FATİH SULAK

16 NİSAN 1979

YENİ ZİRAAT MAH. 657. SOK. GÖÇMENOĞLU APT. 5/4 06110
ALTINDAĞ ANKARA

Tel : +90 312 5868283 • e-posta : fatih.sulak@atilim.edu.tr

EĞİTİM DURUMU

2011 – 2012	Doktora sonrası	Leuven Katolik Üniversitesi Elektrik Mühendisliği, Kriptoloji Grubu, Belçika
2006 – 2011	Doktora	ODTÜ Uygulamalı Matematik Enstitüsü, Kriptografi Bölümü, Ankara
2003 – 2006	Yüksek lisans	ODTÜ Uygulamalı Matematik Enstitüsü, Kriptografi Bölümü, Ankara
1999 – 2003	Çift anadal	ODTÜ Matematik Bölümü, Ankara
1997 – 2003	Anadal	ODTÜ Elektrik - Elektronik Mühendisliği, Ankara

DENEYİM

2014 – Halen Atılım Üniversitesi Matematik Bölümü

- Yardımcı Doçent. Verilen dersler: calculus I, calculus II, algoritmalar, veri yapıları, ayrık matematik ve uygulamaları, kodlama teorisi, genel matematik, kimlik denetimi ve şifrelemeye giriş

2012 – 2014 Atılım Üniversitesi Matematik Bölümü

- Öğretim Üyesi Doktor. Verilen dersler: calculus I, calculus II, algoritmalar, veri yapıları, ayrık matematik

2011 – 2012 Leuven Katolik Üniversitesi Elektrik Mühendisliği Bölümü

- "Symmetric Crypto" grubunda doktora sonrası araştırmacı

2005 – 2010 Orta Doğu Teknik Üniversitesi Matematik Bölümü

- Araştırma Görevlisi. Verilen dersler: calculus I, calculus II, lineer cebir, sayılar teorisi, kombinatorik, geometri, blok şifre kriptanalizi, hafif blok şifre tasarımı

2004 – 2005 Türkiye Zeka Vakfı – Halıcı Yazılım, ODTÜ Teknokent

- Yazılım Mühendisi - Java programcısı

DİĞER:

- TÜBİTAK ulusal ve uluslararası olimpiyatlara hazırlık kampları, ulusal olimpiyat soruları hazırlama komitesi, 2003 - 2014.
- Genç Balkan matematik olimpiyatları Türkiye takım lider yardımcısı, Makedonya, 2014.
- Balkan matematik olimpiyatları Türkiye takım lider yardımcısı, Makedonya, 2008.
- OYAK liselerarası matematik yarışması soru hazırlama komitesi 2004 – 2011.

ÖDÜLLER ve BAŞARILAR

MATEMATİK YARIŞMALARI

- Uluslararası Matematik Olimpiyatı gümüş madalya, Arjantin 1997
- Balkan Matematik Olimpiyatı mansiyon, Yunanistan 1997
- Ulusal Matematik Olimpiyatı gümüş madalya 1996, bronz madalya 1995
- Avrasya Matematik Yarışması altın madalya 1996
- Ulusal Matematik Olimpiyatı birinci aşama Ege bölge birincisi 1996

ÖSYM SINAVLARI

- Anadolu Öğretmen Lisesi giriş sınavı Türkiye birincisi, 1994
- Devlet Parasız Yatılı sınavı Türkiye beşincisi, 1994
- Fen Lisesi giriş sınavı Türkiye on yedincisi, 1994
- LES Sayısal puan Türkiye sekizincisi, 2003
- ÖSS Sayısal puan Türkiye 111., 1997

ZEKÂ OYUNLARI

- Türkiye Go Şampiyonu 2010, 2009, 2008, 2007, 2002, 2001.
- Uluslararası Go turnuvaları Türkiye temsilcisi, Japonya, Hollanda ve Kore 2012, 2009, 2008, 2005, 2004, 2002, 2001.
- Türkiye Zeka Vakfı, Türkiye Zeka Oyunları Yarışması ikincilik (1999), üçüncülük (1997), dördüncülük (1998).

PROJELER

2014 – 2017	TÜBİTAK 3501	Caesar Yarışmasına Katılan Kimlik Denetimini Sağlayan Algoritmaların Kriptoanalizi, **Yürütücü**
2014 – 2016	TÜBİTAK BİLGEM	Kriptoanaliz Danışmanlık Hizmeti Alımı, **Yürütücü**
2011 – 2011	TÜBİTAK 1001	Cebirsel Eğriler ve Üssel Toplamlar Kullanarak Bazı Kriptografik Uygulamalar, **Bursiyer**
2010 – 2011	TÜBİTAK 1001	Hafif kriptosistem tasarım projesi, **Bursiyer**
2009 – 2010	TÜBİTAK 1001	Özet fonksiyonların güvenlik ölçütleri ve analiz metotları geliştirme ve uygulama projesi, **Bursiyer**
2008 – 2008	ASELSAN	NIST yarışması için özet algoritma tasarımı ve blok tipi algoritmalar için istatistiksel ve yapısal test yazılımı geliştirilmesi, **Araştırmacı**
2007 – 2008	TÜBİTAK 1001	Özet fonksiyon geliştirme projesi, **Bursiyer**
2006 – 2007	ASELSAN	Blok tipi algoritmaların istatistiksel ve yapısal testine yönelik analiz projesi, **Araştırmacı**
2003 – 2006	ODTÜ UME	Simetrik anahtarlı kriptosistem tasarım ve analiz testleri

YAYINLAR

SCI-Expanded Dergiler

- "Mutual correlation of NIST statistical randomness tests and comparison of their sensitivities on transformed sequences", A.Doğanaksoy, F.Sulak, M.Uğuz, O.Şeker, Z.Akcengiz, Turkish Journal of Electrical Engineering & Computer Science, 2015.
- "New Statistical Randomness Tests Based on Length of Runs", A.Doğanaksoy, F.Sulak, M.Uğuz, O.Şeker, Z.Akcengiz, Mathematical Problems in Engineering, 2015.

Diğer İndeksli Dergiler

- "A New Statistical Randomness Test: Saturation Point Test", F. Sulak, International Journal of Information Security Science, Vol 2, No 3, 5 pages, 2013.
- "Statistical Analysis of Reduced Round Compression Functions of SHA-3 Finalists", F. Sulak, B. Ege, O. Koçak, International Journal of Research and Reviews in Applied Sciences, Vol 15, 6 pages, 2013.

Uluslararası Konferanslar

- "Kanarya: A Lightweight Block Cipher", F.Sulak, A.Doğanaksoy, O.Koçak, International Conference on Applied and Computational Mathematics, 2012.
- "Evaluation of Randomness Test Results for Short Sequences", F.Sulak,

A.Doğanaksoy, B.Ege, O.Koçak, Sequences and Their Applications, 2010.

- "Statistical Testing of Some SHA-3 Candidates", A.Doğanaksoy, B.Ege, O.Koçak, F.Sulak, 4th International Information Security and Cryptology Conference, 2010.
- "A Survey of the Attacks on AES", A.Doğanaksoy, A.Darbuka, D.Özberk, N.Öztop, F.Sulak, 3rd International Information Security and Cryptology Conference, 2008.
- "A Survey of the Related-Key Attacks on AES", A.Doğanaksoy, A.Darbuka, D.Özberk, N.Öztop, F.Sulak, 3rd International Information Security and Cryptology Conference, 2008.
- "Cryptanalysis of the Dedicated Hash Functions", A.Doğanaksoy, O.Özen, F.Sulak, K.Varıcı, E.Yüce, 3rd International Information Security and Cryptology Conference, 2007.

Ulusal Konferanslar ve Çalıştaylar

- "Observations on SHA-3 Candidate Algorithm LUX", B.Bozdemir, O.Koçak, M.Öğünç, E.Saygı, F.Sulak, II. Ulusal Kripto Günleri Çalıştayı, 2015.
- "Observations on Hellman's Cryptanalytic Time-Memory Trade-off", A.Doğanaksoy, Ç.Çalık, F.Sulak, 2. Ulusal Kriptoloji Sempozyumu, Ankara 2006.
- "New Randomness Tests Using Random Walk", A.Doğanaksoy, Ç.Çalık, F.Sulak, M.S.Turan, 2. Ulusal Kriptoloji Sempozyumu, Ankara 2006.
- "A Survey on Bent Functions and Normality", A.Doğanaksoy, B.G.Dündar, F.Göloğlu, Z.Saygı, F.Sulak, M.Uğuz, 2. Ulusal Kriptoloji Sempozyumu, Ankara 2006.
- "Constructions of Highly Nonlinear Balanced Boolean Functions", A.Doğanaksoy, B.G.Dündar, F.Göloğlu, Z.Saygı, F.Sulak, M.Uğuz, 1. Ulusal Kriptoloji Sempozyumu, Ankara 2005.

REFERANSLAR

- Doç. Dr. Ali Doğanaksoy, ODTÜ Matematik Bölümü, e-posta: aldoks@metu.edu.tr
- Doç. Dr. Şahin Emrah, Ankara Üniversitesi Bilgisayar Mühendisliği e-posta: sahin.emrah@eng.ankara.edu.tr
- Prof. Dr. Vincent Rijmen, Leuven Katolik Üniversitesi Elektrik Mühendisliği, Belçika, e-posta: Vincent.Rijmen@esat.kuleuven.be