Assoc. Prof. OĞUZ YAYLA

Personal Information

Office Phone: +90 312 780 7709
Email: oguz.yayla@hacettepe.edu.tr
Web: https://avesis.hacettepe.edu.tr/oguz.yayla

Education Information

Post Doctorate, Avusturya Bilim Akademisi, Johan Radon Institute For Computational And Applied Mathematics, Discrete Mathematics And Cryptography, Austria 2013 - 2014
Post Doctorate, Middle East Technical University, Institute Of Applied Mathematics, Kriptografi, Turkey 2011 - 2013
Doctorate, Middle East Technical University, Institute Of Applied Mathematics, Kriptografi, Turkey 2006 - 2011
Postgraduate, Middle East Technical University, Institute Of Applied Mathematics, Kriptografi, Turkey 2004 - 2006
Undergraduate Minor, Middle East Technical University, Faculty Of Engineering, Telekomünikasyon, Turkey 2002 - 2005
Undergraduate, Middle East Technical University, Fen Edebiyat Fakültesi, Matematik, Turkey 2000 - 2004

Foreign Languages

English, C1 Advanced

Dissertations

Doctorate, On decoding interleaved Reed-solomon codes, Orta Doğu Teknik Üniversitesi, Muhasebe ve Finansman A.B.D., Kriptografi (Dr), 2011
Postgraduate, Scalar multiplication on elliptic curves, Orta Doğu Teknik Üniversitesi, Muhasebe ve Finansman A.B.D., Kriptografi (Yl) (Tezli), 2006

Research Areas

Mathematics, Computer Science, Algebraic Geometry, Combinatorics, Number Theory, Natural Sciences

Academic Titles / Tasks

Assistant Professor, Hacettepe University, Fen Fakültesi, Matematik Bölümü, 2018 - Continues
Assistant Professor, Hacettepe University, Fen Fakültesi, Matematik Bölümü, 2015 - 2018
Expert, Oesterreichische Akademie Der Wissenschaften, Johan Radon Institute For Computational And Applied Mathematics, 2013 - 2014
Research Assistant, Middle East Technical University, Institute Of Applied Mathematics, 2008 - 2011

Courses

KRİPTOGRAFİ, Undergraduate, 2017 - 2018
ELİPTİK EĞRİ KRİPTOGRAFİSİ, Postgraduate, 2017 - 2018
BİLGİSAYAR DESTEKLİ MATE. PROJESİ I, Undergraduate, 2017 - 2018, 2016 - 2017
ÇALIŞMA METODLARI I, Undergraduate, 2017 - 2018, 2016 - 2017
KRİPTOGRAFİK FONKSİYONLAR, Doctorate, 2017 - 2018
MÜHENDİSLİK MATEMATİĞİ I, Undergraduate, 2017 - 2018
TASARIM TEORİSİ, Postgraduate, 2017 - 2018, 2016 - 2017
KRİPTOGRAFİ, Postgraduate, 2016 - 2017
KRİPTOGRAFİYE GİRİŞ, Undergraduate, 2016 - 2017
CEBİRSEL SAYILAR TEORİSİ, Doctorate, 2016 - 2017
BİLGİSAYAR DES.MATE.PRO.II, Undergraduate, 2016 - 2017
ÇALIŞMA METODLARI II, Undergraduate, 2016 - 2017
UYGULAMALI BİLGİSAYAR CEBİRİ, Undergraduate, 2016 - 2017

Advising Theses

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

Published journal articles indexed by SCI, SSCI, and AHCI

I. **A new lower bound on the family complexity of Legendre sequences**
Cakiroglu Y., YAYLA O.
APPLICABLE ALGEBRA IN ENGINEERING COMMUNICATION AND COMPUTING, vol.33, no.2, pp.173-192, 2022 (SCI-Expanded)

II. **Almost p-ary sequences**
Ozden B., YAYLA O.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, vol.12, no.6, pp.1057-1069, 2020 (SCI-Expanded)

III. **Nearly perfect sequences with arbitrary out-of-phase autocorrelation**
YAYLA O.
Advances in Mathematics of Communications, vol.10, no.2, pp.401-411, 2016 (SCI-Expanded)

IV. **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 (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, vol.10, no.1, pp.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, vol.338, no.11, pp.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, vol.76, no.2, pp.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, vol.520, pp.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, vol.37, no.6, pp.908-913, 2013 (SCI-Expanded)

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 (ESCI)

II. **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 (ESCI)

III. **F11 üzerinde çok noktalı cebirsel egriler**
YAYLA O.
8. Ankara Matematik Günleri, vol.8, pp.94, 2013 (Non Peer-Reviewed Journal)

Refereed Congress / Symposium Publications in Proceedings

I. **Near Butson-Hadamard Matrices and Nonlinear Boolean Functions**
Kurt S., YAYLA O.
1st International Conference on Number-Theoretic Methods in Cryptology (NuTMiC), Warszawa, Poland, 11 - 13 September 2017, vol.10737, pp.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, Turkey, 16 - 17 October 2014, vol.9024, pp.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, Turkey, 27 - 28 September 2014, vol.9061, pp.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, Portugal, 15 - 18 September 2014, vol.3, pp.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, Canada, 4 - 08 June 2012, pp.13-24

Supported Projects

YAYLA O., TUBITAK Project, Diziler Ve Onların Kriptografideki Ve Kodlama Teorisindeki Uygulamaları, 2017 - Continues
YAYLA O., Project Supported by Higher Education Institutions, Neredeyse Butson-Hadamard Matrisleri ve Doğrusal

Olmayan Boole Fonksiyonları, 2017 - 2017
YAYLA O., TUBITAK Project, Yeni gamma Butson Hadamard Matrislerinin Üretilmesi ve Onların Kriptografiye Uygulanması, 2016 - 2017

Metrics

Publication: 17
Citation (WoS): 5
Citation (Scopus): 8
H-Index (WoS): 2
H-Index (Scopus): 2