Prof. ERSAN AKYILDIZ

Personal Information

Email: ersan@metu.edu.tr

Advising Theses

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

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

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

AKYILDIZ E., Carrell J. B.
MICHIGAN MATHEMATICAL JOURNAL, vol.61, pp.543-553, 2012 (Journal Indexed in SCI)

- **Congressional contributions to Computational and Applied Mathematics Preface**
  Goovaerts M. J. , Gebizlioglu O. L. , BAYRAMOĞLU İ., AKYILDIZ E.
  JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, vol.235, pp.4517-4518, 2011 (Journal Indexed in SCI)

Citations

Total Citations (WOS):7
h-index (WOS):2