

Kişisel Bilgiler

E-posta: ersan@metu.edu.tr

Web: <https://avesis.metu.edu.tr/ersan>

Yönetilen Tezler

- AKYILDIZ E., Eliptik eğriler ve onların endomorfizma halkalarının kriptografide kullanımı, Yüksek Lisans, A.Mert(Öğrenci), 2019
- AKYILDIZ E., Finansal veri tabanlarında gizlilik ve doğruluk sistemleri, Doktora, A.Bilgen(Öğrenci), 2019
- 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.JAVANI(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., FGPA tabanlı kriptografi işlem platformu ve bileşik sonlu cisimlerde baz dönüşümü, Doktora, M.Riaz(Öğrenci), 2013
- AKYILDIZ E., On the trace based public key cryptosystems over finite fields, Doktora, M.ASHRAF(Öğrenci), 2013
- AKYILDIZ E., On secure electronic auction process of government domestic debt securities in Turkey, Doktora, A.BEKTAŞ(Öğrenci), 2013
- AKYILDIZ E., On provable security of some public key encryption schemes, Doktora, T.HANOYMAK(Öğrenci), 2012
- Akyıldız E., Kişisel A. U. Ö., Fixed point scheme of the Hilbert scheme under a 1-dimesional additive algebraic group action, Doktora, E.ÖZKAN(Öğrenci), 2011
- AKYILDIZ E., KİŞİSEL A. U. Ö., Hilbert Şeması'nın belirli bir 1-boyutlu toplamsal cebirsel grup etkisi altındaki sabit nokta şeması, 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., Yüksek frekanslı finansal veri için optimize edilebilir çok çözünürlüklü karesel varyasyon filtresi, Yüksek Lisans, A.Şen(Öğrenci), 2009
- AKYILDIZ E., Algebraic properties of the operations used in block cipher idea, Doktora, H.MURAT(Öğrenci), 2007
- AKYILDIZ E., Kredi riskinin stokastik volatilitite, sıçrama süreçleri ve stokastik faiz oranları ile modellenmesi, Yüksek Lisans, A.Yüksel(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.BAKI(Öğrenci), 1994

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

- I. **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-Expanded)
- II. **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-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, cilt.61, sa.3, ss.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, cilt.235, sa.16, ss.4517-4518, 2011 (SCI-Expanded)

Kitap & Kitap Bölümleri

- 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

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

- 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, Türkiye, 30 - 31 Ekim 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, Türkiye, 25 - 28 Ağustos 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, Türkiye, 11 - 12 Mayıs 2015, ss.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, Türkiye, 20 - 21 Eylül 2013
- V. **PKI lite A PKI system with limited resources**
AKYILDIZ E., YAYLA O.
II. International Conference on Information Security and Cryptology, Türkiye, 13 - 14 Aralık 2007, ss.59-62

VI. Scalar multiplication on elliptic curves

AKYILDIZ E., YAYLA O.

II. National Conference on Cryptology, Türkiye, 15 - 17 Aralık 2006, ss.114-124

Metrikler

Yayın: 13

Atıf (WoS): 10

Atıf (Scopus): 5

H-İndeks (WoS): 2

H-İndeks (Scopus): 1

Akademi Dışı Deneyim

ODTÜ

ODTÜ