Assoc. Prof. OĞUZ YAYLA

Personal Information

Office Phone: +90 312 210 5695

Email: oguz@metu.edu.tr

Other Email: oguz.yayla@gmail.com

Web: https://avesis.metu.edu.tr/oguz

International Researcher IDs

ScholarID: 83UVe60AAAAJ

ORCID: 0000-0001-8945-2780

Publons / Web Of Science ResearcherID: AAZ-7675-2020

ScopusID: 55317276200

Yoksis Researcher ID: 164658

Education Information

Doctorate, Middle East Technical University, Institute of Applied Mathematics, Cryptography, Turkey 2006 - 2011

Postgraduate, 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

Undergraduate, 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

Postgraduate, 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

Associate Professor, Middle East Technical University, Institute of Applied Mathematics, Cryptography, 2022 - Continues

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

Academic and Administrative Experience

Head of Department, Middle East Technical University, Institute of Applied Mathematics, Cryptography, 2022 - 2025

Assistant Director of the Institute, Middle East Technical University, Institute of Applied Mathematics, Cryptography, 2022 - 2024

Courses

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

Advising Theses

Yayla O., A comprehensive study of time lock puzzles and timed signatures in cryptography, Postgraduate, C.DOĞAN(Student), 2023

YAYLA O., Random sequences in vehicle routing problem, Postgraduate, M.EMİN(Student), 2022

YAYLA O., Blockchain based solution for electronic health record integrity, Postgraduate, K.ÇELİK(Student), 2022

Yayla O., MDS MATRICES OVER RINGS FOR DESIGNING LIGHTWEIGHT BLOCKCIPHER, Postgraduate, G.YETİŞER(Student), 2021

Doğanaksoy A., Yayla O., Gröbner basis attack on Stark-friendly symmetric-key primitives: JARVIS, MiMC and GMiMCerf, Postgraduate, G.KARA(Student), 2021

YAYLA O., Combinatorial solutions for consensus algorithms and blockchain sharding, Doctorate, M.SALEH(Student), 2021

YAYLA O., IMPLEMENTATION ANALYSIS OF CRYPTOGRAPHY TOOLBOX IN HYPERLEDGER, Postgraduate, A.ŞİMŞEK(Student), 2021

Doğanaksoy A., Yayla O., Cryptographic modules validation process according tothe FIPS 140 and ISO/IEC 15408, Postgraduate, C.YENER(Student), 2020

Cenk M., Yayla O., Decentralized secure multiparty computation, Postgraduate, B.TAŞCI(Student), 2019

Yayla O., Almost p-ary perfect sequences and their applications to cryptography, Postgraduate, B.ÖZDEN(Student), 2019

Yayla O., Alternative digital signature schemes in blockchain, Postgraduate, F.YAVUZYİĞİT(Student), 2019

Yayla O., γ-Butson-Hadamard matrices and their cryptographic applications, Postgraduate, 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, Postgraduate, A.SINAK(Student), 2012

Jury Memberships

Doctorate, Doctorate, Orta Doğu Teknik Üniversitesi, August, 2022

Doctorate, Doctorate, Orta Doğu Teknik Üniversitesi, March, 2022

PhD Thesis Monitoring Committee Member, PhD Thesis Monitoring Committee Member, Orta Doğu Teknik Üniversitesi, June, 2020

Competition, 2204 B ORTAOKUL ÖĞRENCİLERİ ARAŞTIRMA PROJELERİ YARIŞMASI, TÜBİTAK, March, 2020

Competition, TÜBİTAK 2204 A LİSE ÖĞRENCİLERİ ARAŞTIRMA PROJELERİ YARIŞMASI, TÜBİTAK, March, 2020

Appointment to Academic Staff-Assistant Professorship, Appointment Academic Staff, Üniversite, September, 2018

Published journal articles indexed by SCI, SSCI, and AHCI

I. **Codes on subgroups of weighted projective tori**
ŞAHİN M., YAYLA O.
Designs, Codes, and Cryptography, vol.92, no.5, pp.1201-1218, 2024 (SCI-Expanded)

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

III. **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)

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

V. **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, vol.90, no.10, pp.2407-2417, 2022 (SCI-Expanded)

VI. **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)

VII. **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, vol.81, 2022 (SCI-Expanded)

VIII. **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 (SCI-Expanded)

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

X. **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)

XI. **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)

XII. **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, vol.10, no.1, pp.151-162, 2016 (SCI-Expanded)

XIII. **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)

XIV. **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)

XV. **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)

XVI. **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 (SCI-Expanded)

Articles Published in Other Journals

I. **Random Sequences in Vehicle Routing Problem**

Gülşen M. E., Yayla O.

LECTURE NOTES IN ARTIFICIAL INTELLIGENCE, vol.13858, no.1, pp.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, vol.8, no.4, pp.77-87, 2019 (Peer-Reviewed Journal)

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, vol.12, no.4, pp.465-471, 2018 (Scopus)

IV. **Near Butson-Hadamard Matrices and Nonlinear Boolean Functions**

Kurt S., YAYLA O.

Lecture Notes in Computer Science, 2018 (Peer-Reviewed Journal)

V. **Families of Pseudorandom Binary Sequences with Low Cross Correlation Measure**

YAYLA O.

Lecture Notes in Computer Sciences, vol.9024, pp.31-39, 2015 (Peer-Reviewed Journal)

VI. **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 (Peer-Reviewed Journal)

VII. **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 (Scopus)

Refereed Congress / Symposium Publications in Proceedings

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

ÖZEREN S., YAYLA O.

2023 16th International Conference on Information Security and Cryptology (ISCTürkiye), Turkey, 18 October 2023

II. **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, Israel, 29 - 30 June 2023, vol.13914 LNCS, pp.398-410

III. **Random Sequences in Vehicle Routing Problem**

Gülen M. E., Yayla O.

10th International Conference on Numerical Methods and Applications, NMA 2022, Borovets, Bulgaria, 22 - 26

August 2022, vol.13858 LNCS, pp.159-170

IV. **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,
Indonesia, 22 - 24 August 2023, pp.236-245

V. **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, Turkey, 15 - 19 August 2022, pp.187-188

VI. **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, Turkey, 19 -
20 October 2022, pp.1-7

VII. **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
December 2021

VIII. **PSO based Blockchain Committee Member Selection**
Jameel M., YAYLA O.
6th International Conference on Computer Science and Engineering, UBMK 2021, Ankara, Turkey, 15 - 17
September 2021, pp.725-730

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

X. **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

XI. **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

XII. **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

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

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

XV. **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

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

XVII. **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

XVIII. **RSA Kriptosistemi Parametreleri için Güvenlik Testi Yazılımı**

Alam B., YAYLA O.

6th International Conference on Information Security and Cryptology, Turkey, 23 - 24 May 2013

XIX. **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

XX. **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, Canada, 4 - 08 June 2012, vol.7280 LNCS, pp.13-24

XXI. **Kriptografik Modüllerin Güvenlik Gereksinimleri**

YAYLA O.

III. International Conference on Information Security and Cryptology, Turkey, 25 - 27 December 2008, vol.3, pp.253-256

XXII. **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

XXIII. **On Algebraic Attacks Using Groebner Basis**

Özadam H., YAYLA O.

II. Information Security and Cryptology Conference, Turkey, 13 - 14 December 2007, pp.312-318

XXIV. **DSA Sisteminin Çalıştırılması ve Test Edilmesi**

YAYLA O.

II. Information Security and Cryptology Conference, Turkey, 13 - 14 December 2007, pp.290-297

XXV. **Scalar multiplication on elliptic curves**

AKYILDIZ E., YAYLA O.

II. National Conference on Cryptology, Turkey, 15 - 17 December 2006, pp.114-124

XXVI. **Ayrık Logaritma Problemini Kullanan E İmza**

CENK M., YAYLA O.

Ulusal Elektronik İmza Sempozyumu, Turkey, 7 - 08 December 2006, pp.381-386

Expert Reports

I. **Kripto varlıkların durumu**

Yayla O., Pişirici E. R.

11. Ağır Ceza Mahkemesi, pp.9, Gaziantep, 2022

Supported Projects

CENK M., YAYLA O., TUBITAK Project, Kriptografik Algoritmaların Tasarımı, Gerçekleştirilmeleri ve Uygulamaları, 2019 - 2027

YAYLA O., Project Supported by Higher Education Institutions, Kombinatorik Tasarımlar, Diziler ve Onların Kriptografik Uygulamaları, 2021 - 2022

Yayla O., TUBITAK Project, Simitli Cebirsel Geometri VeKodlama Teorisine Uygulamaları, 2019 - 2022

Yayla O., TÜBİTAK International Bilateral Joint Cooperation Program Project, Ntru Tabanlı KriptosistemlerinTasarımı Ve Biçimsel Yöntemler ile Analizi, 2019 - 2021

Yayla O., Akleylek S., Kırlar B. B., Özsoy A., Saygı Z., TUBITAK Project, Kafes Tabanlı Güvenilir Kriptografik Protokol Tasarımı Ve Verimli Uygulamaları, 2018 - 2020

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

Activities in Scientific Journals

TURKISH JOURNAL OF MATHEMATICS, Article Editor, 2019 - Continues
Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, Committee Member, 2016 - Continues

Scientific Refereeing

TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, Journal Indexed in SCI-E, December 2022
ADVANCES IN MATHEMATICS OF COMMUNICATIONS, Journal Indexed in SCI-E, August 2022
TUBITAK Project, 2204-A High School Students Research Projects Competition , Middle East Technical University, Turkey, June 2022
TUBITAK Project, 2204-B Middleschool Students Research Projects Competition , Middle East Technical University, Turkey, May 2022
TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, Journal Indexed in SCI-E, April 2022
TUBITAK Project, 2204-A High School Students Research Projects Competition , Middle East Technical University, Turkey, April 2022
TURKISH JOURNAL OF MATHEMATICS, Journal Indexed in SCI-E, March 2022
Sinyal İşleme ve İletişim Uygulamaları Kurultayı-2022, Conference Paper (Full Text), March 2022
TUBITAK Project, 2204-B Middleschool Students Research Projects Competition , Middle East Technical University, Turkey, March 2022
TURKISH JOURNAL OF MATHEMATICS, Journal Indexed in SCI-E, February 2022
APPLIED SOFT COMPUTING JOURNAL, Journal Indexed in SCI-E, January 2022
TURKISH JOURNAL OF MATHEMATICS, Journal Indexed in SCI-E, January 2022
TURKISH JOURNAL OF MATHEMATICS, Journal Indexed in SCI-E, January 2022
APPLIED SOFT COMPUTING JOURNAL, SCI Journal, December 2021
TUBITAK Project, 1001 - Program for Supporting Scientific and Technological Research Projects, Middle East Technical University, Turkey, December 2021
TUBITAK Project, 1001 - Program for Supporting Scientific and Technological Research Projects, Middle East Technical University, Turkey, November 2021
DESIGNS, CODES, AND CRYPTOGRAPHY, SCI Journal, August 2021
TUBITAK Project, 2204-B Middleschool Students Research Projects Competition , Middle East Technical University, Turkey, August 2021
TURKISH JOURNAL OF MATHEMATICS, Journal Indexed in SCI-E, June 2021
TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, Journal Indexed in SCI-E, June 2021
TURKISH JOURNAL OF MATHEMATICS, Journal Indexed in SCI-E, June 2021
TUBITAK Project, 1002 - Quick Support Program, Middle East Technical University, Turkey, June 2021
TUBITAK Project, 2204-A High School Students Research Projects Competition , Middle East Technical University, Turkey, June 2021
TUBITAK Project, 1002 - Quick Support Program, Middle East Technical University, Turkey, May 2021
TUBITAK Project, 2204-A High School Students Research Projects Competition , Middle East Technical University, Turkey, April 2021
TUBITAK Project, 2204-B Middleschool Students Research Projects Competition , Middle East Technical University, Turkey, March 2021
TUBITAK Project, 2219 - Yurt Dışı Doktora Sonrası Araştırma Burs Programı, Middle East Technical University, Turkey,

December 2020

TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, SCI Journal, November 2020

APPLIED SOFT COMPUTING, SCI Journal, November 2020

TURKISH JOURNAL OF MATHEMATICS, SCI Journal, September 2020

TURKISH JOURNAL OF MATHEMATICS, SCI Journal, July 2020

TURKISH JOURNAL OF MATHEMATICS, SCI Journal, July 2020

DESIGNS CODES AND CRYPTOGRAPHY, SCI Journal, April 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

TSE, Scientific Consultancy, Middle East Technical University, Institute of Applied Mathematics, Cryptography, Turkey, 2022 - Continues

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

Tasks In Event Organizations

Kestel A. S., Yayla O., Türk Ö., Workshop on 20th Anniversary of the Institute of Applied Mathematics, Workshop Organization, Turkey, 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), Scientific Congress, İstanbul, Turkey, Ağustos 2022

Metrics

Publication: 50
Citation (WoS): 13
Citation (Scopus): 20
H-Index (WoS): 3
H-Index (Scopus): 3

Congress and Symposium Activities

14. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Panelists, Ankara, Turkey, 2021