Dr. Öğr. Üyesi ERDEM ALKIM

Kişisel Bilgiler

E-posta: erdem.alkim@deu.edu.tr
Diğer E-posta: erdemalkim@gmail.com
Web: https://avesis.deu.edu.tr/erdem.alkim

Uluslararası Araştırmacı ID'leri
ScholarID: 3CtAD74AAAAJ
ORCID: 0000-0003-4638-2422
Publons / Web Of Science ResearcherID: JZU-0054-2024
ScopusID: 43261000900
Yoksis Araştırmacı ID: 160467

Eğitim Bilgileri

Doktora, Ege Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Bilimleri (Dr), Türkiye 2013 - 2017
Yüksek Lisans, Ondokuz Mayıs Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği (Yl) (Tezli), Türkiye 2009 - 2013
Lisans, Ondokuz Mayıs Üniversitesi, Fen-Edebiyat Fakültesi, İstatistik Bölümü, Türkiye 2000 - 2007

Yaptığı Tezler

Doktora, Yeni nesil kriptosistemlerin analizi, tasarımı ve verimli uygulamaları, Ege Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Bilimleri (Dr), 2017
Yüksek Lisans, Karmaşık algoritmaların FPGA üzerinde gerçeklenmesi, Ondokuz Mayıs Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği (Yl) (Tezli), 2012

Araştırma Alanları

Başarım Modellemesi ve Değerlendirmesi, Bilgi Sistemi Güvenilirliği, Kriptoloji, Yazılım Güvenliği

Akademik Unvanlar / Görevler

Dr. Öğr. Üyesi, Dokuz Eylül Üniversitesi, Fen Fakültesi, Bilgisayar Bilimleri Bölümü, 2021 - Devam Ediyor
Dr. Öğr. Üyesi, Ondokuz Mayıs Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 2018 - 2021
Öğretim Görevlisi, Kastamonu Üniversitesi, Araç Rafet Vergili Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, 2013 - 2013
Araştırma Görevlisi, Ondokuz Mayıs Üniversitesi, Fen Bilimleri Enstitüsü, 2010 - 2013

Verdiği Dersler

Bilgisayar Bilimlerine Giriş II, Lisans, 2023 - 2024, 2022 - 2023, 2021 - 2022
Veri Güvenliği, Lisans, 2023 - 2024, 2022 - 2023

Gömülü Sistem Programlama, Lisans, 2023 - 2024, 2022 - 2023
Sayısal Sinyal işleme, Lisans, 2023 - 2024, 2022 - 2023
Algoritmaların Tasarımı ve Analizi, Lisans, 2023 - 2024
Sayısal Tasarım, Lisans, 2023 - 2024
Bilgisayar Bilimlerine Giriş I, Lisans, 2023 - 2024, 2022 - 2023, 2021 - 2022
Dağıtık Algoritmalar, Lisans, 2021 - 2022
Information Technologies, Lisans, 2022 - 2023, 2021 - 2022
Sayısal Görüntü İşleme, Lisans, 2021 - 2022

Yönetilen Tezler

ALKIM E., Kafes tabanlı kriptografik protokollerin verimli uygulamaları, Yüksek Lisans, B.KAĞAN(Öğrenci), 2020
ALKIM E., Simetrik kripto-sistemlerin güvenlik analizi, Yüksek Lisans, M.KARATAY(Öğrenci), 2019

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

I. **Efficient, Flexible, and Constant-Time Gaussian Sampling Hardware for Lattice Cryptography**
Karabulut E., Alkim E., Aysu A.
IEEE TRANSACTIONS ON COMPUTERS, cilt.71, sa.8, ss.1810-1823, 2021 (SCI-Expanded)
II. **A Modified Parallel Learning Vector Quantization Algorithm for Real-Time Hardware Applications**
ALKIM E., AKLEYLEK S., KILIÇ E.
JOURNAL OF CIRCUITS SYSTEMS AND COMPUTERS, cilt.26, sa.10, 2017 (SCI-Expanded)
III. **Sparse polynomial multiplication for lattice-based cryptography with small complexity**
Akleylek S., ALKIM E., Tok Z. Y.
JOURNAL OF SUPERCOMPUTING, cilt.72, sa.2, ss.438-450, 2016 (SCI-Expanded)
IV. **A fast and adaptive automated disease diagnosis method with an innovative neural network model**
ALKIM E., Gurbuz E., KILIÇ E.
NEURAL NETWORKS, cilt.33, ss.88-96, 2012 (SCI-Expanded)

Diğer Dergilerde Yayınlanan Makaleler

I. **Multi-Parameter Support with NTTs for NTRU and NTRU Prime on Cortex-M4**
Alkım E., Hwang V., Yang B.
IACR TRANSACTIONS ON CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS, cilt.2022, sa.4, ss.349-371, 2022 (Scopus)
II. **Polynomial Multiplication in NTRU Prime: Comparison of Optimization Strategies on Cortex-M4.**
Alkım E., Cheng D. Y., Chung C. M., Evkan H., Huang L. W., Hwang V., Li C. T., Niederhagen R., Shih C., Wälde J., et al.
IACR TRANSACTIONS ON CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS, cilt.2021, sa.1, ss.217-238, 2020 (Scopus)
III. **A PERFORMANCE COMPARISON OF SOME HASH FUNCTIONS IN HASH-BASED SIGNATURE.**
Karatay M., Alkım E., Kırcalı Gürsoy N., Kurt M.
Journal of Modern Technology and Engineering, cilt.5, sa.3, ss.234-241, 2020 (Hakemli Dergi)
IV. **Cortex-M4 Optimizations for {R,M} LWE Schemes**
Alkım E., Bilgin Y. A., Cenk M., François G.
IACR TRANSACTIONS ON CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS, cilt.2020, sa.3, ss.336-357, 2020 (Scopus)
V. **ISA Extensions for Finite Field Arithmetic Accelerating Kyber and NewHope on RISC-V**
Alkim E., Evkan H., Lahr N., Niederhagen R., Petri R.

IACR TRANSACTIONS ON CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS, cilt.2020, sa.3, ss.219-242, 2020 (Scopus)

VI. **Hatalar ile Öğrenme Tabanlı Anahtar Kapsülleme Protokolleri İçin Uygulama Atakları ve Savunma Yöntemleri**
YAZAR B. K., ALKIM E.
Avrupa Bilim ve Teknoloji Dergisi, ss.251-259, 2020 (Hakemli Dergi)

VII. **qTESLA: Efficient and Post-Quantum Secure Lattice-Based Signature Scheme**
Bindel N., AKLEYLEK S., ALKIM E., Barreto P., Buchmann J., Eaton E., Gutoski G., Juliane K., Longa P., Polat H., et al.
NIST Post-Quantum Standardization Project, 2017 (Hakemsiz Dergi)

VIII. **NewHope without reconciliation**
ALKIM E., Ducas L., Pöppelmann T., Schwabe P.
Cryptology ePrint Archive, 2016 (Hakemsiz Dergi)

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

I. **RevEAL: Single-Trace Side-Channel Leakage of the SEAL Homomorphic Encryption Library**
Aydin F., Karabulut E., Potluri S., ALKIM E., Aysu A.
25th Design, Automation and Test in Europe Conference and Exhibition (DATE), ELECTR NETWORK, 14 - 23 Mart 2022, ss.1527-1532

II. **Effect of DoS Attacks on MTE/LEACH Routing Protocol-Based Wireless Sensor Networks**
Alaadin A., ALKIM E., DEMİRCİ S.
The International Conference on Artificial Intelligence and Applied Mathematics in Engineering., Antalya, Türkiye, 09 Ekim 2020, cilt.76, ss.360-368

III. **Consensus Approaches of High-Value Crypto Currencies and Application in SHA-3**
Emeç M., Karatay M., Dalkılıç G., Alkım E.
International Conference on Artificial Intelligence and Applied Mathematics in Engineering (ICAIAME), Antalya, Türkiye, 20 - 22 Nisan 2019, cilt.43, ss.572-583

IV. **Post Quantum Learning With Errors Problem Based Key Encapsulation Protocols and Matrix Vector Product**
ALKIM E., YAZAR B. K.
2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, Türkiye, 11 - 15 Eylül 2019, ss.301-306

V. **Kriptografik İmzalamada Bazı Özet Fonksiyonların Karşılaştırılması**
Karatay M., Demiroz D., ALKIM E., GÜRSOY A.
International Marmara Science And Social Sciences Congress (IMASCON), Kocaeli, Türkiye, 26 - 28 Nisan 2019

VI. **Compact and Simple RLWE Based Key Encapsulation Mechanism**
ALKIM E., Bilgin Y. A., CENK M.
6th International Conference on Cryptology and Information Security in Latin America (LATINCRYPT), Santiago de Cuba, Küba, 2 - 04 Ekim 2019, cilt.11774, ss.237-256

VII. **Revisiting TESLA in the Quantum Random Oracle Model**
ALKIM E., Bindel N., Buchmann J., Dagdelen Ö., Eaton E., Gutoski G., Kramer J., Pawlega F.
PQCrypto 2017: Post-Quantum Cryptography, Utrecht, Hollanda, 26 - 28 Haziran 2017, ss.143-162

VIII. **Modified Arithmetic Circuits for Galois Rings**
KURAL O. E., ŞAHİN D. Ö., AKLEYLEK S., ALKIM E.
3rd International Conference on Engineering and Natural Sciences (ICENS 2017), Budapest, Macaristan, 3 - 07 Mayıs 2017, ss.327

IX. **NewHope on ARM Cortex-M**
ALKIM E., Jakubeit P., Schwabe P.
Security, Privacy, and Applied Cryptography Engineering, SPACE 2016, 14 - 18 Aralık 2016, cilt.10076, ss.332-349

X. **Post-quantum key exchange - a new hope**

ALKIM E., Ducas L., Pöppelmann T., Schwabe P.
PROCEEDINGS OF THE 25TH USENIX SECURITY SYMPOSIUM, Austin, Amerika Birleşik Devletleri, 10 - 12 Ağustos 2016, ss.327-343

XI. **Chip design for intelligent data classification algorithms and implementation on an FPGA: A case study to classify EMG signals**
Alkim E., Kilic E.
2011 IEEE 19th Signal Processing and Communications Applications Conference (SIU), 20 - 22 Nisan 2011

XII. **New intelligent diagnosis method to determine thyroid disorders**
Alkim E., Gurbuz E., Kilic E.
2011 IEEE 19th Signal Processing and Communications Applications Conference (SIU), 20 - 22 Nisan 2011

Metrikler

Yayın: 26
Atıf (WoS): 345
Atıf (Scopus): 622
H-İndeks (WoS): 5
H-İndeks (Scopus): 8