Arş. Gör. Kübra Seyhan

Kişisel Bilgiler

İş Telefonu: +90 312 191 9 Dahili: 1117
E-posta: kubra.seyhan@omu.edu.tr
Diğer E-posta: kubraseyhan13@gmail.com
Web: https://sites.google.com/view/kubraseyhan/

Uluslararası Araştırmacı ID'leri
ScholarID: 3362rD4AAAAJ
ORCID: 0000-0002-0902-1903
Publons / Web Of Science ResearcherID: IYJ-3199-2023
ScopusID: 57212212152
Yoksis Araştırmacı ID: 279295

Eğitim Bilgileri

Doktora, Ondokuz Mayıs Üniversitesi, Lisansüstü Eğitim Enstitüsü, Hesaplamalı Bilimler Anabilim Dalı, Türkiye 2020 - 2024
Yüksek Lisans, Ondokuz Mayıs Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği (Yl) (Tezli), Türkiye 2017 - 2020
Lisans, Karadeniz Teknik Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Türkiye 2013 - 2016
Lisans, Gebze Teknik Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Türkiye 2010 - 2013

Yaptığı Tezler

Doktora, Post-quantum password authenticated key exchange schemes and their primitives for resource-constrained devices, Ondokuz Mayıs Üniversitesi, Lisansüstü Eğitim Enstitüsü, 2024
Yüksek Lisans, Kafes tabanlı yeni kimliği doğrulanmış anahtar değişim protokolü ve uzlaşma mekanizmaları, Ondokuz Mayıs Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği (Yl) (Tezli), 2020

Araştırma Alanları

Bilgisayar Bilimleri, Bilgi Güvenliği ve Güvenilirliği, Bilgi Gizleme, Bilgi Sistemi Güvenilirliği, Kriptoloji, Kuantum Kriptografi

Akademik Unvanlar / Görevler

Araştırma Görevlisi, Ondokuz Mayıs Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 2018 - Devam Ediyor

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

I. **A new lattice-based password authenticated key exchange scheme with anonymity and reusable key**

Seyhan K., Akleylek S.
PEERJ COMPUTER SCIENCE, 2024 (SCI-Expanded)

II. **Password authenticated key exchange-based on Kyber for mobile devices**
Seyhan K., Akleylek S., DURSUN A. F.
PEERJ COMPUTER SCIENCE, cilt.10, 2024 (SCI-Expanded)

III. **MLWR-2PAKA: A Hybrid Module Learning With Rounding-Based Authenticated Key Agreement Protocol for Two-Party Communication**
Basu S., Seyhan K., Islam S. H., Akleylek S.
IEEE SYSTEMS JOURNAL, cilt.17, sa.4, ss.6093-6103, 2023 (SCI-Expanded)

IV. **A new password-authenticated module learning with rounding-based key exchange protocol: Saber.PAKE**
Seyhan K., Akleylek S.
JOURNAL OF SUPERCOMPUTING, cilt.79, sa.16, ss.17859-17896, 2023 (SCI-Expanded)

V. **Indistinguishability under adaptive chosen-ciphertext attack secure double-NTRU-based key encapsulation mechanism**
Seyhan K., Akleylek S.
PEERJ COMPUTER SCIENCE, cilt.9, 2023 (SCI-Expanded)

VI. **Classification of random number generator applications in IoT: A comprehensive taxonomy**
Seyhan K., Akleylek S.
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, cilt.71, 2022 (SCI-Expanded)

VII. **Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey**
Seyhan K., Nguyen T. N., Akleylek S., CENGİZ K.
CLUSTER COMPUTING-THE JOURNAL OF NETWORKS SOFTWARE TOOLS AND APPLICATIONS, cilt.25, sa.3, ss.1729-1748, 2022 (SCI-Expanded)

VIII. **Module learning with rounding based key agreement scheme with modified reconciliation**
Akleylek S., Seyhan K.
COMPUTER STANDARDS & INTERFACES, cilt.79, 2022 (SCI-Expanded)

IX. **Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security**
Seyhan K., Tu N Nguyen T. N. N., Akleylek S., CENGİZ K., Islam S. K. H.
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, cilt.58, 2021 (SCI-Expanded)

X. **A Probably Secure Bi-GISIS Based Modified AKE Scheme With Reusable Keys**
Akleylek S., Seyhan K.
IEEE ACCESS, cilt.8, ss.26210-26222, 2020 (SCI-Expanded)

Diğer Dergilerde Yayınlanan Makaleler

I. **Kafes-Tabanlı Anahtar Değişim/Paketleme Protokollerinde Kullanılan Uzlaşma Yöntemlerine Ait Bileşenlerin Analizi**
AKLEYLEK S., SEYHAN K.
Bilgisayar Bilimleri ve Mühendisliği Dergisi, cilt.13, sa.1, ss.43-56, 2020 (Hakemli Dergi)

Kitap & Kitap Bölümleri

I. **Kuantum Sonrası Kriptografi: Standardizasyon Çabalarının Bir Anlık Görüntüsü**
Seyhan K., Akleylek S.
Cilt 62: Endüstriyel Kontrol Sistemlerinin Yansıması Yoluyla Kritik Altyapı Koruması için Siber Güvenlik, Oliver B. Popov,Lyudmila Sukhostat, Editör, AP, London , Aberdeen, ss.90-99, 2022

II. **Kuantum Bilgisayar Çağında Kriptosistemlere Bir Bakış**

AKLEYLEK S., SEYHAN K.
Siber Güvenlik ve Savunma: Blokzincir ve Kriptoloji, Sağıroğlu, Şeref, Akleylek, Sedat, Editör, Nobel, Ankara, ss.239-275, 2021

III. **Kuantum Bilgisayarlar Sonrası Güvenilir Kafes Tabanlı Kriptosistem Temellerine Giriş**
AKLEYLEK S., SEYHAN K.
Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık Cilt II, Prof. Dr. Şeref Sağıroğlu, Mustafa Şenol, Editör, Grafiker Yayınları, ss.171-209, 2019

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

I. **Smaug Kem to Smaug-PAKE: A Generic Lattice-Based Password Authenticated Key Exchange**
SEYHAN K., AKLEYLEK S.
Central European Conference on Cryptology, Varşova, Polonya, 20 - 21 Haziran 2024

II. **A Comprehensive Comparison of Lattice-Based Password Authenticated Key Exchange Protocols Defined on Modules**
SEYHAN K., AKLEYLEK S.
2nd International Conference on Information Technologies and Their Applications (ITTA 2024), Baku, Azerbaycan, 23 - 25 Nisan 2024

III. **QUANTUM SECURE INSTANT MESSAGING: REVISITED**
DURSUN A. F., SEYHAN K., AKLEYLEK S.
INFORMATION SECURITY: PROBLEMS AND PROSPECTS, Baku, Azerbaycan, 25 - 26 Kasım 2022

IV. **End-to-End Encrypted Instant Message Application of Post-Quantum Secure Key Encapsulation Mechanisms for Mobile Applications**
DURSUN A. F., SEYHAN K., AKLEYLEK S.
International Conference on Science, Engineering Management and Information Technology, Ankara, Türkiye, 8 - 09 Eylül 2022

V. **Lattice-Based Cryptography, Lattices, NP-Hard Problems in Lattices (SIS, SVP, etc)**
SEYHAN K., AKLEYLEK S.
Intermediate and Advanced Course on Post-Quantum Cryptography, Baku, Azerbaycan, 5 - 10 Eylül 2022

VI. **End-to-End Encrypted Instant Message Application of Post-Quantum Secure Key Encapsulation Mechanisms for Mobile Applications**
Dursun A. F., Seyhan K., Akleylek S.
International Conference on Science, Engineering Management and Information Technology, Ankara, Türkiye, 08 Eylül 2022

VII. **A Three-Party Lattice-Based Hybrid PAKE Protocol with Anonymity**
SEYHAN K., AKLEYLEK S.
Applications of Computer Algebra – ACA 2022, İstanbul, Türkiye, 15 - 19 Ağustos 2022

VIII. **Kafes Tabanlı Anahtar Değişim Protokolleri, Uzlaşma Mekanizmaları ve Sinyal Sızıntısı Atakları**
SEYHAN K., AKLEYLEK S.
3. Kuantum Sonrası Kriptografi Çalıştayı, Türkiye, 29 - 30 Mart 2022

IX. **Adapted KEM Applications for Post-Quantum Security of Mobile Devices Mobil Cihazlarin Kuantum Sonrasi Güvenliği Için Uyarlanmiş KEM Uygulamalari: Adapted KEM Applications for Post-Quantum Security of Mobile Devices**
Dursun A. F., Seyhan K., Akleylek S.
15th International Conference on Information Security and Cryptography, ISCTURKEY 2022, Ankara, Türkiye, 19 - 20 Ekim 2022, ss.31-37

X. **HARD PROBLEMS IN LATTICE-BASED CRYPTOGRAPHY: X-LWE**
SEYHAN K., AKLEYLEK S., KILIÇ E., ORUÇ Y.
INFORMATION SECURITY: PROBLEMS AND PROSPECTS, Azerbaycan, 29 Ekim 2021, ss.112-114

XI. **Reconciliation Methods Used in Lattice-Based Key Exchange/Encapsulation Protocols**

Aldeylek S., Seyhan K.
4th International Conference on Computer Science and Engineering (UBMK), Samsun, Türkiye, 11 - 15 Eylül 2019, ss.91-96

XII. **Blok Zinciri Bileşenleri ve Uygulamaları Üzerine Bir Derleme**
AKLEYLEK S., SEYHAN K.
İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri IV respublika konfransının materialları, 14 Aralık 2018

Desteklenen Projeler

Akleylek S., TÜBİTAK Uluslararası Çoklu İşbirliği Projesi , Kuantum Sonrası Kriptografik Protokollerin Biçimsel Analizi ve Doğrulanması (FAVPQC), 2021 - 2023
Akleylek S., Soysaldı Şahin M., Seyhan K., Yükseköğretim Kurumları Destekli Proje, Maude-NPA ve Proverif Araçları ile Kriptografik Protokollerin Güvenlik Analizi için Yazılım Kütüphanesinin Oluşturulması, 2022 - 2022
Akleylek S., NTRU Tabanlı Kriptosistemlerin Tasarımı ve Biçimsel Yöntemler Ile Analizi, 2019 - 2021
Akleylek S., Kafes Tabanlı Güvenilir Kriptografik Protokol Tasarımı Ve Verimli Uygulamaları, 2018 - 2020

Patent

Kübra S., Akleylek S., Kuantum sonrası güvenli yeni anahtar değişim protokolü 2020/22849, Patent, BÖLÜM H Elektrik, Buluşun Tescil No: 2020/22849 , Standart Tescil, 2022