Asst. Prof. ERDEM ALKIM

Personal Information

Email: erdem.alkim@deu.edu.tr
Other Email: erdemalkim@gmail.com
Web: https://avesis.deu.edu.tr/erdem.alkim

International Researcher IDs
ScholarID: 3CtAD74AAAAJ
ORCID: 0000-0003-4638-2422
Publons / Web Of Science ResearcherID: JZU-0054-2024
ScopusID: 43261000900
Yoksis Researcher ID: 160467

Education Information

Doctorate, Ege University, Fen Bilimleri Enstitüsü, Bilgisayar Bilimleri (Dr), Turkey 2013 - 2017
Postgraduate, Ondokuz Mayis University, Institute Of Science, Bilgisayar Mühendisliği (Yl) (Tezli), Turkey 2009 - 2013
Undergraduate, Ondokuz Mayis University, Faculty Of Arts And Sciences, Department Of Statistics, Turkey 2000 - 2007

Dissertations

Doctorate, Yeni nesil kriptosistemlerin analizi, tasarımı ve verimli uygulamaları, Ege University, Fen Bilimleri Enstitüsü, Bilgisayar Bilimleri (Dr), 2017
Postgraduate, Karmaşık algoritmaların FPGA üzerinde gerçeklenmesi, Ondokuz Mayis University, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği (Yl) (Tezli), 2012

Research Areas

Performance Modelling and Evaluation, Information System Reliability, Cryptography, Software Security

Academic Titles / Tasks

Assistant Professor, Dokuz Eylul University, Fen Fakültesi, Bilgisayar Bilimleri Bölümü, 2021 - Continues
Assistant Professor, Ondokuz Mayis University, Faculty Of Engineering, Department Of Computer Engineering, 2018 - 2021
Lecturer, Kastamonu University, Araç Rafet Vergili Vocational School, Department Of Computer Technologies, 2013 - 2013
Research Assistant, Ondokuz Mayis University, Institute Of Science, 2010 - 2013

Courses

Introduction to Computer Science, Undergraduate, 2023 - 2024, 2022 - 2023, 2021 - 2022
Data Security, Undergraduate, 2023 - 2024, 2022 - 2023

Embedded System Programming, Undergraduate, 2023 - 2024, 2022 - 2023
Digital Signal Processing, Undergraduate, 2023 - 2024, 2022 - 2023
The Design and Analysis of Algorithms, Undergraduate, 2023 - 2024
Digital Design, Undergraduate, 2023 - 2024
Bilgisayar Bilimlerine Giriş I, Undergraduate, 2023 - 2024, 2022 - 2023, 2021 - 2022
Distributed Algorithms, Undergraduate, 2021 - 2022
Information Technologies, Undergraduate, 2022 - 2023, 2021 - 2022
Digital image processing, Undergraduate, 2021 - 2022

Supervised Theses

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

Published journal articles indexed by SCI, SSCI, and AHCI

I. **Efficient, Flexible, and Constant-Time Gaussian Sampling Hardware for Lattice Cryptography**
Karabulut E., Alkim E., Aysu A.
IEEE TRANSACTIONS ON COMPUTERS, vol.71, no.8, pp.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, vol.26, no.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, vol.72, no.2, pp.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, vol.33, pp.88-96, 2012 (SCI-Expanded)

Articles Published in Other Journals

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, vol.2022, no.4, pp.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, vol.2021, no.1, pp.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, vol.5, no.3, pp.234-241, 2020 (Peer-Reviewed Journal)
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, vol.2020, no.3, pp.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, vol.2020, no.3, pp.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, pp.251-259, 2020 (Peer-Reviewed Journal)

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 (Non Peer-Reviewed Journal)

VIII. **NewHope without reconciliation**
ALKIM E., Ducas L., Pöppelmann T., Schwabe P.
Cryptology ePrint Archive, 2016 (Non Peer-Reviewed Journal)

Refereed Congress / Symposium Publications in Proceedings

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 March 2022, pp.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, Turkey, 09 October 2020, vol.76, pp.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, Turkey, 20 - 22 April 2019, vol.43, pp.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, Turkey, 11 - 15 September 2019, pp.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, Turkey, 26 - 28 April 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, Cuba, 2 - 04 October 2019, vol.11774, pp.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, Netherlands, 26 - 28 June 2017, pp.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, Hungary, 3 - 07 May 2017, pp.327

IX. **NewHope on ARM Cortex-M**
ALKIM E., Jakubeit P., Schwabe P.
Security, Privacy, and Applied Cryptography Engineering, SPACE 2016, 14 - 18 December 2016, vol.10076, pp.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, United States Of America, 10 - 12 August 2016, pp.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 April 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 April 2011

Metrics

Publication: 28
Citation (WoS): 523
Citation (Scopus): 626
H-Index (WoS): 6
H-Index (Scopus): 9