEBLİĞLER*.....10
ÇALIŞTAY/ SEMPOZYUM/ KONFERANS/ YAZOKULU.....16
ARAŞTIRMA GRUPLARI/ DOSAP PROGRAMI.....17
YÜRÜTÜCÜLÜĞÜ YAPILAN PROJELER.....19
DİĞER FAALİYETLER.....22
ENSTİTÜ ÜYELERİNİN KISA SÜRELİ YURT DIŞI ZİYARETLERİ.....23
EKLER.....25

ÖNSÖZ

ODTÜ'de Uygulamalı Matematik Enstitüsü kurulması, Matematik Bölümü'nün 1999 yılı dış değerlendirmesi sonucu ortaya çıkmıştır. Fen Edebiyat Fakültesi Dekanlığınca Matematik öğretim üyelerinden oluşturulan bir komisyonun yaklaşık 2 yıl süren çalışmaları sonucunda, Kriptografi, Bilimsel Hesaplama, Finansal Matematik, ve Finansal Matematik Hayat Sigortası Opsiyonu anabilim dallarından oluşan Uygulamalı Matematik Enstitüsü'nün kurulması Üniversite Senatosuna önerilmiştir. Orta Doğu Teknik Üniversitesi'nde Uygulamalı Matematik Enstitüsü kurulması; Milli Eğitim Bakanlığı'nın 8/5/2002 tarihli ve 12293, 12296 sayılı yazıları, 28/3/1983 tarihli ve 2809 sayılı kanunun değişik ek 30'uncu maddesine göre, Bakanlar Kurulu'nca 16/5/2002 tarihinde kararlaştırılmıştır ve bu karar 21 Haziran 2002 tarihinde resmi gazetede yayınlanmıştır.

Uygulamalı Matematik Enstitüsü Misyonunu;

I. Orta Doğu Teknik Üniversitesi'nin araştırma potansiyeli ve ülkemizin ihtiyaçları göz önüne alınarak, disiplinler arası matematik bazlı araştırma/uygulama alanları belirlemek ve bu çerçevede lisansüstü eğitim programlarını geliştirmek. Üniversitemizde yapılmakta olan matematik ağırlıklı araştırmaları koordine ederek Enstitü bünyesinde disiplinler-arası bir çalışma ortamı oluşturmak, bu alanlarda araştırmaya yönelik konferanslar/yaz okulları düzenlemek ve uluslararası işbirliği olanaklarını araştırmak/hayata geçirmek.

II. Matematiğin; doğayı, teknolojik ve ekonomik süreçleri daha iyi anlama yolunda bilim adamlarının ortak dili olduğundan hareketle, lisans/lisansüstü eğitimde ve araştırmalarda matematik kullanımının hem nicelik hem de nitelik açısından arttırılması yolunda çalışmalarda bulunmak, bu çerçevede yeni, uygulanabilir matematik konularında araştırmacıları bilgilendirmek ve bu amaca yönelik yayın yapmak.

III. Uygulamalı matematik alanında ODTÜ-Sanayi/Kamu kuruluşları işbirliğini, gerek proje ve ürün geliştirerek gerekse kısa süreli eğitim/araştırma toplantıları düzenleyerek hayata geçirmek

olarak belirlemiştir.

Bu rapor Uygulamalı Matematik Enstitüsü'nün misyonu çerçevesinde 01.01.2006-31.12.2006 tarihleri arasındaki faaliyetleri içermektedir.

Enstitü Yönetimi

Müdür

Prof. Dr. Ersan AKYILDIZ

Müdür Yardımcıları

Y. Doç. Dr. Yusuf ULUDAĞ

Y. Doç. Dr. Işıl EROL

Enstitü Kurulu*

Prof. Dr. Rüyal ERGÜL

Prof. Dr. Bülent KARASÖZEN

Prof. Dr. Hayri KÖREZLİOĞLU

Enstitü Yönetim Kurulu*

Prof. Dr. Haluk AKSEL

Y. Doç. Dr. Seza DANIŞOĞLU RHOADES

Prof. Dr. Mete SEVERCAN

*Enstitü Yönetimi, bu kurulların doğal üyeleridir.

ÖZET BİLGİLER

- Enstitünün 2006 yılı faaliyetlerinde 5 UME, 30 ODTÜ içi, 13 ODTÜ dışı bağlantılı öğretim üyesi katkıda bulunmuşlardır.
- DOSAP programında Giresun Üniversitesi'nden bir öğretim üyesi aramıza katılmıştır.
- Enstitümüzde toplam 14 araştırma görevlisi göreve devam etmekte olup, bunlardan 8'i Öğretim Üyesi Yetiştirme Programı (ÖYP) ve biri de 35. madde kapsamındadır. Bir asistanımız ise Amerika Birleşik Devletleri Florida State Üniversitesi'nde YÖK burslusu olarak bulunmaktadır.
- Enstitümüzde toplam 139 öğrenci eğitimini sürdürmektedir. Bilimsel Hesaplama'da 13 yüksek lisans ve 8 doktora, Finansal Matematik'de 44 yüksek lisans ve 15 doktora, Kriptografi'de 26 yüksek lisans ve 33 doktora öğrencisi bulunmaktadır.
- Enstitümüz anabilim dallarının 10 araştırma grubu bulunmaktadır.
- Enstitü bağlantısı belirtilmiş olarak 14 yurtdışı 4 yurtiçi yayın, 6 yurtdışı 24 yurtiçi tebliğ, 26 yurtdışı ve 15 yurtiçi sunum yapılmıştır.
- Enstitümüz tarafından düzenlenen bilimsel toplantılar:
  - "II. Ulusal Kriptoloji Sempozyumu" (ODTÜ)
  - "First Conferans of Advanced Mathematical Methods for Finance (AMAMEF)" (Antalya)
  - "Workshop on Advances in Continuous Optimization" (Iceland)
  - "EURO Summer Institute, "Optimization Challenges in Engineering" (Germany)
  - "Turkish-German Summer Academy in Advanced Engineering" (Kuşadası)
  - "Workshop on Networks in Computational Biology" (ODTÜ)
- Yürütücülüğünü enstitümüzün yapacağı Telekomünikasyon Kurumu ile ODTÜ arasında bir protokol imzalanmıştır.
- Enstitümüz öğretim üyeleri tarafından yürütücülüğü yapılan 10, araştırmacı olarak katıldıkları ise 5 proje bulunmaktadır.
- Bu dönemde iki Aselsan ve bir TÜBİTAK-Kamu (Telekomünikasyon Kurumu) projesi başlatılmıştır.
- Daha önce üç yıl olarak onaylanmış olan DPT projesi 250.000-YTL'lik ek bütçeyle bir yıl daha uzatılmıştır.
- Üniversitemizin kuruluşunun 50. yılı kapsamında;
  - Tilburg Üniversitesi öğretim üyelerinden Prof. Dr. Stef Tijss, "Cooperative Game Theory" başlıklı bir dizi seminer vermiştir.
  - The University of British Colombia öğretim üyelerinden Prof. Dr. James B. Carrell ve Universiteit Utrecht öğretim üyelerinden Prof. Dr. Tonny A. Springer "Geometry and Flag Varieties" başlıklı bir dizi seminer vermişlerdir.
  - "Şifrelerin Matematiği Kriptografi" isimli bir kitap yazılmıştır.
- Kırıkkale Üniversitesi öğretim üyelerinden Y. Doç. Dr. Fatih Tank, Hayat Sigortası Opsiyonunda yarı zamanlı olarak görevlendirilmiştir.
- University of Illinois at Urabana-Champaign öğretim üyelerinden Prof. Dr. Hayri Önal, 7. yıl izni çerçevesinde enstitümüze gelerek bir ders vermiştir.
- Brown Üniversitesinden Dr. Ali Devin Sezer, yarı zamanlı olarak bir ders vermiştir.
- Enstitümüze yurtdışından 16 misafir öğretim üyesi gelmiş, 5 öğretim elemanı/araştırma görevlisi de enstitümüz tarafından desteklenerek yurt dışında görevlendirilmiştir.
- Matematik Bölümü'nün düzenlemiş olduğu Arf Konferansı ve bu konferansın konuşmacılarından Prof. Dr. Jean-Pierre Serre enstitü tarafından desteklenmiştir.
- Enstitü Müdür Yardımcımız Doç. Dr. Tanıl Ergenç emekli olmuştur.
- Müdür Yardımcılığı görevlerine Y. Doç. Dr. Işıl Erol ve Y. Doç. Dr. Yusuf Uludağ atanmışlardır.
- Kriptoloji Laboratuar binası inşaatı bitirilmiş ve kullanılmaya başlanmıştır.

ENSTİTÜNÜN PROGRAMLARI

Bilimsel Hesaplama
Tezli Yüksek Lisans
Doktora

Finansal Matematik
Tezli Yüksek Lisans
Tezsiz Yüksek Lisans
Doktora

Kriptografi
Tezli Yüksek Lisans
Tezsiz Yüksek Lisans
Doktora

Finansal Matematik Hayat Sigortası Opsiyonu
Tezsiz Yüksek Lisans

İNSAN KAYNAKLARI

Öğretim Elemanları
Prof. Dr. Hayri Körezlioğlu
Prof. Dr. Gerhard- Wilhelm Weber
Y. Doç. Dr. Hakan Öktem
Y. Doç. Dr. Emrah Çakçak
Dr. Ömür Uğur

DOSAP
Y. Doç. Dr. Pakize Taylan
(Dicle Üniversitesi)
Y. Doç. Dr. Nedim Dikmen
(Giresun Üniversitesi)

Araştırma Görevlileri
Sedat Akleylek (ÖYP, Samsun)
Zeynep Sırma Alparslan (ÖYP, Isparta)
Derya Altıntan (ÖYP, Konya)
Derviş Bayazıt (YÖK Bursu ile yurtdışında)
Canan Çimen
Zehra Ekşi
Rita İsmailova (ÖYP, Kırgızistan)
Ayşegül İşcanoğlu (ÖYP, Konya)
Turgut Hanoymak (ÖYP, Van)
Barış Bülent Kırlar (ÖYP, Isparta)
Süreyya Özöğür
Zülfükar Saygı
Oktay Sürücü*
Mesut Taştan (ÖYP, Van)*
Nurbek Baryk Ulu (ÖYP, Kırgızistan)
Çekdar Vakıfahmetoğlu*
Enes Yılmaz (35. madde)
Yeliz Yolcu*

*2006 yılı içinde araştırma görevliliğinden ayrılmışlardır.

BAĞLANTILI ÖĞRETİM ÜYELERİ

ORTA DOĞU TEKNİK ÜNİVERSİTESİ

Matematik Bölümü
Marat U. Akhmet
Ersan Akyıldız
Muhammed Dabbagh
Ali Doğanaksoy
Bülent Karasözen
Ferruh Özbudak
Münevver Tezer
Muhiddin Uğuz

Elektrik-Elektronik Mühendisliği Bölümü
Yeşim Serinağaoğlu Doğrusöz
F. Rüyal Ergül
Nevzat G. Gençer
Kemal Leblebicioğlu
Osman Sevaioğlu
Mete Severcan
Melek Yücel

İşletme Bölümü
Nuray Güner
Adil Oran
Seza Danışoğlu Rhoades

İktisat Bölümü
Işıl Erol
Esma Gaygısız

Biyoloji Bölümü
Meryem Beklioğlu
Semra Kocabıyık
İnci Togan

Gıda Müh.Bl.
Zümrüt Begüm Ögel

Kimya Bölümü
Ali Gökmen

Kimya Müh. Bl.
Yusuf Uludağ

Beden Eğitimi ve Spor Bl.
Feza Korkusuz

Enformatik Enstitüsü
Erkan Mumcuoğlu

İstatistik Bölümü
İnci Batmaz

Makine Müh. Bl.
Haluk Aksel

ÜNİVERSİTELER

ANKARA ÜNİV.
İstatistik Bölümü
Ömer Gebizlioğlu

ATILIM ÜNİV.
Matematik Bölümü
Tanıl Ergenç

HACETTEPE ÜNİV.
İstatistik Bölümü
Gül Ergün

ALBERT-LUDWIGS UNIVERSITY FREIBURG
Department of Economics
Sevtap Selçuk Kestel

İZMİR YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
Matematik Bölümü
Ali İhsan Neslitürk

KOÇ ÜNİV.
Mühendislik Fakültesi
Metin Türkay

KIRIKKALE ÜNİV.
İstatistik Bölümü
Fatih Tank

TRAKYA ÜNİV.
İktisat Bölümü
Kasırga Yıldırak

KURUMLAR

TCMB
C.Coşkun Küçüközmen

TÜBİTAK-UEKAE
Orhun Kara

DİĞER

Azize Hayfavi
A.Devin Sezer
Hayri Önal

İDARİ PERSONEL

Sekreter
Nejla Erdoğdu
Rukiye Ekinci

Memur
M. Kemal Yaşar

TÜBİTAK-KAMU Proje Elemanı
Burçin Ak

İdari Amir
Saffet Aykın

Görevli
Muharrem Kayabel
Serkan Demiröz

PROTOKOLLER

Universitat Kaiserslautern and Middle East Technical University Instute of Applied Mathematics	Cooperation in the Field of Financial and Insurance Mathematics
- The Institute of Mathematics "Siroion Stoiow" of the Romainan, Academy (IMAR)-Romania **- The Institute of Mathematical Statistics and Applied Mathematics "Gheorghe Mihoc-Caius Iacob (ISMMA)-Romania** **- The Institute of Applied Mathematics and of the Middle East Technical University (IAM-METU)**	Cooperation in the fields of Financial Mathematics, and Cryptography
University of the Aegean, Greece (Department of Statistics and Actuarial Science), Middle East Technical University (Institute of Applied Mathematics)	Cooperation in the fields of Financial Mathematics, Actuarial Sciences and Establishment of a Joint Doctoral Program
General Memorandum of Agreement on Cooperation Between Institute of Mathematics of The Polish Academy of Sciences and The Institute of Applied Mathematics and Department Mathematics and Middle East Technical University	Memorandum on Extending and Strengthening Links Beetween Polish Academy of Sciences and the Department of Mathematics and Institute of Applied Mathematics
Turkish-French University and Scientific Cooperation Projects, Laboratoire de Mathématiques et Applications Université de La Rochelle and Institute of Applied Mathematics, Middle East Technical University, Ankara	Exchange of know-how in Financial Mathematics, Development of common teaching and research programs, Joint participation to European research projects.
Telekomünikasyon Kurumu- ODTÜ	Bilgi ve İletişim Teknolojileri Konularında Eğitim, Araştırma, Geliştirme Çalışmaları ve Uygulamalarında İşbirliği Yapılması

ÖĞRENCİ BİLGİLERİ

SIAM-IAM ODTÜ ÖĞRENCİ TOPLULUĞU

SIAM (Society of Industrial and Applied Mathematics) IAM (ODTÜ) Öğrenci Topluluğu; Uygulamalı Matematik Enstitüsü'nün çalışmaları sonucu Amerika ve Kanada dışında kurulan ilk SIAM öğrenci grubudur. Grubun amaçları, SIAM'ı ve SIAM'ın faaliyetlerini Üniversite'de ve Türkiye'de tanıtmaktır. Bu topluluk tarafından 2006 yılı içinde Mathawareness Month etkinlikleri çerçevesinde 27-28 Nisan 2006 tarihleri arasında "Internet Security and Cryptography" konulu seminerler düzenlenmiştir.
Grup hakkında ayrıntılı bilgiye www.siam.metu.edu.tr adresinden ulaşılabilinir.

Enstitümüzün Toplam Öğrenci Sayısı:
139

2006 yılında Kayıt Yaptıran Öğrenci Sayısı:
48

2006 Yılında Mezun Olan Öğrenci Sayısı*:
21

* Bu öğrencilerin listesi **Ek 4**'de verilmiştir.

Enstitümüz Öğrencilerinin Programlara göre Dağılımı

Anabilim Dalı	Yüksek Lisans	Doktora	Bilimsel Hazırlık	İngilizce Hazırlık
Bilimsel Hesaplama **(21)**	**13**	**8**	**-**	**-**
Finansal Matematik **(50)**	**34**	**12**	**3**	**1**
Finansal Matematik **(9)** Hayat Sigortası Opsiyonu	**9**	**-**	**-**	**-**
Kriptografi **(59)**	**26**	**31**	**2**	**-**
Toplam: **(139)**	**82**	**51**	**5**	**1**

2006 yılında Kayıt Yaptıran Öğrencilerin B.S. Derecelerini Aldıkları Bölümlere Göre Dağılımları*

MATH	STAT	CENG	ECON	EE	CE	CHE	IE	ME	PHYS
28	**5**	**5**	**3**	**2**	**1**	**1**	**1**	**1**	**1**

UME Derslerini Alan Öğrencilerin Bölümlere Göre Dağılımı**

Dönem	UME	Özel Öğr.	EE	BIOL	CE	CHE	CHEM	GGIT	IS	CENG	ECON	IE	MATH	STAT	PETE	ENVE	MI	PHIL	CEIT	GENE	COGS	TOTAL
2005-2006 II	**152**	**7**	**7**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**182**
2006-2007 I	**235**	**17**	**8**	**3**	**3**	**2**	**-**	**4**	**1**	**1**	**5**	**6**	**5**	**3**	**3**	**1**	**1**	**1**	**1**	**1**	**1**	**302**

Dönemsel Ders İstatistikleri:

	Verilen Ders Sayısı	Toplam Öğrenci Sayısı	Ders Başına Verilen Not Sayısı
2005-2006 II.Dönem	16	182	11
2006-2007 I.Dönem	24	302	13

*Bölüm isimlerinde ODTÜ Katalogunda ki kısaltmalar kullanılmıştır.

** Enstitümüzde 2005-2006 II ve 2006-2007 I. Döneminde verilen derslerin listesi **Ek 6**'da verilmektedir.

Öğrenci Başarı Durumları

	2005-2006 II.Dönem				2006-2007 I.Dönem			
	Başarılı	**Başarısız**	**İlişiği Kesilen**	**İzinli**	**Başarılı**	**Başarısız**	**İlişiği Kesilen**	**İzinli**
Kriptografi (Bil.Haz.)	-	-	-	-	2	-	-	-
Kriptografi (M.Sc.)	13	3	3	1	16	7	2	1
Kriptografi (Ph.D.)	22	5	-	-	23	4	-	4
Bilimsel Hesaplama (M.Sc.)	9	-	2	2	10	2	-	1
Bilimsel Hesaplama (Ph.D.)	5	-	1	-	8	-	-	-
Finansal Matematik (Bil. Haz.)	1	2	3	-	-	2	1	-
Finansal Matematik (İng. Haz.)	-	-	-	-	1	-	-	-
Finansal Matematik (M.Sc.)	18	3	3	5	23	8	1	2
Finansal Matematik (Ph.D.)	6	2	1	-	8	1	-	3
Hayat Sigortası (Bil. Haz.)	-	-	-	-	1	-	-	-
Hayat Sigortası (M.Sc.)	8	-	4	-	6	2	-	-
TOPLAM	**82**	**15**	**17**	**8**	**98**	**26**	**4**	**11**

ÖYP Öğrencileri Başarı Durumları

	Bilimsel Hesaplama			Finansal Matematik			Kriptografi					
Üniversitesi	YL	Doktora	LSD	YL	Doktora	LSD	YL	Doktora	LSD	Başarılı	Başarısız	Mezun
Selçuk Üniversitesi KONYA	-	1	-	-	1	-	-	-	-	2	-	-
Süleyman Demirel Üniversitesi ISPARTA	-	-	1	-	-	-	-	1	-	2	-	-
Yüzüncü Yıl Üniversitesi VAN	1	-	-	-	-	-	-	-	1	1	1	-
Ondokuz Mayıs Üniversitesi SAMSUN	-	-	-	-	-	-	1	-	-	1	-	-
Kırgız Milli Üniversitesi	-	-	-	-	-	-	1	-	-	-	1	-
Kırgız Türkiye Manas Üniversitesi	-	-	-	-	-	-	-	1	-	1	-	-

ARAŞTIRMA FAALİYETLERİ

YAYINLAR/TEBLİĞLER*

Yurtdışı Yayın	Yurtdışı Tebliğ	Yurtdışı Sunum
14	**6**	**26**

YURTDIŞI YAYINLAR

- **S. Ling, C. Xing, F. Özbudak**, "An Explicit Class of Codes with Good Parameters and Their Duals" , Discrete Applied Mathematics, Vol. 154, No. 2, pp. 346–356, 2006.
- **F. Özbudak, Z. Saygı**, "Some constructions of systematic authentication codes using galois rings" Designs, Codes and Cryptography, vol 41, No. 3, pp. 343-357, 2006.
- **V.G. Tsybulin, B. Karasözen, T. Ergenç,** "Selection of steady states in planar Darcy convection", Physics Letters A, 356, 189–194, 2006.
- **T. Ergenç, B. Karasözen**, "Poisson integrators for Volterra lattice equations", Applied Numerical Mathematics, 56, 879-887, 2006.
- **M.Tezer-Sezgin, S.Han Aydın**, "Solution of magnetohydrodynamic flow problems using the boundary element method", Engin. Analy. with Boundary Elements, 30, 411-418, 2006.
- **O. Ugur, M. U. Akhmet,** "The Sturm-Liouville operator on the space of functions with discontinuity conditions", Comput. Math. Appl., 51, no. 6-7,889-896, 2006.
- **O. Ugur, M. U. Akhmet,** "Boundary value problems for higher order linear impulsive differential equatins", J. Math. Anal. Appl., 319, no. 1, 139-156, 2006.
- **Akhmet M.U., M. Turan**, "The differential equations on time scales through impulsive differential equations", Nonlinear Analysis, 65, 2043-2060, 2006.
- **Akhmet M.U., Beklioglu M., Ergenc T., Tkachenko V.,** "On impulsive ratio-dependent predator-prey system with duffusion", Nonlinear Analysis: Real World Applications, 7, 1255-1267, 2006.
- **Akhmet M.U., Kirane M., Tleubergenova M.A., Weber G.W.**, "Control and optimal response problems for quasi-linear impulsive integro-differential equations", European Journal of Operational Research, 169, 1128-1147, 2006.
- **M.U. Akhmet**, "On the integral manifolds of the differential equations with piecewise constant argument of generalized type", Proceedings of the Conference on Differential and Difference Equations at the Florida Instituite of Technology, Melbourne, Florida, Editors: R.P. Agarval and K. Perera, Hindawi Publishing Corporation, 11-20, 2006.
- **M.U. Akhmet, D. Arugaslan, M. Beklioglu**, "Impulsive control of the population dynamics", Proceedings of the Conference on Differential and Difference Equations at the Florida Instituite of Technology, Melbourne, Florida, Editors: R.P. Agarval and K. Perera, Hindawi Publishing Corporation, 21-30, 2006.
- **G.-W. Weber, A. Tezel,** "New views: Generalized semi-infinite optimization of genetic networks, TOP", the Operational Research journal of SEIO (Spanish Statistics and Operations Research Society), 14, 1, 48-55, June 2006.
- **J. Gebert, M. Latsch, S.W. Pickl, G.-W. Weber, R. Wünschiers,** An algorithm to analyze stability of gene-expression pattern, to appear in: special issue Discrete Mathematics and Data Mining II of Discrete Applied Mathematics 154,guest editors: M. Anthony, E.Boros, P.L. Hammer and A. Kogan, 1140-1156, 2006.

* Tüm araştırma faaliyetlerinde sadece UME bağlantılarını belirtmiş öğretim üyelerimizin faaliyetleri dikkate alınmıştır.

YURTDIŞI TEBLİĞLER

- **S. B. G. Dündar, F. Göloğlu, A. Doğanaksoy, Z. Saygı**, "A method of constructing highly nonlinear balanced Boolean functions", BFCA'06, "Boolean Functions Cryptography and Applications", Rouen, Fransa, 13-15 Mart 2006.
- **A. Doğanaksoy, S. Sağdıçoğlu, Z. Saygı, M. Uğuz,** "A note on linearity and homomorphicity", BFCA'06, "Boolean Functions Cryptography and Applications", Rouen, Fransa, 13-15 Mart 2006.
- **F. Göloğlu, M. D. Yücel**, "Necessary conditions on balanced Boolean functions with maximum nonlinearity", BFCA'06, "Boolean Functions Cryptography and Applications", Rouen, Fransa, 13-15 Mart 2006.
- **M. Sönmez Turan, A. Doğanaksoy, Ç. Çalık**, "Statistical Analysis of Synchronous Stream Ciphers", SASC06 Stream Ciphers Revisited, Leuven, Belgium 2006.
- **S. Altay, C. C. Küçüközmen,** Efficient Market Hypothesis and Identification of Linear and Non-linear Dependence in Stock Market Returns, Paper presented at the 13th Annual Conference of the Multinational Finance Society, 25-27 June 2006, Edinburgh, UK, Organized by University of Edinburgh, U.K. and Rutgers University, U.S.A..
- **C. C. Küçüközmen, A. Yüksel,** (2006). A Macro-econometric Credit Risk Model for Stress Testing the Turkish Credit Portfolio, Paper presented at the 13th Annual Conference of the Multinational Finance Society, 25-27 June 2006, Edinburgh, UK, Organized by University of Edinburgh, U.K. and Rutgers University, U.S.A..

YURTDIŞI SUNUMLAR

- **B. Karasözen, A. Bagirov, M. Sezer**, "A derivative free discrete gradient method for nonsmooth optimization", 21st European Conference on Operational Research, 2-5 July, Iceland, 2006.
- **B. Karasözen**, "Interpolatory Derivative Free Optimization Problems", The 5th Ballarat Workshop on Global and Nonsmooth Optimization, Australia, 28-30 November 2006.
- **U. Kaplan, M. Türkay, B. Karasözen, L. T. Biegler**, "Hybrid Systems Approach to Modeling and Simulation of Metabolic Networks", Networks in Compt. Biology, 10-12 September, 2006.
- **S. Han Aydın**, Dual reciprocity BEM solution of Grad-Sahfranov equation for the distribution of magnetic flux in nuclear fusion devices, IABEM 2006 Conference, Graz, Austria, July 10-12, 2006.
- **M. Tezer-Sezgin, C. Bozkaya**, BEM solution of MHD duct flow in a rectangular duct with conducting walls parallel to applied magnetic field, IABEM 2006 Conference, Graz, Austria, July 10-12, 2006.
- **H. Öktem**, Dynamic Information Handling in Continuous Time Boolean Network Model of Gene Interactions. "International Conference of Hybrid Systems and Applications", La Fayette, Louisiana, ABD, 22-26 Mayıs 2006.
- **G. W. Weber, O. Ugur,** "Generalized Semi-Infinite Optimization for Modeling, Dynamics and Prediction of Gene-Environment Networks", 5th Ballarat Workshop on Global and Non-Smooth Optimization Theory, Methods and Applications, Ballarat, Victoria, Australia, November 28-30, 2006.
- **G. W .Weber, O. Ugur, A. Tezel , T. Ergenc**, "On Discrete-Continuous and Generalized Semi-Infinite Optimization of Genetic Networks", GO V, Graphs and Optimisation V, Leukerbad, Switzerland, August 20-24, 2006.
- **G. W. Weber, O. Ugur, A. Tezel, T. Ergenc**, "On Discrete-Continuous and Generalized Semi-Infinite Optimization of Genetic Networks, The 1st Summer School `Achievements and Applications of Contemporary Informatics, Mathematics and Physics', Kiev, Ukraine, August 6-20, 2006.

- **G.-W. Weber, A. Tezel**, On generalized semi-infinite optimization of genetic networks, at: 5th EUROPT Workshop "Advances in Continuous Optimization", Reykjavik, Iceland, June 30 - July 1, 2006.
- **G.-W. Weber,** A dynamical, optimization and algorithmic approach to analyze gene- environment networks, at: EURO XXI 2006, Reykjavik, Iceland, July 2-5, 2006.
- **P. Taylan, G.-W. Weber**, New approaches to regression in financial mathematics by generalized additive models (Conic Quadratic Programming), at: EURO XXI 2006, Reykjavik, Iceland, July 2-5, 2006.
- **S. Özöğür, G.-W. Weber, J. Shawe-Taylor**, Biological Data Mining by using SVM and Pattern Analysis, at: EURO XXI 2006, Reykjavik, Iceland, July 2-5, 2006.
- **A. Gökmen, G.-W. Weber, D. DeTombe, I. Gökmen**, Improving Sustainable Living in Rural Areas in Turkey, at: EURO XXI 2006, Reykjavik, Iceland, July 2-5, 2006.
- **B. Akteke-Öztürk, G.-W. Weber**, Semidefinite programming approach for support vector clustering, at: EURO XXI 2006, Reykjavik, Iceland, July 2-5, 2006.
- **R. Ak, G.-W. Weber**, A new approach credit rating with Hidden Markov Model about Turkish economy, at: EURO XXI 2006, Reykjavik, Iceland, July 2-5, 2006.
- **M. Türkay, G.-W. Weber**, Foundation Meeting of EURO WG "OR in Computational Biology and Bioinformatics", at: EURO XXI 2006, Reykjavik, Iceland, July 2-5, 2006.
- **L. White, G.-W. Weber, M. Shutler**, Foundation Meeting of EURO WG "OR for Development", at: EURO XXI 2006, Reykjavik, Iceland, July 2-5, 2006.
- **A. Gökmen, I. Gökmen, G.-W. Weber, D. DeTombe**, Discussion Presentation: Improving sustainable living in rural areas in Turkey, at: EURO XXI 2006, Reykjavik, Iceland, July 2-5, 2006.
- **G.-W. Weber, A. Kuba, Ö. Yaşar, O. Özgür,** Discrete tomography: a joint contribution by optimization theory, equivariance analysis and statistical learning, at: 1st Summer School "Achiements and Applications of Contemporay Informatics, Mathematics and Physics", Kiev, Ukraine, August 4-20, 2006.
- **G.-W. Weber, Ö. Uğur, A. Tezel, T. Ergenç**, On generalized semi-infinite optimization of genetic networks, at: 1st Summer School "Achiements and Applications of Contemporay Informatics, Mathematics and Physics", Kiev, Ukraine, August 4-20, 2006.
- **S.Z. Alparslan, B. Karasözen, H. Körezlioğlu, Ö. Uğur, G.-W. Weber, S.W. Pickl**, On energy management and sustainable development, at: 1st Summer School "Achiements and Applications of Contemporay Informatics, Mathematics and Physics", Kiev, Ukraine, August 4-20, 2006.
- **M.U. Ahkmet, H. Öktem, G.-W. Weber, S.W. Pickl**, An anticipatory extension of Malthusian model, at: 1st Summer School "Achiements and Applications of Contemporay Informatics, Mathematics and Physics", Kiev, Ukraine, August 4-20, 2006.
- **G.-W. Weber**, 6 years EUROPT – foundation EURO ORD – foundation EURO CBBM, at: 1st Summer School "Achiements and Applications of Contemporay Informatics, Mathematics and Physics", Kiev, Ukraine, August 4-20, 2006.
- **G.-W. Weber, Ö. Uğur, A. Tezel, T. Ergenç,** On Discrete-Continuous and Generalized Semi-Infinite Optimization of Genetic Networks, GO V Meeting, Leukerbad, Switzerland, August 20-24, 2006.
- **G.-W. Weber, Ö. Uğur, B. Akteke-Öztürk, S.Z. Alparslan-Gök, S. Özöğür, P. Taylan, A. Tezel**, Generalized semi-infinite optimization for modeling, dynamics and prediction of gene-environment networks, at: 5th Ballarat Workshop on Global and Nonsmooth Optimization: Theory, Methods and Applications Ballarat, Australia, November 28-30, 2006.
- **S. Altay, C. C. Küçüközmen,** Efficient Market Hypothesis and Identification of Linear and Non-linear Dependence in Stock Market Returns, Paper presented at the 13th Annual Conference of the Multinational Finance Society, Edinburgh, UK, Organized by University of Edinburgh, U.K. and Rutgers University, U.S.A., 25-27 June 2006.
- **C. C. Küçüközmen, A. Yüksel,** A Macro-econometric Credit Risk Model for Stress Testing the Turkish Credit Portfolio, Paper presented at the 13th Annual Conference of the Multinational Finance Society, Edinburgh, UK, Organized by University of Edinburgh, U.K. and Rutgers University, U.S.A., 25-27 June 2006.

Yurtiçi Yayın	Yurtiçi Tebliğ	Yurtiçi Sunum
4	**24**	**15**

YURTİÇİ YAYINLAR

- **M. Taştan, Ö. Çelik, G. W. Weber, B. Karasözen, F. Korkusuz,** "Mathematical Modeling of Proximal Femur Geometry and Bone Mineral Density", Joint Dis Rel Surg, 17(3): 128-136, 2006.
- **C.C. Küçüközmen,** Basel-II is an Opportunity, [in Turkish], Finans Kulup Web Site – Turkiye Finans Yoneticileri Vakfi (Finance Managers Trust of Turkey), 21.08.2006.
- **C.C. Küçüközmen,** Address à Basel-2, Block-3: Enhancing Market Discipline and Transparency Through Disclosure, Finans Kulup Web Site – Turkiye Finans Yoneticileri Vakfi (Finance Managers Trust of Turkey), 01.05.2006.
- **C.C. Küçüközmen,** Mathematics of Banking and Risk Measurement Models, [in Turkish], Finans Kulup Web Site – Turkiye Finans Yoneticileri Vakfi (Finance Managers Trust of Turkey), 25.04.2006.

YURTİÇİ TEBLİĞLER:

- **A. Doğanaksoy, Ç. Çalık, F. Sulak, M. Sönmez Turan**, "Rassal Gezinti Testi", IGS06 İstatistik Gunleri Sempozyumu, Antalya, 2006.
- **A. Doğanaksoy, B. G. Dündar, F. Göloğlu, Z. Saygı, F. Sulak, M. Uğuz**, "A Survey on Bent Functions and Normality", 2. Ulusal Kriptoloji Sempozyumu, pp. 19-26, 2006.
- **İ. Sertkaya, A. Doğanaksoy**, "On Nonlinearity Preserving Bijective Transformations", 2. Ulusal Kriptoloji Sempozyumu, pp. 27-36, 2006.
- **M. Cenk, F. Özbudak,** "Isomorphism Classes of Elliptic Curves Over Finite Fields of Characteristic 3", 2. Ulusal Kriptoloji Sempozyumu, pp. 62-69, 2006.
- **A. Doğanaksoy, Ç. Çalık**, **F. Sulak,** "Observations on Hellman's Cryptanalytic Time-Memory Trade-off", 2. Ulusal Kriptoloji Sempozyumu, pp. 83-90, 2006.
- **B. G. Dündar, S. Kalkan, K. Kaya, A. A. Selçuk**, "Threshold Paillier and Naccache-Stern Cryptosystems Based on Asmuth-Bloom Secret Sharing", 2. Ulusal Kriptoloji Sempozyumu, pp. 91- 100, 2006.
- **O. Çetinkaya, A. Doğanaksoy,** "A Practical Privacy Preserving E-Voting Protocol Using Dynamic Ballots", 2. Ulusal Kriptoloji Sempozyumu, pp. 101-113, 2006.
- **E. Akyıldız, O. Yayla,** "Scalar Multiplication on Elliptic Curves", 2. Ulusal Kriptoloji Sempozyumu, pp. 114-124, 2006.
- **A. Doğanaksoy, E. Saygı**, "Quadratic Feedback Shift Registers Generating Maximum Length Sequences", 2. Ulusal Kriptoloji Sempozyumu, pp. 141-145, 2006.
- **M. S. Turan, O. Kara**, "Finding Linear Approximations for the Stream Cipher Trivium", 2. Ulusal Kriptoloji Sempozyumu, pp. 146-153, 2006.
- **A. Doğanaksoy, Ç. Çalık, F. Sulak, M. S. Turan**, "New Randomness Tests Using Random Walk", 2. Ulusal Kriptoloji Sempozyumu, pp. 166-172, 2006.
- **M. S. Turan, A. Doğanaksoy, Ç. Çalık**, "Detailed Statistical Analysis of Synchronous Stream Ciphers", 2. Ulusal Kriptoloji Sempozyumu, pp. 173-186, 2006.
- **Z. Saygı, S. Yeşil,** "Bir TÜBİTAK Kamu Projesi: Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar", 1. Ulusal Elektronik İmza Sempozyumu, pp.35, 2006.
- **Ç. Çalık, M. Sönmez Turan, Z. Yüce**, "E-İmzada SHA-1 Özetleme Algoritmasının Kullanımı", 1. Ulusal Elektronik İmza Sempozyumu, pp. 167, 2006.
- **M. Cenk, O. Yayla,** "Ayrık Logaritma Problemini Kullanan E-İmza", 1. Ulusal Elektronik İmza Sempozyumu, pp.236, 2006.

- **M. Schaefer, B. Karasözen, Ö. Uğur, Y. Yapıcı**, "Derivative Free Optimization of Stirrer Configuration", ENUMATH 2005 the 6th European Conference on Numerical Mathematics and Advanced Applications, Springer, 1031-1039, 2006.
- **M. Schaefer, B. Karasözen, Ö. Uğur, K. Yapıcı**, "Derivative Free Optimization of Stirrer Configurations", in: Proceedings of The Sixth European Conference on Numerical Mathematics and Advanced Applications, ENUMATH 2005, USC, Santiago de Compostela, Spain, 2005, Springer-Verlag, 2006, pp.~1031--1039.
- **K. Yıldırak**, "A Statistical Credit Rating Model for Large Turkish Manufacturing Companies", 2. International Conference on Business, Management and Economics, Çeşme,15-18 Haziran 2006.
- **K. Yıldırak**, **H. Artam**, "A Macro-Finance Model for Turkish Government Bond Yields", 2. International Conference on Business, Management and Economics, Çeşme,15-18 Haziran 2006.
- **H. Körezlioğlu**, Representation of Zero Coupon Bond Prices in Terms of Two-Parameter Brownian Martingales, AMAMEF 2006, Side, Nisan 2006.
- **H. Körezlioğlu,** Representation of Zero Coupon Bond Prices in Terms of Two-Parameter Brownian Martingales (working paper) 2006.

YURTİÇİ SUNUMLAR

- **Z. Alparslan, B. Karasozen, H. Korezlioglu, S.W. Pickl, O.Ugur, G.W. Weber**, "On Energy Management and Sustainable Development", First Conference of Advanced Mathematical Methods for Finance, AMAMEF 2006, Side/Antalya, Turkey, pp.~107-108, 2006.
- **A. Aydın, B. Karasözen**, "Soliton çözümlü lineer olmayan ikili Schrödinger denkleminin çoklu simplektik yöntemlerle çözümü", 19. Ulusal Matematik Sempozyumu, Dumlupınar Üniversitesi, 22-25 Agustos 2006.
- **G.-W. Weber, Ö. Uğur, A. Tezel, A. Soyler, M. Çetin**, On discrete-continuous modeling and generalized semi-infinite optimization of gene-environment networks, at: Workshop on Networks in Computational Biology, IAM, METU, Ankara, Turkey, August 20-24, 2006.
- **B. Karasözen**, "Interpolatory Derivative Free Optimization Methods", Turkish-German Summer Academy on Advanced Engineering, Kuşadası, 26 August-3 September 2006.
- **Z. Alparslan, B. Karasözen, H. Körezlioğlu, S.W. Pickl, Ö. Uğur, G.-W. Weber, "**On Energy Management and Sustainable Development", The First Conference of Advanced Mathematical Methods for Finance, Side, Antalya, April 26-29 2006.
- **P. Taylan and G.-W. Weber,** New approaches to regression in financial mathematics by generalized additive models, at: First Conference of Advanced Mathematical Methods for Finance, Side, Antalya, Turkey, April 29, 2006.
- **K. Yıldırak**, "A Statistical Credit Rating Model for Large Turkish Manufacturing Companies", 2. International Conference on Business, Management and Economics, Çeşme,15-18 Haziran 2006.
- **K. Yıldırak**, **H. Artam**, "A Macro-Finance Model for Turkish Government Bond Yields", 2. International Conference on Business, Management and Economics, Çeşme,15-18 Haziran 2006.
- **H. Körezlioğlu**, Representation of Zero Coupon Bond Prices in Terms of Two-Parameter Brownian Martingales, AMAMEF 2006, Side, Nisan 2006.
- **H. Körezlioğlu,** Representation of Zero Coupon Bond Prices in Terms of Two-Parameter Brownian Martingales (working paper) 2006.
- **S. Altay, C. C. Küçüközmen,** An Assessment of Value-at-Risk (VaR) and Expected Tail Loss (ETL) Under a Stress Testing Framework for Turkish Stock Market, Paper presented at the 2nd International Conference on Business, Management and Economics, Organized by Yaşar University, Çeşme, İzmir, 15-18 June 2006
- **T. Aktürk, C. C. Küçüközmen**, An Econometric Approach to Tourism Demand: Arrivals from UK and Australia to Turkey, Paper presented at The Third Graduate Research in Tourism Conference, Anatolia: Turizm Araştırmaları Dergisi, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale, 25-28 May 2006.

- **T. Aktürk, C. C. Küçüközmen,** Tourism Demand for Turkey: Models, Analysis and Results, Paper presented at The Third Graduate Research in Tourism Conference, Anatolia: Turizm Araştırmaları Dergisi, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale, 25-28 May 2006.

Yurtdışı Kitapta Makale
1

- **M. Cenk, F. Özbudak,** "Isomorphism Classes of Ordinary Elliptic Curves Over Fields of Characteristic 3", Mathematical Methods in Engineering, Springer Publications, 151-158, K.Taş, J.A. Tenreiro Machado, D. Baleanu.

UME Preprint Serisi (IAM Preprint Series)*: 18 (No: 48-65)

(www.iam.metu.edu.tr/research Preprint Series)

*Bu Preprintlerin listesi **Ek 1**'de verilmektedir.

ÇALIŞTAY/ SEMPOZYUM/ KONFERANS/ YAZOKULU

- **II. Ulusal Kriptoloji Sempozyumu** (15-17 Aralık 2006, Ankara)
  Uygulamalı Matematik Enstitüsü tarafından II. Ulusal Kriptoloji Sempozyumu düzenlenmiştir. 5 davetli konuşmacı (İstanbul Doğuş Üniversitesi'den İsmail GÜLOĞLU, İstanbul Ticaret Üniversitesi 'nden Çetin Kaya KOÇ, TÜBİTAK UEKAE'den Murat APOHAN, Worcester Polytechnic Enstitüsü'nden Berk SUNAR ve ASELSAN'dan Ali YAZICI) 6 konuşma yapmıştır. 19 sözlü sunum yapılmıştır. 1 davetli konuşma ve 17 makale bildiriler kitabında yer almıştır. Toplam 120 civarı katılım olmuştur. Sempozyum TÜBİTAK ve ODTÜ'nün destekleriyle düzenlenmiştir. Detaylı bilgiler http://www.iam.metu.edu.tr/sempozyum adresinde bulunabilir.

- **First Conferans of Advanced Mathematical Methods for Finance (AMAMEF)** (26-29 Nisan 2006, Antalya)
  Advanced Mathematical Methods for Finance (AMAMEF), bir Avrupa Bilim Fonu (ESF) projesidir. Söz konusu projenin öncelikli amacı Avrupa'da stokastik analiz, kontrol teorisi, diferansiyel denklemler gibi finans uygulamalarında kullanımı gün geçtikçe artan disiplinlerde çalışan farklı grupları bir araya getirmektir. İkinci amacı ise matematiksel araştırmaların finans endüstrisine aktarılması ve bu endüstrideki gelişmelere katkı sağlamasıdır. Türkiye dahil 15 ülkeden seçkin akademisyenlerin liderliğinde birçok araştırma grubu tarafından yürütülen çalışmalar, bu proje sayesinde, Avrupa finansal sistemine katkı sağlamaktadır.
  Yukarıdaki amaçlar doğrultusunda ESF her yıl üye ülkelerin birinde ilgili konuları kapsayan ve araştırmacıları bir araya getirecek olan bir konferans düzenleme kararı almıştır. Bu konuda ESF ile işbirliğine gidilmiş ve kuruluşun yürüttüğü AMAMEF projesinin ilk konferansı, bu yıl, bölümümüz tarafından düzenlenmiştir. Konferansın yerel organizasyon komitesinde enstitümüz öğretim elemanlarından Prof. Dr. Hayri Körezlioğlu, Doç.Dr Azize Hayfavi, Dr. Ömür Uğur, Yrd. Doç. Dr. Kasırga Yıldırak ve Prof. Dr. Gerhard W. Weber yer almışlardır. Bilim komitesini Ole Barndorf-Nielsen(DK), Mark Davis(UK), Giulia Di Nunno(NO), Claudia Klüppelberg(DE), Roberto Natalini(IT), Bernt Øksendal(NO), ve Damien Lamberton(FR)'nın oluşturmuş olduğu AMAMEF konferanslarının ilki 26-29 Nisan 2006 tarihleri arasında Side-Antalya'da yapılmıştır. Konferans kapsamında başlıca finansal ürün fiyatlaması, riskten korunma, faiz haddi modelleri, piyasa riski, kredi riski, ve kredi derecelendirmesi olmak üzere bir çok konu finansal matematik alanındaki en yeni gelişmeler çerçevesinde ele alınmıştır. Bu konferansla ilgili daha detaylı bilgi Amamef Konferans Değerlendirme Raporu'nda bulunmaktadır.

- **Ö. Akın, B. Karasözen, B. Kristjansson, S. Olafsson, J. Pinter, O. Stein, G. Still, G. W. Weber**, Workshop on Advances in Continuous Optimization, 30 June-1 July, Iceland, 2006.

- **T. Kinnunen, S. Olafsson, B. Kristjansson, G.-W. Weber, et al.,** EURO XXI 2006, 21st International Conference on Operational Research, Reykjavik, 2-5 July, 2006.

- **M. Dür, P. Huhn, K. Klammroth, C. Tammer, U. Wildburger, B. Karasözen, G. Leugering, G. W. Weber,** EURO Summer Institute, "Optimization Challenges in Engineering, Wittenberg Germany, August 2006.

- **B. Karasözen, M. Schaefer**, Turkish-German Summer Academy in Advanced Engineering, Kuşadası, August 2006.

- **W. M. Dress, B. Karasözen, P. Stadler, G.W.Weber,** Workshop on Networks in Computational Biology, METU-Institute of Applied Mathematics, 8-10 September, 2006.

- **D. DeTombe, A. Gökmen, I. Gökmen, B. Karasözen, S. Kayalıgil, H. Körezlioğlu,G.-W. Weber,** Workshop on "Complex Societal Problems, Sustainable Living and Development", Ankara, 15-21 April, 2006.

- **A. Kence, G.-W. Weber et al.,** Workshop of Geometric Morphometry, Ankara, 12-16 June, 2006.

ARAŞTIRMA GRUPLARI/ DOSAP PROGRAMI

AÇIK ANAHTAR ALTYAPISI (AAA) ARAŞTIRMA GRUBU

Grup üyeleri

Muhiddin UĞUZ (MATH)
Ersan AKYILDIZ (Koordinatör) (MATH)
Rüyal ERGÜL (EE)
Ali DOĞANAKSOY (MATH)
Zülfükar SAYGI (Koordinatör Yrd.) (UME)
Feyza Taşkazan ERYOL (TÜBİTAK Bilten)
Faruk GÖLOĞLU
H. Murat YILDIRIM
Kadir ERDOĞAN
Murat CENK
Atilla BEKTAŞ (Webmaster)
Oğuz YAYLA
Elif SAYGI
Meltem Sönmez TURAN
Ayşe Nurdan SARAN
Fatih SULAK
Çağdaş ÇALIK

Grup Web Sayfası: www.pki.iam.metu.edu.tr

AKAN ŞİFRE SİSTEMLERİ ÇALIŞMA GRUBU

Grup Üyeleri

Ali DOĞANAKSOY(Koordinatör) (MATH)
İsmail Şuayip GÜLOĞLU (Doğuş Üniv.)
Muhiddin UĞUZ (MATH)
Orhun KARA (TÜBİTAK-UEKAE)
Elif SAYGI
Zülfükar SAYGI
Meltem Sönmez TURAN
Ayşe Nurdan SARAN
Çağdaş ÇALIK

BOOLE FONKSİYONLARI ÇALIŞMA GRUBU

Grup Üyeleri

Ali DOĞANAKSOY(Koordinatör)(MATH)
İsmail Şuayip GÜLOĞLU (Doğuş Üniv.)
Muhiddin UĞUZ (MATH)
Baha Güçlü DÜNDAR
Elif SAYGI
Zülfükar SAYGI
Faruk GÖLOĞLU
Fatih SULAK
H. Murat YILDIRIM
İsa Sertkaya (TÜBİTAK-UEKAE)
Kayhan Uluer (TÜBİTAK-UEKAE)
M. Rıdvan Bakkal (TÜBİTAK-UEKAE)
Serhat Sağdıçoğlu (TÜBİTAK-UEKAE)

Grup Web Sayfası: http://www.math.metu.edu.tr/bfwg

DİNAMİK SİSTEMLER ARAŞTIRMA GRUBU

Grup Üyeleri:

Marat U. AKHMET (MATH)
Yesim SERİNAGAOGLU (EE)
Enes YILMAZ
S. BERKİNBAEV (Aktobe State Medical Academy, Kazakhstan)
Meryem BEKLİOGLU (BIO)
Mehmet TURAN (MATH)
Cemil BÜYÜKADALI (MATH)
G. BEKMUKHAMBETOVA (Aktobe State Medical Academy, Kazakhstan)
Tanıl ERGENÇ (Atılım Üniv.)
Duygu ARUGASLAN (MATH)
Derya ALTINTAN
Viktor TKACHENKO (Inst.of Math., Kiev, Ukraine)

Grup Web Sayfası: http://www.iam.metu.edu.tr/research

EUROPT OPTİMİZASYON ARAŞTIRMA GRUBU

2003 yılından itibaren Uygulamalı Matematik Enstitüsü, EUROPT ve EURO Sürekli Optimizasyon çalışma grubuna ev sahipliği yapmaktadır. Bu araştırma grubunun amacı, uluslararası işlevsel araştırma ve uygulamalı matematik çalışmalarını özellikle avrupa birliğindeki araştırmacılarla birlikte uluslararası düzeyde canlı tutmaktır. EUROPT Optimizasyon Araştırma Gurubu olarak popüler dergilerin özel sayılarına yayınlar hazırlanmış, birçok çalıştay düzenlenmiş, her düzeyde çeşitli bilimsel aktiviteler gerçekleştirilmiştir. Bunların dışında iki yeni EURO çalışma grubu ile çalışmalar devam etmektedir.

Grup üyeleri

G. Wilhelm Weber
Marco A. Lopez-Cerda (Alicante University, Spain)
Mirjam Dür (Technische Universität Darmstadt, Germany)
Kaisa Miettinen (Helsinki School of Economics, Finland)
Leonidas Sakalauskas (Institute of Mathematics and Informatics, Lithuania)

Grup Web Sayfası: http://www.iam.metu.edu.tr/EUROPT/

FİNANSAL RİSK ARAŞTIRMA GRUBU

Grup Üyeleri:

Hayri KÖREZLİOGLU (Koordinatör)
Ömer GEBİZLİOGLU (STAT/Ankara Üniv.)
Gerhard-Wilhelm WEBER
Azize HAYFAVİ
Esma GAYGISIZ (ECON)
Işıl EROL (ECON)
Kasırga YILDIRAK (ECON/Trakya Üniv.)
Dr. Stefan PİCKL (Uni. of Cologne, IMCACS)
Muhammed DABBAGH (MATH)
Ayşegül İŞCANOĞLU
Zehra EKŞİ
İbrahim Ethem GÜNEY
İrem YILDIRIM
Yeliz YOLCU OKUR
Sühan ALTAY (BA)
K. Korhan NAZLIBEN
Hatice ANAR
Nilüfer ÇALIŞKAN
Sibel KORKMAZ
Serkan ZEYTUN

Grup Web Sayfası: http://www.iam.metu.edu.tr/research/groups/riskman.html

HESAPLAMALI BİYOLOJİ VE TIP ARAŞTIRMA GRUBU

Grup Üyeleri:

Marat AKHMET (MATH)
Mahinur AKKAYA (CHEM)
Taylan BALİ (ECON)
Nazife BAYKAL (Inf. Inst.)
Meryem BEKLİOĞLU (BIO)
Pınar ÇALIK (FDE)
Tanıl ERGENÇ (Atılım Univ.)
Hayri ERTAN (PES)
Murat EYÜBOĞLU (EE)
Nevzat G. Gençer (EE)
A.Gülçin SAĞDIÇOĞLU (Gazi Üniv.)
Burcu BAREN (Medicine-HÜ)
Alp BASSA (Essen-Germany)
Biter BİLEN (BI-METU)
Ceren BERKMAN (BIO)
Mehmet Ulaş ÇINAR (MATH-EGE)
Mehmet ÇETİN (BİO)
Aslihan DEMİRKAYA (Cansas-USA)
Jutta GEBERT (Cologme-Germany)
Yusuf GÜL (PHYS)
Ali GÖKMEN (CHEM)
Mesude İŞCAN (BİO)
Bülent KARASÖZEN (MATH)
Feza KORKUSUZ (Phys.Edu.Sports)
Erkan MUMCUOĞLU (Inf. Inst.)
Yeşim SERİNAĞAOĞLU (EE)
Oğuz TANRISEVER
Metin TÜRKAY (EE-KOÇ)
Ömür UĞUR
Batchev VİHREN (Unv of Athens)
Volkan ATALAY (CE)
Martin LAETSCH (Cologme-Germany)
Alp MARANGOZ (AEO)
Mert ÖZARAR (CE)
Süreyya ÖZÖĞÜR
Betül SÖYLER (FDE)
Nicole RADDE (Cologme-Germany)
Ahmet SAÇAN (CE)
Mehmet SOMEL (Max-Plimer-Ins-USA)
Sinan SARAÇ (CE)
Gerhard Wilhelm WEBER (Coordinator)
Tolga CAN (CE)
R. WÜNSCHİERS (Cologme-Germany)
Özlem YILMAZ (Company)
Zümrüt ÖGEL (FDE)
Hakan ÖKTEM
Stefan W. PİCKL (Math-KOLN)
J.A.A.QUİTZAU (Scylla Bioinf-Portekiz)
Andrea Schulte-THOMAS
İnci TOGAN (BIO)
Aysun TEZEL (MATH)
Can Ozan TAN (Boston-USA)
Zeynep ALPARSLAN
Mesut TAŞTAN (Texas-USA)
Özgür ÇELİK (FES)
Çiğdem GÖKCEK (BİO)
Hüseyin MERDAN (Math-TOBB)
Bilge YILMAZ (Company)
Alper SÖYLER (FDE)
Pakize TAYLAN (Dicle Üniv.)

Grup Web Sayfası: http://www.iam.metu.edu.tr/research/groups/compbio/index.html

HİBRİD SİSTEMLER ARAŞTIRMA GRUBU

Grup Üyeleri:

Marat U. AKHMET (MATH)
Larry BİEGLER (Carnegie Mellon Univ.)
Bülen KARASÖZEN (MATH)
Mustafa KAHRAMAN
Hakan ÖKTEM
Metin TÜRKAY (Koc University)
Gerhard Wilhelm WEBER
Aysun TEZEL (MATH)
Ahmet Melih SELÇUK
Nilüfer ÇALIŞKAN
Nurgül GÖKGÖZ
Müşerref TÜRKMEN

Grup Web Sayfası: http://www.iam.metu.edu.tr/research/groups/hybrg/index.html

KODLAMA TEORİSİ ARAŞTIRMA GRUBU

Grup Üyeleri

Ferruh ÖZBUDAK (Koordinatör) (MATH)
Ersan AKYILDIZ (MATH)
Emrah ÇAKÇAK
Murat CENK
Zülfükar SAYGI

OPTİMİZASYON TEORİSİ ARAŞTIRMA GRUBU

Grup Üyeleri:

Haluk AKSEL (ME)
Yusuf ULUDAĞ (CHE)
Ömür UĞUR
Gerhard-W. WEBER
Kerim YAPICI (CHE)
Ronald HOPPE (Univ. of Augsburg)
Bülent KARASÖZEN (MATH)
M. SCHAEFER (Tech. Univ. Darmstadt)
Tamas TERLAKY (Mc Masters University)
Katya SCHEİNBERG (IBM Thomas Watson Center)
Başak AKTEKE ÖZTÜRK
Zeynep ALPARSLAN GÖK
Georg STİLL (TU Twente)
Miriam DUERR (TU Darmstadt)
Oliver STEİN (RWTH Aachen, Germany)
Aysun TEZEL (MATH)
Süreyya ÖZÖĞÜR
Stefan W.PİCKL (Uni.of Cologne, IMCACS)

Grup Web Sayfası: http://www.iam.metu.edu.tr/EUROPT

TERS PROBLEMLER ARAŞTIRMA GRUBU

Grup Üyeleri:

Nevzat Ü. GENÇER (EE)
Gerhard-Wilhelm WEBER
Bülent KARASÖZEN (MATH)
Hakan ÖKTEM
Osman ÖZGÜR (TÜBİTAK)
Öznur YAŞAR (Memorial Univ.)
Andreas TIEFENBACH (MATH)
Yesim SERİNAGAOGLU (EE)
Attila KULA (Univ. of Szeged, Hungary)
Sedat SARIKAYA
Çağrı DİNER (Memorial Univ.)
Gülser KÖKSAL (IE)
Ömür UĞUR
Murat EYÜBOĞLU (EE)
Ali GÖKMEN (CHEM)
Başak AKTEKE ÖZTÜRK

Grup Web Sayfası: http://www.iam.metu.edu.tr/research

DOSAP PROGRAMI

- **Pakize Taylan** (Dicle Üniversitesi, Matematik Bölümü), Finansal Piyasalarda Matematiksel Optimizasyon Tekniklerinin Kullanımı (1 Ekim 2005- 1 Eylül 2007)
- **Nedim Dikmen** (Giresun Üniversitesi, Ekonometri Bölümü), Faiz haddinin modellenmesi: Makro Finans yaklaşımı (1 Eylül 2006- 1 Eylül 2008).

YÜRÜTÜCÜLÜĞÜ YAPILAN PROJELER

Projenin Adı: Kriptografi Konusunda Araştırma, Geliştirme; Algoritma Tasarımı, Analizi ve Uygulanması (BAP-07-05-DPT.2004K120700 DPT)
Yürütücüsü: Ersan Akyıldız
Araştırmacıları: Rüyal Ergül, Ali Doğanaksoy, Melek Yücel, Ferruh Özbudak, Muhiddin Uğuz, Emrah Çakçak
Süresi: 1.1.2004-31.12.2007
Bütçesi: 2.903.000- YTL

Projenin Adı: Açık Anahtar Altyapı Konusunda Araştırma, Geliştirme Ve Uygulamalar (TÜBİTAK Kamu Projesi)
Yürütücüsü: Rüyal Ergül
Araştırmacıları: Ersan Akyıldız, Ali Doğanaksoy, Ferruh Özbudak, Muhiddin Uğuz, Emrah Çakçak, Mustafa Alkan, K. Sacit Sarıkaya, Sezen Yeşil, Özgür Öztürk, Onur Gençer
Süresi: 1.7.2006-1.7.2008
Bütçesi: 450.000- YTL

Projenin Adı: Modeling Multistationary Processes by Using Hybrid System Formulation: A study with priority on functional genomics (TÜBİTAK 1001 Projesi)
Yürütücüsü: Hakan Öktem
Araştırmacıları: Didem Akçay, Özgür Hakanoğlu
Süresi: Haziran 2005 –Haziran 2010
Bütçesi: 162.400- YTL

Projenin Adı: Nükleer Füzyon Reaktör Problemlerinin Sınır Elemanları ve Sonlu Elamanlar Yöntemleri ile Çözümü (TÜBİTAK 1001 Projesi)
Yürütücüsü: M. Tezer
Araştırmacıları: Ali İhsan Neslitürk, Selçuk Han Aydın, Sevin Gümgüm
Süresi: 1 Kasım 2005 – 1 Kasım 2007
Bütçesi: 41.100- YTL

Projenin Adı: Sürekli Optimizasyon Yöntemleri ve Uygulamaları (TÜBİTAK Bütünleşik Doktora Programı projesi)
Yürütücüsü: Bülent Karasözen
Araştırmacıları: Gerhard W. Weber, Tanıl Ergenç, Yusuf Uludağ
Süresi: 2005-...

Projenin Adı: Özgün Eliptik Eğri Tasarlanması ve Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi (ASELSAN)
Yürütücüsü: Ersan Akyıldız, Rüyal Ergül
Süresi: 1.10.2006-30.3.2008
Bütçesi: 200.000- YTL

Projenin Adı: Blok Tipi Algoritmaların İstatistiksel ve Yapısal Test Yazılımlarının Geliştirilmesi (ASELSAN)
Yürütücüsü: Ali Doğanaksoy
Süresi: 1.12.2006-30.11.2007
Bütçesi: 100.000- YTL

Projenin Adı: Doğrulama Kodlarının Üretilme Metodlarının İncelenmesi, Geliştirilmesi ve Uygulanması (BAP-2006-07-05-02)
Yürütücüsü: Ferruh Özbudak
Araştırmacıları: Murat Cenk, Zülfükar Saygı, Emrah Çakçak.
Süresi: 1.1.2006-31.12.2007
Bütçesi: 6.000- YTL

Projenin Adı: Biyolojik Veri Madenciliğinin ve Sınıflandırılmasının İstatistiksel Öğrenmesi, Sürekli Optimizasyon, Makina Öğrenmesi ve Semi(yarı)-Sonsuz Programlama Kullanılarak Geliştirilmesi (BAP-2006-07-05-01)
Yürütücüsü: Gerhard W. Weber
Araştırmacıları: Zümrüt B. Ögel, Bülent Karasözen, Volkan Atalay, John Shawe Taylor, Pakize Taylan, Ömür Uğur, Süreyya Özöğür
Süresi: 1 Ocak 2006 – 31 Aralık 2006
Bütçesi: 4.000- YTL

Projenin Adı: Türkiye Finans Piyasalarına Uyum Sağlayacak Risk Modelleri Araştırma, Geliştirme Ve Uygulamaları (BAP-2005(R)-07-05-01)
Yürütücüsü: Hayri Körezlioğlu
Araştırmacıları: İrini Dimitriyadis, Esma Gaygısız, Adil Oran, Nuray Güner, Coşkun Küçüközmen, Azize Hayfavi, Ş. Kasırga Yıldırak, G. W. Weber, Hakan Öktem, Ömür Uğur, Ayşegül İşcanoğlu, Yeliz Yolcu Okur, Oktay Sürücü, Zehra Ekşi, İrem Yıldırım, Serkan Zeytun
Süresi: 1 Ocak 2006-31 Aralık 2006
Bütçesi: 3.000- YTL

ENSTİTÜ BAĞLANTILI ÖĞRETİM ÜYELERİNİN ARAŞTIRMACI OLARAK KATILDIKLARI PROJELER

Projenin Adı: Development of Modeling and Optimization Tools for Hybrid Systems (NSF-TÜBİTAK INT projesi)
Yürütücüsü: B. Karasözen
Araştırmacıları: L. Biegler (Koç Üniversitesi ve Carnegie Mellon Üniversitesi Kimya Müh. Bl.), H. Öktem, M. Türkay ve U. Yılmaz (Koç Üniversitesi, Endüstri Müh. Bl.)
Süresi: 2005-2007

Projenin Adı: Kalite İyileştirmede Veri Madenciliği Kullanımı ve Geliştirilmesi (TÜBİTAK Araştırma projesi)
Yürütücüsü: G. Köksal (Endüstri Mühendisliği)
Araştırmacıları: B. Karasözen, G. W. Weber
Süresi: 2005-2008

Projenin Adı: Meteoroloji/Oşinografi Mükemmeliyet Ağı (MOMA) pilot projesi: Uydu ve yer gözlem, veri asimilasyonu, öngörü, erken uyarı sistemleri ve kullanıcı hizmetleri geliştirilmesi (TÜBİTAK Kamu projesi)
Yürütücüsü: E. Özsoy (Deniz Bilimleri Endüstri)
Araştırmacıları: B. Karasözen, Ö. Uğur, H. Öktem
Süresi: 2005-2007

Projenin Adı: Composable Derivative Contracts (ComDeCo Projesi)
Yürütücüsü: Ralf Korn (Univ. of Kaiserslautern), Arnd Poetzsch-Heffter
Araştırmacıları: Stefanie Müller, Ulrich Nögel, Markus Reitz, Ömür Ugur
Süresi: 2005 - 2007

Projenin Adı: Balaban Valley Project Sürekli Optimizasyon Yöntemleri ve Uygulamaları
Yürütücüsü: A. Gökmen
Araştırmacıları: S. Kayalıgil, G. W. Weber, İ. Gökmen, M. Ecevit, A. Sürmeli, T. Bali, Y. Ecevit, H. Gökmen, D. J. DeTombe
Süresi: 2004-...

ÖĞRETİM ÜYESİ YETİŞTİRME PROGRAMI (ÖYP) PROJELERİ

Danışmanı: Hayri Körezlioğlu
Öğrencinin Adı: Ayşegül İşcanoğlu
Üniversitesi: Selçuk Üniversitesi, KONYA
Bütçesi: 2.456

Danışmanı: Marat Akhmet
Öğrencinin Adı: Derya Altıntan
Üniversitesi: Selçuk Üniversitesi, KONYA
Bütçesi: 2.350

Danışmanı: Ersan Akyıldız
Öğrencinin Adı: Barış Bülent Kırlar
Üniversitesi: Süleyman Demirel Üniversitesi, ISPARTA
Bütçesi: 4.385

Danışmanı: G. Wilhelm Weber
Öğrencinin Adı: S. Zeynep Alparslan
Üniversitesi: Süleyman Demirel Üniversitesi, ISPARTA
Bütçesi: 1.775

Danışmanı: Melek D. Yücel
Öğrencinin Adı: Sedat Akleylek
Üniversitesi: Ondokuz Mayıs Üniversitesi, SAMSUN
Bütçesi: 6.030

Danışmanı: Ersan Akyıldız
Öğrencinin Adı: Turgut Hanoymak
Üniversitesi: Yüzüncü Yıl Üniversitesi, VAN
Bütçesi: 2.364

Danışmanı: Melek D. Yücel
Öğrencinin Adı: Rita İsmailova
Üniversitesi: Kırgız Türkiye Manas Üniversitesi, KIRGIZİSTAN
Bütçesi: 5.524

Danışmanı: Melek D. Yücel
Öğrencinin Adı: Nurbek Ulu Baryk
Üniversitesi: Kırgız Milli Üniversitesi, KIRGIZİSTAN
Bütçesi: 6.930

DİĞER FAALİYETLER

HALKA AÇIK KISA SÜRELİ KURSLAR/SEMİNERLER

- **Dorien De Tombe** (Amsterdam University), "Lectures on Complex Societal Problems ", 17-21 Nisan 2006.
- **Stef Tijs** (Tilburg Üniversitesi), "Lectures on Cooperative Game Theory", 11-23 Kasım 2006.
- **Slava Tsybulin**, (Rostov State Üniversitesi), "Dynamical systems and computer study", 29 Kasım - 22 Aralık 2006.
- **Ronald H. W. Hoppe**, "Optimization of partial differential equations ", (Houston Üniversitesi), 10-17 Aralık 2006.
- **Zeev Volkovich** (ORT Braude College), "Lectures on Optimization and Data Mining", 26-29 Aralık 2006.
- **Sevtap Kestel** (Freiburg Üniversitesi), "The Model-Based Approach in Insurance Applications", 4-8 Aralık 2006.

ENSTİTÜMÜZÜ KISA SÜRELİ ZİYARET EDENLER

- **Dorien DeTombe**, University of Amsterdam, Chair of International and EURO Working Group on Complex Societal Problems, Netherlands, 17-21 Nisan 2006.
- **Roger Jwatt Gray,** University of Edinburgh, UK, 21 Şubat 2006.
- **Alan Newell,** The University of Arizona, USA, 17-19 Nisan 2006.
- **Oliver Ewald,** University of Leeds, UK, 4-17 Mayıs 2006.
- **James B. Carell,** The University of British Columbia, Canada, 9-16 Mayıs 2006.

- **T. A. Springer**, Universiteit Utrecht, Nedherlands, 9-16 Mayıs 2006.
- **Nikolai Kolev,** University of Sao Paulo, Brazil, 12-16 Haziran 2006.
- **M. Fernandes,** University of Sao Paulo, Brazil, 12-16 Haziran 2006.
- **Pooya Farshim,** University of Bristol, UK, 9-11 Temmuz 2006.
- **Andreas Dress,** Max-Planck Institute, Germany, 9-13 Eylül 2006.
- **Stadler,** Max-Planck Institute, Germany, 9-13 Eylül 2006.
- **George Still,** University of Twente, Nedherlands, 1-14 Ekim 2006.
- **Stef Tijs** Tilburg Üniversitesi, Nedherlands, 11-23 Kasım 2006.
- **Jean Pierre Serre,** College de France, 16-22 Kasım 2006.
- **Z. Volkovich,** ORT, Braude College, Israel, 24-29 Aralık 2006.
- **Slava Tsybulin**, Rostov State University, Rusia, 29 Kasım - 22 Aralık 2006.
- **Ronald H. W. Hoppe**, Houston University, USA, 10-17 Aralık 2006.
- **Zeev Volkovich,** ORT Braude College, Israel,26-29 Aralık 2006.
- **Sevtap Kestel,** Freiburg University, Germany, 4-8 Aralık 2006.

ENSTİTÜ ÜYELERİNİN KISA SÜRELİ YURT DIŞI ZİYARETLERİ

- **Oktay Sürücü, Ayşegül İşcanoğlu,** Kaiserslautern University, Almanya, 31 Temmuz-13 Ağustos 2006.
- **Yeliz Yolcu Okur**, Oslo Üniversitesi, Norveç, 1 Ağustos-20 Ekim 2006.
- **Süreyya Özöğür**, Southampton Üniversitesi, İngiltere, 15 Mayıs-10 Ağustos 2006.
- **Hakan Öktem**, TBAG-U/114(1041253) TUBİTAK-NSF projesi ile Carnegie Mellon University, Amerika, 12 Temmuz - 12 Ağustos 2006.
- **Süreyya Özöğür**, University College London, İngiltere, 17 Ağustos-31 Aralık 2006.

DERGİ EDİTÖRLÜKLERİ

- **G. W. Weber**, Member of Editorial Board of Journal of Computational Technologies.
- **B. Karasözen, M. Pinar, T. Terlaky and G.-W. Weber**, Advances in Continuous Optimization, special issue of European Journal of Operational Research 169, 3 (2006).
- **B. Karasözen, A. Rubinov, G.-W. Weber, J. Teghem,** Optimization in Data Mining, special issue of European Journal of Operational Research (2005-2006).
- **M. Dür, B. Karasözen, T. Terlaky and G.-W. Weber, J. Teghem**, Challenges of Continuous Optimizatiom in Theory and Applications, special issue of European Journal of Operational Research (2005-2006).

ENSTİTÜ DESTEKLİ KONFERANS KATILIMLARI

- **Çağdaş Çalık ve Meltem Sönmez Turan,** SASC'06, Belçika, 2-3 Şubat 2006
- **Melek D. Yücel, Selçuk Kavut, Baha Güçlü Dündar ve Faruk Göloğlu,** BFCA'06, Rouen-Fransa, 13-15 Mart 2006.
- **Ersan Akyıldız ve Emrah Çakçak**, Antalya Algebra Days VIII, Antalya , 17-21 Mayıs 2006.
- **Ersan Akyıldız,** EUROCRYPT'06, Rusya, 28 Mayıs-1 Haziran 2006.
- **Fatih Sulak ve Meltem Sönmez Turan,** 5. İstatistik Günleri Sempozyumu (İGS'06), Antalya, 24-27 Mayıs 2006.
- **Zülfükar Saygı ve Murat Cenk,** The 26th Annual International Cryptology Conference, Amerika 20-24 Ağustos 2006.
- **Ersan Akyıldız, Melek Yücel ve Selçuk Kavut,** Indocrypt 2006, Kalkuta-Hindistan 11-13 Aralık 2006.

- **Ersan Akyıldız,** Asiacrypt 2006, Shanghai Çin, 3-7 Aralık 2006.
- **Rüyal Ergül, Turgut Hanoymak, B. Bülent Kırlar, Canan Çimen, İlksen Acunalp, Pelin Erdem, Çağdaş Çalık, Zaliha Yüce, Meltem Sönmaz Turan, Elif Saygı, Zülfükar Saygı, Oğuz Yayla, Murat Cenk, Atilla Bektaş, A. Kadir Altan, Mert Özarar, Sedat Akleylek,** 1. Ulusal E-imza Sempozyumu, Sheraton-ANKARA 7-8 Aralık 2006.
- **Bülent Karasözen, Gerhard Wilhelm Weber, Pakize Taylan, Rengin Ak, Süreyya Özöğür, Başak Akteke-Öztürk, Oktay Sürücü,** 21st European Conference on Operational Research, 2-5 July, Iceland, 2006.
- **Bülent Karasözen,** The 5th Ballarat Workshop on Global and Nonsmooth Optimization, Australia, 28-30 November 2006.
- **Bülent Karasözen,** Turkish-German Summer Academy on Advanced Engineering, Kuşadası, 26 August-3 September 2006.
- **Gerhard-Wilhelm Weber,** Discrete tomography: a joint contribution by optimization theory, equivariance analysis and statistical learning, at: 1st Summer School "Achiements and Applications of Contemporay Informatics, Mathematics and Physics", Kiev, Ukraine, August 4-20, 2006.
- **Gerhard-Wilhelm Weber,** "Workshop on Global and Non-Smooth Optimization: Theory, Methods and Applications" Avustralya, 28-30 Kasım 2006.
- **Hakan. Öktem**, "International Conference of Hybrid Systems and Applications", La Fayette, Louisiana, ABD, 22-26 Mayıs 2006.
- **Bülent Karasözen,** Workshop on Advances in Continuous Optimization, 2-5 July, Iceland, 2006.
- **Bülent Karasözen,** EURO Summer Institute, "Optimization Challenges in Engineering, Wittenberg Germany, August 2006.
- **Bülent Karasözen, Gerhard-Wilhelm Weber**, Workshop on Networks in Computational Biology, METU-Institute of Applied Mathematics, 10-12 September, 2006.
- **Hayri Körezlioğlu, Azize Hayfavi, Gül Ergün, Kasırga Yıldırak, Ömür Uğur**, **Gerhard Wilhelm Weber, Pakize Taylan, Rengin Ak, Oktay Sürücü,Yeliz Yolcu, Ayşegül İşcanoğlu, Zehra Ekşi, İrem Yıldırım, Sühan Altay, Serkan Zeytun, K. Korhan Nazlıben, Şirzat Çetinkaya, Halil Artam, Nilüfer Çalışkan, Özge Sezgin,** First Conferans of Advanced Mathematical Methods for Finance (AMAMEF), Workshop On Risk Analysis & Management, Antalya, 23-25 Nisan 2006.
- **Hayri Körezlioğlu, Azize Hayfavi, Gül Ergün, Kasırga Yıldırak, Ömür Uğur**, **Gerhard Wilhelm Weber, Pakize Taylan, Rengin Ak, Oktay Sürücü,Yeliz Yolcu, Ayşegül İşcanoğlu, Zehra Ekşi, İrem Yıldırım, Sühan Altay, Serkan Zeytun, K. Korhan Nazlıben, Şirzat Çetinkaya, Halil Artam, Nilüfer Çalışkan, Özge Sezgin,** First Conferans of Advanced Mathematical Methods for Finance (AMAMEF), Antalya, 26-29 Nisan 2006.
- **Kasırga Yıldırak**, "2. International Conference on Business, Management and Economics" Çeşme, 15-18 Haziran 2006.

EKLER

EK: 1
IAM PREPRINT SERİSİ

IAM PREPRINT SERIES

No	Title - Abstract	Author	Date
48	Memorization in Neutrally Stable Circuits Involving Delay	H. Öktem	01.25.2006
49	Derivative Free Optimization Methods for Optimizing Stirrer Configurations	Ö.Uğur, B. Karasözen, M. Schafer, K. Yapıcı	01.25.2006
50	Operational Research Meets Biology:An Algorithmic Approach to Analyze Genetic Networks and Biological Energy Production	Ö. Uğur, S. W. Pickl , G.-W. Weber , R. Wünschiers	02.08.2006
51	Almost periodic solutions of differential equations with piecewise constant argument of generalized type	M.U.Akhmet	03.07.2006
52	New Approaches to Regression in Financial Mathematics by Generalized Additive Models	P. Taylan, G.W. Weber	04.14.2006
53	On Generalized Semi-Infinite Optimization of Genetic Networks	G.W. Weber, A. Tezel	04.23.2006
54	Discrete gradient method: a derivative free method for nonsmooth optimization	A. M. Bagirov, B. Karasözen, M. Sezer	01.05.2006
55	On Dynamics of Optimization of Gene-Environment Networks	G.-W. Weber, A. Tezel, P. Taylan, A. Soyler, M. Çetin	09.01.2006
56	New Approaches to Regression by Generalized Additive Models and Continuous Optimization for Modern Applications in Finance, Science and Techology	P. Taylan, G.-W. Weber, A. Beck	09.14.2006
57	Optimization and Dynamics of Gene-Environment Networks with Intervals	Ö. Uğur, G.-W. Weber	09.21.2006
58	Survey of Trust-Region Derivative Free Optimization Methods	B. Karasözen	09.29.2006
59	Stability of differential equations with piecewise constant arguments of generalized type	M.U.Akhmet	10.02.2006
60	On the reduction principle for differential equations with piecewise constant argument of generalized type	M.U.Akhmet	10.02.2006
61	Numerical Investigation of the Effect of the Rushton Type Turbine Design Factors on Agitated Tank Flow Characteristics	K. Yapici, B. Karasozen, M. Schäfer, Y. Uludag	10.02.2006
62	Some Extensions To Creditrisk+: Fft, Fft-Panjer And Poisson-Inar Process	K. K. Nazlıben -K. Yıldırak	12.06.2006
63	Optimizing Gene-Environment Networks:Generalized Semi-Infinite Programming Approach With Intervals	G.-W. Weber, Ö.Uğur	12.06.2006
64	Optimization of Gene-Environment Networks in the Presence of Errors and Uncertainty with Chebychev Approximation	G.-W.Weber, P.Taylan, Z.Alparslan-Gök, S.Özöğür, B. Akteke-Öztürk	12.06.2006
65	A Survey and Results on Semidefinite and Nonsmooth Optimization for Minimum Sum of Squared Distances Problem	G.-W. Weber-B. Akteke-Öztürk	12.06.2006

EK: 2
UME SEMİNERLERİ

Genel Seminerler

The Laplace Transform on Time Scales	**Gusein Sh. Guseinov** (Atılım University)	19 12 2006
Adaptive Finite Element Methods for Control Constrained Distributed and Boundary Control Problems	**Ronald H. W. Hoppe** (Dept. of Math., Univ. of Houston)	12 12 2006
A Variational Characterization of the Largest Eigenvalue of a Matrix with Positive Entries	**Devin Sezer** **(**UME**)**	31 10 2006
From Biological Reserves to Political Districting: What Mathematicians Can Offer in Spatial Design	**Hayri Önal** **(**Univ. of Illinois at Urabana-Champaign**)**	10 10 2006
Optimization Problems wıth infinitely many constraints	**George Stil** (University of Twente)	03 10 2006
Extensions of hybrid encryption to the identity-based and certificateless settings	**Pooya Farshim** (University of Bristol / United Kingdom)	10 07 2006
A New Key Exchange Primitive	**Yeşem Kurt** (Dept. of Math., Indiana Univ.)	20 06 2006
Bounds for Quantile-Based Measures of Dependent Risks' Functions	**N. Kolev and M. Fernandes** (Department of Statistics, University of Sao Paulo)	14 06 2006
Bivariate Density Classification by the Geometry of Marginals	**N. Kolev and M. Fernandes** (Department of Statistics, University of Sao Paulo)	13 06 2006
What did game theory wait for more than a century?	**Koray Semih** (Bilkent Univ)	16 05 2006
Function Sharing Schemes based on the Chinese Remainder Theorem	**Ali Aydın Selçuk** (Department of Computer Engineering, Bilkent University)	09 05 2006
Mathematical Analysis of Melodies (Songs)	**Güngör Gündüz** (Department of Chemical Engineering)	02 05 2006
Patterns on Plants, Phyllotaxis and Fibonacci Sequences	**Alan C. Newell** (The University of Arizona, USA)	18 04 2006
Renormalization Group Methods in Applied Mathematics Problems	**Hüseyin Merdan** (TOBB ETU)	11 04 2006
An Introduction to Infinite Dimensional Neural Networks	**M. Kemal Leblebicioğlu** (Electrical and Electronics Engineering)	04 04 2006
Necessary Conditions on Balanced Boolean Functions with Maximum Nonlinearity	**Faruk Göloğlu** (UME)	28 03 2006
How much mathematics can be loaded into a Smart Card chip	**Emrah Çakçak** (UME)	14 03 2006
Managing solvency risk: ruin and reinsurance	**Gray, Roger JWatt** (University, Edinburgh, UK)	28 02 2006
Portfolio Management by Artificial Intelligence : A real life application on Istanbul Stock Exchange	**Ali Veysoglu** (Toros Menkul Kiymetler, İstanbul)	21 02 2006
An Alternative Proof of the Fritz-John and Karush-Kuhn-Tucker Conditions in Nonlinear Optimization	**S. İlker Birbil** (Sabancı Univ.)	17 02 2006

HESAPLAMALI BİYOLOJİ VE TIP ARAŞTIRMA GRUBU SEMİNERLERİ

LFM-Pro: A Tool for Detecting Significant Local Structural Sites in Proteins	**Ahmet Saçan** (Computer Engineering)	22.12.2006
Subsequence based feature map for protein function annotation	**Sinan Saraç** (Computer Engineering)	15.12.2006
Semidefinite and Nonsmooth Optimization for Minimum Sum of Squared Distances Problem	**Başak Akteke-Öztürk** (UME)	08.12.2006
On cryptographic smart cards in security mechanisms	**Mert Özarar** (UME)	01.12.2006
Level Set Methods for Identifying Solvent Excluded Surfaces of Proteins -	**Tolga Can** (Computer Engineering)	24.11.2006
Yield Curve Prediction	**Kasırga Yıldırak** (Trakya Univ./UME)	20.11.2006
Biological Data Mining by Using SVM and Pattern Analysis – Prediction of Eukoryatic Pro-Peptide Cleavage Sites	**Süreyya Özöğür** (UME) with **John Shawe-Taylor** (College University), **Z. Begüm Ögel**(Food Engineering), **Volkan Atalay** (Computer Engineering), **Gerhard-Wilhelm Weber** (UME)	10.11.2006
Mysteries of Adaptation in Filamentous Monsters	**Betül Söyler** (Food Engineering)	03.11.2006
Rare event simulation with importance sampling	**Devin Sezer** (UME)	27.10.2006
New Approaches to Regression by Generalized Additive Models and Continuous Optimization for Modern Applications in Science, Finance and Technology	**Pakize Taylan & G.Wilhelm Weber** (Dicle University&UME)	20.10.2006
Small-world Properties of a Probabilistic Functional Gene Network	**Mehmet Çetin** (Biological Sciences)	13.10.2006
Optimum Dewatering of an Excavation Site	**Halil Önder & A. Burcu Altan Sakarya** (Civil Engineering)	06.10.2006
Language Replacement Related Admixture in Anatolia	**Ceren Caner Berkman** (Biological Sciences)	29.09.2006
Gene-Environment Networks: Discrete-Continuous and Generalized Semi-Infinite Optimization Used for Modeling with Intervals	**G. Wilhelm Weber & Ömür Uğur** (UME)	22.09.2006
Workshop on Networks in Computational Biology		10 -12.09.2006
General Meeting of Balaban Valley Group on improving living conditions on Turkish rural countryside		15.06.2006
General Project Meeting of Balaban Valley Group on Traffic		25.05.2006
General Project Meeting of Balaban Valley Group		17.05.2006
Some Remarks on Energy Management and Sustainable Development	**G. Wilhelm Weber & Zeynep Alparslan** (UME)	12.05.2006
Disaster Traffic Management: Mathematical Modeling of Evacuation Strategies and Solution Approaches	**Hediye Tüydeş** (Civil Engineering)	01.05.2006
Short Tutorial on Support Vector Machines(SVM) with Their Modern Applications	**Süreyya Özöğür** (UME)	28.04.2006
A new Methodology for Evaluating Coastal Scenery: Fuzzy Logic Systems	**Ayşen Ergin** (Civil Engineering)	21.04.2006
Medicinal plants and their antioxidant activities	**A. Gülçin Sağdıçoğlu Celep** (Biochemistry)	14.04.2006
Discrete Tomography: A New Research Area in Modern OR	**G. Wilhelm Weber** (UME)	07.04.2006
Generative Versus Discriminative Methods for Object Recognition	**İlkay Ulusoy** (Electrical and Electronics Engineering)	24.03.2006
Analysis of pulsed pump-and-treat remediation using optimization-simulation method	**Ayşegül Aksoy** (Environmental Engineering)	20.03.2006

In Silico Analysis for Transcription Factors with $Zn(II)_2C_6$ Binuclear Cluster DNA-binding Domains in Aspergillus fumigatus and Aspergillus nidulans	**Alper Söyler** (Food Engineering)	10. 03. 2006
Survey on neuroimaging: Current practices in the analysis of MR and fMR images to unveil the structure and function of the brain	**Didem Gökçay** (Informatics Institute)	03.03.2006
Optimization of Metabolic Networks	**Süreyya Özöğür** (UME)	24.02.2006
An Alternative Proof of the Fritz-John and Karush-Kuhn-Tucker Conditions in Nonlinear Optimization	**S. İlker Birbil** (Sabancı University)	17.02.2006
An Introduction Into Metabolic Networks	**Süreyya Özöğür** (UME)	10.02.2006
HMM-based Subsequence Feature Map for Proteome Classification	**Sinan Saraç** (Computer Engineering)	20. 01. 2006
Construction and Analysis of Genome-Wide Protein Networks	**Tolga Can** (Computer Engineering)	06. 01. 2006

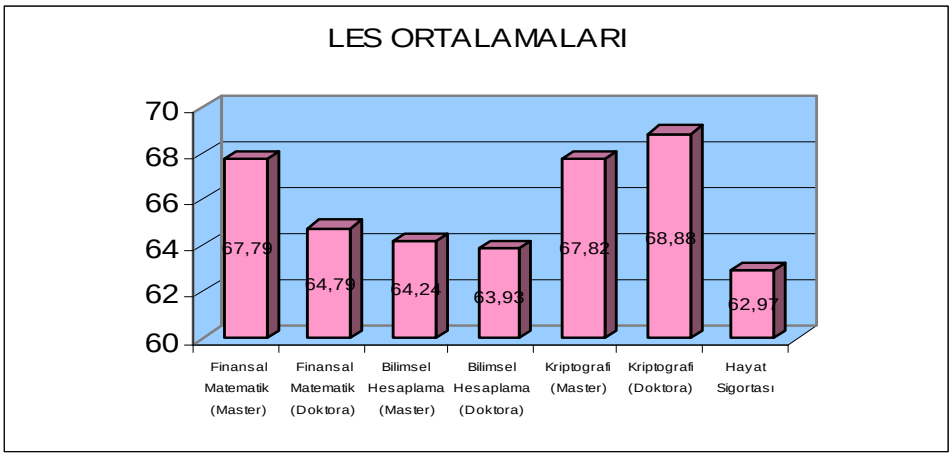
EK: 3
EĞİTİM VE ÖĞRENCİ İSTATİSTİKLERİ

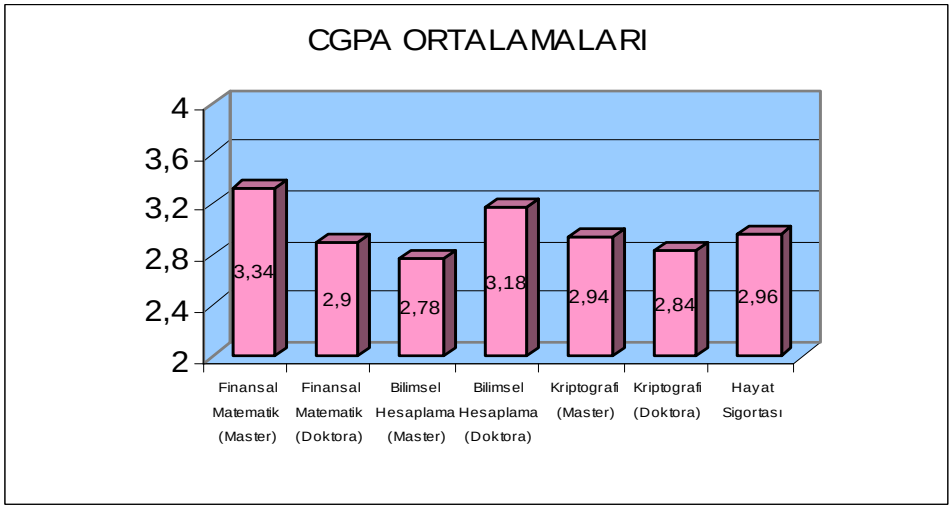
BAŞVURULAR

	2006-2007 I. Dönem		
	BAŞVURU	**KABUL**	**KAYIT**
Bilimsel Hesaplama	14	10	8
Finansal Matematik	49	36	18
Hayat Sigortası	15	15	7
Kriptografi	46	28	17
Toplam	124	89 (72%)	50 (40%)

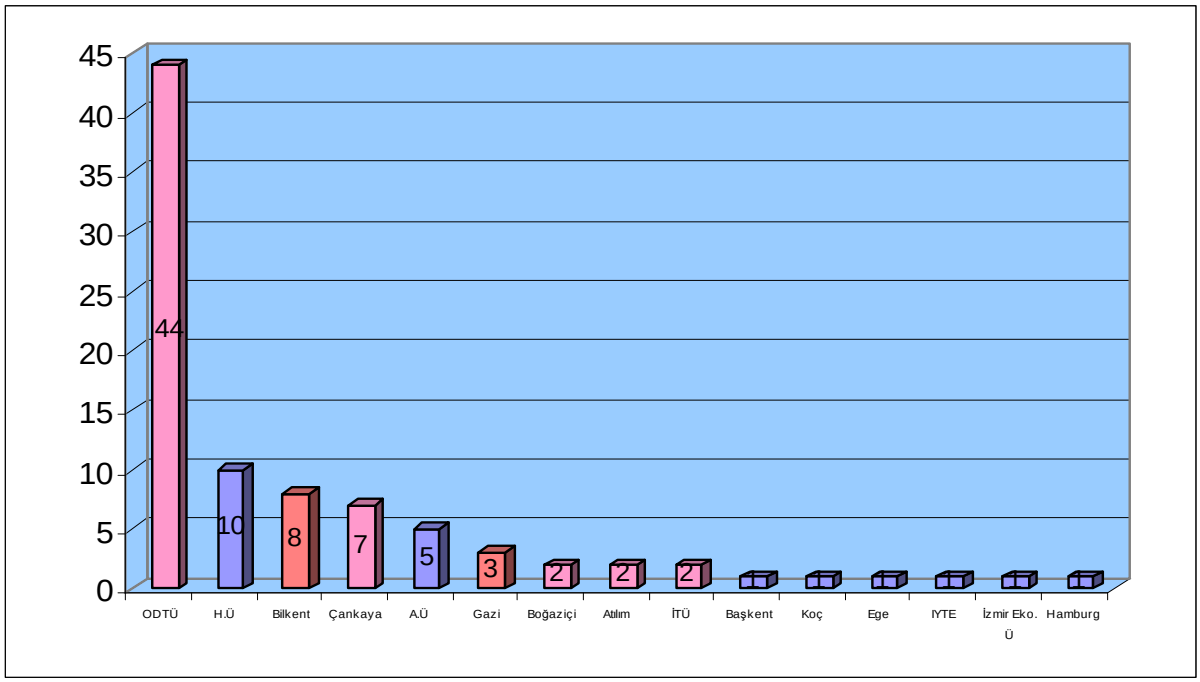
UME ÖĞRENCİLERİNİN LES VE CGPA ORTALAMALARI

2006-2007 I. DÖNEM KABUL EDİLEN ÖĞRENCİLER





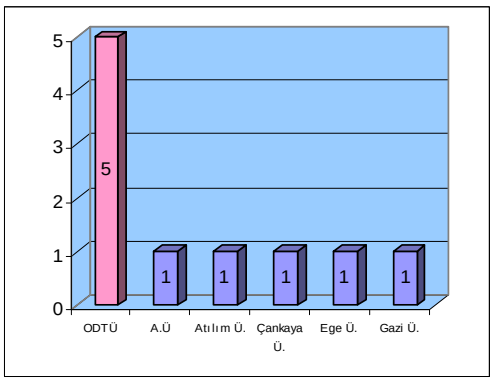
UME'YE KABUL EDİLEN ÖĞRENCİLERİN MEZUN OLDUKLARI ÜNİVERSİTELERE GÖRE DAĞILIMI



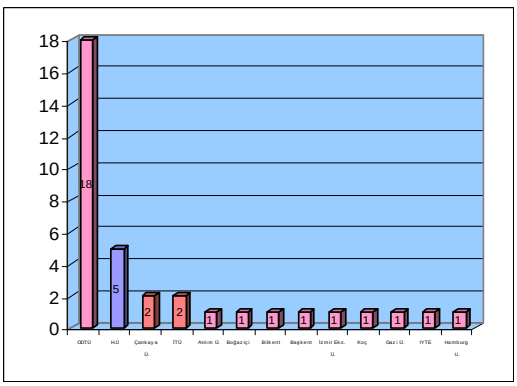
UME'YE KABUL EDİLEN ÖĞRENCİLERİN LİSANS DERECESİNİ ALDIKLARI ÜNİVERSİTELER

2006-2007 I. DÖNEM

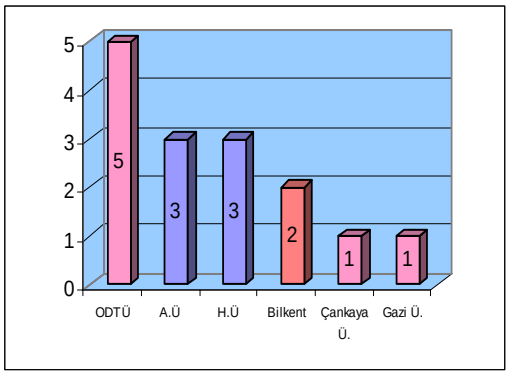
BİLİMSEL HESAPLAMA



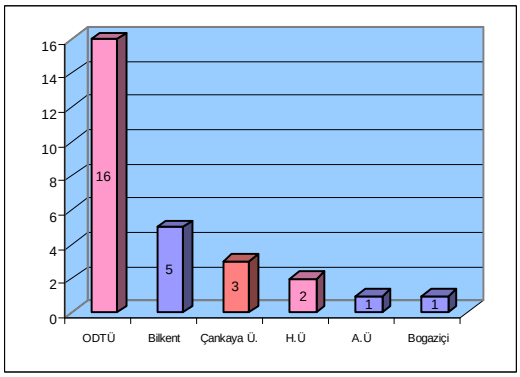
FİNANSAL MATEMATİK



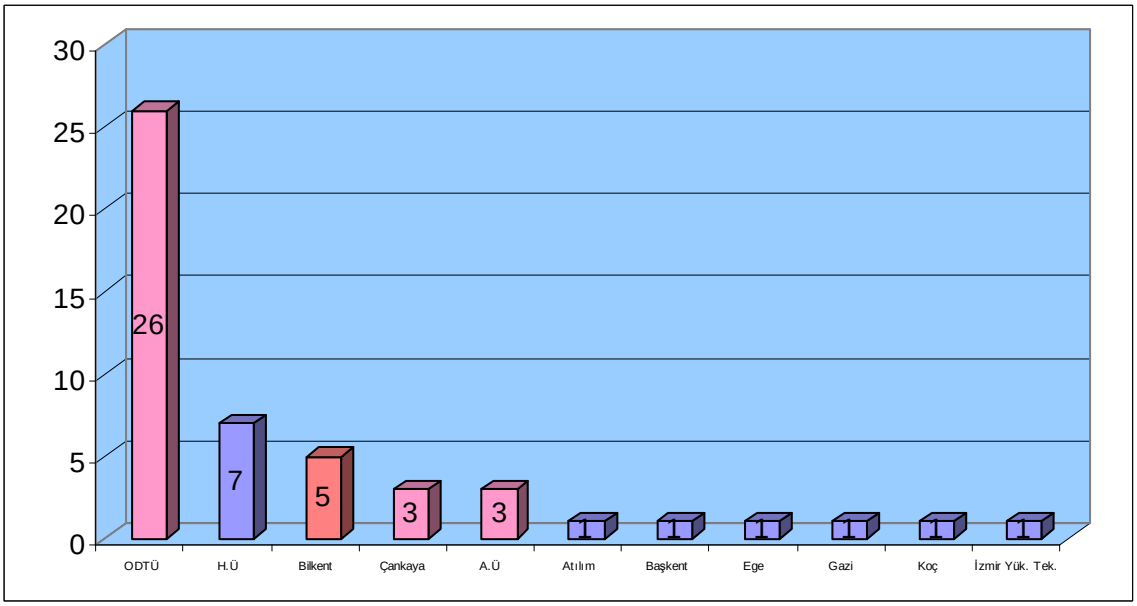
HAYAT SİGORTASI



KRİPTOGRAFİ



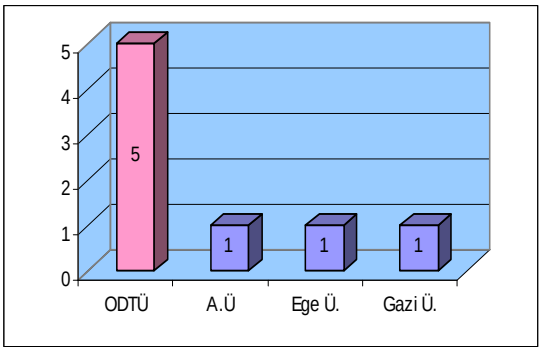
UME'YE KAYIT YAPTIRAN ÖĞRENCİLERİN MEZUN OLDUKLARI ÜNİVERSİTELERE GÖRE DAĞILIMI



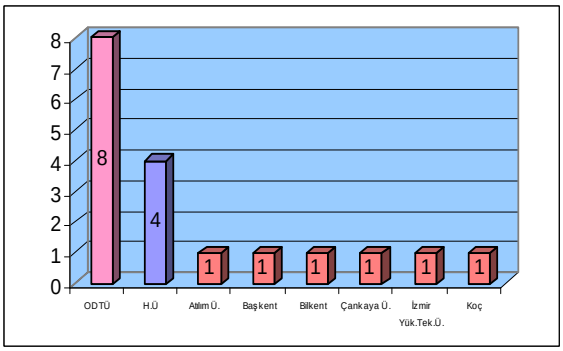
UME'YE KAYIT YAPTIRAN ÖĞRENCİLERİN LİSANS DERECESİNİ ALDIKLARI ÜNİVERSİTELER

2006-2007 I. DÖNEM

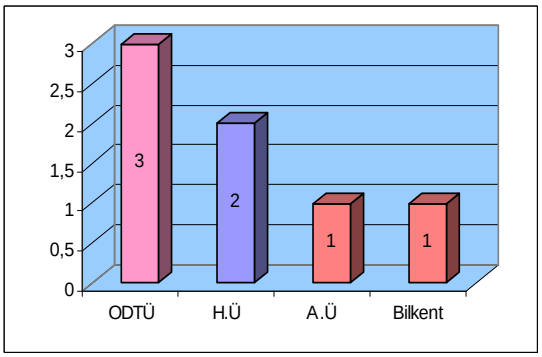
BİLİMSEL HESAPLAMA



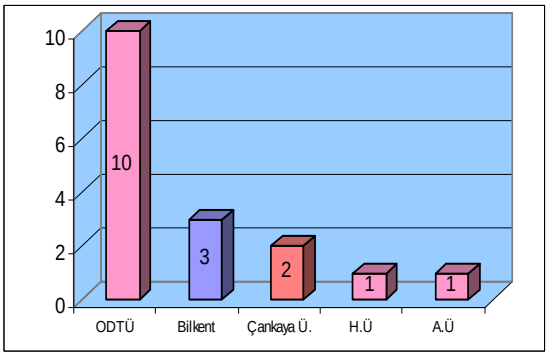
FİNANSAL MATEMATİK



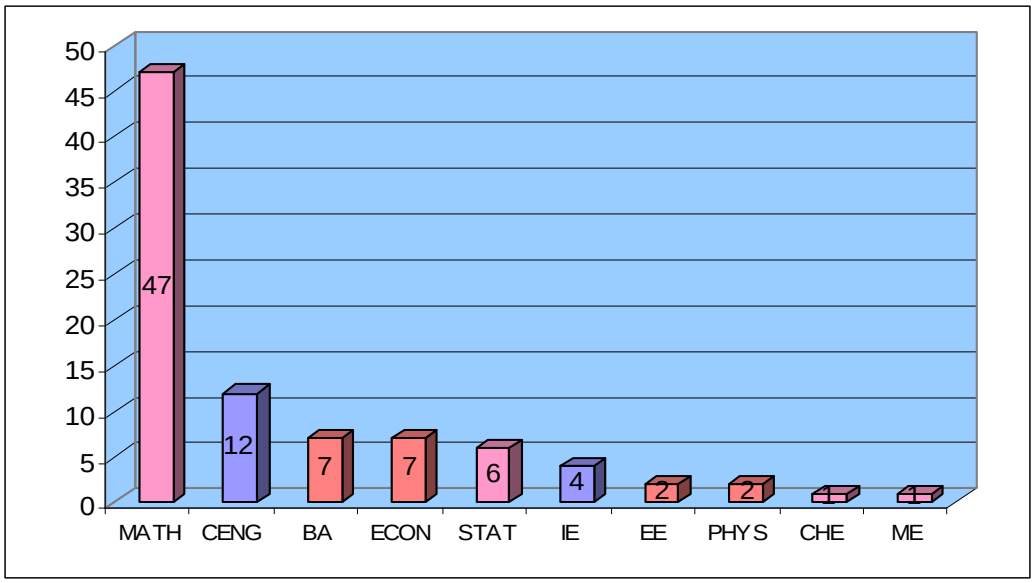
HAYAT SİGORTASI



KRİPTOGRAFİ



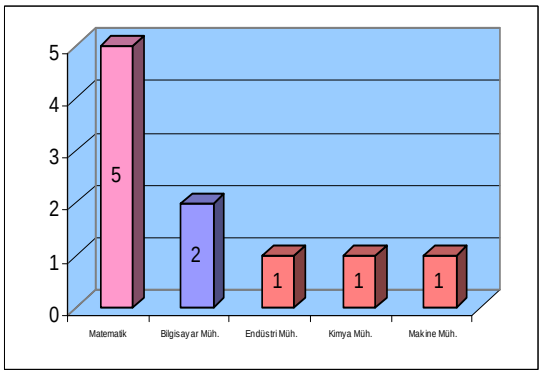
UME'YE KABUL EDİLEN ÖĞRENCİLERİN MEZUN OLDUKLARI BÖLÜMLERE GÖRE DAĞILIMI



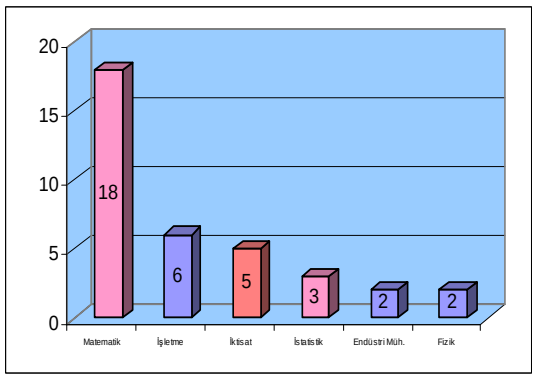
UME'YE KABUL EDİLEN ÖĞRENCİLERİN LİSANS DERECELERİNİ ALDIKLARI BÖLÜMLER

2006-2007 I. DÖNEM

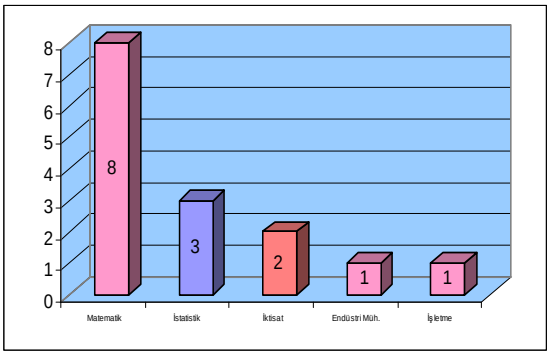
BİLİMSEL HESAPLAMA



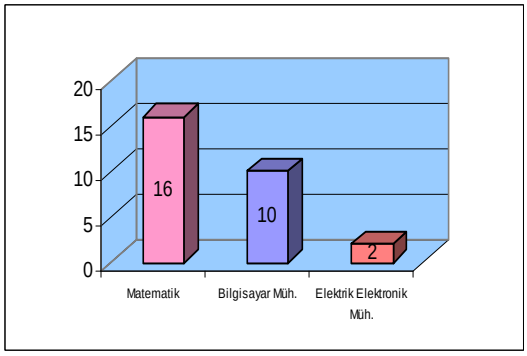
FİNANSAL MATEMATİK



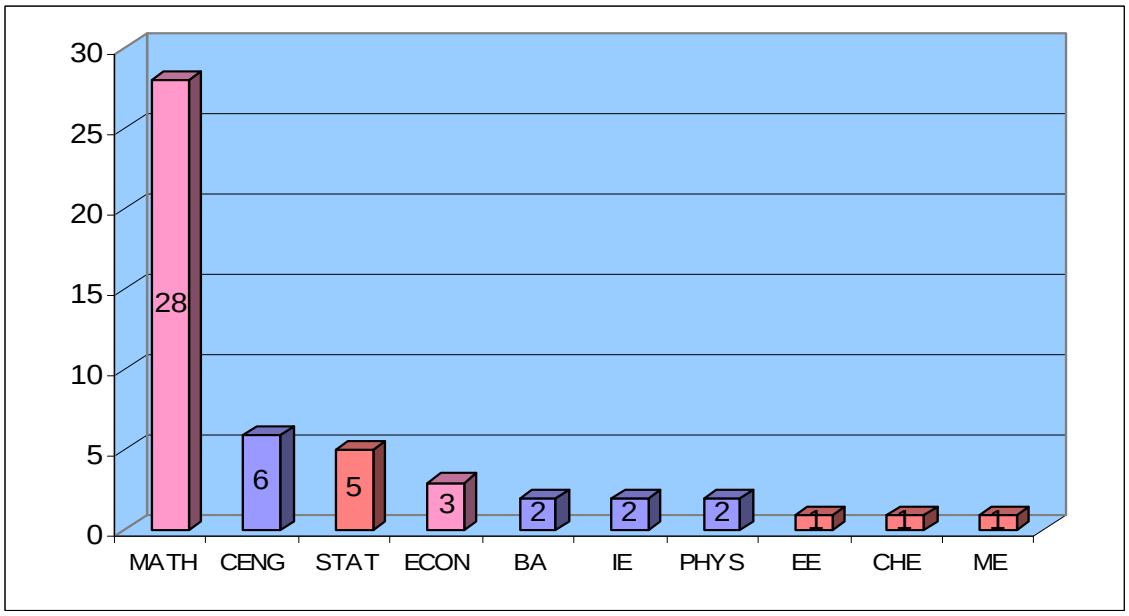
HAYAT SİGORTASI



KRİPTOGRAFİ



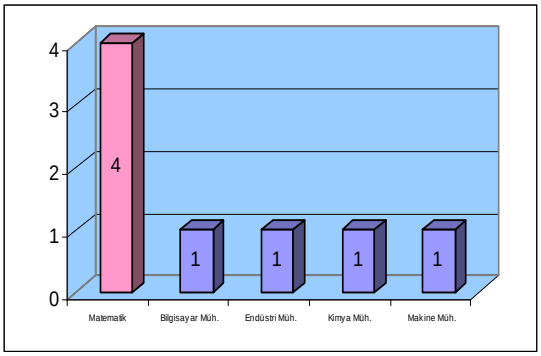
UME'YE KAYIT YAPTIRAN ÖĞRENCİLERİN MEZUN OLDUKLARI BÖLÜMLERE GÖRE DAĞILIMI



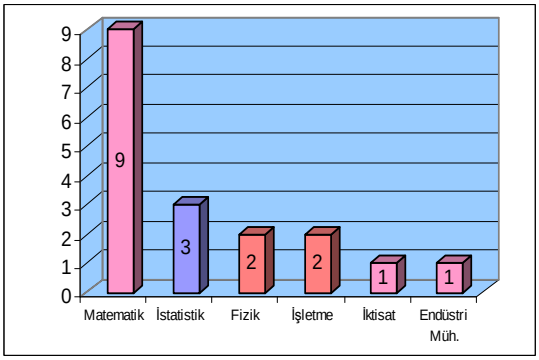
UME'YE KAYIT YAPTIRAN ÖĞRENCİLERİN LİSANS DERECELERİNİ ALDIKLARI BÖLÜMLER

2006-2007 I. DÖNEM

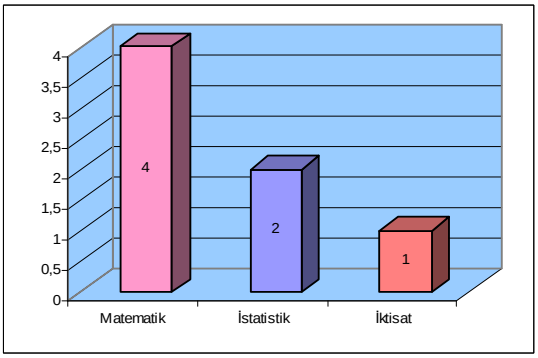
BİLİMSEL HESAPLAMA



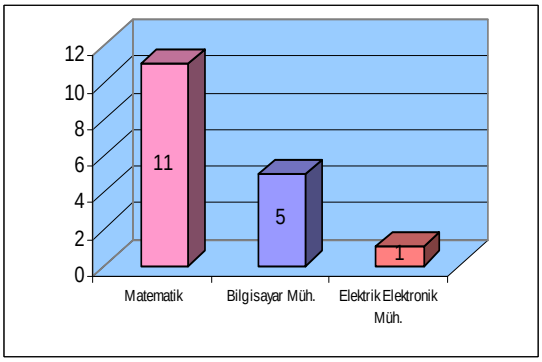
FİNANSAL MATEMATİK



HAYATSİGORTASI

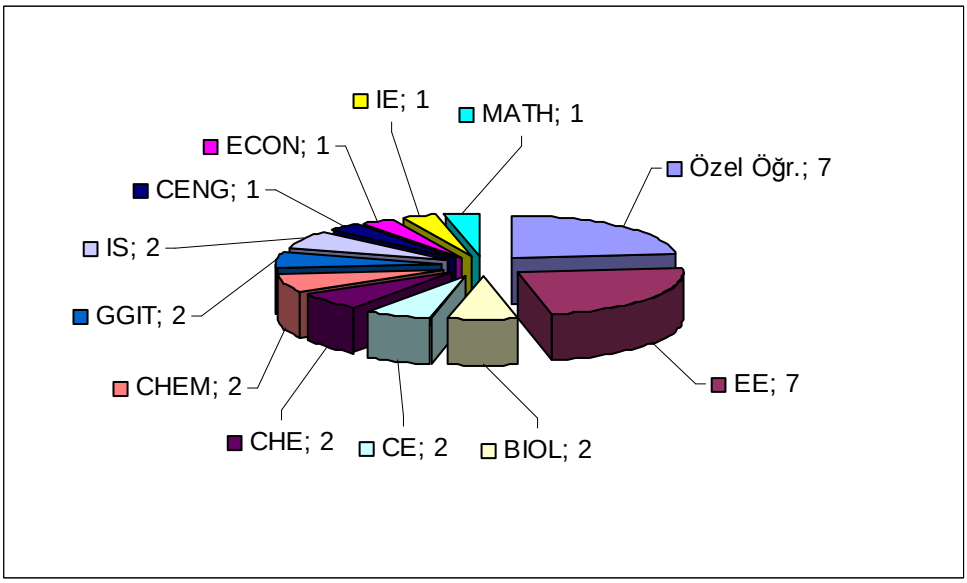


KRİPTOGRAFİ



UME DERSLERİNİ ALAN UME DIŞI ÖĞRENCİLERİN BÖLÜMLERE GÖRE DAĞILIMI

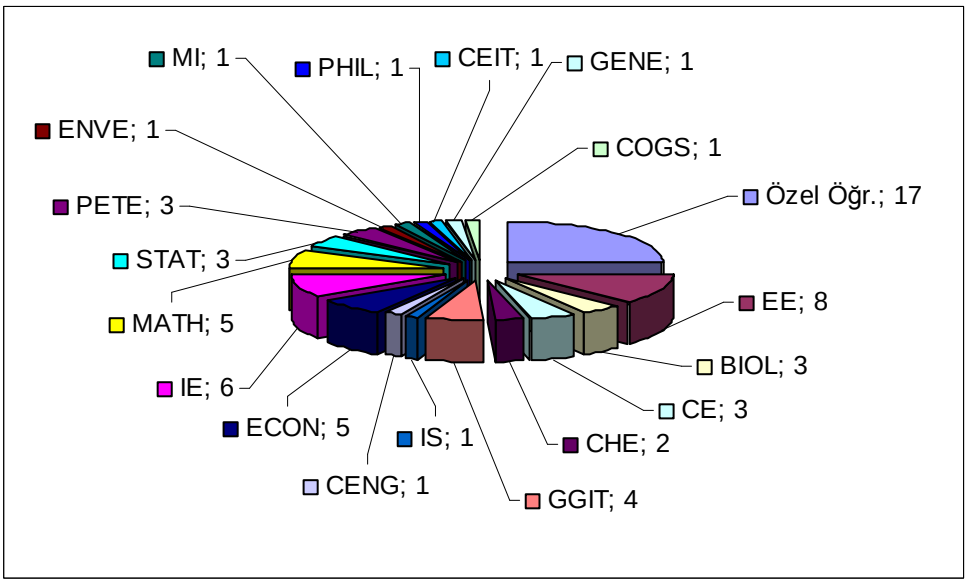
2005-2006 II.Dönem



Toplam Öğrenci Sayısı = 182

UME Dışı Öğrenci Sayısı = 30 (17%)

2006-2007 I.Dönem

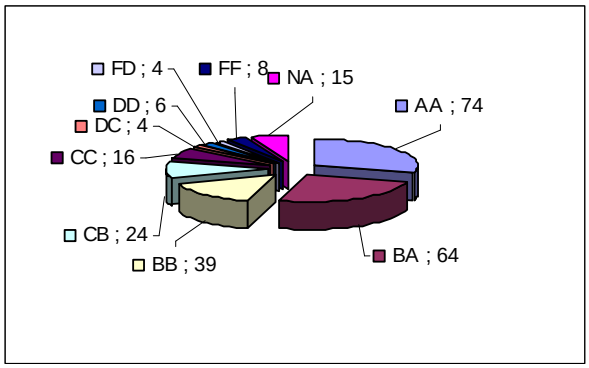


Toplam Öğrenci Sayısı = 302

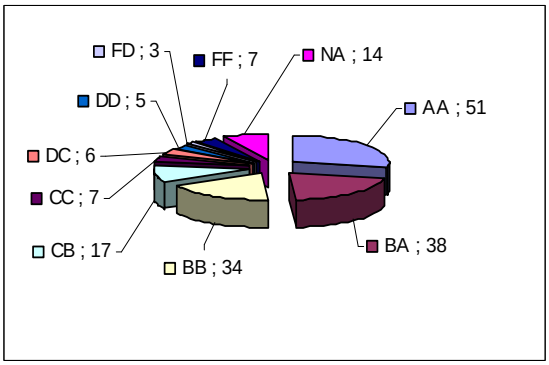
UME Dışı Öğrenci Sayısı = 67 (22%)

DÖNEMSEL VERİLEN TOPLAM NOT SAYISI

2005-2006 I. Dönem



2005-2006 II. Dönem



EK: 4
2006 YILINDA MEZUN OLAN ÖĞRENCİLER

Kriptografi Programı

***Özkan Boztaş**	"Differential Cryptanalysis and Linear Cryptanalysis of Block Ciphers" (Bitirme Projesi)	**Ali Doğanaksoy**
Recep Doğan Ersöz	"Crypxor - A Stream Cipher Based Encryption and RSA Based Digital Signature Generation and Verification Tool" (Bitirme Projesi)	**Ali Doğanaksoy**
Abdullah Öner	"RSA Key Supplier and Test Application" (Bitirme Projesi)	**Ersan Akyıldız**
Burçin Eröcal	"Algebraic Cryptanalysis of Stream Ciphers" (Y. Lisans Tezi)	**Ferruh Özbudak**
***Oğuz Yayla**	"Scalar Multiplication on Elliptic Curves" (Y. Lisans Tezi)	**Ersan Akyıldız**
***Çağdaş Çalık**	"How To Invert One-Way Functions : Time-Memory Trade-Off" (Y. Lisans Tezi)	**Ali Doğanaksoy**

Finansal Matematik Programı

Halil Artam	**"**Term Structure Of Government Bond Yields: A Macro-Fınance Approach" (Y. Lisans Tezi)	**Kasırga Yıldırak**
***Özge Sezgin**	"Statictical Methods in Credit Rating" (Y. Lisans Tezi)	**Kasırga Yıldırak**
***Sibel Korkmaz**	"Dynamic Coherent Risk Measures" (Bitirme Projesi)	**Hayri Körezlioğlu**
***K. Korhan Nazlıben**	"Some extensions to creditrisk+: fft,Fft-panjer and poisson-inar process" (Y. Lisans Tezi)	**Hayri Körezlioğlu**
***Nilüfer Çalışkan**	"Asset Pricing Models: Stochastic Volatility and Information-based Approaches" (Y. Lisans Tezi)	**Azize Hayfavi**
***Şirzat Çetinkaya**	"Valuation of Life Insurance Contracts According To Stochastic Mortality Rate And Risk Process Modeling" (Y. Lisans Tezi)	**Azize Hayfavi**
Seda Üngör	"Mean Variance Model For Gold Price Per Ounce With U.S Dollar,Yen, South African Rand Currencies" (Bitirme Projesi)	**Coşkun Küçüközmen**

***** Enstitümüzde doktoraya devam eden öğrenciler

Bilimsel Hesaplama Programı

***Derya Altıntan**	"Population Dynamics and Impulsive Differential Equations" (Y. Lisans Tezi)	**Marad Akhmetov**
***İsa Baki**	"Yield Curve Estimation by Spline-Based Models" (Y. Lisans Tezi)	**Tanıl Ergenç**

Hayat Sigortası Programı

Tolga Aktürk	"Tourism Demand for Turkey: Models, Analysis and Results" (Bitirme Projesi)	**Coşkun Küçüközmen**
Fatma Gaye Başaran	"The Relationship Between Market Beta and Financial Performances of Companies in Textile Sector" (Bitirme Projesi)	**Coşkun Küçüközmen**
Başak Çakar	"The Impacts of Macroeconomic Variables on Stock Returns" (Bitirme Projesi)	**Seza Danışoğlu Rhoades**
Utku Bora Geyikçi	"The Effects of Financial Liberalization on Stock Markets in Emerging Markets" (Bitirme Projesi)	**Coşkun Küçüközmen**
Ebru Elif Gökçek	"Determinants of Individual Ratings: A Multivariate Statistical Analysis" (Bitirme Projesi)	**Coşkun Küçüközmen**
Ayşe Kısacık	"High Volatility, Heavy Tails And Extreme Values in Value At Risk Estimation" (Bitirme Projesi)	**Sevtap Kestel**

***** Enstitümüzde doktoraya devam eden öğrenciler

EK: 5
YENİ AÇILAN DERSLER

2005–2006 Güz Dönemi

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Implementation Issues in Cryptography**
Course Code:	**IAM 710**
Credit:	**(3-0) 3**
Instructor's Name:	Emrah Çakçak (cakcak@metu.edu.tr , Ferruh Özbudak (ozbudak@metu.edu.tr)
Prerequisites:	Consent of the department
Content:	Design Criteria and Implementation Issues in Symmetric Key and Public Key Cryptosystems. Key Management, Validation and related issues.
Aims:	The aim of this course is to introduce to the students the practical side of designing cryptographic systems and algorithms, their design and implementation issues.It is also aimed to bring together the students and the people from the industry who are implementing these cryptosystems.
Learning Outcomes:	How to design and implement a cryptosystem and the difficulties encountered during the implementation processes.
Suggested Textbooks:	A number of references and lecture notes will be available.
Outline:	1. Applications of Symmetric Key Cryptosystems (1 week). 2. Designing Stream Cipher Cryptosystems (2 weeks): i) Statistical Tests, NIST criteria, side channel attacks, ii) Implementation constraints: time constraints, hardware and software constraints. 3. Implementations of Block Cipher Algorithms (2 weeks): a. Software implementations, b. Hardware implementations, Examples. 4. Applications of Public Key Cryptosystems and Key Distribution Methods (2 weeks): Authentication, Verification and Digital Signatures, i) Most popular protocols, ii) RSA vs. Elliptic Curve Cryptosystems, iii) Key Distribution Methods. 5. Design Criteria and Implementation Issues of RSA Based Cryptosystems (2 weeks): i) Design Criteria , ii) Random Number Generators and Primality Tests, iii) Software implementations, open source libraries, iv) Hardware implementations, v) Side channel attacks. 6. Design Criteria and Implementation Issues of Elliptic Curve Based Cryptosystems (4 Weeks): i) Design Criteria, ii) Arithmetic on Finite Fields of characteristic 2, iii) Arithmetic on Finite Fields of prime order, iv) Arithmetic on Elliptic Curves over Finite Fields, v) Software Implementations of ECDSA, vi) Hardware Implementations, vii) Side Channel attacks. 7. Validation Issues in Cryptographic Model Validation and Cryptographic Process Validation (1 week).
Resources:	Course will be coordinated by the course coordinator. Lectures will be given by the affiliated faculty and invited lecturers from the industry and other universities.

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics: Cryptanalysis of Recent Stream Ciphers**
Course Code:	**IAM 708**
Credit:	(3-0)3
Suggested Name:	Orhun Kara **(**orhun@uekae.tubitak.gov.tr)
Prerequisites:	Consent of the instructor
Content:	We overview recent stream ciphers, mostly those submitted to eSTREAM project. We evaluate the security level of these ciphers in terms of conventional cryptanalysis methods such as linear complexity profiles, linear consistency test, period analysis, diffusion/confusion, nonlinearity and propagation properties of output functions, correlation immunity and divide and conquer type attacks.
Aims:	The aim of the course is to improve cryptanalysis skills and the skill of organization cryptanalytic experiments of the students, to understand the security level of recent stream ciphers and to exercise well presentation of results.
Outline:	WEEKS 1 Overview of stream ciphers: Stream ciphers, Key Stream Generators, synchronous vs self- synchronizing stream ciphers, LFSRs, PN sequences WEEKS 2-3 Overview of generic attacks on stream ciphers: : Divide and conquer attacks: Correlation type attakcs, guess and determine attacks: subkey guessing, linear consinstency test, resync. attacks, distinguishing attacks, trade off attacks WEEK 4-6 Cryptanalysis of LFSR based stream ciphers:e.g. WG, Sobert16/t32, Snow, SFINKS, CSCSG, Sosemanuk, DECIM: Linear complexity profiles, linear consistency test, period analysis, diffusion/confusion, nonlinearity and propagation properties of output functions, correlation immunity and divide and conquer type attacks against these ciphers. WEEK 7-8 Cryptanalysis of table look up based ciphers: e.g. RC4, Polar Bear, Py: İnitialization r properties, weak keys, symmetric group structures of tables WEEK 9-11 Cryptanalysis of block oriented ciphers and stream ciphers derived from block cipher primitives: e.g. LEX, Phelix, Salsa20, Dragon: Differantial/ linear cryptanalysis, square type attacks, nonlinearity properties of next state functions WEEK 12-14 Cryptanalysis of Nonlinear Feedback Shift Register based ciphers: e.g. Ahterbahn, Trivium, NLS, Grain: Short cycle analysis, weak keys, nonlinearity and diffusion properties of next state functions, linear approximations of registers
Suggested Textbooks:	No Textbook
Resources:	**Auxiliary:** **1.** R.A. Rueppel: Stream Ciphers, in Contemporary Cryptology: The science of Information Integrity, G.J. Simmons, Ed., IEEE Press, 1991. **2.** M.J.B.Robshaw: Stream Ciphers. Technical Report TR-701, 2.0, RSA Laboratories, July 1995. **3.** Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography. CRC Press, 1996.

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Studies: Stochastic and Deterministic Optimal Control with Applications to Finance**
Course Code:	**IAM 745**
Credit:	**(3-0)3**
Instructor's Name:	Ali Devin Sezer (devin.sezer@gmail.com)
Prerequisites:	Probability Theory, consent of the instructor
Content/Aims:	The aim of the course is to introduce the students to the field of (stochastic) optimal control. This field concerns itself with constrained optimization problems over function or measure spaces, and which have a natural dynamic interpretation to them (for example, what is shortest path between two points on a manifold?). This is a vast field with innumerable applications. Our goal is to cover some of the most salient features and ideas of stochastic optimal control problems and their solution methods. Some of these include: existence and uniqueness of minima, feedback and open loop controls, verification theorems, problems involving finite and infinite time horizons, optimal stopping problems, HJB equations and viscosity solutions. Almost exclusively we will emphasize dynamic programming as the solution method. Numerical methods to solve optimal control problems will also be emphasized throughout. Regular programming assignments will be given so that the students get a chance to implement the methods they will have learned. The first half of the course will be more pedagodic and will emphasize the discrete time and finite state space systems, which allow one to think about the important concepts without worrying about the technicalities. Gradually the course will cover systems and problems of increasing technicality. In the later weeks of the course, we will look at the applications of stochastic optimal control in mathematical finance. As time permits we may look at other material including: singular control, and stochastic games.
Learning Outcomes:	By the end of the course the student is expected to have a basic intuitive understanding of optimal control and dynamic programming. He/she will be expected to be able to approach new optimization problems and ask himself/herself `is there a stochastic optimal control structure in this problem?' or `can I approach this problem with the tools of optimal control/dynamic programming?' and then know how to start attacking the problem from this perspective if he/she feels the optimal control approach is a good fit to the problem at hand.
Suggested Textbooks:	1. Bellman, Introduction to the Mathematical Theory of Control Processes Vols I, II 2. Bertsekas, Dynamic Programming and Stochastic Control 3. Fleming and Richel, Deterministic and Stochastic Optimal Control 4. Fwu-Ranq Chang, Stochastic Optimization in Continuous time. 5. Oksendal and Sulem, Applied Stochastic Control of Jump Diffusion 6. Evans, Partial Differential Equations, 7. Soner and Fleming, Controlled Markov Processes and Viscosity Solutions
Outline:	1. A survey of classical stochastic optimal control and calculus of variations problems. 2. Basic Concepts of Control Theory 3. Discrete Control processes and Dynamic Programming 4. Numerical methods and applications in the discrete setup. 5. Optimal control in continuous time. 6. Numerical methods in continuous time. 7. More applications in finance and other fields. 8. Introduction to Viscosity solutions to the HJB equation.

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics: Spatial Optimization**
Course Code:	**IAM 761**
Credit:	**3(3-0)**
Instructor's Name:	Hayri Önal, (h-onal@uiuc.edu)
Prerequisites:	An introductory course in linear programming
Content:	**Linear Programming**, simplex method, LP duality, formulations of prototype spatial optimization problems, transportation and transshipment problems ; **General Algebraic Modeling System** (GAMS), programming basics ; **Integer programming**, Branch and bound method, formulations of prototype IP problems in spatial optimization, modeling land use and land/water conservation, facility location problem, traveling salesman problem, vehicle routing problem, set covering and maximal covering problems and their applications in spatial optimization, the basic conservation reserve design problem; **Nonlinear Programming**, Kuhn-Tucker optimality conditions, market equilibrium analysis with endogenous prices, finding multi-market multi-region (spatial) equilibria using nonlinear optimization; **Graphs and Networks,** basics of graph theory and network flows, minimum spanning trees, the Steiner tree problem, applications of graphs and networks to designing conservation reserve networks with spatial considerations, in particular designing compact reserves and reserves with minimum boundary, reserve connectivity and fragmentation.
Aims:	The course presents models and modeling techniques used for various types of spatial optimization problems and a state-of-the art algebraic modelıng language for solving optimization problems.
Learning Outcomes:	The students will learn modeling techniques to address various types spatial optimization problems faced in practice and how to program and solve optimization problems using an optimization software.
Suggested Textbooks:	Instructor's class notes and various articles published in scientific journals. A complete list of journal articles will be provided.
Outline:	Weeks 1-2: Linear Programming and Applications in Spatial Optimization Week 3: Modeling and programming with GAMS Weeks 4-6: Integer Programming and Applications in Spatial Optimization Weeks 7-8: Nonlinear Programming Applications in Spatial Optimization Weeks 9-12: Graphs and Networks, Applications in Spatial Optimization Weeks 13-14: Term paper presentations and group discussion
Resources:	MS **Bazaraa**, JJ Jarvis, and HD Sherali. Linear Programming and Network Flows. John Wiley & Sons, Chichester, 1990.

EK: 6
2006 YILINDA AÇILAN DERSLERİN LİSTESİ

2005–2006 II. Döneminde verilen dersler

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Kriptografi	IAM 502	Stream Ciphers	Emrah Çakçak	9	2	11
	IAM 504	Public Key Cryptography	Ersan Akyıldız	15	4	19
	IAM 512	Block Ciphers	Melek Yücel	13	5	18
	IAM 708	Special Topics: Cryptoanalysis of Recent Stream Ciphers	Orhun Kara	4		4
	IAM 710	Special Topics: Implementation Issues in Systems	Emrah Çakçak/F. Özbudak	13		13

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Bilimsel Hesaplama	IAM 562	Introduction to Scientific Computing II	Ömür Uğur	11	3	14
	IAM 565	Introduction to Algorithms and Complexity	Hakan Öktem	14		14
	IAM 566	Numerical Optimization	G.W. Weber/B.Karasözen	8	8	16
	IAM 570	Hybrid Systems	Hakan Öktem	3	1	4
	IAM 664	Inverse Problems	Gerhard-Wilhelm Weber	5	7	12

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Finansal Matematik	IAM 520	Financial Derivatives	Seza Danışoğlu Rhoades	22	1	23
	IAM 522	Stochastic Calculus for Finance	Azize Hayfavi	10	2	12
	IAM 524	Financial Economics	Esma Gaygısız	14		14
	IAM 526	Time Series Applied to Finance	Coşkun Küçüközmen	8		8
	IAM 583	Pension Fund Mathematics	Ömer Gebizlioğlu	4		4
	IAM 612	Financial Modeling with Jump Processes	Hayri Körezlioğlu	2	1	3

2006–2007 I. Döneminde verilen dersler

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Kriptografi	IAM 501	Introduction to Cryptography	Ali Doğanaksoy	19	6	25
	IAM 503	Applications of Finite Fields	Emrah Çakçak	21	1	22
	IAM 505	Elliptic Curves in Cryptography	Ersan Akyıldız	19	-	19
	IAM 519	Basic Mathematics for Cryptography	Abdürrahim Yılmaz	2	-	2
	IAM 530	Elements of Statistics and Probability	Gül Ergün	34	-	34
	IAM 701	Cryptological Characteristics of Boolean Function and S-Boxes	Melek Yücel	11	-	11
	IAM 705	Stream Cipher Cryptanalysis	Orhun Kara	4	-	4

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Bilimsel Hesaplama	IAM 529	Applied Nonlinear Dynamics	Ömür Uğur	2	4	6
	IAM 557	Statistical Learning and Simulation	G.W.Weber	8	11	19
	IAM 561	Introduction to Scientific Computing I	Ömür Uğur	11	7	18
	IAM 564	Basic Algorithms and Programming	Hakan Öktem	2	3	5
	IAM 567	Mathematical Modelling	Hakan Öktem G.W.Weber	8	9	17
	IAM 569	Wavelets, Transform Domain and Multiresolution Techniques	Hakan Öktem	5	1	6
	IAM 665	Advanced Continuous Optimization	G. W. Weber B. Karasözen	1	-	1
	IAM 761	Special Topics: Networks and Graphs	Hayri Önal	-	7	7

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Finansal Matematik	IAM 521	Financial Management	Seza Danışoğlu	22	5	27
	IAM 526	Time Series Applied to Finance	Coşkun Küçüközmen	10	-	10
	IAM 530	Elements of Statistics and Probability	Gül Ergün	34	-	34
	IAM 541	Probability Theory	Azize Hayfavi	22	7	29
	IAM 544	Financial Risk Assessment	Kasırga Yıldırak	8	1	9
	IAM 556	Simulation	İnci Batmaz	5	2	7
	IAM 557	Statistical Learning and Simulation	G.W.Weber	8	11	19
	IAM 582	Life Insurance Mathematics	Muhammed Dabbagh	6	-	6
	IAM 584	Advanced Actuarial Mathematics	Ömer Gebizlioğlu	2	-	2
	IAM 745	Special Topics Stochastic and Deterministic Optimal Control with Applications to Finance	A.Devin Sezer	8	2	10