

Doç.Dr. OĞUZ YAYLA

Kişisel Bilgiler

İş Telefonu: [+90 312 780 7709](tel:+903127807709)

E-posta: oguz.yayla@hacettepe.edu.tr

Web: <https://avesis.hacettepe.edu.tr/oguz.yayla>

Eğitim Bilgileri

Post Doktora, Avusturya Bilim Akademisi, Johan Radon Institute For Computational And Applied Mathematics, Discrete Mathematics And Cryptography, Avusturya 2013 - 2014

Post Doktora, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi, Türkiye 2011 - 2013

Doktora, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi, Türkiye 2006 - 2011

Yüksek Lisans, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi, Türkiye 2004 - 2006

Lisans Yandal, Orta Doğu Teknik Üniversitesi, Mühendislik Fakültesi, Telekomünikasyon, Türkiye 2002 - 2005

Lisans, Orta Doğu Teknik Üniversitesi, Fen Edebiyat Fakültesi, Matematik, Türkiye 2000 - 2004

Yabancı Diller

İngilizce, C1 İleri

Yaptığı Tezler

Doktora, On decoding interleaved Reed-solomon codes, Orta Doğu Teknik Üniversitesi, Muhasebe ve Finansman A.B.D., Kriptografi (Dr), 2011

Yüksek Lisans, Scalar multiplication on elliptic curves, Orta Doğu Teknik Üniversitesi, Muhasebe ve Finansman A.B.D., Kriptografi (YI) (Tezli), 2006

Araştırma Alanları

Matematik, Bilgisayar Bilimleri, Cebirsel Geometri, Kombinatorik, Sayılar Kuramı, Temel Bilimler

Akademik Unvanlar / Görevler

Dr.Öğr.Üyesi, Hacettepe Üniversitesi, Fen Fakültesi, Matematik Bölümü, 2018 - Devam Ediyor

Yrd.Doç.Dr., Hacettepe Üniversitesi, Fen Fakültesi, Matematik Bölümü, 2015 - 2018

Uzman, Oesterreichische Akademie Der Wissenschaften, Johan Radon Institute For Computational And Applied Mathematics, 2013 - 2014

Araştırma Görevlisi, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, 2008 - 2011

Verdiği Dersler

KRİPTOGRAFİ, Lisans, 2017 - 2018
ELİPTİK EĞRİ KRİPTOGRAFİSİ, Yüksek Lisans, 2017 - 2018
BİLGİSAYAR DESTEKLİ MATE. PROJESİ I, Lisans, 2017 - 2018, 2016 - 2017
ÇALIŞMA METODLARI I, Lisans, 2017 - 2018, 2016 - 2017
KRİPTOGRAFİK FONKSİYONLAR, Doktora, 2017 - 2018
MÜHENDİSLİK MATEMATİĞİ I, Lisans, 2017 - 2018
TASARIM TEORİSİ, Yüksek Lisans, 2017 - 2018, 2016 - 2017
KRİPTOGRAFİ, Yüksek Lisans, 2016 - 2017
KRİPTOGRAFIYE GİRİŞ, Lisans, 2016 - 2017
CEBİRSEL SAYILAR TEORİSİ, Doktora, 2016 - 2017
BİLGİSAYAR DES.MATE.PRO.II, Lisans, 2016 - 2017
ÇALIŞMA METODLARI II, Lisans, 2016 - 2017
UYGULAMALI BİLGİSAYAR CEBİRİ, Lisans, 2016 - 2017

Yönetilen Tezler

YAYLA O., γ -Butson-Hadamard matrices and their cryptographic applications, Yüksek Lisans, S.KURT(Öğrenci), 2017
YAYLA O., HFE based multi-variate quadratic cryptosystems and Dembowski Ostrom polynomials, Doktora, B.ALAM(Öğrenci), 2013
YAYLA O., Existence problem of almost p-ary perfect and nearly perfect sequences, Doktora, C.CENGİZ(Öğrenci), 2012
YAYLA O., On verification of restricted extended affine equivalence of vectorial boolean functions, Yüksek Lisans, A.SINAK(Öğrenci), 2012

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

- I. **A new lower bound on the family complexity of Legendre sequences**
Cakiroglu Y., YAYLA O.
APPLICABLE ALGEBRA IN ENGINEERING COMMUNICATION AND COMPUTING, cilt.33, sa.2, ss.173-192, 2022 (SCI-Expanded)
- II. **Almost p-ary sequences**
Ozden B., YAYLA O.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, cilt.12, sa.6, ss.1057-1069, 2020 (SCI-Expanded)
- III. **Nearly perfect sequences with arbitrary out-of-phase autocorrelation**
YAYLA O.
Advances in Mathematics of Communications, cilt.10, sa.2, ss.401-411, 2016 (SCI-Expanded)
- IV. **Family complexity and cross-correlation measure for families of binary sequences**
WINTERHOF A., Yayla O.
Ramanujan Journal, cilt.39, sa.3, ss.639-645, 2016 (SCI-Expanded)
- V. **Further results on fibre products of kummer covers and curves with many points over finite fields**
ÖZBUDAK F., Temür B. G., YAYLA O.
Advances in Mathematics of Communications, cilt.10, sa.1, ss.151-162, 2016 (SCI-Expanded)
- VI. **Improving results on the pseudorandomness of sequences generated via the additive order of a finite field**
Merai L., YAYLA O.
DISCRETE MATHEMATICS, cilt.338, sa.11, ss.2020-2025, 2015 (SCI-Expanded)
- VII. **On some bounds on the minimum distance of cyclic codes over finite fields**
ÖZBUDAK F., Tutdere S., Yayla O.
DESIGNS CODES AND CRYPTOGRAPHY, cilt.76, sa.2, ss.173-178, 2015 (SCI-Expanded)

- VIII. **Improved probabilistic decoding of interleaved Reed-Solomon codes and folded Hermitian codes**
ÖZBUDAK F., Yayla O.
THEORETICAL COMPUTER SCIENCE, cilt.520, ss.111-123, 2014 (SCI-Expanded)
- IX. **An exhaustive computer search for finding new curves with many points among fibre products of two Kummer covers over F_5 and F_7**
ÖZBUDAK F., Temur B. G., Yayla O.
TURKISH JOURNAL OF MATHEMATICS, cilt.37, sa.6, ss.908-913, 2013 (SCI-Expanded)

Diğer Dergilerde Yayınlanan Makaleler

- I. **Non-existence of Some Nearly Perfect Sequences, Near Butson-Hadamard Matrices, and Near Conference Matrices**
Winterhof A., YAYLA O., Ziegler V.
MATHEMATICS IN COMPUTER SCIENCE, cilt.12, sa.4, ss.465-471, 2018 (ESCI)
- II. **Classes of weak Dembowski-Ostrom polynomials for multivariate quadratic cryptosystems**
Alam B., ÖZBUDAK F., Yayla O.
JOURNAL OF MATHEMATICAL CRYPTOLOGY, cilt.9, sa.1, ss.11-22, 2015 (ESCI)
- III. **F11 üzerinde çok noktalı cebirsel egriler**
YAYLA O.
8. Ankara Matematik Günleri, cilt.8, ss.94, 2013 (Hakemsiz Dergi)

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

- I. **Near Butson-Hadamard Matrices and Nonlinear Boolean Functions**
Kurt S., YAYLA O.
1st International Conference on Number-Theoretic Methods in Cryptology (NuTMiC), Warszawa, Polonya, 11 - 13 Eylül 2017, cilt.10737, ss.254-266
- II. **Families of Pseudorandom Binary Sequences with Low Cross-Correlation Measure**
Yayla O.
1st International Conference on Cryptography and Information Security in the Balkans (BalkanCryptSec), İstanbul, Türkiye, 16 - 17 Ekim 2014, cilt.9024, ss.31-39
- III. **On Verification of Restricted Extended Affine Equivalence of Vectorial Boolean Functions**
ÖZBUDAK F., Sinak A., Yayla O.
5th International Workshop on the Arithmetic of Finite Fields (WAIFI), Gebze, Türkiye, 27 - 28 Eylül 2014, cilt.9061, ss.137-154
- IV. **On Fibre Products of Kummer Curves with Many Rational Points over Finite Fields**
ÖZBUDAK F., Temur B. G., Yayla O.
4th International Castle Meeting Coding Theory and Applications (4ICMCTA), Palmela Castle, Portekiz, 15 - 18 Eylül 2014, cilt.3, ss.307-315
- V. **Nonexistence of certain almost p-ary perfect sequences**
ÖZBUDAK F., Yayla O., Yildirim C. C.
7th International Conference on Sequences and Their Applications, SETA 2012, Waterloo, ON, Kanada, 4 - 08 Haziran 2012, ss.13-24

Desteklenen Projeler

YAYLA O., TÜBİTAK Projesi, Diziler Ve Onların Kriptografideki Ve Kodlama Teorisindeki Uygulamaları, 2017 - Devam Ediyor

YAYLA O., Yükseköğretim Kurumları Destekli Proje, Neredeyse Butson-Hadamard Matrisleri ve Doğrusal Olmayan Boole Fonksiyonları, 2017 - 2017

YAYLA O., TÜBİTAK Projesi, Yeni gamma Butson Hadamard Matrislerinin Üretilmesi ve Onların Kriptografiye Uygulanması, 2016 - 2017

Metrikler

Yayın: 17

Atıf (WoS): 5

Atıf (Scopus): 8

H-İndeks (WoS): 2

H-İndeks (Scopus): 2