Assoc. Prof. Barış Bülent KIRLAR

Personal Information

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

Education Information

Doctorate, Middle East Technical University, Uygulamalı Matematik Enstitüsü, Kriptografi, Turkey 2005 - 2010
Post Graduate, Middle East Technical University, Fen Bilimleri Enstitüsü, Matematik, Turkey 2002 - 2005
Under Graduate, Ankara University, Fen Fakültesi, Matematik, Turkey 1997 - 2001

Research Areas

Computer Sciences, Information Security and Reliability, Cryptography, Engineering and Technology

Professional Experience

Assistant Director of the Institute, Suleyman Demirel University, Fen Bilimleri Enstitüsü, 2015 - 2018

Courses

Matematik I (İngilizce), Under Graduate, 2016 - 2017
Matematik II (İngilizce), Under Graduate, 2016 - 2017

Advising Theses

KIRLAR B. B. , Sonlu Cisimler Üzerinde Tanımlı Polinomların Kökleri Üzerine Bir Çalışma, Post Graduate, B.YAYLALI(Student), 2019
KIRLAR B. B. , On the Trace Based Public Key Cryptosystems over Finite Fields, Doctorate, M.ASHRAF(Student), 2013

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

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, vol.16, no.4, pp.1927-1941, 2020 (Journal Indexed in SCI)

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, vol.260, pp.217-231, 2018 (Journal Indexed in SCI)

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, vol.260, pp.217-231, 2018 (Journal Indexed in SCI Expanded)

IV. **ON THE k-TH ORDER LFSR SEQUENCE WITH PUBLIC KEY CRYPTOSYSTEMS**
Kirlar B. B. , Cil M.
MATHEMATICA SLOVACA, vol.67, no.3, pp.601-610, 2017 (Journal Indexed in SCI)

V. **New methods for public key cryptosystems based on XTR**
Akleylek S., KIRLAR B. B.
SECURITY AND COMMUNICATION NETWORKS, vol.8, no.18, pp.3682-3689, 2015 (Journal Indexed in SCI)

VI. **Message transmission for GH-public key cryptosystem**
Ashraf M., Kirlar B. B.
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, vol.259, pp.578-585, 2014 (Journal Indexed in SCI)

VII. **On the elliptic curves y(2)=x(3)-c with embedding degree one**
Kirlar B. B.
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, vol.235, no.16, pp.4724-4728, 2011 (Journal Indexed in SCI)

Articles Published in Other Journals

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, vol.9, no.4, pp.19-21, 2015 (Non-Refreed Journal)

II. **On the Alternate Models of Elliptic Curves**
ASHRAF M., KIRLAR B. B.
INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, vol.1, no.2, pp.49-66, 2012 (Refereed Journals of Other Institutions)

III. **The Final Exponentiation in Pairing Based Cryptography**
KIRLAR B. B.
International Journal of Information Security Science, vol.1, no.1, pp.1-12, 2012 (Refereed Journals of Other Institutions)

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, vol.1, no.0, pp.5-10, 2011 (Refereed Journals of Other Institutions)

Books & Book Chapters

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.
in: Kalkülüse Giriş, Yusuf Civan, Editor, Nobel, Ankara, pp.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.
in: KALKÜLÜSE GİRİŞ: Grafikler ve Modeller - COLLEGE ALGEBRA Graphs and Models, Yusuf Civan, Editor, Nobel, pp.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.
in: Kalkülüse Giriş: Grafikler ve ModellerCollege Algebra: Graphs and Models, Yusuf Civan, Editor, Nobel Akademik Yayıncılık, pp.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.
in: Kalkülüse Giriş: Grafikler ve Modeller, Yusuf Civan, Editor, Nobel, pp.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.
in: Kalkülüse Giriş, Yusuf Civan, Editor, Nobel, pp.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.
in: Kalkülüse Giriş: Grafikler ve Modeller, Yusuf Civan, Editor, Nobel, Isparta, pp.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.
in: KALKÜLÜSE GİRİŞ: Grafikler ve Modeller - COLLEGE ALGEBRA Graphs and Models, Civan Yusuf, Editor, Nobel Akademik Yayıncılık Eğitim Danışmanlık Tic. Ltd. Şti., Ankara, pp.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.
in: KALKÜLÜSE GİRİŞ: Grafikler ve Modeller, Yusuf Civan, Editor, Nobel Yayıncılık, 2017

Refereed Congress / Symposium Publications in Proceedings

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, Georgia, 6 - 09 December 2017, pp.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, Turkey, 25 - 26 October 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 May 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, Turkey, 25 - 29 October 2014, pp.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, Turkey, 2 - 05 June 2013, pp.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, Turkey, 3 - 06 October 2012, pp.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, Turkey, 17 - 18 May 2012, pp.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, Turkey, 17 - 18 May 2012, pp.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, Turkey, 17 - 18 May 2012, pp.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, Estonia, 22 - 23 November 2010, pp.1-5

XI. **Efficient Exponentiation in Pairing-Based Cryptography**
KIRLAR B. B.
4th International Information Security and Cryptology Conference (ISCTURKEY 2010), Ankara, Turkey, 6 - 08 May 2010, pp.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, Turkey, 29 September - 02 October 2009, pp.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, Austria, 7 - 09 July 2009, pp.1

XIV. **Pairing-Based Cryptography: A Survey**
AKLEYLEK S., KIRLAR B. B. , SEVER Ö., YÜCE Z.
Information Security and Cryptography Conference (ISCTURKEY 2008), Ankara, Turkey, 25 - 27 December 2008, pp.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, Turkey, 25 - 27 December 2008, pp.115-120

Supported Projects

KIRLAR B. B. , TUBITAK Project, Design and Analysis of NTRU-based Cryptosystems Using Formal Methods - Ntru Tabanlı Kriptosistemlerin Tasarımı Ve Biçimsel Yöntemler İle Analizi, 2019 - Continues
KIRLAR B. B. , TUBITAK Project, Lattice-Based Cryptographic Protocol Design and Efficient Implementations - Kafes Tabanlı Güvenilir Kriptografik Protokol Tasarımı ve Verimli Uygulamaları, 2018 - Continues
KIRLAR B. B. , TUBITAK Project, 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. , Project Supported by Other Official Institutions, Pairing-Based Cryptosystems Research and Development, 2008 - 2009

Activities in Scientific Journals

Süleyman Demirel Universitesi Fen Bilimleri Enstitüsü Dergisi, Editor, 2017 - 2018

Süleyman Demirel Universitesi Fen Bilimleri Enstitüsü Dergisi, Assistant Editor, 2015 - 2016

Citations

Total Citations (WOS):6
h-index (WOS):1