DOÇ.DR. ORHUN KARA

Adres
İYTE Matematik Bölümü
TR- 35430, İYTE Gülbahçe Urla / İZMİR
TÜRKİYE

+90 232 750 77 50 (ofis)
orhunkara@iyte.edu.tr
URL: http://web.iyte.edu.tr/~orhunkara/

ÇALIŞMA ALANLARI

Kodlama Teorisi, Kriptoloji, Kriptografik Fonksiyonlar ve Yapı Taşları, Sonlu Cisim Uygulamaları

EĞİTİM

Doktora – Matematik –Bilkent Üniversitesi *2003*
Tez Konusu: .Modüler Eğriler Üzerine Kod İnşası (Code Construction on Modular Curve)
Tez Danışmanı: Alexander Klyachko

Yüksek Lisans - Matematik –Bilkent Üniversitesi *1998*
Tez Konusu: Modüler Eğrilerin Düzlem Modellerinin Tekillikleri (Singularities of Plane Models of Modular Curves)
Tez Danışmanı: Alexander Klyachko

Lisans – Matematik –Bilkent Üniversitesi *1996*
Bitirme Tezi Konusu: Bazı Cebirsel Kümelerin Projektif Kapalılıkları (Projective Closures of Some Algebraic Sets)

DİL

- İngilizce: İleri Düzeyde (e-YDS 88,75)
- Almanca: Başlangıç Düzeyinde

İŞ DENEYİMİ

İYTE İzmir Yüksek Teknoloji Enstitüsü *2020– devam ediyor*
https://en.iyte.edu.tr/
Fen Fakültesi Matematik Bölümü
Urla/İzmir Türkiye
Faculty member, Assoc. Prof. Dr.

TÜBİTAK - BİLGEM- Blokzincir Araştırma Labı *2020 – devam ediyor*
https://blokzincir.bilgem.tubitak.gov.tr/en/
Gebze/Kocaeli Türkiye
Danışman

Fame Crypt Co. Ltd. *2021 – 2023*
https://famecrypt.com.tr/en/
ODTÜ/Ankara, Türkiye
Danışman

2002 – 2020

TÜBİTAK - Bilişim ve Bilgi Güvenliği İleri Teknolojiler ve Enformatik Araştırma Merkezi
TUBITAK-BİLGEM-UEKAE
Kriptoloji Bölümü
Gebze
Bölüm Yöneticisi/Proje Yürütücüsü
Başuzman Araştırmacı (2007'ye kadar Uzman Araştırmacı)

Institute de Mathématiques de Luminy – IML, CNRS *2001-2002*
Matematik Bölümü
Marsilya/ Fransa
Misafir Araştırmacı (Prof. Serge Vladut'un misafiri olarak)

TÜBİTAK - UEKAE *2000-2001*
Kriptoloji Bölümü
Gebze
Araştırmacı

Bilkent Üniversitesi *1996-2000*
Matematik Bölümü
Ankara
Asistan

PANALİST VE DELEGELİK

- AB IC1403 Cryptacus ICT Cost aksiyonu Yönetim Kurulu Üyesi (Management Committee Member); 2015-2019
- AB IC1306 CryptoAction ICT Cost aksiyonu Yönetim Kurulu Yedek Üyesi (Management Committee Subsitute Member); 2014-2018
- Springer CCIS (Commnucations in Computer Information Science) Serisi editörlüğü; 2012-2017
- Panelist – NATO SfP ISEG (Independent Scientific Elavuation Group) Panel üyeliği; 2011- 2013
- Panelist – NATO SfP ICS (Information and Communication Security) Panel üyeliği; 2008- 2011
- OECD "Global Science Forum Math in Industry" Türkiye Delegesi OECD; 2006
- AB 6. Çerçeve programı IST uzmanı; AB 2006-2008

PROJELER

- TUBITAK 1001 Araştırma Projesi: Hafifsıklet akan şifreleme algoritmaları tasarım ve analizi, 2021-2024
- Avrupa Birliği IC1403- Cryptacus (Cryptanalysis of Ubiquitous Computing Systems) ICT Cost Aksiyonu: Yönetim Komitesi Üyesi 2015-2019
- Avrupa Birliği ICE FP7- REGPOT 2007-1 Projesi –İş Paketi Yöneticisi/ ICE Projesi yaklaşık 1M Avro bütçeli AB 7. çerçeve bir altyapı geliştirme projesidir. Projede eğitim iş paketi (Training Activities WP) Yöneticisi 2008-2011
- Avrupa Birliği IC1306 CryptoAction ICT Cryptography for Secure Digital Interaction adlı Cost aksiyonu Yönetim Kurulu Yedek Üyesi (Management Committee Subsitute Member); 2014-2018.
- TÜBİTAK 1001 Güvenli ve Kullanışlı Resim-Şifre Yöntemlerinin Tasarlanması ve Gerçekleştirilmesi Projesi – 2008-2010
- TÜBİTAK BİLGEM IFF Mod5 Projesi (TÜBİTAK 1007) – Kriptografik Fonksiyonların Tasarımları İş Paketi Yöneticisi, 2007-20012
- TÜBİTAK BİLGEM Göktürk-1 Projesi – Kriptografik Fonksiyonların Tasarımı İş Paketi Yöneticisi, 2008-2012
- TÜBİTAK BİLGEM Güvenli IP Haberleşme Cihazı Geliştirme Projesi- Kriptografik Mimari ve Fonksiyonların Tasarımı İş Paketinin Yöneticisi, 2007 - Devam ediyor
- TÜBİTAK BİLGEM MAMSİS Projesi – Kriptografik Fonksiyonların Tasarımı İş Paketi Yöneticisi, 2004-2007
- TÜBİTAK BİLGEM MİLSEC-4 Güvenli Ses Haberleşmesi Projesi – Kriptografik Mimari ve Fonksiyonların Tasarımı İş Paketi Yöneticisi, 2013-2019
- TÜBİTAK BİLGEM EKADAS Anahtar Dağıtımı ve Yönetimi Projesi (TÜBİTAK SAVTAK) – Kriptografik Mimari ve Fonksiyonların Tasarımı İş Paketi Yöneticisi, 2012-2019

BURS VE ÖDÜLLER

TÜBİTAK BİLGEM inovasyon ödülü	*2012*
BİLKENT Üniversitesi Matematik Alisbah en iyi lisansüstü öğrenci ödülü	*2002*
TÜBİTAK Yurtdışı Bütünleştirilmiş Doktora Bursu	*2001-2002*
Bilkent Üniversitesi Yüksek lisans/Doktora tam burslu	*1996-2000*
Bilkent Üniversitesi lisans tam burslu	1991-1996

YÖNETİLEN TEZLER

- Sırrı Erdem Ulusoy, “Extensive Cryptanalysis of Authenticated Encryption with Associated Data Algorithm COLM”, Doktora tezi, Hacettepe Üniversitesi, 2023.

  Tezden çıkan yayın: Sırrı Erdem Ulusoy, Orhun Kara, and Mehmet Önder Efe. "Plaintext recovery and tag guessing attacks on authenticated encryption algorithm COLM." *Journal of Information Security and Applications* 70, pp. 103342, (2022) DOI: 10.1016/j.jisa.2022.103342

- Çağdaş Gül, “Security and performance analysis of symmetric ciphers with SPN construction, and their design”, Yüksek lisans tezi, Marmara Üniversitesi, 2022.

  Tezden çıkan yayın: Çağdaş Gül, Orhun Kara, “A New Construction Method for Keystream Generators”, IEEE Transactions on Information Forensics and Security, vol.18, pp 3735 – 3744 (2023). DOI: 10.1109/TIFS.2023.3287412

- Fatih Demirbaş, “Enhancement of Integral Cryptanalysis for some block ciphers”, Yüksek lisans tezi, Marmara Üniversitesi, 2020.

  Tezden çıkan yayın: Fatih Demirbaş and Orhun Kara. "Integral characteristics by keyspace partitioning." *Designs, Codes and Cryptography* 90, no. 2 (2022): 443-472. DOI: 10.1007/s10623-021-00989-y

- Ebru Küçükkubat, “Parametric guess and determine attack on stream ciphers”, MSc Thesis, İstanbul City University- Yüksek lisans tezi, İstanbul Şehir Üniversitesi - Marmara Üniversitesi, 2019.

  Tezden çıkan yayın: Orhun Kara, Ebru Küçükkubaş, Parametric Guess and Determine Attack on Stream Ciphers, W06. Workshop on Machine Learning for Security and Cryptography of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 8-11 Sept 2019, Istanbul, Turkey

- İlker Yasin Yıldız, “An improved attack on keystream generators with Boolean keyed feedback function”, MSc Thesis, Yüksek lisans tezi, İstanbul Şehir Üniversitesi - Marmara Üniversitesi, 2019.

  Tezden çıkan yayın: Yok.

KİTAPLAR VE KİTAP BÖLÜMLERİ

- Mehmet Emin Gönen, Orhun Kara and Ferhat Karakoç, “Simetrik Sistemlerde Kriptoanaliz Yöntemleri”, *Siber Güvenlik ve Savunma: Blokzincir ve Kriptoloji* (Vol. 5). Nobel Akademik Yayıncılık, Ankara, ISBN: 978-625-417-110-9, pp. 347-428, 2021 (In Turkish),
- Orhun Kara "Tradeoff Attacks on Symmetric Ciphers." In *Cryptography-Recent Advances and Future Developments*. IntechOpen, pp-127-141, ISBN-13 : 978-1839625657, 2021.
- Gildas Avoine, Orhun Kara: Lightweight Cryptography for Security and Privacy - Second International Workshop, LightSec 2013 Lightweight Cryptography for Security & Privacy, Revised Selected Papers. Lecture Notes in Computer Science LNCS 8162, Springer 2013, ISBN 978-3-642-40391-0.
- Orhun Kara, Alexander Klyachko: How to Break Gilbert-Varshamov Bound: Goppa Codes on Modular Curves, VDM Verlag ISBN-13: 978-3639143195, 2009.
- Vasily Mikhalev, Miodrag Mihaljevic, Orhun Kara, Frederik Armknecht, Selected Design and Analysis Techniques of Contemporary Symmetric Encryption, Book Chapter, Security of Ubiquitous Computing Systems, Cryptacus Project, ISBN 978-3-030-10591-4, pp. 35-48, Springer, 2021.
- Aleksandra Mileva, Vesna Dimitrova, Orhun Kara, Miodrag J. Mihaljevic, Catalog and Illustrative Examples on Lightweight Cryptographic Primitives, Book Chapter, Security of Ubiquitous Computing Systems, Cryptacus Project, ISBN 978-3-030-10591-4, pp. 17-34, Springer 2021.

ULUSLARARASI DERGİ YAYINLARI

- Orhun Kara, “"New Security Proofs and Complexity Records for Advanced Encryption Standard," in *IEEE Access*, vol. 11, pp. 131205-131220, 2023. DOI: 10.1109/ACCESS.2023.3335271.
- Çağdaş Gül, Orhun Kara, “A New Construction Method for Keystream Generators”, IEEE Transactions on Information Forensics and Security, vol.18, pp 3735 – 3744 (2023). DOI: 10.1109/TIFS.2023.3287412
- Sırrı Erdem Ulusoy, Orhun Kara, and Mehmet Önder Efe. "Plaintext recovery and tag guessing attacks on authenticated encryption algorithm COLM." *Journal of Information Security and Applications* 70, pp. 103342, (2022) DOI: 10.1016/j.jisa.2022.103342
- Fatih Demirbaş and Orhun Kara. "Integral characteristics by keyspace partitioning." *Designs, Codes and Cryptography* 90, no. 2 (2022): 443-472. DOI: 10.1007/s10623-021-00989-y

---

- Orhun Kara and Muhammed Esgin, On Analysis of Lightweight Stream Ciphers with Keyed Update, IEEE Transactions on Computers, 68(1): 99-110 (2019) DOI: 10.1109/TC.2018.2851239
- Orhun Kara, İmran Ergüler and Emin Anarım, A new security relation between information rate and state size of a keystream generator, Turk J Elec Eng & Comp Sci, 24, 1916-1929, 2016 DOI:10.3906/ELK-1311-54
- Orhun Kara, Square Reflection Cryptanalysis of 5-round Feistel Networks with Permutations. Inf. Process. Lett. 113(19-21): 827-831, 2013. DOI: 10.1016/J.IPL..2013.08.001
- Adnan Baysal and Orhun Kara, How biased are linear biases? International Journal of Information Security Science, Vol.1 No:1, pp.20-31, 2012.
- Orhun Kara and Adem Atalay, Tradeoff tables for compression functions: how to invert hash values, Turk J Elec Eng & Comp Sci, Vol.20, No.1 pp 57-70, 2012. DOI:10.3906/ELK-1003-412
- Alexander Klyachko and Orhun Kara, Singularities of Modular Curve, Finite Fields and Their Applications, 7, 2001, pp. 415-420. DOI: 10.1006/FFTA.2001.0319

ULUSLARARASI BİLDİRİLER

- Orhun Kara, "How to Exploit Biham-Keller ID Characteristic to Minimize Data," 2022 15th International Conference on Information Security and Cryptography (ISCTURKEY), Ankara, Turkey, 2022, pp. 44-48, DOI: 10.1109/ISCTURKEY56345.2022.9931847
- Orhun Kara, Ebru Küçükkubaş, Parametric Guess and Determine Attack on Stream Ciphers, W06. Workshop on Machine Learning for Security and Cryptography of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 8-11 Sept 2019, Istanbul, Turkey
- Muhammed F. Esgin, Orhun Kara: Practical Cryptanalysis of Full Sprout with TMD Tradeoff Attacks. Selected Areas in Cryptography SAC 2015: Lecture Notes in Computer Science, LNCS Volume 9566, 67-85, 2016, DOI: 10.1007/978-3-319-31301-6_4, Sackville, Canada.
- Orhun Kara, Ferhat Karakoç: Fixed Points of Special Type and Cryptanalysis of Full GOST. CANS 2012, The 11th International Conference on Cryptology and Network Security: Lecture Notes in Computer Science, LNCS Volume 7712, 86-97, 2012, DOI: 10.1007/978-3-642-35404-5_8, Darmstadt, Germany.
- Orhun Kara, Ferhat Karakoç, Success Probability of the first attack on full round GOST, In Proc. ISCTurkey 2012, The 5th international Information Security and Cryptology Conference, pp 230-234, 2012, Ankara, Turkey
- Orhun Kara, Security Margin of 5-round DEAL, In Proc. ISCTurkey 2012, The 5th international Information Security and Cryptology Conference, pp 183-186, 2012, Ankara, Turkey
- Adnan Baysal, Orhun Kara, How biased are linear biases? In Proc. ISCTurkey 2012, The 5th international Information Security and Cryptology Conference, pp 187-194, 2012, Ankara, Turkey
- Orhun Kara, Süleyman Kardaş, M.Ali Bingöl, Gildas Avoine, Optimal Security Limits of RFID Distance Bounding Protocols, RFIDSEC 2010, RADIO FREQUENCY IDENTIFICATION: SECURITY AND PRIVACY ISSUES, Lecture Notes in Computer Science, LNCS Volume 6370/2010, 220-238, Springer, 2010, DOI: 10.1007/978-3-642-16822-2_18, Istanbul, Turkey
- Süleyman Kardaş, Muhammed Bingöl, Orhun Kara, Ali Özhan Gürel, A new RFID Distance Bounding Protocol, In Proc. of ISCTurkey 2010, The 3rd.international Information Security and Cryptology Conference, pp. 3-8 2010, Ankara, Turkey
- Adem Atalay, Orhun Kara, DES'in FPGA'de Hafifsıklet Gerçeklenmesi, In Proc. IN PROC. ISCTURKEY 2010, The 3rd international Information Security and Cryptology Conference, pp. 279-283, 2010, Ankara, Turkey
- Orhun Kara, Adem Atalay, Preimages Of Hash Functions Through Rainbow Tables, ISCIS 2009, The 24th Symposium on Computer and Information Sciences, 2009, DOI: 10.1109/ISCIS.2009.5291831, Güzelyurt, KKTC

- Orhun Kara, Reflection Cryptanalysis of Some Ciphers, Proc. Indocrypt 2008, Lecture Notes on Computer Science LNCS 5365, pp. 294-307, Springer, 2008 DOI: 10.1007/978-3-540-89754-5_23 Karaghpur, India
- Orhun Kara, Imran Ergüler, A new Approach to Keystream Based Cryptosystems, In proc. of SASC 2008 - The State of the Art of Stream Ciphers, pp. 205-222, Ecrypt, 2008, DOI: 10.1007/978-3-540-74619-5_11, Lousanne, Switzerland
- Esen Akkemik, Orhun Kara. Real Time Cryptanalysis of Unsystematic Cipher,In proc. SAM 2008 The 2008 International Conference on Security and Management, pp. 514-522, CSREA Press, 2008, Las Vegas, USA
- Orhun Kara, Cyrptanalysis of Strengtened Magenta, Proc. ISCTurkey 2008, The 2nd international Information Security and Cryptology Conference, pp. 27-30, 2008 Ankara Turkey
- Esen Akkemik, Orhun Kara, Ayşegül Kurşunlu, On Meier-Staffelbachs Fast Correlation Attack, In Proc. ISCTurkey, The 2nd international Information Security and Cryptology Conference, pp. 107-113, 2008, Ankara Turkey
- Orhun Kara, Cevat Manap, A New Class of Weak Keys for Blowfish, proceedings of FSE 2007, Fast Software Encryption 2007. Lecture Notes on Computer Science, LNCS 4593, pp 167-180, Springer 2007, DOI: 10.1007/978-3-540-74619-5_11, Luxemburg
- Meltem Sönmez Duran, Orhun Kara, Linear Approximations for 2-Round Trivium, In Proc. of SASC 2007, pp. 22-37, 2007, Bochum Gernany
- Esen Akkemik, Orhun Kara, Cevat Manap, Success rate of reflection attack on some DES variants, SINCONF 2007, International conference on Security of Information and Networks, 2007, Gazi Magusa, KKTC

ULUSAL BİLDİRİLER

- Meltem Sönmez Turan and Orhun Kara, Finding Linear Approximations for the Stream Cipher Trivium, II. Ulusal Kriptoloji Sempozyumu, pp. 146-153, 2006, Ankara Turkey
- Orhun Kara, Self Similarity Analysis of Iterated Functions, II. Ulusal Kriptoloji Sempozyumu, pp. 11-18, 2006, Ankara Turkey

DAVETLİ KONUŞMALAR

- How to design secure stream ciphers vulnerable to tradeoff attacks! 13 October 2023, CNRS, IRISA, INSA Rennes, France.
- Impossible differential attacks on Substitution Permutation Networks, 20-21 July 2023, METU, Ankara, Türkiye.
- Fundamental building blocks of post-quantum cryptography, NATO SfS activity 22 September 2022, Baku, Azerbaijan.
- Integral Analysis of Some Block Ciphers, 7 December 2021, Acıbadem University, İstanbul, Türkiye.
- Cryptographic Functions Need secure and efficient RNGs, 16 October 2020, NChain, London, United Kingdoms.
- Kuantum Bilgisayarlara Önlem Almalı mıyız? ISCTurkey 12. Uluslararası Bilgi Güvenliği Konferansı, Siber Güvenlik ve kuantum Sonrası Kriptoloji, BTK, 16 Ekim 2019, Ankara
- Kuantum Bilgisayar Sonrası Şifreleme, TOBB ETÜ, Genel Seminer, 30 Eylül 2019, Ankara

- Cryptology in our daily lifes, Boğaziçi Üniversitesi Fen Fakültesi, 21 Mart 2019, İstanbul
- Geçmişten Günümüze Hayatımızda Kriptoloji ve Bilgi Güvenliği, Koç Universitesi, Engineering Seminars, 26 Şubat 2019, İstanbul
- Do Lightweight Stream Ciphers Become Extinct? SRG (Security Research Group) Seminars, TOBB ETÜ, 19 Şubat 2019, Ankara
- Security analysis of Keystream Generators with Keyed Update Functions, Lightweight Crypto Day 2018, Bar Ilan University, 24-29 Nisan 2018, Tel Aviv
- Block Ciphers vs Stream Ciphers on Ultra Lightweight Platforms, Keynote speech, Lightsec 2016 Lightweight Cryptography for Security & Privacy, Aksaray Üniversitesi, 20-21 Eylül 2016, Aksaray
- The security of Lightweight Algorithms, Lightweight Crypto Day, Technion Israel Institute of Technology, 28 Mart 2016, Haifa.
- Cryptanalysis of stream ciphers with keyed update functions, Atılım Üniversitesi I. Atılım Kripto Çalıştayı, 30-31 Mayıs 2016, Ankara
- Kriptolojinin Temel Kavramları, Yıldız Teknik Üniversitesi, Kriptoloji ve Cebirsel Kodlama Çalıştayı, 10-12 Eylül 2015, İstanbul
- Hafif Sıklet Kripto Algoritmaları Güvenlikte de Hafif Sıklet midir? II. Ulusal Kripto Günleri, TÜBİTAK BİLGEM, 9-11 Nisan 2015, Gebze
- Şifreleme Bilimi ve Uygulama Alanları, Sakarya Üniversitesi Bilgisayar Mühendisliği, 22 Mart 2013, Sakarya
- "RFID Uygulamalarında Yeni Trendler", İTÜ/3. RFID Uygulamaları Sempozyumu, İstanbul Teknik Üniversitesi, 10 Haziran 2010, İstanbul
- Kriptoloji ve Hayatımızdaki Yeri, Eskişehir Osmangazi Üniversitesi Sektörde Matematik Sempozyumu, 2011, Eskişehir
- Kriptolojinin Temelleri, TÜBİTAK Feza Gürsoy Kriptoloji Bilgi Günü, 13 Ekim 2010, Ankara

VERİLEN DERSLER

- İYTE Matematik, MATH 583 Post Quantum Cryptography
- İYTE Matematik, MATH 406 Mathematics of Public Key Cryptography
- İYTE Matematik, MATH 313 Introduction to Cryptography
- İYTE Matematik, MATH 366 Number Theory
- İYTE Matematik, MATH 151-152 Calculus for math students
- İYTE Matematik, MATH 141-142 Calculus for eng. and sci. faculties
- ODTÜ Uygulamalı Matematik Enstitüsü – IAM 704 Hash Functions, Authentication Codes and Nonlinearity
- ODTÜ Uygulamalı Matematik Enstitüsü – IAM 705 Stream Ciphers Cryptanalysis
- ODTÜ Uygulamalı Matematik Enstitüsü – IAM 708 Cryptanalysis of Recent Stream Ciphers
- ODTÜ Uygulamalı Matematik Enstitüsü – IAM 706 Selected Topics in Cryptanalysis of Recent Symmetric Ciphers
- Gebze Teknik Üniversitesi Bilgisayar Mühendisliği – SİB 532 Advanced Topics in Cryptography
- Gebze Teknik Üniversitesi Bilgisayar Mühendisliği – SİB 569 Special Studies in Information Security

- Gebze Teknik Üniversitesi Bilgisayar Mühendisliği – SİB 533 Symmetric Ciphers and Their Security Analysis
- İstanbul Şehir Üniversitesi, Doğal ve Uygulamalı Bilimler Enstitüsü – BGM 501 Introduction to Cryptography