Doç.Dr. Barış Bülent KIRLAR

Kişisel Bilgiler

E-posta: bariskirlar@sdu.edu.tr
Web: http://w3.sdu.edu.tr/personel/02919/doc-dr-baris-bulent-kirlar
Posta Adresi: Süleyman Demirel Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, 32260 Çünür/Isparta

Eğitim Bilgileri

Doktora, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi, Türkiye 2005 - 2010
Yüksek Lisans, Orta Doğu Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Matematik, Türkiye 2002 - 2005
Lisans, Ankara Üniversitesi, Fen Fakültesi, Matematik, Türkiye 1997 - 2001

Araştırma Alanları

Bilgisayar Bilimleri, Bilgi Güvenliği ve Güvenilirliği, Kriptoloji, Mühendislik ve Teknoloji

Mesleki Deneyim

Enstitü Müdür Yardımcısı, Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü, 2015 - 2018

Verdiği Dersler

Matematik I (İngilizce), Lisans, 2016 - 2017
Matematik II (İngilizce), Lisans, 2016 - 2017

Yönetilen Tezler

KIRLAR B. B. , Sonlu Cisimler Üzerinde Tanımlı Polinomların Kökleri Üzerine Bir Çalışma, Yüksek Lisans, B.YAYLALI(Öğrenci), 2019
KIRLAR B. B. , On the Trace Based Public Key Cryptosystems over Finite Fields, Doktora, M.ASHRAF(Öğrenci), 2013

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

I. **AN APPLICATION OF CRYPTO CLOUD COMPUTING IN SOCIAL NETWORKS BY COOPERATIVE GAME THEORY**
Ergun S., KIRLAR B. B. , ALPARSLAN GÖK S. Z. , Weber G.
JOURNAL OF INDUSTRIAL AND MANAGEMENT OPTIMIZATION, cilt.16, sa.4, ss.1927-1941, 2020 (SCI İndekslerine Giren Dergi)

II. **A game-theoretical and cryptographical approach to crypto-cloud computing and its economical and financial aspects**
KIRLAR B. B. , Ergun S., Gok S. Z. A. , Weber G.
ANNALS OF OPERATIONS RESEARCH, cilt.260, ss.217-231, 2018 (SCI İndekslerine Giren Dergi)

III. **A Game Theoretical Approach to Crypto Cloud Computing and Its Economical and Financial Aspects**
KIRLAR B. B. , ERGÜN S., ALPARSLAN GÖK S. Z. , Weber G. W.
ANNALS OF OPERATIONS RESEARCH, cilt.260, ss.217-231, 2018 (SCI Expanded İndekslerine Giren Dergi)

IV. **ON THE k-TH ORDER LFSR SEQUENCE WITH PUBLIC KEY CRYPTOSYSTEMS**
Kirlar B. B. , Cil M.
MATHEMATICA SLOVACA, cilt.67, sa.3, ss.601-610, 2017 (SCI İndekslerine Giren Dergi)

V. **New methods for public key cryptosystems based on XTR**
Akleylek S., KIRLAR B. B.
SECURITY AND COMMUNICATION NETWORKS, cilt.8, sa.18, ss.3682-3689, 2015 (SCI İndekslerine Giren Dergi)

VI. **Message transmission for GH-public key cryptosystem**
Ashraf M., Kirlar B. B.
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, cilt.259, ss.578-585, 2014 (SCI İndekslerine Giren Dergi)

VII. **On the elliptic curves y(2)=x(3)-c with embedding degree one**
Kirlar B. B.
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, cilt.235, sa.16, ss.4724-4728, 2011 (SCI İndekslerine Giren Dergi)

Diğer Dergilerde Yayınlanan Makaleler

I. **Crypto Cloud Computing and Its Economical and Financial Aspects with Cooperative Game Theory**
ERGÜN S., ALPARSLAN GÖK S. Z. , KIRLAR B. B. , WEBER G. W.
Internat ional Federat ion of Operat ional Research Societ ies (IFORS) News, cilt.9, sa.4, ss.19-21, 2015 (Hakemsiz Dergi)

II. **On the Alternate Models of Elliptic Curves**
ASHRAF M., KIRLAR B. B.
INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, cilt.1, sa.2, ss.49-66, 2012 (Diğer Kurumların Hakemli Dergileri)

III. **The Final Exponentiation in Pairing Based Cryptography**
KIRLAR B. B.
International Journal of Information Security Science, cilt.1, sa.1, ss.1-12, 2012 (Diğer Kurumların Hakemli Dergileri)

IV. **A New Short Signature Scheme with Random Oracle from Bilinear Pairings**
AKLEYLEK S., KIRLAR B. B. , SEVER Ö., YÜCE Z.
JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY, cilt.1, sa.0, ss.5-10, 2011 (Diğer Kurumların Hakemli Dergileri)

Kitap & Kitap Bölümleri

I. **Konik Kesitler**
DAĞHAN H. A. , AYTAR S., ARUĞASLAN ÇİNÇİN D., YAKIT ONGUN M., YÜCESAN A., GÜRDAL M., KIRLAR B. B. , ÖZKAN TÜKEL G., TURHAN T., ŞAHİNER A.
Kalkülüse Giriş, Yusuf Civan, Editör, Nobel, Ankara, ss.219-306, 2017

II. **3. Bölüm İkinci Dereceden Denklemler ve Fonksiyonlar Eşitsizlikler**
ŞAHİNER A., ARUĞASLAN ÇİNÇİN D., KIRLAR B. B. , YÜCESAN A., GÜRDAL M., AYTAR S., TURHAN T., YAKIT ONGUN M., DAĞHAN H. A. , ÖZKAN TÜKEL G.
KALKÜLÜSE GİRİŞ: Grafikler ve Modeller - COLLEGE ALGEBRA Graphs and Models, Yusuf Civan, Editör, Nobel, ss.393-474, 2017

III. **Bölüm 2 Fonksiyonlar Hakkında Daha Fazlası**

ŞAHİNER A., YÜCESAN A., ARUĞASLAN ÇİNÇİN D., KIRLAR B. B. , ÖZKAN TÜKEL G., DAĞHAN H. A. , GÜRDAL M., YAKIT ONGUN M., AYTAR S., TURHAN T.
Kalkülüse Giriş: Grafikler ve ModellerCollege Algebra: Graphs and Models, Yusuf Civan, Editör, Nobel Akademik Yayıncılık, ss.93-162, 2017

IV. **5. Bölüm Üstel ve Logaritmik Fonksiyonlar**
DAĞHAN H. A. , AYTAR S., ARUĞASLAN ÇİNÇİN D., YAKIT ONGUN M., YÜCESAN A., GÜRDAL M., KIRLAR B. B. , ÖZKAN TÜKEL G., TURHAN T., ŞAHİNER A.
Kalkülüse Giriş: Grafikler ve Modeller, Yusuf Civan, Editör, Nobel, ss.391-482, 2017

V. **Polinom Fonksiyonlar ve Rasyonel Fonksiyonlar**
DAĞHAN H. A. , AYTAR S., ARUĞASLAN ÇİNÇİN D., YAKIT ONGUN M., YÜCESAN A., GÜRDAL M., KIRLAR B. B. , ÖZKAN TÜKEL G., TURHAN T., ŞAHİNER A.
Kalkülüse Giriş, Yusuf Civan, Editör, Nobel, ss.219-306, 2017

VI. **Grafikler, Fonksiyonlar ve Modeller**
DAĞHAN H. A. , AYTAR S., ARUĞASLAN ÇİNÇİN D., YAKIT ONGUN M., YÜCESAN A., GÜRDAL M., KIRLAR B. B. , ÖZKAN TÜKEL G., TURHAN T., ŞAHİNER A.
Kalkülüse Giriş: Grafikler ve Modeller, Yusuf Civan, Editör, Nobel, Isparta, ss.1-92, 2017

VII. **Bölüm 3, İkinci Dereceden (Kuadratik) Fonksiyonlar ve Denklemler Eşitsizlikler**
YAKIT ONGUN M., ŞAHİNER A., YÜCESAN A., ARUĞASLAN ÇİNÇİN D., KIRLAR B. B. , ÖZKAN TÜKEL G., DAĞHAN H. A. , GÜRDAL M., AYTAR S., TURHAN T.
KALKÜLÜSE GİRİŞ: Grafikler ve Modeller - COLLEGE ALGEBRA Graphs and Models, Civan Yusuf, Editör, Nobel Akademik Yayıncılık Eğitim Danışmanlık Tic. Ltd. Şti., Ankara, ss.163-218, 2017

VIII. **Diziler, Seriler ve Kombinatorikler**
ŞAHİNER A., YÜCESAN A., ARUĞASLAN ÇİNÇİN D., KIRLAR B. B. , ÖZKAN TÜKEL G., DAĞHAN H. A. , YAKIT ONGUN M., AYTAR S., TURHAN T.
KALKÜLÜSE GİRİŞ: Grafikler ve Modeller, Yusuf Civan, Editör, Nobel Yayıncılık, 2017

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

I. **Computing Square Roots in Prime Fields via Singular Elliptic Curves**
AKLEYLEK S., KIRLAR B. B.
The Third International Conference on Applications of Mathematics and Informatics in Natural Sciences and Engineering (AMINSE 2017), Tiflis, Gürcistan, 6 - 09 Aralık 2017, ss.1

II. **Some Correspondence of Certain Type of Irreducible Polynomials over Finite Fields**
ÇİL M., KIRLAR B. B.
9th International Information Security and Cryptology Conference (ISCTURKEY 2016), Ankara, Türkiye, 25 - 26 Ekim 2016

III. **A Game Theoretical Approach to Crypto Cloud Computing and ItsEconomical and Financial Aspects**
ERGÜN S., ALPARSLAN GÖK S. Z. , KIRLAR B. B.
55th meeting of the EWGCFM, 14 - 16 Mayıs 2015

IV. **On the fifth order LFSR sequence over GF p 2**
MUHAMMAD A., KIRLAR B. B.
International Conference on Computational and Experimental Science and Engineering (ICCESEN 2014), Antalya, Türkiye, 25 - 29 Ekim 2014, ss.190

V. **On the generalized k th order Lucas numbers by matrix representation**
KIRLAR B. B. , MELEK Y.
4th International Conference of Matrix Anaylsis and Applications, Konya, Türkiye, 2 - 05 Haziran 2013, ss.12-13

VI. **Speeding Up GH-Public Key Cryptosystem Through Novel Encryption Scheme**
ASHRAF M., KIRLAR B. B.
International Conference on Applied and Computational Mathematics (ICACM), Ankara, Türkiye, 3 - 06 Ekim 2012, ss.28-29

VII. **Alternate Models of Elliptic Curves: A Survey**
ASHRAF M., KIRLAR B. B.
5th International Information Security and Cryptology Conference (ISCTURKEY 2012), Ankara, Türkiye, 17 - 18 Mayıs 2012, ss.160-168

VIII. **Compressed Data Public Key Cryptosystems with DLP Over Extension Field**
ASHRAF M., KIRLAR B. B.
5th International Information Security and Cryptology Conference (ISCTURKEY 2012), Ankara, Türkiye, 17 - 18 Mayıs 2012, ss.132-137

IX. **Compressed Data Public Key Cryptosystems with DLP Over Extension Fields**
ASHRAF M., KIRLAR B. B.
5th International Information Security and Cryptology Conference (ISCTURKEY 2012), Ankara, Türkiye, 17 - 18 Mayıs 2012, ss.132-137

X. **Short Signature Scheme from Bilinear Pairings**
AKLEYLEK S., KIRLAR B. B. , SEVER Ö., YÜCE Z.
Information Assurance and Cyber Defense (IST-091), Tallinn, Estonya, 22 - 23 Kasım 2010, ss.1-5

XI. **Efficient Exponentiation in Pairing-Based Cryptography**
KIRLAR B. B.
4th International Information Security and Cryptology Conference (ISCTURKEY 2010), Ankara, Türkiye, 6 - 08 Mayıs 2010, ss.145-149

XII. **On the elliptic curves y 2 x 3 c with embedding degree one**
KIRLAR B. B.
4th International Congress on Computational and Applied Mathematics (ICCAM 2009), Antalya, Türkiye, 29 Eylül - 02 Ekim 2009, ss.161

XIII. **Short Signature Scheme from Bilinear Pairings**
AKLEYLEK S., KIRLAR B. B. , SEVER Ö., YÜCE Z.
Western European Workshop on Research in Cryptology (WEWoRC 2009), Graz, Avusturya, 7 - 09 Temmuz 2009, ss.1

XIV. **Pairing-Based Cryptography: A Survey**
AKLEYLEK S., KIRLAR B. B. , SEVER Ö., YÜCE Z.
Information Security and Cryptography Conference (ISCTURKEY 2008), Ankara, Türkiye, 25 - 27 Aralık 2008, ss.121-125

XV. **Arithmetic on Pairing-Friendly Fields**
AKLEYLEK S., KIRLAR B. B. , SEVER Ö., YÜCE Z.
Information Security and Cryptography Conference (ISCTURKEY 2008), Ankara, Türkiye, 25 - 27 Aralık 2008, ss.115-120

Desteklenen Projeler

KIRLAR B. B. , TÜBİTAK Projesi, Design and Analysis of NTRU-based Cryptosystems Using Formal Methods - Ntru Tabanlı Kriptosistemlerin Tasarımı Ve Biçimsel Yöntemler İle Analizi, 2019 - Devam Ediyor
KIRLAR B. B. , TÜBİTAK Projesi, Lattice-Based Cryptographic Protocol Design and Efficient Implementations - Kafes Tabanlı Güvenilir Kriptografik Protokol Tasarımı ve Verimli Uygulamaları, 2018 - Devam Ediyor
KIRLAR B. B. , TÜBİTAK Projesi, Efficiency Analysis and Implementation of Post-Quantum Cryptographic Schemes in Software/Hardware - Kuantum Sonrası Kriptografik Protokol Bileşenlerinin Verimlilik Analizi Ve Yazılım/Donanım Uygulamaları, 2017 - 2019
KIRLAR B. B. , Diğer Resmi Kurumlarca Desteklenen Proje, Pairing-Based Cryptosystems Research and Development, 2008 - 2009

Bilimsel Dergilerdeki Faaliyetler

Süleyman Demirel Universitesi Fen Bilimleri Enstitüsü Dergisi, Editör, 2017 - 2018
Süleyman Demirel Universitesi Fen Bilimleri Enstitüsü Dergisi, Yardımcı Editör, 2015 - 2016

Atıflar

Toplam Atıf Sayısı (WOS):6
h-indeksi (WOS):1