KÖKSAL MUŞ

Curriculum Vitae

İstanbul Aydin University
Department of Computer Eng.,
K Building İstanbul, TURKEY
+90 (505) 249 0759
koksalmus@aydin.edu.tr

Work & ResearchExperience

2016- **Assist. Prof.**, İstanbul Aydin University, Computer Engineering, İstanbul.

2013–2016 **Senior Researcher**, METU & TÜBİTAK-BİLGEM, Ankara.
Blockcipher Cryptanalysis Research Project

2013 **Instructor**, Süleyman Şah University, Humanities and Social Sciences Department, İstanbul.

2007–2013 **Teaching Assistant**, METU, Department of Mathematics, Ankara.
- Calculus With Analytic Geometry I-II,
- Basic Mathematics I and II,

2010-2016 **Aikido Instructor**, METU Aikido Society, Ankara.

Research Interest

Applied Cryptography, Verifiable I-voting Systems, PublicKey Cryptography, Randomness Tests

Education

2009–2016 **PhD, Cryptography Department**, *Institute of Applied Mathematics,Middle East Technical University*, Ankara, Turkey.
Thesis: *On Verifiable Internet Voting Systems*,
Supervisors: Assoc. Prof. Dr. Murat Cenk & Assist. Prof. Dr. Mehmet Sabır Kiraz

2007–2009 **MSc, Cryptography Department**, *Institute of Applied Mathematics, Middle East Technical University*, Ankara, Turkey.
Thesis: *An Alternative Normal Form For Elliptic Curve Cryptograhpy: Edwards Curves*,
Supervisors: Prof. Dr. Ersan AKYILDIZ & Assoc. Prof. Dr. Feza ARSLAN

1999–2004 **BSc, Department of Mathematics**, *Yıldız Technical University*, İstanbul, Turkey.

Publications

2016 **A Potential Privacy Leakage in the Estonian Voting Verification Mechanism**, K. Muş, M.S. Kiraz, M. Cenk, İ. Sertkaya, Submitted to Esorics2016.

2008 **Extended Results for Independence and Sensitivity of NIST Randomness Tests**, A. Doganaksoy, B. Ege, K. Mus, 3^{rd} National Cryptology Symposium, Ankara,Turkey.

Patents

2016 **A Verification Mechanism of I-voting System**, K. Muş, M.S. Kiraz, M. Cenk, İ. Sertkaya, Under Evaluation.

Computer skills

Programming Languages: java, MySQL, html

General Knowledge: LaTeX, Microsoft Windows and Office, Hardware

Languages

English **Fluent**

Turkish **Native**

Conferences and Workshops Attended

ICACM **International Conference on Applied and Computational Mathematics**, *Ankara, Turkey*, October 3-6th 2012.

ISC 2^{nd}, 3^{rd} **and** 4^{th} **Information Security & Cryptology Conference**, *Ankara, Turkey*, 2007, 2008, 2010.

DIAMANT **Summer School on Elliptic and Hyperelliptic Curve Cryptography**, *The Netherlands*, September 2008.

Eurocrypt **Istanbul, Turkey**, *April 13-17th 2008*.

REU Program **Research Experience for Undergraduates**, *Indiana University, Indiana, USA*, Summer 2003.

Volunteer Activities

İLKYAR **İlköğretim Okullarına Yardım Vakfı-Volunteer** *2005-2006*

TEGV **Eğitim Gönüllüleri Vakfı-Volunteer** *1999-2005*

Interests

Aikido **Instructor, 3rd degree black belt** *2005-Still*

Judo **Black belt, National team member (1999)** *1988-2001*

Chess **Arbiter,TSF** *2005*