Lect. ALİ DOĞANAKSOY

Personal Information

Email: aldoks@metu.edu.tr
Web: https://avesis.metu.edu.tr/aldoks

Advising Theses

DOĞANAKSOY A., Cryptographic protocols of signal and signal based instant messaging applications, Postgraduate, H.DİNÇER(Student), 2022
DOĞANAKSOY A., Permutation polynomials and construction of bent functions, Doctorate, P.ONGAN(Student), 2021
DOĞANAKSOY A., On measuring security bounds of some ciphers using mixed integer linear programming (MILP) approach, Postgraduate, C.TÜRESİN(Student), 2021
DOĞANAKSOY A., A new lightweight statistical randomness test suite and itsevaluation by comparison with other test suites, Doctorate, Z.AKCENGİZ(Student), 2021
DOĞANAKSOY A., On password-based authenticated key exchange (PAKE) protocols., Postgraduate, M.Tonga(Student), 2020
DOĞANAKSOY A., Secure message authentication protocol for can (controller area network)., Postgraduate, S.Mertol(Student), 2020
DOĞANAKSOY A., A study of lightweight cryptography, Postgraduate, Z.Çamur(Student), 2020
DOĞANAKSOY A., Statistical iid tests of integer sequences, Postgraduate, S.Yılmaz(Student), 2019
DOĞANAKSOY A., A survey on the provable security using indistinguishability notion on cryptographic encryption schemes, Postgraduate, E.AYAR(Student), 2018
DOĞANAKSOY A., TEZCAN C., DIFFERENTIAL CRYPTANALYSIS ON LBLOCK USING DIFFERENTIAL FACTORS, Postgraduate, M.ÖĞÜNÇ(Student), 2018
DOĞANAKSOY A., Slide attack and its applications, Postgraduate, E.USLU(Student), 2017
DOĞANAKSOY A., Character sums of quadratic forms over finite fields and the number of rational points for some classes of artin-schreier type curves, Doctorate, A.Coşgun(Student), 2017
DOĞANAKSOY A., Sonlu cisimler üzerinde kuadratik formların karakter toplamları ve bazı Artin-Schreier tipi eğri sınıflarının rasyonel nokta sayıları, Doctorate, A.COŞGUN(Student), 2017
DOĞANAKSOY A., Secure password generation through statistical randomness tests, Postgraduate, A.USLU(Student), 2017
DOĞANAKSOY A., A unified evaluation of statistical randomness tests and experimental analysis of their relations, Doctorate, O.KOÇAK(Student), 2016
DOĞANAKSOY A., Server notaries: A complementary approach to the web pki trust model, Doctorate, E.YÜCE(Student), 2016
DOĞANAKSOY A., Secure electronic exam, Doctorate, L.TARKAN(Student), 2016
DOĞANAKSOY A., Improvement on bit diffusion analysis of Pi-Cipher, Postgraduate, B.BOZDEMİR(Student), 2016
DOĞANAKSOY A., On constructions and enumeration of bent and semi-bent functions, Doctorate, N.KOÇAK(Student), 2015
DOĞANAKSOY A., Relating undisturbed bits to other properties of substitution boxes, Postgraduate, R.HASAN(Student), 2014
DOĞANAKSOY A., A Randomness test based on postulate r-2 on the number of runs, Postgraduate, O.Şeker(Student), 2014
DOĞANAKSOY A., A randomness test based on postulate r-2 on the number of runs, Postgraduate, O.ŞEKER(Student), 2014

DOĞANAKSOY A., AKYILDIZ E., Improbable differential cryptanalysis, Doctorate, C.TEZCAN(Student), 2014
DOĞANAKSOY A., On nonlinearity and hamming weight preserving bijective mappings acting on boolean functions, Doctorate, İ.SERTKAYA(Student), 2014
DOĞANAKSOY A., Mutual correlation of randomness test and analysis of test outputs of transformed and biased sequences, Postgraduate, Z.Akcengiz(Student), 2014
DOĞANAKSOY A., Mutual correlation of randomness tests and analysis of test outputs of transformed and biased sequences, Postgraduate, Z.AKCENGİZ(Student), 2014
DOĞANAKSOY A., Analysis of Boolean functions with respect to Walsh spectrum, Doctorate, E.UYAN(Student), 2013
DOĞANAKSOY A., Computing cryptographic properties of Boolean functions from the algebraic normal orm representation, Doctorate, Ç.Çalık(Student), 2013
DOĞANAKSOY A., Computing cryptographic properties of Boolean functions from the algebraic normal form representation, Doctorate, Ç.ÇALIK(Student), 2013
DOĞANAKSOY A., Statistical analysis of block ciphers and hash functions, Doctorate, F.SULAK(Student), 2011
DOĞANAKSOY A., Basic cryptanalysis methods on block ciphers, Postgraduate, D.ÇELİK(Student), 2010
DOĞANAKSOY A., Generating functions and their applications, Postgraduate, B.BİLGİN(Student), 2010
DOĞANAKSOY A., Design and analysis of hash functions, Postgraduate, O.KOÇAK(Student), 2009
DOĞANAKSOY A., Combined attacks on block ciphers, Postgraduate, N.ÖZTOP(Student), 2009
DOĞANAKSOY A., Time memory trade off attack on symmetric ciphers, Doctorate, A.NURDAN(Student), 2009
DOĞANAKSOY A., Related-key attacks on block ciphers, Postgraduate, A.DARBUKA(Student), 2009
DOĞANAKSOY A., Spectral modular multiplication, Doctorate, İ.HALUK(Student), 2009
DOĞANAKSOY A., Impossible differential cryptanalysis of reduced round HIGHT, Postgraduate, C.TEZCAN(Student), 2009
DOĞANAKSOY A., On statistical analysis of synchronous stream ciphers, Doctorate, M.Sönmez(Student), 2008
DOĞANAKSOY A., Sarmal: A cryptographic hash function, Postgraduate, K.VARICI(Student), 2008
DOĞANAKSOY A., On the security of tiger hash function, Postgraduate, O.ÖZEN(Student), 2008
DOĞANAKSOY A., How to invert one-way functions: Time-memory trade-off method, Postgraduate, Ç.ÇALIK(Student), 2007
DOĞANAKSOY A., Verifiability and receipt-freeness in cryptographic voting systems, Doctorate, O.ÇETİNKAYA(Student), 2007
DOĞANAKSOY A., Constructions of bent functions, Postgraduate, F.SULAK(Student), 2006
DOĞANAKSOY A., Nonlinearity preserving post-transformations, Postgraduate, İ.SERTKAYA(Student), 2004
DOĞANAKSOY A., Counting and constructing boolean functions with particular difference distribution vectors /, Postgraduate, E.YILDIRIM(Student), 2004
DOĞANAKSOY A., Cryptological viewpoint of boolean function, Postgraduate, S.SAĞDIÇOĞLU(Student), 2003
DOĞANAKSOY A., Alpha invariant for foliated manifolds, Postgraduate, K.ULUER(Student), 1997

Published journal articles indexed by SCI, SSCI, and AHCI

I. **LS-14 test suite for long sequences**
Akcengiz Z., ASLAN M., DOĞANAKSOY A., Sulak F., UĞUZ M.
Hacettepe Journal of Mathematics and Statistics, vol.53, no.1, pp.230-250, 2024 (SCI-Expanded)

II. **Periodic template tests: A family of statistical randomness tests for a collection of binary sequences**
SULAK F., Doganaksoy A., Uguz M., Kocak O.
DISCRETE APPLIED MATHEMATICS, vol.271, pp.191-204, 2019 (SCI-Expanded)

III. **R-2 composition tests: a family of statistical randomness tests for a collection of binary sequences**
UĞUZ M., DOĞANAKSOY A., SULAK F., Kocak O.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, vol.11, no.5, pp.921-949, 2019 (SCI-Expanded)

IV. **Mutual correlation of NIST statistical randomness tests and comparison of their sensitivities on transformed sequences**
DOĞANAKSOY A., SULAK F., UĞUZ M., Seker O., Akcengiz Z.

TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, vol.25, no.2, pp.655-665, 2017 (SCI-Expanded)

V. **On the independence of statistical randomness tests included in the NIST test suite**
SULAK F., UĞUZ M., Kocak O., DOĞANAKSOY A.
TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, vol.25, no.5, pp.3673-3683, 2017 (SCI-Expanded)

VI. **New Statistical Randomness Tests Based on Length of Runs**
DOĞANAKSOY A., SULAK F., UĞUZ M., Seker O., Akcengiz Z.
MATHEMATICAL PROBLEMS IN ENGINEERING, 2015 (SCI-Expanded)

VII. **Counting Boolean functions with specified values in their Walsh spectrum**
Uyan E., Calik C., DOĞANAKSOY A.
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, vol.259, pp.522-528, 2014 (SCI-Expanded)

VIII. **On Lempel-Ziv complexity of sequences**
Doganaksoy A., Gologlu F.
SEQUENCES AND THEIR APPLICATIONS - SETA 2006, vol.4086, pp.180-189, 2006 (SCI-Expanded)

Articles Published in Other Journals

I. **MODIFICATIONS OF KNUTH RANDOMNESS TESTS FOR INTEGER AND BINARY SEQUENCES**
Kocak O., SULAK F., DOĞANAKSOY A., UĞUZ M.
COMMUNICATIONS FACULTY OF SCIENCES UNIVERSITY OF ANKARA-SERIES A1 MATHEMATICS AND STATISTICS, vol.67, no.2, pp.64-81, 2018 (ESCI)

Books & Book Chapters

I. **İşletme, İktisat, Yaşam Bilimleri ve Sosyal Bilimler için Sonlu Matematik**
DOĞANAKSOY A., UĞUZ M., SAYGI Z., SEVİNİK ADIGÜZEL R., SULAK F., ÜRTİŞ Ç.
Palme Yayıncılık, Ankara, 2017

II. **Yarışmalara Hazırlananlar İçin Çözümlü Matematik Problemleri**
DOĞANAKSOY A., SAYGI Z., SULAK F., UĞUZ M., ÜRTİŞ Ç.
OYAK, 2010

Refereed Congress / Symposium Publications in Proceedings

I. **A New Randomness Test Based on the Overlapping Blocks**
UĞUZ M., DOĞANAKSOY A., SULAK F.
Combinatorics 2016, Maratea (PZ), Italy, 29 May - 04 June 2016, pp.138

II. **Affine Equivalency and Nonlinearity Preserving Bijective Mappings over F-2**
Sertkaya I., DOĞANAKSOY A., Uzunkol O., Kiraz M. S.
5th International Workshop on the Arithmetic of Finite Fields (WAIFI), Gebze, Turkey, 27 - 28 September 2014, vol.9061, pp.121-136

III. **MORALS OF AN ANECDOTE AS STARTING POINT OF A LECTURE IN MATHEMATICS**
DOĞANAKSOY A.
35th Annual Conference of the International-Group-for-the-Psychology-of-Mathematics-Education (PME), Ankara, Turkey, 10 - 15 July 2011, pp.23-30

IV. **Evaluation of Randomness Test Results for Short Sequences**
Sulak F., DOĞANAKSOY A., Ege B., Kocak O.
6th International Conference on Sequences and Their Applications, Paris, France, 13 - 17 September 2010,

vol.6338, pp.309-319

V. **Choosing Parameters to Achieve A Higher Success Rate for Hellman Time Memory Trade Off Attack**
SARAN A. N., DOĞANAKSOY A.
4th International Conference on Availability, Reliability and Security, Fukuoka, Japan, 16 - 19 March 2009, pp.504-505

VI. **Alternative Approach to Maurer's Universal Statistical Test**
TEZCAN C., DOĞANAKSOY A.
3rd Information Security and Cryptology Conference ISC Turkey, Turkey, 25 - 27 December 2008

VII. **New Distinguishers Based on Random Mappings against Stream Ciphers**
Turan M. S., Calik C., Saran N. B., DOĞANAKSOY A.
5th International Conference on Sequences and Their Applications (SETA 2008), Kentucky, United States Of America, 14 - 18 September 2008, vol.5203, pp.30-31

VIII. **On Independence and Sensitivity of Statistical Randomness Tests**
Turan M. S., DOĞANAKSOY A., Boztas S.
5th International Conference on Sequences and Their Applications (SETA 2008), Kentucky, United States Of America, 14 - 18 September 2008, vol.5203, pp.18-19

IX. **A Survey on Bent Functions and Normality**
DOĞANAKSOY A., Dündar B. G., Göloğlu F., SAYGI Z., SULAK F., UĞUZ M.
2. Ulusal Kriptoloji Sempozyumu, Turkey, 15 - 17 December 2007

X. **A practical verifiable e-voting protocol for large scale elections over a network**
Cetinkaya O., DOĞANAKSOY A.
2nd International Conference on Availability, Reliability and Security, Vienna, Austria, 10 - 13 April 2007, pp.432-433

XI. **Pseudo-voter identity (PVID) scheme for e-voting protocols**
Cetinkaya O., DOĞANAKSOY A.
2nd International Conference on Availability, Reliability and Security, Vienna, Austria, 10 - 13 April 2007, pp.1190-1191

XII. **A NOTE ON LINEARITY AND HOMOMORPHICITY**
DOĞANAKSOY A., Sağdıçoğlu S., SAYGI Z., UĞUZ M.
Boolean Functions: Cryptography, Applications, BFCA 2006, Paris, France, 13 March 2006, vol.387, pp.99-106

XIII. **Constructions of Highly Nonlinear Balanced Boolean Functions**
DOĞANAKSOY A., Dündar B. G., Göloğlu F., SAYGI Z., SULAK F., UĞUZ M.
1. Ulusal Kriptoloji Sempozyumu, Turkey, 18 - 20 November 2005

Metrics

Publication: 25
Citation (WoS): 99
Citation (Scopus): 45
H-Index (WoS): 7
H-Index (Scopus): 4

Non Academic Experience

METU
METU