Zülfükar SAYGI January 29, 2015

Associate Professor, Department of Mathematics zsaygi@etu.edu.tr
TOBB University of Economics and Technology http://zsaygi.etu.edu.tr/
Ankara – Turkey Cell: +90 533 6466499

EDUCATION:

- Ph.D. in Cryptography, Middle East Technical University, Ankara, Turkey, 2007
- M.S. in Mathematics, Middle East Technical University, Ankara, Turkey, 2003
- B.S. in Mathematics, Middle East Technical University, Ankara, Turkey, 2000

RESEARCH INTEREST:

- Cryptography: Block Ciphers, Stream ciphers, Authentication Codes, Secret Sharing Schemes
- Finite Fields and Their Applications, Algebraic Curves over Finite Fields

EMPLOYMENTS:

- TOBB University of Economics and Technology, Department of Mathematics: Associate Professor, since 2014
- TOBB University of Economics and Technology, Department of Mathematics: Assistant Professor, 2009-2014
- TOBB University of Economics and Technology, Department of Mathematics: Lecturer, 2007-2009
- Middle East Technical University, Institute of Applied Mathematics, Department of Cryptography:
  Research Assistant, 2002-2007
- TUBITAK, UEKAE:
  Researcher, 2000-2002

AWARDS:

- METU, Thesis of the year award, 2008
- Prof. Dr. Mustafa Parlar Foundation, Thesis of the year award, 2008

PUBLICATIONS:

A. Journals and Book Chapters

1. F. Özbudak, Z. Saygı, Rational Points of the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over F_{q^m}, In Applied Algebra and Number Theory, Edited By G. Larcher, F. Pillichshammer, A. Winterhof and C. Xing, pp. 297 – 306, 2014

2. N. Öztop, O. Koçak, F. Özbudak, Z. Saygı, Characterisation and Enumeration of a Class of Semi-Bent Quadratic Boolean Functions, Int. J. of Information and Coding Theory, 2015, Accepted.
3. F. Özbudak, Z. Saygı, On the number of quadratic forms having codimension 2 radicals in characteristic 2 giving maximal/minimal curves, Comm. in Algebra, vol 42, No 9, pp. 3795-3810 (2014).
4. N. Öztop, O. Koçak, O. Kurt, Z. Saygı, Notes on Bent Functions of the Polynomial Form, International Journal of Information Security Science, Vol. 1, No 2, (2012).
5. F. Özbudak, E. Saygı, Z. Saygı, Quadratic Forms of Codimension 2 over Finite Fields Containing F_4 and Artin-Schreier Type Curves, Finite Fields and Their Applications, vol. 18, No. 2, pp. 396-433 (2012).
6. F. Özbudak, E. Saygı, Z. Saygı, A New Class of Quaternary LCZ Sequence Sets, Designs, Codes and Cryptography, vol. 62, No. 2, pp. 189-198 (2012).
7. F. Özbudak, E. Saygı, Z. Saygı, Quadratic forms of codimension 2 over certain finite fields of even characteristic, Cryptography and Communications, vol. 3, No. 4, pp. 241-257 (2011).
8. E. K. Özbudak, F. Özbudak, Z. Saygı, A Class of Authentication Codes with Secrecy, Designs, Codes and Cryptography, vol. 59, No. 1-3, pp. 287-318 (2011).
9. F. Özbudak, Z. Saygı, Systematic Authentication Codes Using Additive Polynomials, Designs, Codes and Cryptography, vol. 49, No. 1-3, pp. 61-77 (2008).
10. F. Özbudak, Z. Saygı, Some constructions of systematic authentication codes using galois rings, Designs, Codes and Cryptography, vol. 41, No. 3, pp. 343-357 (2006).

B. International Conference Papers:

1. F. Özbudak, Z. Saygı, L-polynomials of the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over F_{q^m} , International Workshop on the Arithmetic of Finite Fields-WAIFI 2014, Gebze, Turkey
2. H.Dilek, E.Tilenbaev, Z.Saygı, Ç.Ürtiş, Some Results On Three-Valued Walsh Transforms from Decimations of Helleseth-Gong Sequences, ISCTURKEY 2013, Proceedings of 6th International Conference on Information Security and Cryptology, pp. 149-152, September, 2013, Ankara, Turkey.
3. E.Tilenbaev, H.Dilek, Z.Saygı, Ç.Ürtiş, Some Observations on Distribution of Cross Correlation of Two Nonbinary Sequences, ISCTURKEY 2013, Proceedings of 6th International Conference on Information Security and Cryptology, pp. 137-141, September, 2013, Ankara, Turkey.
4. F. Özbudak, Z. Saygı, On the exact number of solutions of certain linearized equations, WCC 2013, Proceedings of International Workshop on Coding and Cryptography, April 15-19, 2013, Bergen, Norway.
5. S. Kahraman, Z. Saygı, Optimal Frekans Atlamalı Diziler, ISCTURKEY 2012, Proceedings of 5th International Conference on Information Security and Cryptology, pp. 169-174, May 17-18, 2012, Ankara, Turkey.

6. K. Otal, Z. Saygı, Ç. Ürtiş, Cyclotomic Sayılar ve Sidel'nikov Dizileri, ISCTURKEY 2012, Proceedings of 5th International Conference on Information Security and Cryptology, pp. 175-178, May 17-18, 2012, Ankara, Turkey.
7. N. Öztop, O. Koçak, O. Kurt, Z. Saygı, Notes on Bent Functions in Polynomial Forms, ISCTURKEY 2012, Proceedings of 5th International Conference on Information Security and Cryptology, pp. 179-182, May 17-18, 2012, Ankara, Turkey.
8. F. Özbudak, Z. Saygı, Counting quadratic forms of codimension 2 in characteristic 2 and relations to maximal curves, WCC 2011, Proceedings of International Workshop on Coding and Cryptography, pp. 379-387, April 11-15, 2011, Paris, France.
9. E. K. Özbudak, F. Özbudak, Z. Saygı, A Class of Authentication Codes with Secrecy, WCC 2009, Proceedings of International Workshop on Coding and Cryptography, pp. 273-285, May 10-15, 2009, Ullensvang, Norway.
10. A. Doğanaksoy, E. Saygı, Z. Saygı, Some Necessary Conditions for a Quadratic Feedback Shift Register to Generate a Maximum Length Sequence, BFCA-07, Proceedings of Third International Workshop on Boolean Functions : Cryptography and Applications, May 2-3, 2007, Paris, France.
11. F. Özbudak, Z. Saygı, Constructions of Systematic Authentication Codes Using Additive Polynomials, WCC 2007, Proceedings of International Workshop on Coding and Cryptography, pp. 405-414, April 16-20, 2007, Versailles, France.
12. B. G. Dündar, F. Göloğlu, A. Doğanaksoy, Z. Saygı, A method of constructing highly nonlinear balanced Boolean functions, BFCA-06, Proceedings of Second International Workshop on Boolean Functions: Cryptography and Applications, pp. 1-11, March 13-15, 2006, Rouen, France.
13. A. Doğanaksoy, S. Sağdıçoğlu, Z. Saygı, M. Uğuz, A note on linearity and homomorphicity, BFCA-06, Proceedings of Second International Workshop on Boolean Functions: Cryptography and Applications, pp. 99-106, March 13-15, 2006, Rouen, France.
14. E. Saygı, Z. Saygı, M. S. Turan, A. Doğanaksoy, Statistical approach on the number of SAC satisfying functions, BFCA-05, Proceedings of First International Workshop on Boolean Functions: Cryptography and Applications, pp. 39-48, March 7-9, 2005, Rouen, France.

C. National Conference Papers:

1. H. Özadam, F. Özbudak, Z. Saygı, Secret sharing schemes and linear codes, Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı 101-106, 13-14 Aralık 2007, Ankara, Türkiye.
2. Doğanaksoy, B. G. Dündar, F. Göloğlu, Z. Saygı, F. Sulak, M. Uğuz, A Survey on Bent Functions and Normality, II. Ulusal Kriptoloji Sempozyumu Bildiriler Kitabı 19-26, 15-17 Aralık 2006, Ankara, Türkiye.
3. Z. Saygı, S. Yeşil, Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar, I. Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı 28-34, 7-8 Aralık 2006, Ankara, Türkiye.

4. F. Özbudak, Z. Saygı, Construction of Systematic Authentication Codes, I. Ulusal Kriptoloji Sempozyumu Bildiriler Kitabı 142-148 , 18-20 Kasım 2005, Ankara, Türkiye.

D. Other:

1. Constructions of Authentication Codes, Ph.D. Thesis, 2007, METU.
2. A Method of Constructing Secure S-boxes, M.S. Thesis, 2003, METU.

DOCTORAL STUDENTS:

1. Neşe Öztop Koçak, On Bent and Semi Bent Functions, METU, 2015 Expected
2. Ayhan Coşgun, Rational Points of Some Special Artin-Schreier Type Curves over Finite Fields, METU, 2016 Expected
3. Kübra Bayraktar, Number of Irreducible Polynomials over Finite Fields Having Prescribed Coefficients, Ankara Univ., 2016 Expected
4. Seda Kahraman, New Frequency Hopping Sequences, TOBB ETU, 2016 Expected
5. Ernist Tilenbaev, Cross Correlation Properties of Sequences over Finite Fields, TOBB ETU, 2016 Expected
6. Hasan Dilek, New Sequences over Finite Fields Having Good Croos Correlation Properties, TOBB ETU, 2017 Expected

MASTER'S STUDENTS:

1. KübraBayraktar, Frequncy Hopping Sequences, TOBB ETU, 2010.
2. Seda Kahraman, Optimal Frequency Hopping Sequences, TOBB ETU, 2011.
3. Kamil Otal, Cyclotomy and Some Applications in Cryptography, TOBB ETU, 2012.
4. Emrah S. Yılmaz, Generalized bent functions with perfect nonlinear functions on arbitrary groups, METU, 2012, (Co-Advisor).
5. Hasan Dilek, Some results on correlations of Helleseth-Gong sequences, TOBB ETU, 2013.

PROJECTS:

- Some Cryptographic Applications using algebraic curves and exponential sums, sponsored by TUBITAK - 15.February.2010 - 15.February.2013 Researcher and Project Manager
- Algebraic Curves and Their Applications on Some Problems in Coding Theory and Cryptography, sponsored by TUBITAK, 01.May.2010 - 01.May.2013 - Researcher
- Some Applications over Finite Fields and Finite Rings, sponsored by TUBITAK, 01.March.2008 - 01. March.2011 Researcher
- Research, Improvements and Applications on PKI, sponsored by TUBITAK, 01.July.2006 - 01.July.2008 Researcher

COURSES:

- Calculus-I
- Calculus-II

- Linear Algebra
- Linear Algebra for Math. Students
- Discrete Mathematics
- Introduction to Cryptography
- Introduction to Coding Theory
- Introduction to Finite Field
- Algebra