Lect. PhD MUHİDDİN UĞUZ

Personal Information

Office Phone: +90 312 210 5364
Email: muhid@metu.edu.tr
Web: https://avesis.metu.edu.tr/muhid
Address: Middle East Technical University Department of Mathematics Dumlupınar Bulvarı, Universiteler mahallesi 06800 Ankara TURKİYE

International Researcher IDs
ORCID: 0000-0003-2344-503X
Yoksis Researcher ID: 163720

Education Information

Doctorate, Middle East Technical University, Graduate School of Natural and Applied Sciences, Matematik (Dr), Turkey 1992 - 1999

Foreign Languages

English, C2 Mastery

Dissertations

Doctorate, Modul space for invariant solutions of Seiberg-Witten equations, Middle East Technical University, Faculty of Arts and Sciences, Department of Mathematics, 1999

Research Areas

Computer Science, Algebraic Topology, Differential Geometry, General Mathematics, General Topology, Combinatorics, Mathematics Education

Academic Titles / Tasks

Lecturer PhD, Middle East Technical University, Faculty of Arts and Sciences, Department of Mathematics, 1992 - Continues

Academic and Administrative Experience

Middle East Technical University, Faculty of Arts and Sciences, Department of Mathematics, 2003 - Continues

Courses

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

Advising Theses

UĞUZ M., Internet voting based on homomorphic encryption, Postgraduate, H.YILDIRIM(Student), 2014

Taught Courses And Trainings

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

Published journal articles indexed by SCI, SSCI, and AHCI

I. **LS-14 test suite for long sequences**
Akcengiz Z., ASLAN M., DOĞANAKSOY A., Sulak F., UĞUZ M.
Hacettepe Journal of Mathematics and Statistics, vol.53, no.1, pp.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, vol.271, pp.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, vol.11,

no.5, pp.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, vol.25, no.5, pp.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, vol.25, no.2, pp.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)

Articles Published in Other Journals

I. **Graph Theoretic Approach to Randomness Test Based on the Overlapping Blocks**
UĞUZ M.
INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, vol.12, no.2, pp.42-52, 2023 (Peer-Reviewed Journal)

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, vol.67, no.2, pp.64-81, 2018 (ESCI)

Books & Book Chapters

I. **Bölüm 8:KRİPTOGRAFİDE RASTGELELİK**
UĞUZ M.
in: BGD Siber Güvenlik ve Savunma Kitap Serisi 5 Blokzincir ve Kriptoloji, Şeref Sağıroğlu, Sedat Akleylek, Editor, NOBEL AKADEMİK YAYINCILIK EĞİTİM DANIŞMANLIK TİC. LTD. ŞTİ. SERTİFİKA NO.: 40340, Ankara, pp.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.
in: Kalkülüs II E-book, TUBITAK, 2016, Korkmaz Belgin, Editor, Tübitak, Ankara, pp.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

Refereed Congress / Symposium Publications in Proceedings

I. **A New Randomness Test Based on the Overlapping Blocks**
UĞUZ M., DOĞANAKSOY A., SULAK F.
Combinatorics 2016, Maratea (PZ), Italy, 29 May - 04 June 2016, pp.138

II. **Cebirsel Kriptoanaliz ve Acorn Algoritmasına Uygulanması**
Bozdemir B., SULAK F., UĞUZ M.
2018 SAVTEK 9 Savunma Teknolojileri Kongresi, Ankara, Turkey, 30 - 29 June 2018, pp.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 October 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, Turkey, 15 - 17 December 2007

V. **A NOTE ON LINEARITY AND HOMOMORPHICITY**
DOĞANAKSOY A., Sağdıçoğlu S., SAYGI Z., UĞUZ M.
Boolean Functions: Cryptography, Applications, BFCA 2006, Paris, France, 13 March 2006, vol.387, pp.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, Turkey, 18 - 20 November 2005

Metrics

Publication: 21
Citation (WoS): 27
Citation (Scopus): 9
H-Index (WoS): 3
H-Index (Scopus): 2

Non Academic Experience

MİLLİ SAVUNMA BAKANLIĞI
FAME Crypt
MİLLİ EĞİTİM BAKANLIĞI