Ahmet SINAK Curriculum Vitae

Cryptography Program,
Institute of Applied Mathematics,
Middle East Technical University,
ÇANKAYA, ANKARA, TURKEY.

Phone: +90 312 210 29 87
e-mail: ahmet.sinak@metu.edu.tr

APPOINTMENTS

• Research Assistant	Middle East Technical University	27/02/2012-going on
• Research Assistant	Necmettin Erbakan University	25/08/2011-24/02/2012
• Research Assistant	Artvin Çoruh University	20/12/2011-14/08/2011

EDUCATIONS

• **Ph.D., Cryptography,**	Middle East Technical University	GPU:4.00/4.00	2012-2017
• **M.S., Cryptography,**	Middle East Technical University	GPU:3.93/4.00	2011-2012
• **B.S., Economics,**	Anadolu University	GPU:2.63/4.00	2010-2015
• **B.S., Mathematics,**	Muğla Sıtkı Koçman University	GPU:3.67/4.00	2005-2009
• **High School**	Serik Anatolian High School	GPU:4.57/5.00	2000-2004

RESEARCH INTERESTS

- Cryptographic Functions (Bent Functions, Plateaued functions, etc.),
- Public Key Cryptography,
- Cryptographic Protocols, E-Voting,
- Algebraic Function Field.

PUBLICATIONS

1. Mesnager, S., Özbudak, F., Sınak, A.: On the p-ary (Cubic) Bent and Plateaued (Vectorial) Functions. International Journal of Designs, Codes and Cryptography (DCC), in press (2017)
2. Mesnager, S., Özbudak, F., Sınak, A., Cohen, G.: On q-ary Plateaued Functions over $\F_q$ and their Explicit Characterizations. European Journal of Combinatorics (EJC), in press, (2017).
3. Akyıldız, E., Harold, N.Y., Sınak, A.: Free storage basis conversion over finite field. Turk J Math, 41, 96-109, doi:10.3906/mat-1503-84, January 2017.

4. Sınak, A., Özkan, S., Yıldırım, H., Sabır Kiraz, M.: End-2-End Verifiable Internet Voting Protocol Based on Homomorphic Encryption, International Journal of Information Security Science, Vol.3, No.2, pp.165-181, June 2014.

CHAPTER IN BOOK

- Akyıldız, E., Cenk, M., Sınak, A.:"Algorithms and Complexity in Cryptography", Handbook of Codes and Sequences with Applications in Communication, Computing and Information Security, Editors: S.Boztas ve U. Parampalli, CRC Press Taylor & Francis Group, in press, April 2018.

- ***INTERNATIONAL BOOK PAPER***

1. Mesnager S., Özbudak F., Sınak A., "Results on Characterizations of Plateaued Functions in Arbitrary Characteristic", Cryptography and Information Security in the Balkans, Second International Conference, BalkanCryptSec 2015, Koper, Slovenia, Revised Selected Papers, Eds: Enes Pasalic and Lars R. Knudsen, LNCS 9540, Springer, ISBN: 978-3-319-29171-0, pp: 17-30, 2016.
2. Özbudak F., Sınak A., Yayla O., "On Verification of Restricted Extended Affine Equivalence for Vectorial Boolean Functions", Arithmetic of Finite Fields, WAIFI 2014, Gebze, Turkey, Revised Selected Papers, Eds. Ç. K. Koç, S. Mesnager and E. Savaş, LNCS 9061, Springer, ISBN 978-3-319-16276-8, pp:137-154, 2015 (http://link.springer.com/chapter/10.1007%2F978-3-319-16277-5_8)

INTERNATIONAL CONFERENCE PRESENTATIONS AND PROCCEDINGS

1. Mesnager, S., Özbudak, F., Sınak, A.: "A new class of three-weight linear codes from weakly regular plateaued functions", Proceedings of Extended Abstract of the tenth International Workshop on Coding and Cryptography (WCC)-2017, September 18-22, 2017, Saint-Petersburg, Russia.
2. Carlet, C., Mesnager S., Özbudak F., Sınak A.: "Explicit Characterizations for Plateaued-ness of p-ary (Vectorial) Functions", Second International Conference on Codes, Cryptology and Information Security (C2SI-2017), Editors: S. El Hajji, A. Nitaj, E. M. Souidi. In Honor of Claude Carlet. Proceedings, LNCS 10194, Springer, pp:328-345, 9 March 2017, DOI: 10.1007/978-3-319-55589-8_22, April 10-12, 2017, Rabat, Morocco.
3. Mesnager S., Özbudak F., Sınak A., "Characterizations of plateaued functions in arbitrary characteristic", Proceedings of Abstract Book of the International Conference on Coding theory and Cryptography (ICCC)-2015, 2-5 November 2015, Alger, Algeria.
4. Mesnager S., Özbudak F., Sınak A., "Results on characterizations of plateaued functions in arbitrary characteristic", Pre-Proceedings of BalkanCryptSec 2015, Ed. Enes Pasalic, 3-4 September 2015, Koper, Slovenia.

5. Özbudak F., Sınak A., Yayla O., "On Verification of Restricted Extended Affine Equivalence for Vectorial Boolean Functions", Pre-Proceedings of Arithmetic of Finite Fields, WAIFI 2014, September 26-28, 2014, Gebze, Turkey.
6. Sınak, A., Sabır Kiraz, M., Özkan, S., Yıldırım, H.,"A Secure Internet Voting Protocol Based on Homomorphic Encryption'', ISCTURKEY 2013, Proceedings of 6th International Conference on Information Security and Cryptology, pp.142-148, September 20-21, 2013. Ankara, Turkey.

PREPRINT

1. Mesnager, S., Özbudak, F., Sınak, A.: Linear codes with three-weights from weakly regular plateaued functions, Submitted to Designs, Codes and Cryptography (DCC) in October 2017
2. Mesnager, S., Özbudak, F., Sınak, A.: Secondary Constructions of (Non)-Weakly Regular Plateaued p-ary Functions and their Characterizations. Submitted to the 20th Annual International Conference on Information Security and Cryptology (ICISC- 2017), Seoul, Korea
3. Mesnager, S., Özbudak, F., Sınak, A.: On q-ary Partially Bent Functions over Fq and their Characterizations, Preprint.

POSTER PRESENTATIONS

1. Mesnager, S., Özbudak, F., Sınak, A.: A new class of three-weight linear codes from weakly regular plateaued functions, 15th Anniversary of the Foundation of the Institute of Applied Mathematics, METU, 9 October, 2017, Ankara, Turkey.
2. Sınak, A., Sabır Kiraz, M.: Security Requirements of Electronic Voting and Cryptographic Measures, International Symposium on Digital Forensics, 30 May-1 June 2014, Ankara, Turkey.
3. Sınak, A., Cenk, M.: Modular Multiplication Algorithms For Finite Field Multiplication in GF(p), Antalya Algebra Days XVI, May 9-13 2014, ANTALYA, Turkey.
4. Sınak, A., Sabır Kiraz, M., Özkan, S., Yıldırım, H.: An Efficient and Secure Internet Voting Protocol Based on Homomorphic Encryption, CryptoDays 2013, June 14-15, 2013, Tübitak, Gebze, Turkey.

INTERNATIONAL CONFERENCES ATTENDED

1. 5 th International Conference on Information Security and Cryptology (ISCTurkey), 2012, ANKARA, Turkey.
2. International Conference on Applied and Computational Mathematics (ICACM) 2012, METU-IAM, ANKARA , Turkey.

3. 2th International Workshop on Lightweight Cryptography for Security & Privacy Lightsec 2013, Gebze, Turkey.
4. Open Problems Conference: 18 – 20 September 2013, Istanbul, Turkey.
5. 6 th International Conference on Information Security and Cryptology (ISCTurkey), 2013, ANKARA, Turkey.
6. Algebraic curves over finite fields, Special Semester on Applications of Algebra and Number Theory, 11-15 November 2013, Linz, AUSTRIA.
7. Antalya Algebra Days XVI, 9-13 May 2014, Antalya, Turkey.
8. International Symposium on Digital Forensics, 2014, Ankara, Turkey.
9. Workshop on Function Field Arithmetic, 9-13 June 2014, Nesin Mathematics Village-Şirince, İzmir, Turkey.
10. International Workshop on the Arithmetic of Finite Fields, WAIFI 2014, Gebze, Turkey.
11. International Conference on Cryptography and Information Security, BalkanCryptSec 2014, 16-17 October 2014, Istanbul, Turkey.
12. 7 th International Conference on Information Security and Cryptology (ISCTurkey), 2014, İstanbul, Turkey.
13. The Ninth International Workshop on Coding and Cryptography (WCC) 2015, 13-17 April 2015, Paris, France.
14. Cryptography and Information Security in the Balkans, BalkanCryptSec 2015, 3-4 September 2015, Koper, Slovenia.
15. 8 th International Conference on Information Security and Cryptology (ISCTurkey), 30-31 October 2015, Ankara, Turkey
16. The International Conference on Coding theory and Cryptography ICCC2015, 2-5 November 2015, Alger, Algeria.
17. 9 th International Conference on Information Security and Cryptology (ISCTurkey), 25-26 October 2016, Ankara, Turkey.
18. Paris Crypto Day, Ecole Normale Superieure, 12 January 2017, Paris, France.
19. Workshop on Security for Embedded and Mobile Systems (SEMS 2017), Ecole Normale Superieure, 30 April 2017, Paris, France.
20. EUROCRYPT 2017, 1-4 May 2017, Paris, France.
21. The Tenth International Workshop on Coding and Cryptography (WCC)-2017, September 18-22, 2017, Saint-Petersburg, Russia.

Tutorial Presentations

- Kriptografi ve Terskod Mühendisliğine Giriş, Linux Yaz Kampı, Bolu, Türkiye, 11-12 Ağustos 2014.
- Kriptografinin Temelleri ve Bilgi-Iletişim Teknolojilerindeki Uygulamaları", XVII. Akademik Bilişim Konferansı, Anadolu Üniversitesi, Eskişehir, 30 Ocak-3 Şubat 2015.
- Kriptografi II Eğitimi, XVII. Akademik Bilişim Konferansı, Anadolu Üniversitesi, Eskişehir, 30 Ocak-3 Şubat 2015.

- Kriptografi ve Terskod Mühendisliğine Giriş, Linux Yaz Kampı, Bolu, Türkiye, 8-9 Ağustos 2015.
- Kriptoloji'ye Giriş ve Uygulamalar, XVIII. Akademik Bilişim Konferansı, Adnan Menderes Üniversitesi, Aydın, 30 Ocak-2 Şubat 2016.
- Kriptografi ve Terskod Mühendisliğine Giriş, Linux Yaz Kampı, Bolu, Türkiye, 7 Ağustos 2016.
- Kriptografi ve Terskod Mühendisliğine Giriş, Linux Yaz Kampı, Bolu, Türkiye, 22-24 Temmuz 2017.

Professional Affiliations:

- Member of the organizing committee, IAM Allumni Meeting: Cryptography and Applications, METU, Ankara, 2014
- Member, Turkish Mathematical Society (2011- going on)
- Member, METU SIAM Student Chapter (2011- going on)
- Vice-President at METU SIAM Student Chapter (2014 - 2015)
- President at METU SIAM Student Chapter (2015 - 2016)
- Student Representative of Institude of Aplied Mathematics at METU (2014 - 2016)
- Presedent of Health, Sports and Culture at METU (2014 - 2016)

Scholarships and Awards:

- High Honor Certificate, B.S., Mathematics, Muğla Sıtkı Koçman University (2005-2009)
- TÜBİTAK (Turkish Scientific and Research Council)-BİDEB 2210 (2011-2012)
- TÜBİTAK (Turkish Scientific and Research Council)-BİDEB 2211 (2012-2017)
- TÜBİTAK (Turkish Scientific and Research Council)-BİDEB 2214/A (November 2016- July 2017)

Computer & other skills/experiences

- **Programming Languages:** C, MAGMA
- **Computational Products:** Maple