Öğr. Gör. Dr. MUHİDDİN UĞUZ

Kişisel Bilgiler

İş Telefonu: +90 312 210 5364
E-posta: muhid@metu.edu.tr
Web: https://avesis.metu.edu.tr/muhid
Posta Adresi: Middle East Technical University Department of Mathematics Dumlupınar Bulvarı, Universiteler mahallesi 0680 Ankara TURKİYE

Uluslararası Araştırmacı ID'leri
ORCID: 0000-0003-2344-503X
Yoksis Araştırmacı ID: 163720

Eğitim Bilgileri

Doktora, Orta Doğu Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Matematik (Dr), Türkiye 1992 - 1999

Yabancı Diller

İngilizce, C2 Ustalık

Yaptığı Tezler

Doktora, Modul space for invariant solutions of Seiberg-Witten equations, Orta Doğu Teknik Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, 1999

Araştırma Alanları

Bilgisayar Bilimleri, Cebirsel Topoloji, Diferansiyel Geometri, Genel Matematik, Genel Topoloji, Kombinatorik, Matematik Eğitimi

Akademik Unvanlar / Görevler

Öğretim Görevlisi Dr., Orta Doğu Teknik Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, 1992 - Devam Ediyor

Akademik İdari Deneyim

Orta Doğu Teknik Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, 2003 - Devam Ediyor

Verdiği Dersler

STREAM CIPHERS , Yüksek Lisans, 2018 - 2019, 2016 - 2017, 2014 - 2015, 2011 - 2012, 2010 - 2011

MATHEMATICS FOR INFORMATICS, Lisans, 2019 - 2020, 2018 - 2019
INTRODUCTION TO CRYPTOGRAPHY , Yüksek Lisans, 2019 - 2020, 2013 - 2014, 2012 - 2013, 2011 - 2012
CALCULUS OF FUNCTIONS OF SEVERAL VARIABLES , Lisans, 2018 - 2019, 2017 - 2018, 2016 - 2017, 2015 - 2016, 2014 - 2015, 2013 - 2014, 2012 - 2013, 2011 - 2012, 2010 - 2011
CALCULUS WITH ANALYTIC GEOMETRY, Lisans, 2019 - 2020, 2018 - 2019
MATHEMATICAL ASPECTS OF CRYPTOGRAPHY, Lisans, 2018 - 2019, 2016 - 2017, 2013 - 2014, 2012 - 2013
SPECIAL TOPICS:BLOCK CIPHER CRYPTANALYSIS, Doktora, 2017 - 2018
BASIC MATHEMATICS II, Lisans, 2017 - 2018, 2014 - 2015
Introduction to Probability Theory, Lisans, 2017 - 2018, 2016 - 2017
DIFFERENTIAL EQUATIONS, Lisans, 2017 - 2018
CALCULUS II , Lisans, 2016 - 2017, 2015 - 2016, 2014 - 2015, 2013 - 2014
Çok Değişkenli Analiz, Lisans, 2016 - 2017
BASIC MATHEMATICS I , Lisans, 2017 - 2018, 2014 - 2015
ELEMENTARY NUMBER THEORY I, Lisans, 2016 - 2017, 2013 - 2014, 2012 - 2013
ABSTRACT ALGEBRA, Lisans, 2015 - 2016, 2010 - 2011
CALCULUS FOR MATHEMATICS STUDENTS II, Lisans, 2011 - 2012
CALCULUS FOR MATHEMATICS STUDENTS I, Lisans, 2011 - 2012
ADVANCED CALCULUS II, Lisans, 2009 - 2010
ADVANCED CALCULUS I, Lisans, 2009 - 2010
DISCRETE MATHEMATICS, Lisans, 2008 - 2009
ANALYTIC GEOMETRY, Lisans, 2008 - 2009
INTRODUCTION TO DIFFERENTIAL EQUATIONS, Lisans, 2007 - 2008
DIFFERENTIAL GEOMETRY, Lisans, 2005 - 2006, 2000 - 2001
ADVANCED CALCULUS IN STATISTICS, Lisans, 2006 - 2007
COMPLEX CALCULUS , Lisans, 2005 - 2006, 2004 - 2005
LINEAR ALGEBRA II, Lisans, 2003 - 2004
LINEAR ALGEBRA I, Lisans, 2003 - 2004

Yönetilen Tezler

UĞUZ M., Internet voting based on homomorphic encryption, Yüksek Lisans, H.YILDIRIM(Öğrenci), 2014

Verdiği Kurs ve Eğitimler

Uğuz M., APPLIED MATHEMATICS CERTIFICATE PROGRAM (CRYPTOLOGY), 2007 - 2007

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

I. **LS-14 test suite for long sequences**
Akcengiz Z., ASLAN M., DOĞANAKSOY A., Sulak F., UĞUZ M.
Hacettepe Journal of Mathematics and Statistics, cilt.53, sa.1, ss.230-250, 2024 (SCI-Expanded)

II. **Periodic template tests: A family of statistical randomness tests for a collection of binary sequences**
SULAK F., Doganaksoy A., Uguz M., Kocak O.
DISCRETE APPLIED MATHEMATICS, cilt.271, ss.191-204, 2019 (SCI-Expanded)

III. **R-2 composition tests: a family of statistical randomness tests for a collection of binary sequences**
UĞUZ M., DOĞANAKSOY A., SULAK F., Kocak O.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, cilt.11, sa.5, ss.921-949, 2019 (SCI-Expanded)

IV. **On the independence of statistical randomness tests included in the NIST test suite**
SULAK F., UĞUZ M., Kocak O., DOĞANAKSOY A.
TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, cilt.25, sa.5, ss.3673-3683, 2017 (SCI-Expanded)

V. **Mutual correlation of NIST statistical randomness tests and comparison of their sensitivities on transformed sequences**
DOĞANAKSOY A., SULAK F., UĞUZ M., Seker O., Akcengiz Z.
TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, cilt.25, sa.2, ss.655-665, 2017 (SCI-Expanded)

VI. **New Statistical Randomness Tests Based on Length of Runs**
DOĞANAKSOY A., SULAK F., UĞUZ M., Seker O., Akcengiz Z.
MATHEMATICAL PROBLEMS IN ENGINEERING, 2015 (SCI-Expanded)

Diğer Dergilerde Yayınlanan Makaleler

I. **Graph Theoretic Approach to Randomness Test Based on the Overlapping Blocks**
UĞUZ M.
INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, cilt.12, sa.2, ss.42-52, 2023 (Hakemli Dergi)

II. **MODIFICATIONS OF KNUTH RANDOMNESS TESTS FOR INTEGER AND BINARY SEQUENCES**
Kocak O., SULAK F., DOĞANAKSOY A., UĞUZ M.
COMMUNICATIONS FACULTY OF SCIENCES UNIVERSITY OF ANKARA-SERIES A1 MATHEMATICS AND STATISTICS, cilt.67, sa.2, ss.64-81, 2018 (ESCI)

Kitap & Kitap Bölümleri

I. **Bölüm 8:KRİPTOGRAFİDE RASTGELELİK**
UĞUZ M.
BGD Siber Güvenlik ve Savunma Kitap Serisi 5 Blokzincir ve Kriptoloji, Şeref Sağıroğlu, Sedat Akleylek, Editör, NOBEL AKADEMİK YAYINCILIK EĞİTİM DANIŞMANLIK TİC. LTD. ŞTİ. SERTİFİKA NO.: 40340, Ankara, ss.311-346, 2021

II. **İşletme, İktisat, Yaşam Bilimleri ve Sosyal Bilimler için Sonlu Matematik**
DOĞANAKSOY A., UĞUZ M., SAYGI Z., SEVİNİK ADIGÜZEL R., SULAK F., ÜRTİŞ Ç.
Palme Yayıncılık, Ankara, 2017

III. **Kalkülüs II E-book, TUBITAK, 2016**
Uğuz M., Atalan F., Korkmaz B.
TUBİTAK, Ankara, 2016

IV. **Elementer Diferansiyel Denklemler ve Sınır Değer Problemleri**
ÜRTİŞ Ç., UĞUZ M.
Palme Yayınevi - Akademik Kitaplar, Ankara, 2016

V. **Tamamı ortak yazıldı**
UĞUZ M., ATALAN F., KORKMAZ B.
Kalkülüs II E-book, TUBITAK, 2016, Korkmaz Belgin, Editör, Tübitak, Ankara, ss.1, 2016

VI. **Yarışmalara Hazırlananlar İçin Çözümlü Matematik Problemleri**
DOĞANAKSOY A., SAYGI Z., SULAK F., UĞUZ M., ÜRTİŞ Ç.
OYAK, 2010

VII. **Kalkülüs Kavram ve Kapsam**
KORKMAZ B., DÖNMEZ D., KUZUCUOĞLU F., ALPAY Ö. Ş., ERGENÇ T., NURLU M. Z., ARSLAN S. F., KORKMAZ M., UĞUZ M.
TÜBA Akademik Bilimler Akademisi, Ankara, 2001

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

I. **A New Randomness Test Based on the Overlapping Blocks**
UĞUZ M., DOĞANAKSOY A., SULAK F.
Combinatorics 2016, Maratea (PZ), İtalya, 29 Mayıs - 04 Haziran 2016, ss.138

II. **Cebirsel Kriptoanaliz ve Acorn Algoritmasına Uygulanması**
Bozdemir B., SULAK F., UĞUZ M.
2018 SAVTEK 9 Savunma Teknolojileri Kongresi, Ankara, Türkiye, 30 - 29 Haziran 2018, ss.843-853

III. **A Survey of Zero Correlation Linear Cryptanalysis**
AKCENGİZ Z., UĞUZ M., SULAK F., Şahin H. A.
8th International Conference on Information Security and Cryptology, 30 - 31 Ekim 2015

IV. **A Survey on Bent Functions and Normality**
DOĞANAKSOY A., Dündar B. G., Göloğlu F., SAYGI Z., SULAK F., UĞUZ M.
2. Ulusal Kriptoloji Sempozyumu, Türkiye, 15 - 17 Aralık 2007

V. **A NOTE ON LINEARITY AND HOMOMORPHICITY**
DOĞANAKSOY A., Sağdıçoğlu S., SAYGI Z., UĞUZ M.
Boolean Functions: Cryptography, Applications, BFCA 2006, Paris, Fransa, 13 Mart 2006, cilt.387, ss.99-106

VI. **Constructions of Highly Nonlinear Balanced Boolean Functions**
DOĞANAKSOY A., Dündar B. G., Göloğlu F., SAYGI Z., SULAK F., UĞUZ M.
1. Ulusal Kriptoloji Sempozyumu, Türkiye, 18 - 20 Kasım 2005

Metrikler

Yayın: 21
Atıf (WoS): 27
Atıf (Scopus): 9
H-İndeks (WoS): 3
H-İndeks (Scopus): 2

Akademi Dışı Deneyim

MİLLİ SAVUNMA BAKANLIĞI
FAME Crypt
MİLLİ EĞİTİM BAKANLIĞI