Öğr.Gör. ALİ DOĞANAKSOY

Kişisel Bilgiler

E-posta: aldoks@metu.edu.tr

Yönetilen Tezler

DOĞANAKSOY A., A survey on the provable security using indistinguishability notion on cryptographic encryption schemes, Yüksek Lisans, E.AYAR(Öğrenci), 2018
DOĞANAKSOY A., DIFFERENTIAL CRYPTANALYSIS ON LBLOCK USING DIFFERENTIAL FACTORS, Yüksek Lisans, M.ÖĞÜNÇ(Öğrenci), 2018
DOĞANAKSOY A., Slide attack and its applications, Yüksek Lisans, E.USLU(Öğrenci), 2017
DOĞANAKSOY A., Sonlu cisimler üzerinde kuadratik formların karakter toplamları ve bazı Artin-Schreier tipi eğri sınıflarının rasyonel nokta sayıları, Doktora, A.COŞGUN(Öğrenci), 2017
DOĞANAKSOY A., Secure password generation through statistical randomness tests, Yüksek Lisans, A.USLU(Öğrenci), 2017
DOĞANAKSOY A., Improvement on bit diffusion analysis of Pi-Cipher, Yüksek Lisans, B.BOZDEMİR(Öğrenci), 2016
DOĞANAKSOY A., Server notaries: A complementary approach to the web pki trust model, Doktora, E.YÜCE(Öğrenci), 2016
DOĞANAKSOY A., A unified evaluation of statistical randomness tests and experimental analysis of their relations, Doktora, O.KOÇAK(Öğrenci), 2016
DOĞANAKSOY A., Secure electronic exam, Doktora, L.TARKAN(Öğrenci), 2016
DOĞANAKSOY A., On constructions and enumeration of bent and semi-bent functions, Doktora, N.KOÇAK(Öğrenci), 2015
DOĞANAKSOY A., On nonlinearity and hamming weight preserving bijective mappings acting on boolean functions, Doktora, İ.SERTKAYA(Öğrenci), 2014
DOĞANAKSOY A., Mutual correlation of randomness tests and analysis of test outputs of transformed and biased sequences, Yüksek Lisans, Z.AKCENGİZ(Öğrenci), 2014
DOĞANAKSOY A., AKYILDIZ E., Improbable differential cryptanalysis, Doktora, C.TEZCAN(Öğrenci), 2014
DOĞANAKSOY A., Relating undisturbed bits to other properties of substitution boxes, Yüksek Lisans, R.HASAN(Öğrenci), 2014
DOĞANAKSOY A., A randomness test based on postulate r-2 on the number of runs, Yüksek Lisans, O.ŞEKER(Öğrenci), 2014
DOĞANAKSOY A., Computing cryptographic properties of Boolean functions from the algebraic normal form representation, Doktora, Ç.ÇALIK(Öğrenci), 2013
DOĞANAKSOY A., Analysis of Boolean functions with respect to Walsh spectrum, Doktora, E.UYAN(Öğrenci), 2013
DOĞANAKSOY A., Statistical analysis of block ciphers and hash functions, Doktora, F.SULAK(Öğrenci), 2011
DOĞANAKSOY A., Basic cryptanalysis methods on block ciphers, Yüksek Lisans, D.ÇELİK(Öğrenci), 2010
DOĞANAKSOY A., Generating functions and their applications, Yüksek Lisans, B.BİLGİN(Öğrenci), 2010
DOĞANAKSOY A., Spectral modular multiplication, Doktora, İ.HALUK(Öğrenci), 2009
DOĞANAKSOY A., Design and analysis of hash functions, Yüksek Lisans, O.KOÇAK(Öğrenci), 2009
DOĞANAKSOY A., Impossible differential cryptanalysis of reduced round HIGHT, Yüksek Lisans, C.TEZCAN(Öğrenci), 2009
DOĞANAKSOY A., Time memory trade off attack on symmetric ciphers, Doktora, A.NURDAN(Öğrenci), 2009
DOĞANAKSOY A., Combined attacks on block ciphers, Yüksek Lisans, N.ÖZTOP(Öğrenci), 2009
DOĞANAKSOY A., Related-key attacks on block ciphers, Yüksek Lisans, A.DARBUKA(Öğrenci), 2009
DOĞANAKSOY A., On the security of tiger hash function, Yüksek Lisans, O.ÖZEN(Öğrenci), 2008
DOĞANAKSOY A., Sarmal: A cryptographic hash function, Yüksek Lisans, K.VARICI(Öğrenci), 2008

DOĞANAKSOY A., Verifiability and receipt-freeness in cryptographic voting systems, Doktora, O.ÇETİNKAYA(Öğrenci), 2007

DOĞANAKSOY A., How to invert one-way functions: Time-memory trade-off method, Yüksek Lisans, Ç.ÇALIK(Öğrenci), 2007

DOĞANAKSOY A., Constructions of bent functions, Yüksek Lisans, F.SULAK(Öğrenci), 2006

DOĞANAKSOY A., Counting and constructing boolean functions with particular difference distribution vectors, Yüksek Lisans, E.YILDIRIM(Öğrenci), 2004

DOĞANAKSOY A., Nonlinearity preserving post-transformations, Yüksek Lisans, İ.SERTKAYA(Öğrenci), 2004

DOĞANAKSOY A., Cryptological viewpoint of boolean function, Yüksek Lisans, S.SAĞDIÇOĞLU(Öğrenci), 2003

DOĞANAKSOY A., Alpha invariant for foliated manifolds, Yüksek Lisans, K.ULUER(Öğrenci), 1997

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

- **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, cilt.271, ss.191-204, 2019 (SCI İndekslerine Giren Dergi)
- **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, cilt.11, ss.921-949, 2019 (SCI İndekslerine Giren Dergi)
- **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, cilt.25, ss.3673-3683, 2017 (SCI İndekslerine Giren Dergi)
- **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, cilt.25, ss.655-665, 2017 (SCI İndekslerine Giren Dergi)
- **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 İndekslerine Giren Dergi)
- **Counting Boolean functions with specified values in their Walsh spectrum**
  Uyan E., Calik C., DOĞANAKSOY A.
  JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, cilt.259, ss.522-528, 2014 (SCI İndekslerine Giren Dergi)
- **On Lempel-Ziv complexity of sequences**
  Doganaksoy A., Gologlu F.
  SEQUENCES AND THEIR APPLICATIONS - SETA 2006, cilt.4086, ss.180-189, 2006 (SCI İndekslerine Giren Dergi)

Diğer Dergilerde Yayınlanan Makaleler

- **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, cilt.67, ss.64-81, 2018 (ESCI İndekslerine Giren Dergi)

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

- **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, Türkiye, 27 - 28 Eylül 2014, cilt.9061, ss.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, Türkiye, 10 - 15 Temmuz 2011, ss.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, Fransa, 13 - 17 Eylül 2010, cilt.6338, ss.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, Japonya, 16 - 19 Mart 2009, ss.504-505
- **Alternative Approach to Maurer's Universal Statistical Test**
  TEZCAN C., DOĞANAKSOY A.
  3rd Information Security and Cryptology Conference ISC Turkey, Türkiye, 25 - 27 Aralık 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, Amerika Birleşik Devletleri, 14 - 18 Eylül 2008, cilt.5203, ss.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, Amerika Birleşik Devletleri, 14 - 18 Eylül 2008, cilt.5203, ss.18-19
- **Pseudo-voter identity (PVID) scheme for e-voting protocols**
  Cetinkaya O., DOĞANAKSOY A.
  2nd International Conference on Availability, Reliability and Security, Vienna, Avusturya, 10 - 13 Nisan 2007, ss.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, Avusturya, 10 - 13 Nisan 2007, ss.432-433

Atıflar

Toplam Atıf Sayısı (WOS):73
h-indeksi (WOS):5