Oğuz Yayla

Özgeçmiş

Kişisel Bilgiler

Doğum tarihi ve yeri	1981, Ankara
Uyruğu	T.C.
Medeni hali	Evli

Akademik Dereceler

2011 — **Doktora**, *Kriptografi, Orta Doğu Teknik Üniversitesi*, Ankara.

2006 2006 — **Yüksek Lisans**, *Kriptografi, Orta Doğu Teknik Üniversitesi*, Ankara.

2004 2005 — **Yan Dal**, *Elektrik-Elektronik Mühendisliği (Telekomünikasyon), Orta Doğu Teknik Üniversitesi*, Ankara.

2002 — **Lisans**, *Matematik, Orta Doğu Teknik Üniversitesi*, Ankara.

2004 2000 — **İngilizce**, *Yabancı Diller Yüksek Okulu, Orta Doğu Teknik Üniversitesi*, Ankara.

2000 1999 — **Lise**, *Bursa Erkek Lisesi*, Bursa.

1999

Doktora Tezi

Başlık	*On Decoding Interleaved Reed-Solomon Codes (Geçişmeli Reed-Solomon Kodlarının Ayrıştırılması Üzerine)*
Danışman	Prof. Dr. Ferruh Özbudak, ODTÜ, Matematik
Tarih	16 Eylül 2011

Yüksek Lisans Tezi

Başlık	*Scalar Multiplication on Elliptic Curves (Eliptik Eğriler Üzerinde Katsayı Çarpımı)*
Danışman	Prof. Dr. Ersan Akyıldız, ODTÜ, Matematik
Tarih	24 Ağustos 2006

Mesleki Deneyim

... — **Yardımcı Doçent**, *Hacettepe Üniversitesi/Matematik*, Ankara.

01/2015 12/2014 — **Yarı Zamanlı Öğretim Görevlisi**, *Atılım Üniversitesi/Matematik*, Ankara.

10/2014

Hacettepe Üniversitesi, Matematik Bölümü, No:259, Beytepe, Ankara – 06800 – Türkiye
☎ +90 (312) 780 7709 • ✉ oguz.yayla@hacettepe.edu.tr

10/2014
10/2013

Araştırmacı, *Johann Radon Institute for Computational and Applied Mathematics (RICAM)*, Linz, Avusturya.
TÜBİTAK Yurt Dışı Doktora Sonrası Araştırmacı (2219) Bursuyla

04/2013
09/2011

Doktora Sonrası Araştırmacı, *TÜBİTAK 1001-Projesi - ODTÜ*, Ankara.
Yürütücü: Prof. Dr. Ferruh Özbudak

09/2011
01/2008

Araştırma Görevlisi, *Orta Doğu Teknik Üniversitesi*, Ankara.

Projeler

05/2017
05/2016

Yürütücü, *TÜBİTAK 1002-Projesi - Hacettepe*, Ankara.
Yeni γ-Butson-Hadamard Matrislerinin Üretilmesi ve Onların Kriptografiye Uygulanması

06/2013
05/2013

Araştırmacı, *TÜRKTRUST-ODTÜ*, Ankara.
RSA Kriptosistemi Parametreleri için Güvenlik Testleri

04/2013
09/2011

Doktora Sonrası Araştırmacı, *TÜBİTAK 1001-Projesi - ODTÜ*, Ankara.
Cebirsel Eğriler ve Onların Bazı Kriptografik ve Kodlama Teorisindeki Problemlerdeki Uygulamaları

07/2008
07/2006

Araştırmacı, *TÜBİTAK(1007)-ODTÜ*, Ankara.
Açık Anahtar Altyapı Konusunda Araştırma, Geliştirme ve Uygulamalar

03/2008
10/2006

Araştırmacı, *ASELSAN-ODTÜ*, Ankara.
Özgün Eliptik Eğri Tasarlanması ve Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi

Araştırma Alanları

Kombinatorik Tasarımlar, Kriptografi, Kodlama Teorisi, Cebirsel Sayılar Teorisi, Cebirsel Fonksiyon Cisimleri, Cebirsel Eğriler, Sonlu Cisimler

Burslar ve Ödüller

10/2014
10/2013

TÜBİTAK, Bir yıl süreli Yurt Dışı Doktora Sonrası Bursu.

2007

ODTÜ, *Kriptografi Ders Performans Ödülü (Doktora)*.

2005

ODTÜ, *Kriptografi Ders Performans Ödülü (Yüksek Lisans)*.

2011
2004

TÜBİTAK, *Yüksek Lisans - Doktora Bursiyeri*.

2004

ODTÜ, *Matematik Bölümü en yüksek ortalamaya sahip mezun ödülü*.

2004
2001

TÜBİTAK, *Lisans Bursiyeri*.

Düzenleme ve Bilim Komitesi Üyelikleri

17–18 Mayıs 2012 V. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara

18–19 Ağustos 2007 CIMPA-UNESCO-TÜBİTAK Yaz okulu - Codes over Rings, Ankara

Editörlük

Turk J Math

SDÜ Fen Bilimleri Enstitüsü Dergisi

Hakemlik

Turk J Elec Eng & Comp Sci

Turk J Math

Machine Learning

Bilgi Güvenliği ve Kriptoloji Konferansları

Tez Yöneticiliği

Doktora

24 Mayıs 2013 **Bilal Alam**, *HFE Based Multi-Variate Quadratic Cryptosystems and Dembowski-Ostrom Polynomials (HFE Tabanlı İkinci Dereceden Çok Değişkenli Kriptosistemler ve Dembowski-Ostrom Polinomlar)*, Kriptografi, ODTÜ, Ortak Tez Yöneticisi

13 Eylül 2012 **Cemal Cengiz Yıldırım**, *Existence Problem of Almost p-Ary Perfect and Nearly Perfect Sequences (Yaklaşık p-ary Mükemmel ve Mükemmele Yakın Dizilerin Varolabilirlik Problemi)*, Kriptografi, ODTÜ, Ortak Tez Yöneticisi

Yüksek Lisans

13 Eylül 2012 **Ahmet Sınak**, *On Verification of Restricted Extended Affine Equivalence of Vectorial Boolean Functions (Vektor Boole Fonksiyonlarının Kısıtlı Genişletilmiş Afin Denkliği Üzerine)*, Kriptografi, ODTÜ, Ortak Tez Yöneticisi

Verdiği Eğitimler

2015,2016 **Kriptoloji**, Linux Yaz Kampı 2015, 2016 (Bolu)

2015,2016 **Kriptoloji**, Akademik Bilişim 2015 (Eskişehir), 2016 (Aydın)

10 Mayıs 2013 **Kriptoloji - Açık Anahtar Altyapısı**, Savunma Sanayii ve Teknoloji Eğitim Merkezi (SATEM) Komutanlığı, Ankara

10 Mayıs 2013 **Kriptoloji - Açık Anahtar Altyapısı**, Savunma Sanayii ve Teknoloji Eğitim Merkezi (SATEM) Komutanlığı, Ankara

25 Aralık 2008 **Açık Anahtar Altyapısı**, III. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara

Verdiği Konuşmalar

4 Aralık 2013 **Conference matrices**, Linz Algebra Days, RICAM, Linz, Avusturya

13 Haziran 2013 **GF(11) Üzerinde Çok Noktalı Cebirsel Eğriler**, 8. Ankara Matematik Günleri, Ankara

3–6 Ekim 2012 **Probabilistic Decoding of RS Codes with Extended BKY Algorithm**, International Conference on Applied and Computational Mathematics (ICACM), Ankara

Yabanci Diller

İngilizce **İleri düzey konuşma, yazama ve okuma** *YDS: 82.5/100 Mayıs, 2015*

Almanca **Temel düzey**

Matematik Yazılım Paketleri

- Magma, Maple, Mathematica, Matlab, Sage, NTL, Latex
- C, C++, Java

Konferans ve Çalıştaylar

14 Ekim–13 Aralık 2013 **Special Semester on Applications of Algebra and Number Theory**, RICAM, Linz, Avusturya

13–14 Haziran 2013 **8. Ankara Matematik Günleri**, Çankaya Üniversitesi, Ankara

03–06 Ekim 2012 **International Conference on Applied and Computational Mathematics (ICACM)**, Orta Doğu Teknik Üniversitesi, Ankara

04–08 Hazıran 2012 **SETA 2012: SEquences and Their Applications**, Waterloo, Canada

25–29 Eylül 2009 **Workshop on Sequences, Codes and Curves**, Antalya

18–29 Ağustos 2008 **Codes over Rings**, CIMPA-UNESCO-TÜBİTAK Yaz okulu, Ankara

02–12 Temmuz 2008 **Algebraic coding theory**, S3CM Yaz okulu, Soria, İspanya

2006–2013 **Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansları**, Ankara

Yayınlar

Değerlendirme Aşamasında

[1] Arne Winterhof and Oğuz Yayla. Extended familes of binary sequences with high family complexity and low cross correlation measure. *(In preperation)*.

[2] Arne Winterhof, Oğuz Yayla, and Volker Ziegler. Non-existence of some nearly perfect sequences, near Butson-Hadamard matrices, and near conference matrices. *arXiv preprint arXiv:1407.6548*, 2014.

Dergi Yayınları

[1] Oğuz Yayla. Nearly perfect sequences with arbitrary out-of-phase autocorrelation. *Adv. Math. Commun.*, 10(2):401–411, 2016. doi:10.3934/amc.2016014.

[2] Arne Winterhof and Oğuz Yayla. Family complexity and cross-correlation measure for families of binary sequences. *Ramanujan J.*, 39(3):639–645, 2016. doi:10.1007/s11139-014-9649-5.

[3] Ferruh Özbudak, Burcu Gülmez Temür, and Oğuz Yayla. Further results on fibre products of Kummer covers and curves with many points over finite fields. *Adv. Math. Commun.*, 10(1):151–162, 2016. doi:10.3934/amc.2016.10.151.

[4] Oğuz Yayla. Families of pseudorandom binary sequences with low cross-correlation measure. In *BalkanCryptSec 2014*, volume 9024 of *Lecture Notes in Comput. Sci.*, pages 31–39. Springer, 2015. doi:10.1007/978-3-319-21356-9_3.

[5] Ferruh Özbudak, Ahmet Sınak, and Oğuz Yayla. On verification of restricted extended affine equivalence of vectorial Boolean functions. In *Arithmetic of finite fields*, volume 9061 of *Lecture Notes in Comput. Sci.*, pages 137–154. Springer, Cham, 2015. doi:10.1007/978-3-319-16277-5_8.

[6] László Mérai and Oğuz Yayla. Improving results on the pseudorandomness of sequences generated via the additive order of a finite field. *Discrete Math.*, 338(11):2020–2025, 2015. doi:10.1016/j.disc.2015.04.015.

[7] Ferruh Özbudak, Seher Tutdere, and Oğuz Yayla. On some bounds on the minimum distance of cyclic codes over finite fields. *Des. Codes Cryptogr.*, 76(2):173–178, 2015. doi:10.1007/s10623-014-9927-7.

[8] Bilal Alam, Ferruh Özbudak, and Oğuz Yayla. Classes of weak Dembowski-Ostrom polynomials for multivariate quadratic cryptosystems. *J. Math. Cryptol.*, 9(1):11–22, 2015. doi:10.1515/jmc-2013-0019.

[9] Ferruh Özbudak and Oğuz Yayla. Improved probabilistic decoding of interleaved Reed-Solomon codes and folded Hermitian codes. *Theoret. Comput. Sci.*, 520:111–123, 2014. doi:10.1016/j.tcs.2013.10.025.

[10] Ferruh Özbudak, Burcu Gülmez Temür, and Oğuz Yayla. An exhaustive computer search for finding new curves with many points among fibre products of two Kummer

covers over F_5 and F_7. *Turkish J. Math.*, 37(6):908–913, 2013. doi:10.3906/mat-1206-26.

[11] Ferruh Özbudak, Oğuz Yayla, and C. Cengiz Yıldırım. Nonexistence of certain almost p-ary perfect sequences. In *Sequences and their applications—SETA 2012*, volume 7280 of *Lecture Notes in Comput. Sci.*, pages 13–24. Springer, Heidelberg, 2012. doi:10.1007/978-3-642-30615-0_2.

Konferans Yayınları

[1] Sibel Kurt and Oğuz Yayla. Near Butson-Hadamard matrices with small off-diagonal entries. 3rd Istanbul Design Theory, Graph Theory and Combinatorics Workshop. İstanbul, June 13 - 17, 2016. URL: http://portal.ku.edu.tr/~eyazici/Research/Design2016/abstracts/abstract_kurt.pdf.

[2] Ersan Akyıldız, Çağdaş Çalık, Mert Özarar, Zaliha Tok, and Oğuz Yayla. RSA kriptosistemi parametreleri için güvenlik testi yazılımı. In *VI. International Conference on Information Security and Cryptology Proceedings*, pages 124–127. Ankara, 20–21 Sep 2013. URL: http://www.iscturkey.org/iscold/ISCTURKEY2013/files/paper67.pdf.

[3] Bilal Alam and Oğuz Yayla. Recent attacks against HFE/multi–HFE MQ cryptosystems and connection with Ore's p-polynomial decomposition. In *VI. International Conference on Information Security and Cryptology Proceedings*, pages 192–198. Ankara, 20–21 Sep 2013. URL: http://www.iscturkey.org/iscold/ISCTURKEY2013/files/paper93.pdf.

[4] Sedat Akleylek and Oğuz Yayla. PKI–lite: A PKI system with limited resources. In *II. International Conference on Information Security and Cryptology Proceedings*, pages 59–62. Ankara, 13–14 Dec 2007. URL: http://www.iscturkey.org/iscold/ISCTURKEY2007/papers/05.pdf.

[5] Ersan Akyıldız and Oğuz Yayla. Scalar multiplication on elliptic curves. In *II. National Conference on Cryptology Proceedings*, pages 114–124. Ankara, 15–17 Dec 2006. URL: http://goo.gl/KfDBKu.

Poster Yayınları

[1] Oğuz Yayla. Kriptografik modüllerin güvenlik gereksinimleri. In *III. International Conference on Information Security and Cryptology Proceedings*, pages 253–256. Ankara, 25–27 Dec 2008. URL: http://www.iscturkey.org/iscold/ISCTURKEY2008/posters/02.pdf.

[2] Hakan Özadam and Oğuz Yayla. On algebraic attacks using Gröbner basis. In *II. International Conference on Information Security and Cryptology Proceedings*, pages 312–318. Ankara, 13–14 Dec 2007. URL: http://www.iscturkey.org/2010/2008/2007/pdf/poster/6.pdf.

[3] Oğuz Yayla. DSA sisteminin çalıştırılması ve test edilmesi. In *II. International Conference on Information Security and Cryptology Proceedings*, pages 290–297. Ankara, 13–14 Dec 2007. URL: http://www.iscturkey.org/iscold/ISCTURKEY2007/papers/43.pdf.

[4] Murat Cenk and Oğuz Yayla. E–imza uygulamaları ve karşılaştırmaları. In *Ulusal Elektronik İmza Sempozyumu Proceedings*. Ankara, 7–8 Aralık 2006. URL: http://ueimzas.gazi.edu.tr/pdf/poster/38.pdf.

Problemler onları ortaya çıkaran bilgi birikimiyle çözülemez.
A. Einstein

Ankara, 26 Temmuz 2016.