

Asst. Prof. Meryem Soysaldı Şahin

Personal Information

Email: meryem.soysaldi@omu.edu.tr

Web: <https://avesis.omu.edu.tr/meryem.soysaldi>

International Researcher IDs

ScholarID: T6e57RUAAAAJ

ORCID: 0000-0002-1674-2768

Yoksis Researcher ID: 248797

Education Information

Doctorate, Ondokuz Mayıs University, Lisansüstü Eğitim Enstitüsü, Hesaplamalı Bilimler Anabilim Dalı, Turkey 2018 - 2022

Postgraduate, Ondokuz Mayıs University, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği (YI) (Tezli), Turkey 2016 - 2018

Undergraduate, Firat University, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Turkey 2010 - 2013

Dissertations

Postgraduate, ÇOK DEĞİŞKENLİ POLİNOM SİSTEMLERİNE DAYALI KUANTUM BİLGİSAYARLAR SONRASI GÜVENİLİR YENİ KİMLİK DOĞRULAMA VE İMZALAMA ŞEMALARI, Ondokuz Mayıs University, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği (YI) (Tezli), 2018

Academic Titles / Tasks

Research Assistant, Ondokuz Mayıs University, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 2016 - Continues

Published journal articles indexed by SCI, SSCI, and AHCI

- I. **A survey of quantum secure group signature schemes: Lattice-based approach**
Şahin M., Akleylek S.
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, vol.73, 2023 (SCI-Expanded)
- II. **A constant-size lattice-based partially-dynamic group signature scheme in quantum random oracle model**
Şahin M., Akleylek S.
Journal of King Saud University - Computer and Information Sciences, vol.34, no.10, pp.9852-9866, 2022 (SCI-Expanded)
- III. **A new lattice-based authentication scheme for IoT**
Akleylek S., Soysaldı M.
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, vol.64, 2022 (SCI-Expanded)
- IV. **Novel Postquantum MQ-Based Signature Scheme for Internet of Things With Parallel Implementation**
Akleylek S., Soysaldı Şahin M., Lee W., Hwang S. O., Wong D. C.
IEEE INTERNET OF THINGS JOURNAL, vol.8, no.8, pp.6983-6994, 2021 (SCI-Expanded)
- V. **A Novel Method for Polar Form of Any Degree of Multivariate Polynomials with Applications in IoT**

Akleylek S., Soysaldı Şahin M., Boubiche D. E., Toral-Cruz H.

SENSORS, vol.19, no.4, 2019 (SCI-Expanded)

VI. A novel 3-pass identification scheme and signature scheme based on multivariate quadratic polynomials

Akleylek S., Soysaldı Şahin M.

TURKISH JOURNAL OF MATHEMATICS, vol.43, no.1, pp.241-257, 2019 (SCI-Expanded)

Articles Published in Other Journals

I. JAVA LIBRARY FOR LATTICE-BASED IDENTIFICATION SCHEMES

MURZAEVA A., SOYSALDI M., AKLEYLEK S.

Journal of Modern Technology and Engineering, vol.5, no.1, pp.5-17, 2020 (Peer-Reviewed Journal)

Books & Book Chapters

I. Kafes Tabanlı Grup İmzalama Şemalarının Özellikleri Ve Değerlendirilmesi

SOYSALDI ŞAHİN M., AKLEYLEK S.

in: Siber Güvenlik ve Savunma: BlokZincir ve Kriptoloji, Sağiroğlu Şeref, Akleylek Sedat, Editor, Nobel Akademik Yayıncılık Eğitim Danışmanlık Ltdi. Şti., Ankara, pp.491-541, 2021

II. Identification schemes in the post-quantum area based on multivariate polynomials with applications in cloud and IoT

AKLEYLEK S., SOYSALDI M.

in: Authentication Technologies for Cloud Technology, IoT, and Big Data, Dr. Yasser M. Alginahi Dr. Muhammad N. Kabir, Editor, The Institution of Engineering and Technology (The IET), pp.181-207, 2019

III. Kuantum Bilgisayarlar ile Kriptoanaliz ve Kuantum Sonrası Güvenilir Kripto Sistemleri

AKLEYLEK S., SOYSALDI M.

in: Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık Cilt II, Prof. Dr. Şeref Sağiroğlu, Mustafa Şenol, Editor, Grafiker Yayınları, Ankara, pp.137-168, 2019

Refereed Congress / Symposium Publications in Proceedings

I. A Lattice-based Group Signature Scheme with Applications in Blockchain

SOYSALDI ŞAHİN M., AKLEYLEK S.

Applications of Computer Algebra - ACA 2022, Turkey, 15 - 19 August 2022

II. Survey on Implementation of Lattice-based Identification Schemes

Murzaeva A., SOYSALDI ŞAHİN M., AKLEYLEK S.

4th International Students Science Congress, İzmir, Turkey, 15 January 2021, pp.194-206

III. A Novel Lattice-Based Threshold Ring Signature Scheme

Akleylek S., Soysaldı Şahin M.

5th International Conference on Computer Science and Engineering (UBMK), Diyarbakır, Turkey, 9 - 11 September 2020, pp.219-223

IV. Migration Pool Technique for Parallel Particle Swarm Optimization Algorithm

Aslan S., Soysaldı Şahin M.

4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11 - 15 September 2019, pp.414-417

V. A New 3-pass Zero-knowledge Lattice-based Identification Scheme

Akleylek S., Soysaldı Şahin M.

4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11 - 15 September

2019, pp.409-413

- VI. **Kuantum Sonrası Güvenilir Yeni Kimlik Doğrulama Şeması**
AKLEYLEK S., SOYSALDI ŞAHİN M.
SAVTEK 2018, 9. SAVUNMA TEKNOLOJİLERİ KONGRESİ, 27 June 2018
- VII. **MOVIE RECOMMENDATION SYSTEM USING DISTRIBUTED MACHINE LEARNING**
KARHAN Z., SOYSALDI M., ŞAHİN D. Ö., KILIÇ E.
4th International Conference on Engineering and Natural Sciences (ICENS 2018), Kiev, Ukraine, 2 - 06 May 2018, pp.261
- VIII. **A SURVEY ON DIGITAL RIGHTS MANAGEMENT**
AKLEYLEK S., SOYSALDI M., KARHAN Z., ŞAHİN D. Ö.
4th International Conference on Engineering and Natural Sciences (ICENS 2018), Kiev, Ukraine, 2 - 06 May 2018, pp.260
- IX. **Dağıtık Makine Öğrenmesi Kullanarak Film Öneri Sistemi**
KARHAN Z., SOYSALDI M., ŞAHİN D. Ö., KILIÇ E.
International Conference On Engineering And Natural Sciences (ICENS), Kİev, Ukraine, 2 - 06 May 2018
- X. **Sentiment Analysis On Twitter Data Using Distributed Architecture**
Karhan Z., Soysaldı Şahin M., Ozben Y. O., Kılıç E.
3rd International Conference on Computer Science and Engineering (UBMK), Sarajevo, Bosnia And Herzegovina, 20 - 23 September 2018, pp.357-360
- XI. **On the Generalization of Linear-In-One-Argument Form of Multivariate Polynomials for Post-Quantum Cryptography**
AKLEYLEK S., SOYSALDI M.
3rd International Conference on Applications of Mathematics and Informatics in Natural Sciences and Engineering, 6 - 09 December 2017, vol.3, pp.70-73
- XII. **Kuantum Sonrası Güvenilir Dijital Hak Yönetimi İçin Yeni Kimlik Doğrulama Protokolü**
AKLEYLEK S., SOYSALDI M.
2nd International Conference on Computer Science and Engineering (UBMK'17), 5 - 08 October 2017, pp.322-327
- XIII. **A Novel Identification Scheme for Post-Quantum Secure Digital Right Management**
Akleylek S., Soysaldı Şahin M.
2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 5 - 08 October 2017, pp.322-327