Oğuz Yayla

Curriculum Vitae

Personnel Data

Birth date and place	1981, Ankara
Nationality	Turkish
Marital status	Married

Academic Degrees

2011 — **PhD**, *Cryptography, Middle East Technical University*, Ankara.

2006 2006 — **MS**, *Cryptography, Middle East Technical University*, Ankara.

2004 2005 2002 — **Minor**, *Electrical and Electronics Engineering (Telecommunication), Middle East Technical University*, Ankara.

2004 — **BS**, *Mathematics, Middle East Technical University*, Ankara.

2000 2000 — **English**, *School of Foreign Languages, Middle East Technical University*, Ankara.

1999 1999 — **High-school**, *Bursa Boys High-school*, Bursa.

PhD Thesis

Title	*On Decoding Interleaved Reed-Solomon Codes*
Supervisor	Prof. Dr. Ferruh Özbudak, METU, Mathematics
Date	16 Sep 2011

MS Thesis

Title	*Scalar Multiplication on Elliptic Curves*
Supervisor	Prof. Dr. Ersan Akyıldız, METU, Mathematics
Date	24 Aug 2006

Vocational

... 01/2015 — **Assist. Prof. Dr.**, *Hacettepe Üniversitesi/Matematik*, Ankara.

12/2014 10/2014 — **Part Time Instructor**, *Atilim Üniversitesi/Matematik*, Ankara.

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

10/2014
10/2013

Researcher, *Johann Radon Institute for Computational and Applied Mathematics (RICAM)*, Linz, Austria.
TÜBİTAK Post-Doctoral Scholarship (2219)

04/2013
09/2011

Post-Doctoral Researcher, *TÜBİTAK 1001-Project - METU*, Ankara.
Head: Prof. Dr. Ferruh Özbudak

09/2011
01/2008

Research Assistant, *Middle East Technical University*, Ankara.

Research Projects

05/2017
05/2016

Yürütücü, *TÜBİTAK 1002-Projesi - Hacettepe*, Ankara.
Generation of New γ-Butson-Hadamard Matrices and their Cryptographic Applications

06/2013
05/2013

Researcher, *TÜRKTRUST - METU*, Ankara.
Security test of RSA cryptosystem parameters

04/2013
09/2011

Post-Doctoral Researcher, *TÜBİTAK 1001-Project - METU*, Ankara.
Algebraic curves and their applications in cryptography and coding theory

07/2008
07/2006

Researcher, *TÜBİTAK 1007 Project - METU*, Ankara.
Research and development on public key infrastructure

03/2008
10/2006

Researcher, *ASELSAN - METU*, Ankara.
Selecting secure elliptic curves and Implementing a signature system based on elliptic curves,

Research Areas

combinatorial designs, cryptography, coding theory, algebraic number theory, algebraic function fields, algebraic curves, finite fields

Scholarships and Awards

10/2014
10/2013

TÜBİTAK, Post-Doctorial Scholarship - One year.

2007

METU, *Cryptography Dept. Best performance (Doctorate)*.

2005

METU, *Cryptography Dept. Best performance (MS)*.

2011
2004

TÜBİTAK, *Graduate student scholarship*.

2004

METU, *Highest CGPA among all math graduates*.

2004
2001

TÜBİTAK, *Undergraduate student scholarship*.

Organization of Scientific Events

17–18 May 2012 V. International Conference on Information Security and Cryptology, Ankara
18–19 Aug 2007 CIMPA-UNESCO-TÜBİTAK Summer School - Codes over Rings, Ankara

Editorial Activities

Turk J Math
SDÜ Fen Bilimleri Enstitüsü Dergisi

Referee Activities

Turk J Elec Eng & Comp Sci
Turk J Math
Machine Learning

I–VI International Conference on Information Security and Cryptology

Thesis Supervision

PhD

24 May 2013 **Bilal Alam**, *HFE Based Multi-Variate Quadratic Cryptosystems and Dembowski-Ostrom Polynomials,* Cryptography, METU, Co-supervisor

13 Sep 2012 **Cemal Cengiz Yıldırım**, *Existence Problem of Almost p-Ary Perfect and Nearly Perfect Sequences*, Cryptography, METU, Co-supervisor

MS

13 Sep 2012 **Ahmet Sınak**, *On Verification of Restricted Extended Affine Equivalence of Vectorial Boolean Functions*, Cryptography, METU, Co-supervisor

Tutorials

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

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

10 May 2013 **Cryptology - Public Key Infrastructure**, Savunma Sanayii ve Teknoloji Eğitim Merkezi (SATEM) Komutanlığı, Ankara

25 Dec 2008 **Public Key Infrastructure**, III. International Conference on Information Security and Cryptology, Ankara

Presentations

4 Dec 2013 **Conference matrices**, Linz Algebra Days, RICAM, Linz, Austria

13 June 2013 **Algebraic curves with many points over GF(11)**, 8. Ankara Math Days, Ankara

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

Foreign Languages

English **Advanced** *Exam Result: 83/100, May 2011*

German **Elementary**

Mathematical Software Packages

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

Conferences and Workshops

14 Oct–13 Dec 2013 **Special Semester on Applications of Algebra and Number Theory**, RICAM, Linz, Austria

13–14 June 2013 **8. Ankara Math Days**, Çankaya University, Ankara

03–06 Oct 2012 **International Conference on Applied and Computational Mathematics (ICACM)**, Middle East Technical University, Ankara

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

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

18–29 Aug 2008 **Codes over Rings**, CIMPA-UNESCO-TÜBİTAK Summer School, Ankara

02–12 July 2008 **Algebraic coding theory**, S3CM Summer School, Soria, Spain

2006–2013 **I–VI International Conference on Information Security and Cryptology**, Ankara

Publications

Submitted/In Preperation

[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.

Selected Publications

[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.

Conference Proceedings

[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`.

Posters in Proceedings

[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`.

Problems cannot be solved by the same level of thinking that created them.
A. Einstein

Ankara/Turkey, July 26, 2016.