Res. Asst. Kübra Seyhan

Personal Information

Office Phone: +90 312 191 9 Extension: 1117
Email: kubra.seyhan@omu.edu.tr
Other Email: kubraseyhan13@gmail.com
Web: https://sites.google.com/view/kubraseyhan/

International Researcher IDs
ScholarID: 3362rD4AAAAJ
ORCID: 0000-0002-0902-1903
Publons / Web Of Science ResearcherID: IYJ-3199-2023
ScopusID: 57212212152
Yoksis Researcher ID: 279295

Education Information

Doctorate, Ondokuz Mayis University, Lisansüstü Eğitim Enstitüsü, Hesaplamalı Bilimler Anabilim Dalı, Turkey 2020 - 2024
Postgraduate, Ondokuz Mayis University, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği (Yl) (Tezli), Turkey 2017 - 2020
Undergraduate, Karadeniz Technical University, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Turkey 2013 - 2016
Undergraduate, Gebze Technical University, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Turkey 2010 - 2013

Dissertations

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

Research Areas

Computer Sciences, Information Security and Reliability, Hiding Information, Information System Reliability, Cryptography, Quantum Cryptography

Academic Titles / Tasks

Research Assistant, Ondokuz Mayis University, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 2018 - Continues

Published journal articles indexed by SCI, SSCI, and AHCI

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, vol.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, vol.17, no.4, pp.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, vol.79, no.16, pp.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, vol.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, vol.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, vol.25, no.3, pp.1729-1748, 2022 (SCI-Expanded)

VIII. **Module learning with rounding based key agreement scheme with modified reconciliation**
Akleylek S., Seyhan K.
COMPUTER STANDARDS & INTERFACES, vol.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, vol.58, 2021 (SCI-Expanded)

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

Articles Published in Other Journals

I. **On the Analysis of Components of Reconciliation Mechanisms in Lattice-Based Key Exchange/Encapsulation Protocols**
AKLEYLEK S., SEYHAN K.
Bilgisayar Bilimleri ve Mühendisliği Dergisi, vol.13, no.1, pp.43-56, 2020 (Peer-Reviewed Journal)

Books & Book Chapters

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

II. **Kuantum Bilgisayar Çağında Kriptosistemlere Bir Bakış**
AKLEYLEK S., SEYHAN K.

in: Siber Güvenlik ve Savunma: Blokzincir ve Kriptoloji, Sağıroğlu, Şeref, Akleylek, Sedat, Editor, Nobel, Ankara, pp.239-275, 2021

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

Refereed Congress / Symposium Publications in Proceedings

I. **Smaug Kem to Smaug-PAKE: A Generic Lattice-Based Password Authenticated Key Exchange**
SEYHAN K., AKLEYLEK S.
Central European Conference on Cryptology, Varşova, Poland, 20 - 21 June 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, Azerbaijan, 23 - 25 April 2024

III. **QUANTUM SECURE INSTANT MESSAGING: REVISITED**
DURSUN A. F., SEYHAN K., AKLEYLEK S.
INFORMATION SECURITY: PROBLEMS AND PROSPECTS, Baku, Azerbaijan, 25 - 26 November 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, Turkey, 8 - 09 September 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, Azerbaijan, 5 - 10 September 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, Turkey, 08 September 2022

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

VIII. **Kafes Tabanlı Anahtar Değişim Protokolleri, Uzlaşma Mekanizmaları ve Sinyal Sızıntısı Atakları**
SEYHAN K., AKLEYLEK S.
3. Kuantum Sonrası Kriptografi Çalıştayı, Turkey, 29 - 30 March 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, Turkey, 19 - 20 October 2022, pp.31-37

X. **HARD PROBLEMS IN LATTICE-BASED CRYPTOGRAPHY: X-LWE**
SEYHAN K., AKLEYLEK S., KILIÇ E., ORUÇ Y.
INFORMATION SECURITY: PROBLEMS AND PROSPECTS, Azerbaijan, 29 October 2021, pp.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, Turkey, 11 - 15 September 2019, pp.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 December 2018

Supported Projects

Akleylek S., TÜBİTAK International Multi-Cooperation Project, Kuantum Sonrası Kriptografik Protokollerin Biçimsel Analizi ve Doğrulanması (FAVPQC), 2021 - 2023
Akleylek S., Soysaldı Şahin M., Seyhan K., Project Supported by Higher Education Institutions, 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, CHAPTER H Electricity, The Invention Registration Number: 2020/22849 , Standard Registration, 2022