Prof. ERSAN AKYILDIZ

Personal Information

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

Advising Theses

AKYILDIZ E., Elliptic curves and use of their endomorphism rings in cryptography, Postgraduate, A.Mert(Student), 2019
AKYILDIZ E., Privacy and accuracy systems on financial databases, Doctorate, A.Bilgen(Student), 2019
CENK M., AKYILDIZ E., Homomorphic encryption for data security in cloud computing, Postgraduate, 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, Postgraduate, F.JAVANİ(Student), 2014
AKYILDIZ E., Free storage basis conversion over extension field, Postgraduate, 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., FGPA based cryptography computation platform and the basis conversion in composite finite fields, Doctorate, M.Riaz(Student), 2013
AKYILDIZ E., On the trace based public key cryptosystems over finite fields, Doctorate, M.ASHRAF(Student), 2013
AKYILDIZ E., On secure electronic auction process of government domestic debt securities in Turkey, Doctorate, A.BEKTAŞ(Student), 2013
AKYILDIZ E., On provable security of some public key encryption schemes, Doctorate, T.HANOYMAK(Student), 2012
Akyildiz E., Kişisel A. U. Ö., Fixed point scheme of the Hilbert scheme under a 1-dimesional additive algebraic group action, Doctorate, E.ÖZKAN(Student), 2011
AKYILDIZ E., KİŞİSEL A. U. Ö., Fixed point scheme of the Hilbert Scheme under a 1-dimensional 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, Postgraduate, E.BİLGE(Student), 2010
AKYILDIZ E., Optimizable multiresolution quadratic variation filter for high-frequency financial data, Postgraduate, A.Şen(Student), 2009
AKYILDIZ E., Algebraic properties of the operations used in block cipher idea, Doctorate, H.MURAT(Student), 2007
AKYILDIZ E., Credit risk modeling with stochastic volatility, jumps and stochastic interest rates, Postgraduate, A.Yüksel(Student), 2007
AKYILDIZ E., Scalar multiplication on elliptic curves, Postgraduate, O.YAYLA(Student), 2006
AKYILDIZ E., Isomorphism classes of elliptic curves over finite fields of characteristic two, Postgraduate, B.BÜLENT(Student), 2005
AKYILDIZ E., A method of constructing secure S-boxes, Postgraduate, 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, Postgraduate, H.BENNUN(Student), 2001
AKYILDIZ E., Nonlinearity properties of the mixing operations used in the block cipher Idea, Postgraduate, H.MURAT(Student), 2000
AKYILDIZ E., Grobner bases and standart monomials on grassmannian, Postgraduate, A.İRFAN(Student), 1998

AKYILDIZ E., Linear recurring sequences, Postgraduate, A.EMRAH(Student), 1997
AKYILDIZ E., The Use of elliptic curves in cryptography, Postgraduate, A.BAKİ(Student), 1994

Published journal articles indexed by SCI, SSCI, and AHCI

I. **Recent Advances in Applied and Computational Mathematics: ICACM-IAM-METU**
AKYILDIZ E.
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, vol.259, pp.327-328, 2014 (SCI-Expanded)
II. **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 (SCI-Expanded)
III. **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, no.3, pp.543-553, 2012 (SCI-Expanded)
IV. **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, no.16, pp.4517-4518, 2011 (SCI-Expanded)

Books & Book Chapters

I. **Şifrelerin Matematiği Kriptografi**
AKYILDIZ E., AKLEYLEK S., Çimen C.
ODTÜ Geliştirme Vakfı Yayıncılık, 2007
II. **Diferential Equations**
AKYILDIZ E., Akyıldız Y., Alpay S., ERKİP A. K., YAZICI A.
ODTÜ, Ankara, 1981

Refereed Congress / Symposium Publications in Proceedings

I. **Improved Contract Signing Protocol Based on Certificateless Hybrid Verifiably Encrypted Signature Scheme**
Sever Ö., AKYILDIZ E.
8th International Conference on Information Security and Cryptology, Ankara, Turkey, 30 - 31 October 2015
II. **An Overview fo Discrete Log and Trace Based Public Key Cryptography on Finite Fileds**
AKYILDIZ E.
International Conference on Pure and Applied Mathematics (ICPAM 2015), Van, Turkey, 25 - 28 August 2015
III. **Hybrid Non Repudiation Protocol with Pairing Based Cryptography**
SEVER Ö., AKYILDIZ E.
3rd International Symposium on Digital Forensics and Security (ISDFS 2015), Ankara, Turkey, 11 - 12 May 2015, pp.58-63
IV. **Storage Free Basis conversion over composite finite fields of odd characteristics**
Sial M. R., AKYILDIZ E.
6th International Information security and cryptology conference, Ankara, Turkey, 20 - 21 September 2013
V. **PKI lite A PKI system with limited resources**
AKYILDIZ E., YAYLA O.
II. International Conference on Information Security and Cryptology, Turkey, 13 - 14 December 2007, pp.59-62
VI. **Scalar multiplication on elliptic curves**

AKYILDIZ E., YAYLA O.
II. National Conference on Cryptology, Turkey, 15 - 17 December 2006, pp.114-124

Metrics

Publication: 13
Citation (WoS): 10
Citation (Scopus): 5
H-Index (WoS): 2
H-Index (Scopus): 1

Non Academic Experience

ODTÜ
ODTÜ