Prof.Dr. ERSAN AKYILDIZ

Kişisel Bilgiler

E-posta: ersan@metu.edu.tr

Yönetilen Tezler

CENK M., AKYILDIZ E., Homomorphic encryption for data security in cloud computing, Yüksek Lisans, A.WAINAKH(Öğrenci), 2018
AKYILDIZ E., Pairing based non-repudiation protocols in cryptography, Doktora, Ö.SEVER(Öğrenci), 2017
AKYILDIZ E., On the efficiency of lattice-based cryptographic schemes on graphical processing unit, Doktora, Z.YÜCE(Öğrenci), 2016
DOĞANAKSOY A., AKYILDIZ E., Improbable differential cryptanalysis, Doktora, C.TEZCAN(Öğrenci), 2014
AKYILDIZ E., On lattice based digital signature schemes, Yüksek Lisans, F.JAVANİ(Öğrenci), 2014
AKYILDIZ E., Free storage basis conversion over extension field, Yüksek Lisans, N.HAROLD(Öğrenci), 2014
AKYILDIZ E., FPGA based cryptography computation platform and the basis conversion in composite finite fields, Doktora, R.MUHAMMAD(Öğrenci), 2013
AKYILDIZ E., On secure electronic auction process of government domestic debt securities in Turkey, Doktora, A.BEKTAŞ(Öğrenci), 2013
AKYILDIZ E., On the trace based public key cryptosystems over finite fields, Doktora, M.ASHRAF(Öğrenci), 2013
AKYILDIZ E., On provable security of some public key encryption schemes, Doktora, T.HANOYMAK(Öğrenci), 2012
KİŞİSEL A. U. Ö. , AKYILDIZ E., Fixed point scheme of the Hilbert scheme under a 1-dimesional additive algebraic group action, Doktora, E.ÖZKAN(Öğrenci), 2011
AKYILDIZ E., Elliptic curve pairing-based cryptography, Doktora, B.BÜLENT(Öğrenci), 2010
AKYILDIZ E., A compact cryptographic processor for IPSec applications, Yüksek Lisans, E.BİLGE(Öğrenci), 2010
AKYILDIZ E., Algebraic properties of the operations used in block cipher idea, Doktora, H.MURAT(Öğrenci), 2007
AKYILDIZ E., Scalar multiplication on elliptic curves, Yüksek Lisans, O.YAYLA(Öğrenci), 2006
AKYILDIZ E., Isomorphism classes of elliptic curves over finite fields of characteristic two, Yüksek Lisans, B.BÜLENT(Öğrenci), 2005
AKYILDIZ E., A method of constructing secure S-boxes, Yüksek Lisans, Z.SAYGI(Öğrenci), 2003
AKYILDIZ E., Subfields of the function field of the Deligne-Lusztig curve of ree type, Doktora, E.ÇAKÇAK(Öğrenci), 2002
AKYILDIZ E., Complete analytic functions and Riemann surfaces, Yüksek Lisans, H.BENNUN(Öğrenci), 2001
AKYILDIZ E., Nonlinearity properties of the mixing operations used in the block cipher Idea, Yüksek Lisans, H.MURAT(Öğrenci), 2000
AKYILDIZ E., Grobner bases and standart monomials on grassmannian, Yüksek Lisans, A.İRFAN(Öğrenci), 1998
AKYILDIZ E., Linear recurring sequences, Yüksek Lisans, A.EMRAH(Öğrenci), 1997
AKYILDIZ E., The Use of elliptic curves in cryptography, Yüksek Lisans, A.BAKİ(Öğrenci), 1994

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

- **An overview of trace based public key cryptography over finite fields**
  AKYILDIZ E., Ashraf M.
  JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, cilt.259, ss.599-621, 2014 (SCI İndekslerine Giren Dergi)
- **Recent Advances in Applied and Computational Mathematics: ICACM-IAM-METU**
  AKYILDIZ E.
  JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, cilt.259, ss.327-328, 2014 (SCI İndekslerine Giren Dergi)
- **Betti Numbers of Smooth Schubert Varieties and the Remarkable Formula of Kostant, Macdonald, Shapiro, and Steinberg**
  AKYILDIZ E., Carrell J. B.

MICHIGAN MATHEMATICAL JOURNAL, cilt.61, ss.543-553, 2012 (SCI İndekslerine Giren Dergi)

- **Congressional contributions to Computational and Applied Mathematics Preface**
  Goovaerts M. J. , Gebizlioglu O. L. , BAYRAMOĞLU İ., AKYILDIZ E.
  JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, cilt.235, ss.4517-4518, 2011 (SCI İndekslerine Giren Dergi)

Atıflar

Toplam Atıf Sayısı (WOS):7
h-indeksi (WOS):2