Doç.Dr. OĞUZ YAYLA

Kişisel Bilgiler

E-posta: oguz@metu.edu.tr
Diğer E-posta: oguz.yayla@gmail.com
Web: https://avesis.metu.edu.tr/oguz

Eğitim Bilgileri

Doktora, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, Türkiye 2006 - 2011
Yüksek Lisans, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, Türkiye 2004 - 2006
Lisans Yandal, Orta Doğu Teknik Üniversitesi, Mühendislik Fakültesi, Elektrik ve Elektronik Mühendisliği Bölümü, Türkiye 2002 - 2005
Lisans, Orta Doğu Teknik Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Türkiye 1999 - 2004

Yabancı Diller

İngilizce, C1 İleri

Yaptığı Tezler

Doktora, On decoding interleaved Reed-solomon codes, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, 2011
Yüksek Lisans, Scalar multiplication on elliptic curves, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, 2006

Araştırma Alanları

Donanım Güvenliği, Kriptoloji, Kuantum Kriptografi, Bilgisayar Bilimleri, Kombinatorik, Sayılar Kuramı

Akademik Unvanlar / Görevler

Dr.Öğr.Üyesi, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, 2020 - Devam Ediyor
Yrd.Doç.Dr., Hacettepe Üniversitesi, Fen Fakültesi, Matematik Bölümü, 2015 - 2020
Uzman Dr., Johann Radon Insittute of Computational and Applied Mathematics, 2013 - 2014
Araştırma Görevlisi, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, 2008 - 2011

Yönetilen Tezler

Doğanaksoy A., Yayla O., Cryptographic modules validation process according tothe FIPS 140 and ISO/IEC 15408, Yüksek

Lisans, C.YENER(Öğrenci), 2020
Cenk M., Yayla O., Decentralized secure multiparty computation, Yüksek Lisans, B.TAŞCI(Öğrenci), 2019
Yayla O., Alternative digital signature schemes in blockchain, Yüksek Lisans, F.YAVUZYİĞİT(Öğrenci), 2019
Yayla O., Almost p-ary perfect sequences and their applications to cryptography, Yüksek Lisans, B.ÖZDEN(Öğrenci), 2019
Yayla O., γ-Butson-Hadamard matrices and their cryptographic applications, Yüksek Lisans, S.KURT(Öğrenci), 2017
ÖZBUDAK F., YAYLA O., HFE based multi-variate quadratic cryptosystems and Dembowski Ostrom polynomials, Doktora, B.ALAM(Öğrenci), 2013
ÖZBUDAK F., YAYLA O., Existence problem of almost p-ary perfect and nearly perfect sequences, Doktora, C.CENGİZ(Öğrenci), 2012
ÖZBUDAK F., YAYLA O., On verification of restricted extended affine equivalence of vectorial boolean functions, Yüksek Lisans, A.SINAK(Öğrenci), 2012

Jüri Üyelikleri

Yarışma, TÜBİTAK 2204 A LİSE ÖĞRENCİLERİ ARAŞTIRMA PROJELERİ YARIŞMASI, TÜBİTAK, Mart, 2020
Akademik Kadroya Atama, Akademik Kadroya Atama, Üniversite, Eylül, 2018

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

I. **Threshold-based post-quantum secure verifiable multi-secret sharing for distributed storage blockchain**
Mesnager S., Sınak A., Yayla O.
Mathematics, cilt.8, ss.1-15, 2020 (SCI Expanded İndekslerine Giren Dergi)

II. **Almost p-ary sequences**
Ozden B., Yayla O.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, cilt.12, ss.1057-1069, 2020 (SCI İndekslerine Giren Dergi)

III. **A new lower bound on the family complexity of Legendre sequences**
Cakiroglu Y., YAYLA O.
APPLICABLE ALGEBRA IN ENGINEERING COMMUNICATION AND COMPUTING, 2020 (SCI İndekslerine Giren Dergi)

IV. **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 İndekslerine Giren Dergi)

V. **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 İndekslerine Giren Dergi)

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 İndekslerine Giren Dergi)

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 İndekslerine Giren Dergi)

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 İndekslerine Giren Dergi)

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., GÜLMEZ TEMÜR B., Yayla O.
TURKISH JOURNAL OF MATHEMATICS, cilt.37, sa.6, ss.908-913, 2013 (SCI İndekslerine Giren Dergi)

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 (Diğer Kurumların Hakemli Dergileri)

II. **Near Butson-Hadamard Matrices and Nonlinear Boolean Functions**
Kurt S., YAYLA O.
Lecture Notes in Computer Science, 2018 (Diğer Kurumların Hakemli Dergileri)

III. **Families of Pseudorandom Binary Sequences with Low Cross Correlation Measure**
YAYLA O.
Lecture Notes in Computer Sciences, cilt.9024, ss.31-39, 2015 (Diğer Kurumların Hakemli Dergileri)

IV. **On Verification of Restricted Extended Affine Equivalence of Vectorial Boolean Functions**
ÖZBUDAK F., SINAK A., YAYLA O.
Lecture Notes in Computer Science, cilt.9061, ss.137-154, 2015 (Diğer Kurumların Hakemli Dergileri)

V. **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 (Diğer Kurumların Hakemli Dergileri)

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

I. **Comparison of Randomized Solutions for Constrained Vehicle Routing Problem**
Demirci I. E. , Ozdemir S. E. , YAYLA O.
2nd International Conference on Electrical, Communication and Computer Engineering, ICECCE 2020, İstanbul, Türkiye, 12 - 13 Haziran 2020

II. **Ideal factorization method and its applications**
Kurt S., YAYLA O.
3rd International Conference on Applications of Mathematics and Informatics in Natural Sciences and Engineering, AMINSE 2017, Tbilisi, Gürcistan, 7 - 09 Aralık 2017, cilt.276, ss.149-160

III. **Nearly Perfect Sequences and Cryptographic Functions**
KURT S., YAYLA O.
Workshop on Practical and Theoretical Aspects of Cryptography and Information Security, 08 Aralık 2017

IV. **CDMA Sistemleri için Yeni Mükemmel Dizi Örnekleri**
KURT S., YAYLA O.
Akademik Bilişim 2017, 8 - 10 Şubat 2017

V. **Near Butson Hadamard Matrices with Small off diagonal Entries**
Kurt S., YAYLA O.
3rd Istanbul Design Theory, Graph Theory and Combinatorics Workshop, 13 - 17 Haziran 2016

VI. **F11 üzerinde çok noktalı cebirsel eğriler**
YAYLA O.
8. Ankara Matematik Günleri, Türkiye, 13 - 14 Haziran 2013, ss.94

VII. **RSA Kriptosistemi Parametreleri için Güvenlik Testi Yazılımı**
Alam B., YAYLA O.
6th International Conference on Information Security and Cryptology, Türkiye, 23 - 24 Mayıs 2013

VIII. **Recent attacks against HFE Multi HFE MQ cryptosystems and Connection with Ore s p polynomial decomposition**

Alam B., YAYLA O.
6th International Conference on Information Security and Cryptology, Türkiye, 23 - 24 Mayıs 2013

IX. **Probabilistic Decoding of RS Codes with Extended BKY Algorithm**
YAYLA O., ÖZBUDAK F.
International Conference on Applied and Computational Mathematics, Ankara, Türkiye, 3 - 06 Ekim 2012

X. **Kriptografik Modüllerin Güvenlik Gereksinimleri**
YAYLA O.
III. International Conference on Information Security and Cryptology, Türkiye, 25 - 27 Aralık 2008, cilt.3, ss.253-256

XI. **On Algebraic Attacks Using Groebner Basis**
Özadam H., YAYLA O.
II. Information Security and Cryptology Conference, Türkiye, 13 - 14 Aralık 2007, ss.312-318

XII. **PKI lite A PKI system with limited resources**
AKYILDIZ E., YAYLA O.
II. International Conference on Information Security and Cryptology, Türkiye, 13 - 14 Aralık 2007, ss.59-62

XIII. **DSA Sisteminin Çalıştırılması ve Test Edilmesi**
YAYLA O.
II. Information Security and Cryptology Conference, Türkiye, 13 - 14 Aralık 2007, ss.290-297

XIV. **Scalar multiplication on elliptic curves**
AKYILDIZ E., YAYLA O.
II. National Conference on Cryptology, Türkiye, 15 - 17 Aralık 2006, ss.114-124

XV. **Ayrık Logaritma Problemini Kullanan E İmza**
CENK M., YAYLA O.
Ulusal Elektronik İmza Sempozyumu, Türkiye, 7 - 08 Aralık 2006, ss.381-386

Desteklenen Projeler

Yayla O., TÜBİTAK Projesi, Diziler Ve Onların Kriptografideki Ve Kodlama Teorisindeki Uygulamaları, 2017 - 2020
Yayla O., TÜBİTAK Projesi, Yeni gamma Butson Hadamard Matrislerinin Üretilmesi ve Onların Kriptografiye Uygulanması, 2016 - 2017
Özbudak F., TÜBİTAK Projesi, Cebirsel Eğriler Ve Onların Bazı Kriptografik Ve Kodlama Teorisindeki Problemlerdeki Uygulamaları, 2010 - 2013
Akyıldız E., TÜBİTAK Projesi, Açık Anahtar Altyapı Konusunda Araştırma Geliştirme ve Uygulamalar, 2006 - 2008

Bilimsel Dergilerdeki Faaliyetler

Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, Editörler Kurulu Üyesi, 2016 - Devam Ediyor

Bilimsel Hakemlikler

TÜBİTAK Projesi, 2219 - Yurt Dışı Doktora Sonrası Araştırma Burs Programı, Orta Doğu Teknik Üniversitesi, Türkiye, Aralık 2020
TÜBİTAK Projesi, 1001 - Bilimsel ve Teknolojik Araştırma Projelerini Destekleme Programı, Orta Doğu Teknik Üniversitesi, Türkiye, Mart 2020
TÜBİTAK Projesi, 2219 - Yurt Dışı Doktora Sonrası Araştırma Burs Programı, Hacettepe Üniversitesi, Türkiye, Aralık 2019
TÜBİTAK Projesi, 2209-A - Üniversite Öğrencileri Araştırma Projeleri Destekleme Programı, Hacettepe Üniversitesi, Türkiye, Mart 2019

Bilimsel Danışmanlıklar

Rovenma A.Ş., Kurum veya Organizasyonlar İçin Yapılan Danışmanlık, Hacettepe Üniversitesi, Fen Fakültesi, Matematik Bölümü, Türkiye, 2019 - 2020

Atıflar

Toplam Atıf Sayısı (WOS):6
h-indeksi (WOS):2