Lect. ALİ DOĞANAKSOY

Personal Information

Email: aldoks@metu.edu.tr

Advising Theses

DOĞANAKSOY A., A survey on the provable security using indistinguishability notion on cryptographic encryption schemes, Post Graduate, E.AYAR(Student), 2018
DOĞANAKSOY A., DIFFERENTIAL CRYPTANALYSIS ON LBLOCK USING DIFFERENTIAL FACTORS, Post Graduate, M.ÖĞÜNÇ(Student), 2018
DOĞANAKSOY A., Slide attack and its applications, Post Graduate, E.USLU(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, Post Graduate, A.USLU(Student), 2017
DOĞANAKSOY A., Improvement on bit diffusion analysis of Pi-Cipher, Post Graduate, B.BOZDEMİR(Student), 2016
DOĞANAKSOY A., Server notaries: A complementary approach to the web pki trust model, Doctorate, E.YÜCE(Student), 2016
DOĞANAKSOY A., A unified evaluation of statistical randomness tests and experimental analysis of their relations, Doctorate, O.KOÇAK(Student), 2016
DOĞANAKSOY A., Secure electronic exam, Doctorate, L.TARKAN(Student), 2016
DOĞANAKSOY A., On constructions and enumeration of bent and semi-bent functions, Doctorate, N.KOÇAK(Student), 2015
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 tests and analysis of test outputs of transformed and biased sequences, Post Graduate, Z.AKCENGİZ(Student), 2014
DOĞANAKSOY A., AKYILDIZ E., Improbable differential cryptanalysis, Doctorate, C.TEZCAN(Student), 2014
DOĞANAKSOY A., Relating undisturbed bits to other properties of substitution boxes, Post Graduate, R.HASAN(Student), 2014
DOĞANAKSOY A., A randomness test based on postulate r-2 on the number of runs, Post Graduate, O.ŞEKER(Student), 2014
DOĞANAKSOY A., Computing cryptographic properties of Boolean functions from the algebraic normal form representation, Doctorate, Ç.ÇALIK(Student), 2013
DOĞANAKSOY A., Analysis of Boolean functions with respect to Walsh spectrum, Doctorate, E.UYAN(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, Post Graduate, D.ÇELİK(Student), 2010
DOĞANAKSOY A., Generating functions and their applications, Post Graduate, B.BİLGİN(Student), 2010
DOĞANAKSOY A., Spectral modular multiplication, Doctorate, İ.HALUK(Student), 2009
DOĞANAKSOY A., Design and analysis of hash functions, Post Graduate, O.KOÇAK(Student), 2009
DOĞANAKSOY A., Impossible differential cryptanalysis of reduced round HIGHT, Post Graduate, C.TEZCAN(Student), 2009
DOĞANAKSOY A., Time memory trade off attack on symmetric ciphers, Doctorate, A.NURDAN(Student), 2009
DOĞANAKSOY A., Combined attacks on block ciphers, Post Graduate, N.ÖZTOP(Student), 2009
DOĞANAKSOY A., Related-key attacks on block ciphers, Post Graduate, A.DARBUKA(Student), 2009
DOĞANAKSOY A., On the security of tiger hash function, Post Graduate, O.ÖZEN(Student), 2008

DOĞANAKSOY A., Sarmal: A cryptographic hash function, Post Graduate, K.VARICI(Student), 2008
DOĞANAKSOY A., Verifiability and receipt-freeness in cryptographic voting systems, Doctorate, O.ÇETİNKAYA(Student), 2007
DOĞANAKSOY A., How to invert one-way functions: Time-memory trade-off method, Post Graduate, Ç.ÇALIK(Student), 2007
DOĞANAKSOY A., Constructions of bent functions, Post Graduate, F.SULAK(Student), 2006
DOĞANAKSOY A., Counting and constructing boolean functions with particular difference distribution vectors, Post Graduate, E.YILDIRIM(Student), 2004
DOĞANAKSOY A., Nonlinearity preserving post-transformations, Post Graduate, İ.SERTKAYA(Student), 2004
DOĞANAKSOY A., Cryptological viewpoint of boolean function, Post Graduate, S.SAĞDIÇOĞLU(Student), 2003
DOĞANAKSOY A., Alpha invariant for foliated manifolds, Post Graduate, K.ULUER(Student), 1997

Articles Published in Journals That Entered SCI, SSCI and AHCI Indexes

- **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 (Journal Indexed in SCI)
- **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, pp.921-949, 2019 (Journal Indexed in SCI)
- **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, pp.3673-3683, 2017 (Journal Indexed in SCI)
- **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, pp.655-665, 2017 (Journal Indexed in SCI)
- **New Statistical Randomness Tests Based on Length of Runs**
  DOĞANAKSOY A., SULAK F., UĞUZ M., Seker O., Akcengiz Z.
  MATHEMATICAL PROBLEMS IN ENGINEERING, 2015 (Journal Indexed in SCI)
- **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 (Journal Indexed in SCI)
- **On Lempel-Ziv complexity of sequences**
  Doganaksoy A., Gologlu F.
  SEQUENCES AND THEIR APPLICATIONS - SETA 2006, vol.4086, pp.180-189, 2006 (Journal Indexed in SCI)

Articles Published in Other Journals

- **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, pp.64-81, 2018 (Journal Indexed in ESCI)

Refereed Congress / Symposium Publications in Proceedings

- **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
- **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
- **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
- **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
- **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
- **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
- **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
- **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
- **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

Citations

Total Citations (WOS):73
h-index (WOS):5