

Dr. Öğr. Üyesi Meryem Soysaldı Şahin

Kişisel Bilgiler

E-posta: meryem.soysaldi@omu.edu.tr

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

Uluslararası Araştırmacı ID'leri

ScholarID: T6e57RUAAAAJ

ORCID: 0000-0002-1674-2768

Yoksis Araştırmacı ID: 248797

Eğitim Bilgileri

Doktora, Ondokuz Mayıs Üniversitesi, Lisansüstü Eğitim Enstitüsü, Hesaplamalı Bilimler Anabilim Dalı, Türkiye 2018 - 2022

Yüksek Lisans, Ondokuz Mayıs Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği (YL) (Tezli), Türkiye 2016 - 2018

Lisans, Fırat Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Türkiye 2010 - 2013

Yaptığı Tezler

Yüksek Lisans, ÇOK DEĞİŞKENLİ POLİNOM SİSTEMLERİNE DAYALI KUANTUM BİLGİSAYARLAR SONRASI GÜVENİLİR YENİ KİMLİK DOĞRULAMA VE İMZALAMA ŞEMALARI, Ondokuz Mayıs Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği (YL) (Tezli), 2018

Akademik Unvanlar / Görevler

Araştırma Görevlisi, Ondokuz Mayıs Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 2016 - Devam Ediyor

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

- I. **A survey of quantum secure group signature schemes: Lattice-based approach**
Şahin M., Akleylek S.
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, cilt.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, cilt.34, sa.10, ss.9852-9866, 2022 (SCI-Expanded)
- III. **A new lattice-based authentication scheme for IoT**
Akleylek S., Soysaldı M.
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, cilt.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, cilt.8, sa.8, ss.6983-6994, 2021 (SCI-Expanded)

- V. **A Novel Method for Polar Form of Any Degree of Multivariate Polynomials with Applications in IoT**
Akleyek S., Soysaldı Şahin M., Boubiche D. E., Toral-Cruz H.
SENSORS, cilt.19, sa.4, 2019 (SCI-Expanded)
- VI. **A novel 3-pass identification scheme and signature scheme based on multivariate quadratic polynomials**
Akleyek S., Soysaldı Şahin M.
TURKISH JOURNAL OF MATHEMATICS, cilt.43, sa.1, ss.241-257, 2019 (SCI-Expanded)

Diğer Dergilerde Yayınlanan Makaleler

- I. **JAVA LIBRARY FOR LATTICE-BASED IDENTIFICATION SCHEMES**
MURZAEVA A., SOYSALDI M., AKLEYLEK S.
Journal of Modern Technology and Engineering, cilt.5, sa.1, ss.5-17, 2020 (Hakemli Dergi)

Kitap & Kitap Bölümleri

- I. **Kafes Tabanlı Grup İmzalama Şemalarının Özellikleri Ve Değerlendirilmesi**
SOYSALDI ŞAHİN M., AKLEYLEK S.
Siber Güvenlik ve Savunma: BlokZincir ve Kriptoloji, Sağıroğlu Şeref, Akleyek Sedat, Editör, Nobel Akademik Yayıncılık Eğitim Danışmanlık Ltdi. Şti., Ankara, ss.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.
Authentication Technologies for Cloud Technology, IoT, and Big Data, Dr. Yasser M. Alginahi Dr. Muhammad N. Kabir, Editör, The Institution of Engineering and Technology (The IET), ss.181-207, 2019
- III. **Kuantum Bilgisayarlar ile Kriptoanaliz ve Kuantum Sonrası Güvenilir Kripto Sistemleri**
AKLEYLEK S., SOYSALDI M.
Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık Cilt II, Prof. Dr. Şeref Sağıroğlu, Mustafa Şenol, Editör, Grafiker Yayınları, Ankara, ss.137-168, 2019

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

- I. **A Lattice-based Group Signature Scheme with Applications in Blockchain**
SOYSALDI ŞAHİN M., AKLEYLEK S.
Applications of Computer Algebra - ACA 2022, Türkiye, 15 - 19 Ağustos 2022
- II. **Survey on Implementation of Lattice-based Identification Schemes**
Murzaeva A., SOYSALDI ŞAHİN M., AKLEYLEK S.
4th International Students Science Congress, İzmir, Türkiye, 15 Ocak 2021, ss.194-206
- III. **A Novel Lattice-Based Threshold Ring Signature Scheme**
Akleyek S., Soysaldı Şahin M.
5th International Conference on Computer Science and Engineering (UBMK), Diyarbakır, Türkiye, 9 - 11 Eylül 2020, ss.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, Türkiye, 11 - 15 Eylül 2019, ss.414-417
- V. **A New 3-pass Zero-knowledge Lattice-based Identification Scheme**

Akleylek S., Soysaldi Şahin M.

4th International Conference on Computer Science and Engineering (UBMK), Samsun, Türkiye, 11 - 15 Eylül 2019, ss.409-413

- VI. **Kuantum Sonrası Güvenilir Yeni Kimlik Doğrulama Şeması**
AKLEYLEK S., SOYSALDI ŞAHİN M.
SAVTEK 2018, 9. SAVUNMA TEKNOLOJİLERİ KONGRESİ, 27 Haziran 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, Ukrayna, 2 - 06 Mayıs 2018, ss.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, Ukrayna, 2 - 06 Mayıs 2018, ss.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, Ukrayna, 2 - 06 Mayıs 2018
- X. **Sentiment Analysis On Twitter Data Using Distributed Architecture**
Karhan Z., Soysaldi Şahin M., Ozben Y. O., Kılıç E.
3rd International Conference on Computer Science and Engineering (UBMK), Sarajevo, Bosna-Hersek, 20 - 23 Eylül 2018, ss.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 Aralık 2017, cilt.3, ss.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 Ekim 2017, ss.322-327
- XIII. **A Novel Identification Scheme for Post-Quantum Secure Digital Right Management**
Akleylek S., Soysaldi Şahin M.
2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Türkiye, 5 - 08 Ekim 2017, ss.322-327