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/

RESEARCH INTERESTS

Coding theory, cryptography, symmetric ciphers

EDUCATİON

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
- German: Beginner

WORK EXPERİENCE

IZTECH İzmir Institute of Technology *2020-cont.*
Science Faculty, Department of Mathematics
Urla/İzmir
Faculty member, Assoc. Prof. Dr.

TÜBİTAK - BİLGEM-UEKAE Cryptology *2002 – 2020*
Gebze/Kocaeli
Division Manager/Project Manager
Chief Researcher (Senior researcher until 2007)

Institute de Mathématiques de Luminy – IML, CNRS *2001-2002*
Matematik Bölümü
Marsilya/ Fransa
Visiting Researcher (Prof. Serge Vladut)

TÜBİTAK – UEKAE Cryptology *2000-2001*
Gebze/Kocaeli
Researcher

Bilkent University *1996-2000*
Science Faculty Mathematics Department
Ankara
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

- 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 E budget EU 7. framework. Training Activities WP 2008-2011
- EU IC1306 Crypto Action ICT Cryptography for Secure Digital Interaction, Cost action Management Committee Substitute 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

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

COURSES GIVEN

- Gebze Technical University Computer Eng.– SİB 532 Kriptografide İleri Konular 2019-2020 Spring
- İstanbul Şehir University Graduate School of Natural and Applied Sciences – BGM 501 Kriptolojiye Giriş 2018-2019 Spring
- Gebze Technical University Computer Eng. – SİB 569 Bilgi Güvenliğinde Özel Konular 2018-2019 Fall
- İstanbul Şehir University Graduate School of Natural and Applied Sciences – BGM 501 Kriptolojiye Giriş 2018-2019 Fall
- Gebze Tecnical University Computer Eng.– SİB 533 Simetrik Şifreleme Algoritmaları ve Güvenlik Analizleri 2016-2017 Spring
- İstanbul Şehir University Graduate School of Natural and Applied Sciences – BGM 501 Kriptolojiye Giriş 2016-2017 Fall
- İstanbul Şehir University Graduate School of Natural and Applied Sciences – BGM 501 Kriptolojiye Giriş 2015-2016 Fall
- İstanbul Şehir University Graduate School of Natural and Applied Sciences – BGM 501 Kriptolojiye Giriş 2013-2014 Fall
- METU Institute of Applied Mathematics – IAM 704 Hash Functions, Authentication Codes and Nonlinearity 2012-2013 Spring
- METU Institute of Applied Mathematics – IAM 705 Stream Ciphers Cryptanalysis 2011-2012 Spring
- METU Institute of Applied Mathematics – IAM 705 Stream Ciphers Cryptanalysis 2006-2007 Fall
- METU Institute of Applied Mathematics – IAM 708 Cryptanalysis of Recent Stream Ciphers 2005-2006 Spring
- METU Institute of Applied Mathematics – IAM 705 Stream Ciphers Cryptanalysis 2005-2006 Fall
- METU Institute of Applied Mathematics – IAM 706 Selected Topics in Cryptanalysis of Recent Symmetric Ciphers 2004-2005 Spring
- METU Institute of Applied Mathematics – IAM 705 Stream Ciphers Cryptanalysis 2004-2005 Fall

INVITED TALKS

- 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 ETU, General Seminar, 30 Eylül 2019, Ankara
- Cryptology in our daily lives, Bogazici University Science Faculty, 21 Mart 2019, İstanbul
- Geçmişten Günümüze Hayatımızda Kriptoloji ve Bilgi Güvenliği, Koc University, 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

- 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

BOOKS / EDITORSHIPS / CHAPTERS

- 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, 2020.
- 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 2020.

Journal Papers

- Orhun Kara ; 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, DOI: 10.1016/J.IPL..2013.08.001, 2013
- 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, 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