Assoc. Prof. AHMET SINAK

Personal Information

Email: ahmetsinak@akdeniz.edu.tr
Other Email: ahmetsinak07@gmail.com
Web: https://avesis.akdeniz.edu.tr/ahmetsinak

International Researcher IDs
ScholarID: pqnsLPoAAAAJ
ORCID: 0000-0002-1071-765X
Publons / Web Of Science ResearcherID: AAF-9231-2020
ScopusID: 56529548700
Yoksis Researcher ID: 55128

Biography

Dr. Ahmet Sınak 1984 yılında Antalya'da doğdu. 2005 yılında Muğla Sıtkı Koçman Üniversitesi Fen Fakültesi Matematik Bölümünde Lisans eğitimine başlamış ve 2009 yılında bu bölümden birincilikle mezun olmuştur. 2011 yılında Orta Doğu Teknik Üniversitesi (ODTÜ) Uygulamalı Matematik Enstitüsü (UME) Kriptografi Programında Yüksek Lisans eğitimine başlamış ve "On Verification of Restricted Extended Affine Equivalence of Vectorial Boolean Functions (Vektör Boole Fonksiyonların Kısıtlı Genişletilmiş Afin Denkliği Üzerine)" başlıklı yüksek lisans tezini Prof. Dr. Ferruh Özbudak danışmanlığında ve Doç. Dr. Oğuz Yayla'nın eş-danışmanlığında tamamlayarak 2012 yılında mezun olmuştur. Aynı yıl ODTÜ UME Kriptografi Programında doktoraya başlamış, 8 Eylül 2017'de Prof. Dr. Ferruh Özbudak ve Prof. Dr. Sihem Mesnager (Matematik Bölümü, Paris 8 Üniversitesi, Fransa) ortak danışmanlığında yürüttüğü "Contributions on Plateaued (Vectorial) Functions for Symmetric Cryptography and Coding Theory (Simetrik Kriptografi ve Kodlama Teorisi için (Vektörel) Plato Fonksiyonlar Üzerine Katkılar)" başlıklı doktora tezini savunarak doktorasını tamamlamıştır. 11 Ağustos 2022 tarihinde Üniversitelerarası Kurul Başkanlığından Matematik Bilim alanından Doçent unvanını almıştır.

Doktora sırasında TÜBİTAK-BİDEB 2214/A burs programı kapsamında Kasım 2016 - Temmuz 2017 tarih aralığında tez danışmanı Prof. Mesnager ile doktora tezi üzerine çalışmak için Paris 8 Üniversitesi'nde bulunmuştur. Ayrıca, TÜBİTAK-BİDEB 2219 burs programı kapsamında Haziran-Eylül 2018 ve Fransız Büyükelçiliği araştırma burs programı kapsamında Temmuz-Eylül 2024 tarihlerinde ortak akademik çalışmalar yapmak için doktora sonrası araştırmacı olarak Paris 8 Üniversitesi'nde bulunmuştur.

Aralık 2010 - Ağustos 2011 tarihlerinde Artvin Çoruh Üniversitesi, Fen Fakültesi, Matematik Bölümü'nde, Ağustos 2011-Şubat 2012 tarihlerinde Necmettin Erbakan Üniversitesi Fen Fakültesi Matematik-Bilgisayar Bilimleri Bölümü'nde ve Şubat 2012- Ocak 2018 tarih aralığında ODTÜ UME'de araştırma görevlisi olarak görev yapmıştır. Sırasıyla, Ocak 2018 – Ocak 2020, Ocak 2020-Ağustos 2022 ve Ağustos 2022-Haziran 2024 tarih aralıklarında Necmettin Erbakan Üniversitesi Fen Fakültesi Matematik ve Bilgisayar Bilimleri Bölümü'nde doktor araştırma görevlisi, Dr. Öğretim üyesi ve Doçent olarak görev yapmıştır. 28 Haziran 2024 tarihinden itibaren Akdeniz Üniversitesi, Manavgat Sosyal ve Beşeri Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü'nde doçent olarak görev yapmaktayım.

Çalışma alanı günümüz teknoloji çağının önemli bilim alanlarından olan Kriptografi ve Kodlama Teorisi üzerinedir. Çalışma konuları arasında şifrelemede kullanılan kriptografik fonksiyonlar ve bu fonksiyonların doğrusal kodlar ve gizli anahtar paylaşım şemaları ile ilişkileri yer almaktadır. Mevcut çalışmaları arasında finans ve sağlık sektörü gibi birçok alanda geleceğin teknolojisi olarak gösterilen Blokzincir Teknolojisinde kullanılan kriptografik protokollerin tasarımı ve analizi yer almaktadır. Ayrıca, kuantum sonrası kriptografik algoritmaların tasarımı ve analizi üzerine de çalışmalarını sürdürmektedir.

Education Information

Doctorate, Middle East Technical University, Institute Of Applied Mathematics, Cryptography, Turkey 2012 - 2017
Postgraduate, Middle East Technical University, Institute Of Applied Mathematics, Cryptography, Turkey 2011 - 2012
Undergraduate, Mugla Sitki Kocman University, Faculty of Science, Mathematics, Turkey 2005 - 2009

Foreign Languages

English, C1 Advanced

Dissertations

Doctorate, Contributions on plateaued (Vectorial) functions for symmetric cryptography and coding theory, Middle East Technical University, Institute Of Applied Mathematics, Cryptography, 2017
Postgraduate, On verification of restricted extended affine equivalence of vectorial boolean functions, Middle East Technical University, Institute Of Applied Mathematics, Cryptography, 2012

Research Areas

Information Security and Reliability, Cryptography, Quantum Cryptography, Field Theory and Polynomials, Combinatorics

Academic Titles / Tasks

Associate Professor, Akdeniz University, Manavgat Faculty of Social and Human Sciences, Department of Management Information Systems, 2024 - Continues
Associate Professor, Necmettin Erbakan University, Faculty of Science, Department of Mathematics and Computer Science, 2022 - 2024
Assistant Professor, Necmettin Erbakan University, Faculty of Science, Department of Mathematics and Computer Science, 2020 - 2022
Research Assistant PhD, Necmettin Erbakan University, Faculty of Science, Department of Mathematics and Computer Science, 2018 - 2020
Research Assistant, Middle East Technical University, Institute Of Applied Mathematics, Cryptography, 2012 - 2018
Research Assistant, Necmettin Erbakan University, Faculty of Science, Department of Mathematics and Computer Science , 2011 - 2012
Research Assistant, Artvin Coruh University, Faculty of Science, Mathematics, 2010 - 2011

Courses

Kriptolojinin Temelleri, Undergraduate, 2023 - 2024
İleri Sayılar Teorisi, Undergraduate, 2023 - 2024
Soyut Matematik II, Undergraduate, 2023 - 2024
INE102 Calculus-II, Undergraduate, 2023 - 2024
Calculus 1, Undergraduate, 2023 - 2024
Soyut Matematik 1, Undergraduate, 2023 - 2024
Kriptoloji, Undergraduate, 2023 - 2024
Açık Anahtarlı Kriptografi, Postgraduate, 2022 - 2023

Kodlama Teorisi, Postgraduate, 2022 - 2023
Kriptografiye Giriş ve Uygulamaları, Postgraduate, 2022 - 2023
Temel Bilgisayar Teknolojileri II, Undergraduate, 2020 - 2021
GENEL MATEMATİK-2, Undergraduate, 2018 - 2019
Temel Bilgisayar Teknolojileri I, Undergraduate, 2019 - 2020
GENEL MATEMATİK-I, Undergraduate, 2018 - 2019
LİNEER CEBİR, Undergraduate, 2018 - 2019

Advising Theses

Sinak A., Standart Varsayımlardan Kuantum Güvenli Polinom Taahhüt Şemaları, Doctorate, B.NUR(Student), 2026
Sinak A., Sonlu Cisimler Üzerindeki Kriptografik Fonksiyonlardan Doğrusal Kodların Tasarımı Üzerine bir Çalışma, Postgraduate, M.ALİ(Student), 2024
Sinak A., A study on prime number test methods used in cryptography, Postgraduate, F.ÇETİN(Student), 2021

Jury Memberships

Doctorate, Doctorate, Middle East Technical University, September, 2024
Doctoral Examination, Doctoral Examination, Necmettin Erbakan University, April, 2024
Doctorate, Doctorate, Middle East Technical University, January, 2024
PhD Thesis Monitoring Committee Member, PhD Thesis Monitoring Committee Member, Middle East Technical University, January, 2024
PhD Thesis Monitoring Committee Member, PhD Thesis Monitoring Committee Member, Necmettin Erbakan University, December, 2023
Post Graduate, Post Graduate, Ondokuz Mayis University, July, 2023
Post Graduate, Post Graduate, Middle East Technical University, July, 2023
Doctorate, Doctorate, Ondokuz Mayis University, July, 2023
Doctorate, Doctorate, Middle East Technical University, July, 2023
Doctoral Examination, Doctoral Examination, Necmettin Erbakan University, March, 2023
PhD Thesis Monitoring Committee Member, PhD Thesis Monitoring Committee Member, Middle East Technical University, January, 2023
Doctoral Examination, Doctoral Examination, Middle East Technical University, January, 2023
Post Graduate, Post Graduate, Necmettin Erbakan University, June, 2022
PhD Thesis Monitoring Committee Member, PhD Thesis Monitoring Committee Member, Middle East Technical University, January, 2022
Post Graduate, Post Graduate, Middle East Technical University, July, 2021
Post Graduate, Post Graduate, Middle East Technical University, July, 2021
PhD Thesis Monitoring Committee Member, PhD Thesis Monitoring Committee Member, Middle East Technical University, January, 2021

Published journal articles indexed by SCI, SSCI, and AHCI

I. **Minimal linear codes derived from weakly regular bent and plateaued functions**
Mesnager S., SINAK A.
Journal of Algebra and its Applications, vol.23, no.7, 2024 (SCI-Expanded)
II. **Construction of minimal linear codes with few weights from weakly regular plateaued functions**
SINAK A.
Turkish Journal of Mathematics, vol.46, no.3, pp.953-972, 2022 (SCI-Expanded)

III. **Minimal linear codes from weakly regular plateaued balanced functions**
SINAK A.
Discrete Mathematics, vol.344, no.3, 2021 (SCI-Expanded)

IV. **Secondary constructions of (non)weakly regular plateaued functions over finite fields**
Mesnager S., ÖZBUDAK F., SINAK A.
Turkish Journal of Mathematics, vol.45, no.5, pp.2295-2306, 2021 (SCI-Expanded)

V. **Threshold-based post-quantum secure verifiable multi-secret sharing for distributed storage blockchain**
Mesnager S., SINAK A., YAYLA O.
Mathematics, vol.8, no.12, pp.1-15, 2020 (SCI-Expanded)

VI. **Several classes of minimal linear codes with few weights from weakly regular plateaued functions**
Mesnager S., SINAK A.
IEEE Transactions on Information Theory, vol.66, no.4, pp.2296-2310, 2020 (SCI-Expanded)

VII. **On q-ary plateaued functions over Fq and their explicit characterizations**
Mesnager S., ÖZBUDAK F., SINAK A., Cohen G.
European Journal of Combinatorics, vol.80, pp.71-81, 2019 (SCI-Expanded)

VIII. **Linear codes from weakly regular plateaued functions and their secret sharing schemes**
Mesnager S., ÖZBUDAK F., SINAK A.
Designs, Codes, and Cryptography, vol.87, no.2-3, pp.463-480, 2019 (SCI-Expanded)

IX. **On the p-ary (cubic) bent and plateaued (vectorial) functions**
Mesnager S., ÖZBUDAK F., SINAK A.
Designs, Codes, and Cryptography, vol.86, no.8, pp.1865-1892, 2018 (SCI-Expanded)

X. **Free storage basis conversion over finite fields**
AKYILDIZ E., Harold N. Y., SINAK A.
Turkish Journal of Mathematics, vol.41, no.1, pp.96-109, 2017 (SCI-Expanded)

Articles Published in Other Journals

I. **Minimal linear codes with six-weights based on weakly regular plateaued balanced functions**
SINAK A.
INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, vol.10, no.3, pp.86-98, 2021 (Peer-Reviewed Journal)

II. **Minimal Linear Codes with Few Weights and Their Secret Sharing**
MESNAGER S., SINAK A., YAYLA O.
INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, vol.8, no.4, pp.77-87, 2019 (Peer-Reviewed Journal)

III. **End-2-End Verifiable Internet Voting Protocol Based on Homomorphic Encryption**
SINAK A., Özkan S., Yıldırım H., Kiraz M. S.
INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, vol.3, no.2, pp.165-181, 2014 (Peer-Reviewed Journal)

Books & Book Chapters

I. **Sır Paylaşım Şemaları ve Blokzincir**
SINAK A.
in: Siber Güvenlik ve Savunma: Blokzincir ve Kriptoloji, Akleylek, Sedat; Sağıroğlu, Şeref, Editor, Nobel, Ankara, pp.441-490, 2021

II. **Characterizations of Partially Bent and Plateaued Functions over Finite Fields**
MESNAGER S., ÖZBUDAK F., SINAK A.

in: Arithmetic of Finite Fields, Budaghyan L., Rodríguez-Henríquez F. (eds), Editor, Springer, LNCS Book series, Volume 11321, pp.224-241, 2018

III. **Explicit Characterizations for Plateaued-ness of p-ary (Vectorial) Functions**
CARLET C., MESNAGER S., ÖZBUDAK F., SINAK A.
in: Codes, Cryptology and Information Security, El Hajji, Said, Nitaj, Abderrahmane, Souidi, El Mamoun, Editor, Springer, LNCS Book series, 10194, pp.328-345, 2017

IV. **Results on Characterizations of Plateaued Functions in Arbitrary Characteristic**
Mesnager S., ÖZBUDAK F., SINAK A.
in: Cryptography and Information Security in the Balkans, Pasalic, Enes and Knudsen, Lras R., Editor, Springer, LNCS Book series, Volume 9540, pp.17-30, 2016

V. **On Verification of Restricted Extended Affine Equivalence of Vectorial Boolean Functions**
ÖZBUDAK F., SINAK A., YAYLA O.
in: ARITHMETIC OF FINITE FIELDS, Çetin Kaya Koç, Sihem Mesnager, Erkay Savaş, Editor, Springer, Cham, LNCS Book series, Volume 9061, pp.137-154, 2015

Refereed Congress / Symposium Publications in Proceedings

I. **CODE-BASED CRYPTOSYSTEMS MCNIE REVISITED**
AKLEYLEK S., AYDOĞMUŞ E., SINAK A.
Applications of Computer Algebra (ACA), SCALE, GEBZE, Turkey, 15 August 2022

II. **Infinite Classes of Six-Weight Linear Codes Derived from Weakly Regular Plateaued Functions**
MESNAGER S., SINAK A.
2020 International Conference on Information Security and Cryptology (ISCTURKEY), Turkey, 3 - 04 December 2020, pp.93-100

III. **Strongly Regular Graphs from Weakly Regular Plateaued Functions**
MESNAGER S., SINAK A.
2019 Ninth International Workshop on Signal Design and its Applications in Communications (IWSDA), Dongguan, China, China, 20 - 24 October 2019, pp.1-5

IV. **Minimal linear codes and their secret sharing schemes**
SINAK A.
International Conferenceon MathematicsandMathematics Education(ICMME 2019), Konya, Turkey, 11 - 13 July 2019, pp.239-240

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

VI. **Characterizations of Partially Bent and Plateaued Functions over Finite Fields**
MESNAGER S., ÖZBUDAK F., SINAK A.
WAIFI-2018, Bergen, Norway, 14 - 16 June 2018

VII. **A New Class Of Three-Weight Linear Codes From Weakly Regular Plateaued Functions**
MESNAGER S., ÖZBUDAK F., SINAK A.
The Tenth International Workshop on Coding and Cryptography 2017, Pietersburg, South Africa, 18 - 22 September 2017

VIII. **Explicit Characterizations for Plateaued-ness of p-ary (Vectorial) Functions**
CARLET C., MESNAGER S., ÖZBUDAK F., SINAK A.
Second International Conference, In honor of Professor Claude Carlet (C2SI-2017), Rabat, Malta, 10 - 12 April 2017

IX. **Characterizations of plateaued functions in arbitrary characteristic**
Mesnager S., ÖZBUDAK F., SINAK A.
The International Conference on Coding theory and Cryptography ICCC2015, Alger, Algeria, 2 - 05 November 2015

X. **Results on characterizations of plateaued functions in arbitrary characteristic**

Mesnager S., ÖZBUDAK F., SINAK A.
BalkanCryptSec 2015, Koper, Slovenia, 3 - 04 September 2015

XI. **On Verifiation of Restricted Extended Affine Equivalence of Vectorial Boolean Functions**
ÖZBUDAK F., SINAK A., YAYLA O.
International Workshop on the Arithmetic of Finite Fields, Gebze, Turkey, 26 - 28 September 2014, pp.78-91

XII. **Security Requirements of Electronic Voting and Cryptographic Measures**
SINAK A., Kiraz M. S.
International Symposium on Digital Forensics, 30 May - 01 June 2014

XIII. **A Secure Internet Voting Protocol Based on Homomorphic Encryption**
SINAK A., KİRAZ M. S., ÖZKAN S., YILDIRIM H.
ISCTURKEY 2013, Proceedings of 6th International Conference on Information Security and Cryptology, Turkey, 20 - 21 September 2013, pp.142-148

XIV. **An Efficient and Secure Internet Voting Protocol Based on Homomorphic Encryption**
SINAK A., YILDIRIM H., ÖZKAN S., KİRAZ M. S.
Kripto Günleri, Tübitak, Gebze, TÜRKİYE, Turkey, 14 - 15 June 2013

XV. **Modular Multiplication Algorithms For Finite Field Multiplication in GFp**
CENK M., SINAK A.
Antalya Algebra Days XVI, Turkey, 9 - 11 May 2013

Supported Projects

Sinak A., Akleylek S., TÜBİTAK International Multi-Cooperation Project, Formal Analysis and Verification of Post-Quantum Cryptographic Protocols (FAVPQC), 2021 - 2023
Sinak A., Aybak L., Çomak P., Otal K., Özbudak F., Project Supported by Higher Education Institutions, ARC İNŞAALARI VE WEİERSTASS NOKTALARININ KODLAMA TEORİSİNE VE KRİPTOGRAFİYE UYGULAMALARI, 2017 - 2017
Sinak A., Özbudak F., Project Supported by Higher Education Institutions, Yan Kanal Analizi Aritmetik Karmaşıklık Alt Uzay Kodlar Diziler ve Boole Fonksiyonlar, 2016 - 2016
Sinak A., Özbudak F., Project Supported by Higher Education Institutions, BOOLE FONKSİYONLARI KODLAMA TEORİSİ VE KRİPTOGRAFİ, 2015 - 2015
Sinak A., Özbudak F., Project Supported by Higher Education Institutions, Boole Fonksiyonları, Cebirsel Eğriler ve Ağ Kodlaması, 2014 - 2014

Memberships / Tasks in Scientific Organizations

Algebra, Geometry, Combinatorics, and applications to Cryptography and Coding research group in Laboratory Analysis, Geometry and Applications (LAGA), CNRS, Paris, Member, 2015 - Continues, France
Society for Industrial and Applied Mathematics: SIAM , Member, 2011 - Continues, United States Of America
Turkish Mathematical Society, Member, 2011 - Continues, Turkey

Scientific Refereeing

TUBITAK Project, 1507 - TÜBİTAK SME R&D Start Support Program, AyroTek, Turkey, May 2024
TUBITAK Project, 1507 - TÜBİTAK SME R&D Start Support Program, TALETRO YAZILIM VE BİLGİ TEKNOLOJİLERİ TİCARET LİMİTED ŞİRKETİ, Turkey, April 2024
TUBITAK Project, 1005 - National New Ideas and Products Research Support Program, Turkey, January 2024
TUBITAK Project, 1507 - TÜBİTAK SME R&D Start Support Program, Turkey, December 2023
TUBITAK Project, 1501 - Industry R & D Projects Support Program, Turkey, June 2023
TUBITAK Project, 1002 - Quick Support Program, Turkey, June 2023

TUBITAK Project, 2204-A High School Students Research Projects Competition , Necmettin Erbakan University, Turkey, April 2023
TUBITAK Project, 1507 - TÜBİTAK SME R&D Start Support Program, Necmettin Erbakan University, Turkey, November 2022
TÜBİTAK International Bilateral Joint Cooperation Program Project, The Slovenian Research Agency, ARRS Bilateral Joint Cooperation Program, Necmettin Erbakan University, Turkey, May 2022
TUBITAK Project, 1002 - Quick Support Program, Turkey, April 2022
TUBITAK Project, 2204-A High School Students Research Projects Competition , Necmettin Erbakan University, Turkey, February 2022
TUBITAK Project, 2204-A High School Students Research Projects Competition , Necmettin Erbakan University, Turkey, February 2021
TUBITAK Project, 2204-B Middleschool Students Research Projects Competition , Necmettin Erbakan University, Turkey, March 2020

Tasks In Event Organizations

Sinak A., 17.th International Conference on Information Security and Cryptology (ISCTURKEY), Scientific Congress, Ankara, Turkey, Ekim 2024
Sınak A., Algorithms in Cryptography and Blockchain, The 27th Applications of Computer Algebra (ACA) conference series in SCALE, Scientific Congress, Kocaeli, Turkey, Ağustos 2022
Sinak A., 2020 International Conference on Information Security and Cryptology (ISCTURKEY) - ANATOLIAN CRYPT, Scientific Congress, Ankara, Turkey, Aralık 2020
Sinak A., 12th International Conference on Information Security and Cryptology-ISCTURKEY 2019, Scientific Congress, Ankara, Turkey, Ekim 2019
Sinak A., International Conference on Mathematics and Mathematics Education (ICMME-2019), , Scientific Congress, Konya, Turkey, Temmuz 2019
Sinak A., Second International Workshop on Cryptography and Its Applications (2 IWCA 19), U.S.T.O-MB, Workshop Organization, Oran, Algeria, Haziran 2019

Metrics

Publication: 33
Citation (WoS): 161
Citation (Scopus): 176
H-Index (WoS): 7
H-Index (Scopus): 7

Scholarships

French Embassy Research Fellowship for Visiting Researchers, Official Institutions of Foreign Countries, 2024 - 2024
TÜBİTAK- BİDEB 2219 International Postdoctoral Research Fellowship, TUBITAK, 2018 - 2018
TÜBİTAK- BİDEB 2214/A International Research Fellowship Programme , TUBITAK, 2016 - 2017
TÜBİTAK-BİDEB 2211 Ph.D. Students Scholarships , TUBITAK, 2012 - 2017
TÜBİTAK-BİDEB 2210 Master Students Scholarships , TUBITAK, 2011 - 2012
Ministry of Youth and Sports, Credit and Dormitories Institution (KYK) Master Students Scholarships, YOK, 2009 - 2011

Non Academic Experience

University, Paris 8 University, Department of Mathematics
University, Universities of Paris VIII and XIII, CNRS, LAGA (Laboratory: Analysis, Geometry and Applications Laboratory)
University, Paris 8 University , Department of Mathematics