Assoc. Prof. Dr. Orhun Kara

Address
IZTECH Izmir Institute of Technology
Math Department Science Faculty
TR- 35430, İYTE Gülbahçe Urla / İZMİR
TURKEY

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

ORCID ID: https://orcid.org/0000-0002-9685-6625

RESEARCH INTERESTS

Coding theory, cryptography (symmetric ciphers and hash functions)

Please click the corresponding icon for my Google Scholar, Orcid, ReseachGate, dblp records and LinkedIn profile respectively. The links are provided at the end of this document for hardcopy users.

EDUCATION

PhD – Mathematics –Bilkent University *2003*
Thesis Title. Code Construction on Modular Curve

MSc - Mathematics –Bilkent University *1998*
Thesis Title. Singularities of Plane Models of Modular Curves

BSc – Mathematics –Bilkent University *1996*
Senior Thesis Project: Projective Closures of Some Algebraic Sets

LANGUAGE

- Turkish: Native Language
- English: Good (2019 YDS=88.75, 2024 YÖKDİL=95)
- German: Beginner

WORK EXPERIENCE

IZTECH İzmir Institute of Technology *2020-cont.*
https://en.iyte.edu.tr/
Science Faculty, Department of Mathematics
Urla/İzmir Türkiye
Faculty member, Assoc. Prof. Dr.

TÜBİTAK - BİLGEM- Block Chain lab *2020 – cont.*
https://blokzincir.bilgem.tubitak.gov.tr/en/
Gebze/Kocaeli Türkiye
Scientific consultant

Fame Crypt Co. Ltd. *2021 – 2023*
https://famecrypt.com.tr/en/
METU/Ankara, Türkiye
Scientific consultant

TÜBİTAK - BİLGEM-UEKAE Cryptology *2002 – 2020*
https://bilgem.tubitak.gov.tr/en/
Gebze/Kocaeli, Türkiye
Division Manager/Project Manager
Chief Researcher (Senior researcher until 2007)

Institute de Mathématiques de Luminy – IML, CNRS *2001-2002*
Mathematics Department
Marseille/France
Visiting Researcher (Prof. Serge Vladut)

TÜBİTAK – UEKAE Cryptology *2000-2001*
https://bilgem.tubitak.gov.tr/en/
Gebze/Kocaeli, Türkiye
Researcher

Bilkent University *1996-2000*
https://w3.bilkent.edu.tr/bilkent/
Science Faculty Mathematics Department
Ankara, Türkiye
Teaching Asistant

PANALIST & DELAGACY

- AB IC1403 Cryptacus ICT Cost Action Management Committee Member; 2015-2019
- AB IC1306 CryptoAction ICT Cost Action Management Committee Substitute Member; 2014-2018
- Springer CCIS Communications in Computer Information Science Series editorship; 2012-2017
- Panelist – NATO SfP ISEG (Independent Scientific Evaluation Group); 2011- 2013
- Panelist – NATO SfP ICS (Information and Communication Security); 2008- 2011
- OECD “Global Science Forum Math in Industry” Turkish delegate OECD; 2006
- AB 6. Framework program, IST expert; AB 2006-2008

PROJECTS

- TÜBİTAK 1001 Research project. Recent cryptanalysis methods for symmetric ciphers and encryption design specific to microcontrollers, 2024. Project Manager. In review
- TÜBİTAK 2531/1071-DAAD Germany. Joint Research Project with DUAS Düsseldorf University of Applied Sciences / Germany. Interoperable Secure Communication and Authentication Schemes for Interconnected IoT Devices with Heterogeneous Capabilities. 2024, Turkish Principle Investigator. In review
- TÜBİTAK 1001 121E228 Research Project: Design and analysis of lightweight stream ciphers, Project manager. 2021-2024
- EU IC1403- Cryptacus (Cryptanalysis of Ubiquitous Computing Systems) ICT Cost Action: Management Committee member 2015-2019
- EU ICE FP7- REGPOT 2007-1 Project–Work Package Leader/ 1M EUR budget EU 7. framework. Training Activities Work package leader 2008-2011
- EU IC1306 Crypto Action ICT Cryptography for Secure Digital Interaction, Cost action Management Committee Substitute Member; 2014-2018.
- TÜBİTAK 1001 Research Project: Design of secure figure passwords– 2008-2010. Researcher
- TÜBİTAK BİLGEM IFF Mod5 Project (TÜBİTAK 1007) –2007-20012, Work package leader
- TÜBİTAK BİLGEM Göktürk-1 Secure communication of satellite project–2008-2012, Work package leader
- TÜBİTAK BİLGEM Development of secure IP device project- 2007 – 2015, Work package leader
- TÜBİTAK BİLGEM MAMSİS Secure e-mail Project 2004-2007, Work package leader
- TÜBİTAK BİLGEM MİLSEC-4 Secure Voice Communication Project, 2013-2019, Work package leader
- TÜBİTAK BİLGEM EKADAS Key Management and PKI project (TÜBİTAK SAVTAK), 2012-2019, Work package leader

SCHOLARSHIP AND AWARDS

- TÜBİTAK BİLGEM innovation award 2012
- BİLKENT University Mathematics Alisbah best graduate student award 2001
- TÜBİTAK Abroad integrated PhD study scholarship 2001-2002
- Bilkent University graduate study scholarship 1996-2003
- Bilkent University undergraduate study scholarship 1991-1996

THESES SUPERVISED

- Sırrı Erdem Ulusoy, “Extensive Cryptanalysis of Authenticated Encryption with Associated Data Algorithm COLM”, PhD Thesis, Hacettepe University, 2023.

  Publication from The Thesis: 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”, MSc Thesis, Marmara University, 2022.

Publication from The Thesis: 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”, MSc Thesis, Marmara University, 2020.

  Publication from The Thesis: 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- Marmara University, 2019.

  Publication from The Thesis: 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, İstanbul City University- Marmara University, 2019.

  Publication from The Thesis: No publication.

BOOKS / EDITORSHIPS / CHAPTERS

- Orhun Kara "Tradeoff Attacks on Symmetric Ciphers." In *Cryptography-Recent Advances and Future Developments*. IntechOpen, pp-127-141, ISBN-13 : 978-1839625657, 2021.
- Mehmet Emin Gönen, Orhun Kara and Ferhat Karakoç, “Cryptanalysis Methods in Symmetric Ciphers”,*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),
- 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.

JOURNAL PAPERS

- Orhun Kara, “Square impossible differential attack and security of AES in known plaintext scenario”, *Cryptologia,* (2024), 1–25. DOI: 10.1080/01611194.2024.2320362.
- Orhun Kara, “Lower data attacks on Advanced Encryption Standard”, *Turk J Elec Eng & Comp Sci.,* (2024) Vol. 32: No. 2, Article 8. DOI: 10.55730/1300-0632.4072 Available at: https://journals.tubitak.gov.tr/elektrik/vol32/iss2/8
- 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. https://ieeexplore.ieee.org/abstract/document/10323405

- 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

CONFERENCE PAPERS

- 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, Lausanne, 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
- 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

INVITED TALKS

- AES Encryption Surrounds Us; We Surround AES Encryption, 31 January 2024, Dokuz Eylül University Faculty of Science Department of Mathematics, İzmir, Türkiye
- 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 (online).

- Do we need to care about quantum computers? ISCTurkey 12. Uluslararası Bilgi Güvenliği Konferansı, Siber Güvenlik ve kuantum Sonrası Kriptoloji, BTK, 16 October 2019, Ankara, Türkiye.
- Postquantum encryption, TOBB ETU, General Seminar, 30 September 2019, Ankara, Türkiye.
- Cryptology in our daily lives, Bogazici University Science Faculty, 21 March 2019, İstanbul, Türkiye.
- Cryptology and information security in our daily life, Koc University, Engineering Seminars, 26 February 2019, İstanbul, Türkiye.
- Do Lightweight Stream Ciphers Become Extinct? SRG (Security Research Group) Seminars, TOBB ETÜ, 19 February 2019, Ankara, Türkiye.
- Security analysis of Keystream Generators with Keyed Update Functions, Lightweight Crypto Day 2018, Bar Ilan University, 24-29 April 2018, Tel Aviv, Israel.
- Block Ciphers vs Stream Ciphers on Ultra Lightweight Platforms, Keynote speech, Lightsec 2016 Lightweight Cryptography for Security & Privacy, Aksaray Üniversitesi, 20-21 September 2016, Aksaray, Türkiye.
- The security of Lightweight Algorithms, Lightweight Crypto Day, Technion Israel Institute of Technology, 28 March 2016, Haifa, Israel.
- Cryptanalysis of stream ciphers with keyed update functions, Atılım Üniversitesi I. Atılım Kripto Çalıştayı, 30-31 May 2016, Ankara, Türkiye
- Kriptolojinin Temel Kavramları, Yıldız Teknik University, Kriptoloji ve Cebirsel Kodlama Çalıştayı, 10 September 2015, İstanbul, Türkiye
- Hafif Sıklet Kripto Algoritmaları Güvenlikte de Hafif Sıklet midir? II. Ulusal Kripto Günleri, TÜBİTAK BİLGEM, 9 April 2015, Gebze, Türkiye
- Şifreleme Bilimi ve Uygulama Alanları, Sakarya University, 22 March 2013, Sakarya, Türkiye
- "RFID Uygulamalarında Yeni Trendler", İTÜ/3. RFID symposium, İstanbul Teknik Üniversitesi, 10 June 2010, İstanbul, Türkiye
- Kriptolojinin Temelleri, TÜBİTAK Feza Gürsoy Kriptoloji Bilgi Günü, 13 October 2010, Ankara, Türkiye
- Şifreleme Bilimi ve Uygulama Alanları, Sakarya Üniversitesi Bilgisayar Mühendisliği, 22 March 2013, Sakarya, Türkiye
- Syber security and cryptography, 2010, NATO SfP, Brussels, Belgium.
- "RFID Uygulamalarında Yeni Trendler", İTÜ/3. RFID Uygulamaları Sempozyumu, İstanbul Teknik Üniversitesi, 10 June 2010, İstanbul, Türkiye
- Kriptoloji ve Hayatımızdaki Yeri, Eskişehir Osmangazi Üniversitesi Sektörde Matematik Sempozyumu, 2011, Eskişehir, Türkiye
- Kriptolojinin Temelleri, TÜBİTAK Feza Gürsoy Kriptoloji Bilgi Günü, 13 October 2010, Ankara, Türkiye

COURSES GIVEN

- İzmir Institute of Technology Mathematics
  - MATH 583 Post Quantum Cryptography
  - MATH 558 Mathematical Aspects of Symmetric Encryption and Authentication
  - MATH 406 Mathematics of Public Key Cryptography
  - MATH 313 Introduction to Cryptography
  - MATH 361 Abstract Algebra
  - MATH 366 Number Theory
  - MATH 151-152 Calculus I & Calculus II for Math. students

- MATH 141-142 Calculus I & Calculus II for Eng. and Sci. faculties

- METU Institute of Applied Mathematics
  - IAM 704 Hash Functions, Authentication Codes and Nonlinearity
  - IAM 705 Stream Ciphers Cryptanalysis
  - IAM 708 Cryptanalysis of Recent Stream Ciphers
  - IAM 706 Selected Topics in Cryptanalysis of Recent Symmetric Ciphers
- Gebze Technical University Computer Eng.
  - SİB 532 Advanced Topics in Cryptography
  - SİB 569 Special Studies in Information Security
  - SİB 533 Symmetric Ciphers and Their Security Analysis
- İstanbul Şehir University Graduate School of Natural and Applied Sciences
  - BGM 501 Introduction to Cryptography

https://scholar.google.com/citations?user=lJ4V6w0AAAAJ&hl=tr

https://orcid.org/0000-0002-9685-6625

https://www.researchgate.net/profile/Orhun-Kara/2

https://dblp.org/pid/24/1044.html

https://www.linkedin.com/in/orhun-kara-88862372/?originalSubdomain=tr