Assoc. Prof. OĞUZ YAYLA

Personal Information

Email: oguz@metu.edu.tr
Other Email: oguz.yayla@gmail.com
Web: https://avesis.metu.edu.tr/oguz

Education Information

Doctorate, Middle East Technical University, Institute of Applied Mathematics, Cryptography, Turkey 2006 - 2011
Post Graduate, Middle East Technical University, Institute of Applied Mathematics, Cryptography, Turkey 2004 - 2006
Undergraduate Minor, Middle East Technical University, Faculty of Engineering, Department of Electrical and Electronics Engineering, Turkey 2002 - 2005
Under Graduate, Middle East Technical University, Faculty of Arts and Sciences, Department of Mathematics, Turkey 1999 - 2004

Foreign Languages

English, C1 Advanced

Dissertations

Doctorate, On decoding interleaved Reed-solomon codes, Middle East Technical University, Institute of Applied Mathematics, 2011
Post Graduate, Scalar multiplication on elliptic curves, Middle East Technical University, Institute of Applied Mathematics, Cryptography, 2006

Research Areas

Hardware Security, Cryptography, Quantum Cryptography, Computer Science, Combinatorics, Number Theory

Academic Titles / Tasks

Assistant Professor, Middle East Technical University, Institute of Applied Mathematics, Cryptography, 2020 - Continues
Assistant Professor, Hacettepe University, Fen Fakültesi, Matematik Bölümü, 2015 - 2020
Expert PhD, Johann Radon Insittute of Computational and Applied Mathematics, 2013 - 2014
Research Assistant, Middle East Technical University, Institute of Applied Mathematics, Cryptography, 2008 - 2011

Advising Theses

Doğanaksoy A., Yayla O., Cryptographic modules validation process according tothe FIPS 140 and ISO/IEC 15408, Post Graduate, C.YENER(Student), 2020
Cenk M., Yayla O., Decentralized secure multiparty computation, Post Graduate, B.TAŞCI(Student), 2019

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

Jury Memberships

Competition, TÜBİTAK 2204 A LİSE ÖĞRENCİLERİ ARAŞTIRMA PROJELERİ YARIŞMASI, TÜBİTAK, March, 2020
Appointment Academic Staff, Appointment Academic Staff, Üniversite, September, 2018

Articles Published in Journals That Entered SCI, SSCI and AHCI Indexes

I. **Threshold-based post-quantum secure verifiable multi-secret sharing for distributed storage blockchain**
Mesnager S., Sınak A., Yayla O.
Mathematics, vol.8, pp.1-15, 2020 (Journal Indexed in SCI Expanded)

II. **Almost p-ary sequences**
Ozden B., Yayla O.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, vol.12, pp.1057-1069, 2020 (Journal Indexed in SCI)

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

IV. **NEARLY PERFECT SEQUENCES WITH ARBITRARY OUT-OF-PHASE AUTOCORRELATION**
YAYLA O.
ADVANCES IN MATHEMATICS OF COMMUNICATIONS, vol.10, no.2, pp.401-411, 2016 (Journal Indexed in SCI)

V. **Family complexity and cross-correlation measure for families of binary sequences**
Winterhof A., YAYLA O.
RAMANUJAN JOURNAL, vol.39, no.3, pp.639-645, 2016 (Journal Indexed in SCI)

VI. **Improving results on the pseudorandomness of sequences generated via the additive order of a finite field**
Merai L., YAYLA O.
DISCRETE MATHEMATICS, vol.338, no.11, pp.2020-2025, 2015 (Journal Indexed in SCI)

VII. **On some bounds on the minimum distance of cyclic codes over finite fields**
ÖZBUDAK F., TUTDERE S., YAYLA O.
Designs, Codes, and Cryptography, vol.76, no.2, pp.173-178, 2015 (Journal Indexed in SCI Expanded)

VIII. **Improved probabilistic decoding of interleaved Reed-Solomon codes and folded Hermitian codes**
ÖZBUDAK F., Yayla O.
THEORETICAL COMPUTER SCIENCE, vol.520, pp.111-123, 2014 (Journal Indexed in SCI)

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, vol.37, no.6, pp.908-913, 2013 (Journal Indexed in SCI)

Articles Published in Other Journals

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, vol.12, no.4, pp.465-471, 2018 (Refereed Journals of Other Institutions)

II. **Near Butson-Hadamard Matrices and Nonlinear Boolean Functions**
Kurt S., YAYLA O.
Lecture Notes in Computer Science, 2018 (Refereed Journals of Other Institutions)

III. **Families of Pseudorandom Binary Sequences with Low Cross Correlation Measure**
YAYLA O.
Lecture Notes in Computer Sciences, vol.9024, pp.31-39, 2015 (Refereed Journals of Other Institutions)

IV. **On Verification of Restricted Extended Affine Equivalence of Vectorial Boolean Functions**
ÖZBUDAK F., SINAK A., YAYLA O.
Lecture Notes in Computer Science, vol.9061, pp.137-154, 2015 (Refereed Journals of Other Institutions)

V. **Classes of weak Dembowski-Ostrom polynomials for multivariate quadratic cryptosystems**
ALAM B., ÖZBUDAK F., YAYLA O.
Journal of Mathematical Cryptology, vol.9, no.1, pp.11-22, 2015 (Refereed Journals of Other Institutions)

Refereed Congress / Symposium Publications in Proceedings

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, Turkey, 12 - 13 June 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, Georgia, 7 - 09 December 2017, vol.276, pp.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 December 2017

IV. **CDMA Sistemleri için Yeni Mükemmel Dizi Örnekleri**
KURT S., YAYLA O.
Akademik Bilişim 2017, 8 - 10 February 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 June 2016

VI. **F11 üzerinde çok noktalı cebirsel eğriler**
YAYLA O.
8. Ankara Matematik Günleri, Turkey, 13 - 14 June 2013, pp.94

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

IX. **Probabilistic Decoding of RS Codes with Extended BKY Algorithm**
YAYLA O., ÖZBUDAK F.

International Conference on Applied and Computational Mathematics, Ankara, Turkey, 3 - 06 October 2012

X. **Kriptografik Modüllerin Güvenlik Gereksinimleri**
YAYLA O.
III. International Conference on Information Security and Cryptology, Turkey, 25 - 27 December 2008, vol.3, pp.253-256

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

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

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

XIV. **Scalar multiplication on elliptic curves**
AKYILDIZ E., YAYLA O.
II. National Conference on Cryptology, Turkey, 15 - 17 December 2006, pp.114-124

XV. **Ayrık Logaritma Problemini Kullanan E İmza**
CENK M., YAYLA O.
Ulusal Elektronik İmza Sempozyumu, Turkey, 7 - 08 December 2006, pp.381-386

Supported Projects

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

Activities in Scientific Journals

Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, Committee Member, 2016 - Continues

Scientific Refereeing

TUBITAK Project, 2219 - Yurt Dışı Doktora Sonrası Araştırma Burs Programı, Middle East Technical University, Turkey, December 2020
TUBITAK Project, 1001 - Program for Supporting Scientific and Technological Research Projects, Middle East Technical University, Turkey, March 2020
TUBITAK Project, 2219 - Yurt Dışı Doktora Sonrası Araştırma Burs Programı, Hacettepe University, Turkey, December 2019
TUBITAK Project, 2209-A - Üniversite Öğrencileri Araştırma Projeleri Destekleme Programı, Hacettepe University, Turkey, March 2019

Scientific Consultations

Rovenma A.Ş., Scientific Consultancy, Hacettepe University, Fen Fakültesi, Matematik Bölümü, Turkey, 2019 - 2020

Citations

Total Citations (WOS):6
h-index (WOS):2