Doç. Dr. OĞUZ YAYLA

Kişisel Bilgiler

İş Telefonu: +90 312 210 5695
E-posta: oguz@metu.edu.tr
Diğer E-posta: oguz.yayla@gmail.com
Web: https://avesis.metu.edu.tr/oguz

Uluslararası Araştırmacı ID'leri
ScholarID: 83UVe60AAAAJ
ORCID: 0000-0001-8945-2780
Publons / Web Of Science ResearcherID: AAZ-7675-2020
ScopusID: 55317276200
Yoksis Araştırmacı ID: 164658

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

Doç. Dr., Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, 2022 - Devam Ediyor
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

Akademik İdari Deneyim

Anabilim/Bilim Dalı Başkanı, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, 2022 - 2025
Enstitü Müdür Yardımcısı, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, 2022 - 2024

Verdiği Dersler

Special Topics: Blockchain and Cryptocurrencies: Security & Privacy, Doktora, 2021 - 2022

Yönetilen Tezler

Yayla O., A comprehensive study of time lock puzzles and timed signatures in cryptography, Yüksek Lisans, C.DOĞAN(Öğrenci), 2023
YAYLA O., Random sequences in vehicle routing problem, Yüksek Lisans, M.EMİN(Öğrenci), 2022
YAYLA O., Blockchain based solution for electronic health record integrity, Yüksek Lisans, K.ÇELİK(Öğrenci), 2022
Yayla O., MDS MATRICES OVER RINGS FOR DESIGNING LIGHTWEIGHT BLOCKCIPHER, Yüksek Lisans, G.YETİŞER(Öğrenci), 2021
Doğanaksoy A., Yayla O., Gröbner basis attack on Stark-friendly symmetric-key primitives: JARVIS, MiMC and GMiMCerf, Yüksek Lisans, G.KARA(Öğrenci), 2021
YAYLA O., Combinatorial solutions for consensus algorithms and blockchain sharding, Doktora, M.SALEH(Öğrenci), 2021
YAYLA O., IMPLEMENTATION ANALYSIS OF CRYPTOGRAPHY TOOLBOX IN HYPERLEDGER, Yüksek Lisans, A.ŞİMŞEK(Öğrenci), 2021
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., Almost p-ary perfect sequences and their applications to cryptography, Yüksek Lisans, B.ÖZDEN(Öğrenci), 2019
Yayla O., Alternative digital signature schemes in blockchain, Yüksek Lisans, F.YAVUZYİĞİT(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

Tez Savunma (Doktora), Tez Savunma (Doktora), Orta Doğu Teknik Üniversitesi, Ağustos, 2022
Tez Savunma (Doktora), Tez Savunma (Doktora), Orta Doğu Teknik Üniversitesi, Mart, 2022
Doktora Tez İzleme Komitesi (TİK) Üyeliği, Doktora Tez İzleme Komitesi (TİK) Üyeliği, Orta Doğu Teknik Üniversitesi, Haziran, 2020

Yarışma, TÜBİTAK 2204 A LİSE ÖĞRENCİLERİ ARAŞTIRMA PROJELERİ YARIŞMASI, TÜBİTAK, Mart, 2020
Yarışma, 2204 B ORTAOKUL ÖĞRENCİLERİ ARAŞTIRMA PROJELERİ YARIŞMASI, TÜBİTAK, Mart, 2020
Akademik Kadroya Atama-Yardımcı Doçentlik, Akademik Kadroya Atama, Üniversite, Eylül, 2018

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

I. **Codes on subgroups of weighted projective tori**
ŞAHİN M., YAYLA O.
Designs, Codes, and Cryptography, cilt.92, sa.5, ss.1201-1218, 2024 (SCI-Expanded)

II. **On a group under which symmetric Reed–Muller codes are invariant**
Toplu S. K., ARIKAN T., AYDOĞDU P., YAYLA O.
Journal of Algebra and its Applications, 2024 (SCI-Expanded)

III. **PARTIAL DIRECT PRODUCT DIFFERENCE SETS AND ALMOST QUATERNARY SEQUENCES**
Ozden B., YAYLA O.
ADVANCES IN MATHEMATICS OF COMMUNICATIONS, cilt.17, ss.572-588, 2023 (SCI-Expanded)

IV. **Butson-Hadamard matrices and Plotkin-optimal codes over DOUBLE-STRUCK CAPITAL Z(pe)**
Acar D., SARAÇ B., YAYLA O.
JOURNAL OF ALGEBRA AND ITS APPLICATIONS, 2023 (SCI-Expanded)

V. **Verifiable Timed Accountable Subgroup Multi-signatures**
ÖZDEN D., YAYLA O.
LECTURE NOTES IN ARTIFICIAL INTELLIGENCE, cilt.14424, 2023 (SCI-Expanded)

VI. **The number of irreducible polynomials over finite fields with vanishing trace and reciprocal trace**
Çakıroğlu Y., Yayla O., Yilmaz E. S.
DESIGNS, CODES, AND CRYPTOGRAPHY, cilt.90, sa.10, ss.2407-2417, 2022 (SCI-Expanded)

VII. **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)

VIII. **Application of blockchain technology and internet of things in uroflowmetry for clinical trials: A pilot test**
COŞKUN B. N., YAYLA O., YILDIZ H.
EUROPEAN UROLOGY, cilt.81, 2022 (SCI-Expanded)

IX. **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)

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

XI. **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)

XII. **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)

XIII. **FURTHER RESULTS ON FIBRE PRODUCTS OF KUMMER COVERS AND CURVES WITH MANY POINTS OVER FINITE FIELDS**
ÖZBUDAK F., Temur B. G., YAYLA O.
ADVANCES IN MATHEMATICS OF COMMUNICATIONS, cilt.10, sa.1, ss.151-162, 2016 (SCI-Expanded)

XIV. **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)

XV. **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)

XVI. **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)

XVII. **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-Expanded)

Diğer Dergilerde Yayınlanan Makaleler

I. **Random Sequences in Vehicle Routing Problem**
Gülşen M. E., Yayla O.
LECTURE NOTES IN ARTIFICIAL INTELLIGENCE, cilt.13858, sa.1, ss.159-170, 2023 (Scopus)

II. **Minimal Linear Codes with Few Weights and Their Secret Sharing**
MESNAGER S., SINAK A., YAYLA O.
INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, cilt.8, sa.4, ss.77-87, 2019 (Hakemli Dergi)

III. **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 (Scopus)

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

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

VI. **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 (Hakemli Dergi)

VII. **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 (Scopus)

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

I. **Design and Implementation of a Fast, Platform-Adaptive, AIS-20/31 Compliant PLL-Based True Random Number Generator on a Zynq 7020 SoC FPGA**
YAYLA O., Yılmaz Y. E.
17th International Conference on Computational Intelligence in Security for Information Systems, CISIS 2024 and the 15th International Conference on EUropean Transnational Education, ICEUTE 2024, Salamanca, İspanya, 8 - 10 Ekim 2024, cilt.957 LNNS, ss.45-55

II. **Methods for Masking CRYSTALS-Kyber Against Side-Channel Attacks**

ÖZEREN S., YAYLA O.
2023 16th International Conference on Information Security and Cryptology (ISCTürkiye), Türkiye, 18 Ekim 2023

III. **Improving Performance in Space-Hard Algorithms**
Güner H. K., Mangır C., YAYLA O.
7th International Symposium on Cyber Security, Cryptology, and Machine Learning, CSCML 2023, Be'er-Sheva, İsrail, 29 - 30 Haziran 2023, cilt.13914 LNCS, ss.398-410

IV. **Random Sequences in Vehicle Routing Problem**
Gülen M. E., Yayla O.
10th International Conference on Numerical Methods and Applications, NMA 2022, Borovets, Bulgaristan, 22 - 26 Ağustos 2022, cilt.13858 LNCS, ss.159-170

V. **Verifiable Timed Commitments f or Fair Sealed-bid Auctions**
Ozden D., YAYLA O.
1st IEEE International Conference on Cryptography, Informatics, and Cybersecurity, ICoCICs 2023, Hybrid, Bogor, Endonezya, 22 - 24 Ağustos 2023, ss.236-245

VI. **A General Version of Carlet's Construction of APN Functions**
Yayla O., Acunalp Erleblebii İ.
ALGORITHMS IN CRYPTOGRAPHY AND BLOCKCHAIN: Special Session at the 27th International Conference on Applications of Computer Algebra (ACA'2022), İstanbul, Türkiye, 15 - 19 Ağustos 2022, ss.187-188

VII. **Gröbner Basis Attack on STARK-Friendly Symmetric-Key Primitives: JARVIS, MiMC and GMiMCerf**
Kara G., Yayla O.
15th International Conference on Information Security and Cryptography, ISCTURKEY 2022, Ankara, Türkiye, 19 - 20 Ekim 2022, ss.1-7

VIII. **On the Number of Arithmetic Operations in NTT-based Polynomial Multiplication in Kyber and Dilithium Cryptosystems**
Ilter M. B., Kocak N., Uslu E., Yayla O., Yuca N.
14th International Conference on Security of Information and Networks (SIN), ELECTR NETWORK, 15 - 17 Aralık 2021

IX. **PSO based Blockchain Committee Member Selection**
Jameel M., YAYLA O.
6th International Conference on Computer Science and Engineering, UBMK 2021, Ankara, Türkiye, 15 - 17 Eylül 2021, ss.725-730

X. **Implementation Analysis of Cryptography Toolbox in Hyperledger**
Simsek A., Tasci B., YAYLA O.
14th International Conference on Information Security and Cryptology, ISCTURKEY 2021, Ankara, Türkiye, 2 - 03 Aralık 2021, ss.179-184

XI. **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

XII. **Three-Weight Minimal Linear Codes and Their Applications**
MESNAGER S., SINAK A., YAYLA O.
Second International Workshop on Cryptography and itsApplications, Oran, Cezayir, 18 - 19 Haziran 2019

XIII. **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

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

XV. **CDMA Sistemleri için Yeni Mükemmel Dizi Örnekleri**
KURT S., YAYLA O.

Akademik Bilişim 2017, 8 - 10 Şubat 2017

XVI. **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

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

XVIII. **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

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

XX. **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

XXI. **Nonexistence of certain almost p-ary perfect sequences**
Özbudak F., Yayla O., Yıldırım C. C.
7th International Conference on Sequences and Their Applications, SETA 2012, Waterloo, ON, Kanada, 4 - 08 Haziran 2012, cilt.7280 LNCS, ss.13-24

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

XXIII. **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

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

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

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

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

Bilirkişi Raporları

I. **Kripto varlıkların durumu**
Yayla O., Pişirici E. R.
11. Ağır Ceza Mahkemesi, ss.9, Gaziantep, 2022

Desteklenen Projeler

CENK M., YAYLA O., TÜBİTAK Projesi, Kriptografik Algoritmaların Tasarımı, Gerçekleştirilmeleri ve Uygulamaları, 2019 - 2027
YAYLA O., Yükseköğretim Kurumları Destekli Proje, Kombinatorik Tasarımlar, Diziler ve Onların Kriptografik Uygulamaları, 2021 - 2022
Yayla O., TÜBİTAK Projesi, Simitli Cebirsel Geometri VeKodlama Teorisine Uygulamaları, 2019 - 2022
Yayla O., TÜBİTAK Uluslararası İkili İşbirliği Projesi, Ntru Tabanlı KriptosistemlerinTasarımı Ve Biçimsel Yöntemler ile Analizi, 2019 - 2021
Yayla O., Akleylek S., Kırlar B. B., Özsoy A., Saygı Z., TÜBİTAK Projesi, Kafes Tabanlı Güvenilir Kriptografik Protokol Tasarımı Ve Verimli Uygulamaları, 2018 - 2020
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

Bilimsel Dergilerdeki Faaliyetler

TURKISH JOURNAL OF MATHEMATICS, Makale Editörü, 2019 - Devam Ediyor
Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, Editörler Kurulu Üyesi, 2016 - Devam Ediyor

Bilimsel Hakemlikler

TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, SCI-E Kapsamındaki Dergi, Aralık 2022
ADVANCES IN MATHEMATICS OF COMMUNICATIONS, SCI-E Kapsamındaki Dergi, Ağustos 2022
TÜBİTAK Projesi, 2204-A Lise Öğrencileri Araştırma Projeleri Yarışması, Orta Doğu Teknik Üniversitesi, Türkiye, Haziran 2022
TÜBİTAK Projesi, 2204-B Ortaokul Öğrencileri Araştırma Projeleri Yarışması, Orta Doğu Teknik Üniversitesi, Türkiye, Mayıs 2022
TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, SCI-E Kapsamındaki Dergi, Nisan 2022
TÜBİTAK Projesi, 2204-A Lise Öğrencileri Araştırma Projeleri Yarışması, Orta Doğu Teknik Üniversitesi, Türkiye, Nisan 2022
Sinyal İşleme ve İletişim Uygulamaları Kurultayı-2022, Bildiri (Tam Metin), Mart 2022
TURKISH JOURNAL OF MATHEMATICS, SCI-E Kapsamındaki Dergi, Mart 2022
TÜBİTAK Projesi, 2204-B Ortaokul Öğrencileri Araştırma Projeleri Yarışması, Orta Doğu Teknik Üniversitesi, Türkiye, Mart 2022
TURKISH JOURNAL OF MATHEMATICS, SCI-E Kapsamındaki Dergi, Şubat 2022
APPLIED SOFT COMPUTING JOURNAL, SCI-E Kapsamındaki Dergi, Ocak 2022
TURKISH JOURNAL OF MATHEMATICS, SCI-E Kapsamındaki Dergi, Ocak 2022
TURKISH JOURNAL OF MATHEMATICS, SCI-E Kapsamındaki Dergi, Ocak 2022
APPLIED SOFT COMPUTING JOURNAL, SCI Kapsamındaki Dergi, Aralık 2021
TÜBİTAK Projesi, 1001 - Bilimsel ve Teknolojik Araştırma Projelerini Destekleme Programı, Orta Doğu Teknik Üniversitesi, Türkiye, Aralık 2021
TÜBİTAK Projesi, 1001 - Bilimsel ve Teknolojik Araştırma Projelerini Destekleme Programı, Orta Doğu Teknik Üniversitesi, Türkiye, Kasım 2021
DESIGNS, CODES, AND CRYPTOGRAPHY, SCI Kapsamındaki Dergi, Ağustos 2021
TÜBİTAK Projesi, 2204-B Ortaokul Öğrencileri Araştırma Projeleri Yarışması, Orta Doğu Teknik Üniversitesi, Türkiye, Ağustos 2021
TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, SCI-E Kapsamındaki Dergi, Haziran 2021
TURKISH JOURNAL OF MATHEMATICS, SCI-E Kapsamındaki Dergi, Haziran 2021
TURKISH JOURNAL OF MATHEMATICS, SCI-E Kapsamındaki Dergi, Haziran 2021
TÜBİTAK Projesi, 1002 - Hızlı Destek Programı, Orta Doğu Teknik Üniversitesi, Türkiye, Haziran 2021

TÜBİTAK Projesi, 2204-A Lise Öğrencileri Araştırma Projeleri Yarışması, Orta Doğu Teknik Üniversitesi, Türkiye, Haziran 2021
TÜBİTAK Projesi, 1002 - Hızlı Destek Programı, Orta Doğu Teknik Üniversitesi, Türkiye, Mayıs 2021
TÜBİTAK Projesi, 2204-A Lise Öğrencileri Araştırma Projeleri Yarışması, Orta Doğu Teknik Üniversitesi, Türkiye, Nisan 2021
TÜBİTAK Projesi, 2204-B Ortaokul Öğrencileri Araştırma Projeleri Yarışması, Orta Doğu Teknik Üniversitesi, Türkiye, Mart 2021
TÜBİTAK Projesi, 2219 - Yurt Dışı Doktora Sonrası Araştırma Burs Programı, Orta Doğu Teknik Üniversitesi, Türkiye, Aralık 2020
TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, SCI Kapsamındaki Dergi, Kasım 2020
APPLIED SOFT COMPUTING, SCI Kapsamındaki Dergi, Kasım 2020
TURKISH JOURNAL OF MATHEMATICS, SCI Kapsamındaki Dergi, Eylül 2020
TURKISH JOURNAL OF MATHEMATICS, SCI Kapsamındaki Dergi, Temmuz 2020
TURKISH JOURNAL OF MATHEMATICS, SCI Kapsamındaki Dergi, Temmuz 2020
DESIGNS CODES AND CRYPTOGRAPHY, SCI Kapsamındaki Dergi, Nisan 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

TSE, Kurum veya Organizasyonlar İçin Yapılan Danışmanlık, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, Türkiye, 2022 - Devam Ediyor
Rovenma A.Ş., Kurum veya Organizasyonlar İçin Yapılan Danışmanlık, Hacettepe Üniversitesi, Fen Fakültesi, Matematik Bölümü, Türkiye, 2019 - 2020

Etkinlik Organizasyonlarındaki Görevler

Kestel A. S., Yayla O., Türk Ö., Workshop on 20th Anniversary of the Institute of Applied Mathematics, Çalıştay Organizasyonu, Türkiye, Kasım 2022
Yayla O., Sınak A., ALGORITHMS IN CRYPTOGRAPHY AND BLOCKCHAIN: Special Session at the 27th International Conference on Applications of Computer Algebra (ACA'2022), Bilimsel Kongre / Sempozyum Organizasyonu, İstanbul, Türkiye, Ağustos 2022

Metrikler

Yayın: 52
Atıf (WoS): 13
Atıf (Scopus): 20
H-İndeks (WoS): 3
H-İndeks (Scopus): 3

Kongre ve Sempozyum Katılımı Faaliyetleri

14. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Panelist, Ankara, Türkiye, 2021