


Orhun Kara

0000-0002-0714-1119 

IZTECH
Mathematics, İzmir Türkiye
+90 232 750 77 56
orhunkara@iyte.edu.tr
IZTECH MATH



Education

- 1998 - 2003 **PhD in Mathematics**, *Bilkent University*, Türkiye.
Thesis: **Code construction on modular curves**. Alisbah best graduate student award
- 1996- 1998 **Master of Science in Mathematics**, *Bilkent University*, Türkiye.
- 1991 - 1996 **Bachelor of Science in Mathematics**, *Bilkent University*, Türkiye.

Professional Experience

- 2020 - ongoing **Associate Professor**, *İzmir Institute of Technology*, Department of Mathematics, Türkiye.
- 2002 - 2020 **Chief Researcher**, *TÜBİTAK BİLGEM UEKAE*, Türkiye.
- 2001 -2002 **Visiting researcher**, *Institute de Mathématiques de Luminy* , CNRS, Marseille.
France
- 2000 - 2001 **Researcher**, *TÜBİTAK UEKAE*, Türkiye.
- 1996 - 2000 **Teaching Assistant**, *Mathematics*, Bilkent University, Ankara.
Türkiye

Research Interests

Cryptology.
Coding theory.

Project grants

- 2021-2024 **TÜBİTAK 1001, Türkiye**. Design and analysis of small state stream ciphers.
- 2015-2019 **EU IC1403- Cryptacus, EU**. Cryptanalysis of Ubiquitous Computing Systems ICT Cost Action: Management Committee member.
- 2014-2018 **EU IC1306 Crypto Action ICT, EU**. Cryptography for Secure Digital Interaction, Cost action Management Committee Substitute Member.
- 2008-2011 **EU ICE FP7- REGPOT,EU**. 7. framework. Integration of Cryptography Unit to Europe. Infrastructure project. Training Activities WP.
- 2008-2011 **TÜBİTAK 1001, Türkiye**. Design of secure figure passwords.

Publications

#11, *peer-reviewed journal papers* (Web of Science Core Collection).

#21, *peer-reviewed international conference papers* (published in Proceedings).

#5, *journal papers* (in other journals).

Books and Book Chapters

#3, *published* in Springer.

#1, *published* in Intech Open .

#1, *published* in VDM Verlag .

#1, *published* in Nobel Akademik (in Turkish) .

Doctoral Thesis co-supervision

#1, *completed* .

#2, *ongoing* .

Master Thesis direct supervision

#4, *completed* .

Courses taught related to cryptology

MATH 583 Post Quantum Cryptography , (Izmir Institute of Technology).

MATH 406 Mathematics of Public Key Cryptography, (Izmir Institute of Technology).

MATH 313 Introduction to Cryptography, (Izmir Institute of Technology).

MATH 558 Mathematical Aspect of Symmetric Encryption and Authentication, (Izmir Institute of Technology).

IAM 704 Hash Functions, (METU Institute of Applied Mathematics).

IAM 708 Cryptanalysis of Recent Stream Ciphers, (METU Institute of Applied Mathematics).

IAM 706 Selected Topics in Cryptanalysis of Recent Symmetric Ciphers , (METU Institute of Applied Mathematics).

SIB 569 Special Studies in Information Security, (Gebze Technical University, Computer Science).

SIB 532 Advanced Topics in Cryptography, (Gebze Technical University, Computer Science).

SIB 533 Symmetric Ciphers and Their Security Analysis, (Gebze Technical University, Computer Science).

BGM 501 Introduction to Cryptography , (Istanbul City University).