SEDAT AKLEYLEK

PROF.

Other Email : akleylek@gmail.com
Office Phone : +90 312 191 9 Extension: 1099
International Researcher IDs
ScholarID: plpKMjkAAAAJ
ORCID: 0000-0001-7005-6489
Publons / Web Of Science ResearcherID: D-2090-2015
ScopusID: 15833929800
Yoksis Researcher ID: 18048

Biography

sedat.akleylek@ut.ee

Learning Knowledge

Doctorate 2008 - 2010	Middle East Technical University, Uygulamalı Matematik Enstitüsü, Kriptografi (Dr), Turkey
Postgraduate 2004 - 2008	Middle East Technical University, Uygulamalı Matematik Enstitüsü, Kriptografi (Yl) (Tezli), Turkey
Undergraduate 1999 - 2004	Ege University, Fen Fakültesi, Matematik Bölümü, Turkey

Dissertations

Doctorate, On the representation of finite fields, Middle East Technical University, Uygulamalı Matematik Enstitüsü, Kriptografi (Dr), 2010
Postgraduate, On the avalanche properties of MISTY1, KASUMI, KASUMI-R, Middle East Technical University, Uygulamalı Matematik Enstitüsü, Kriptografi (Yl) (Tezli), 2008

Academic Titles / Tasks

Professor 2024 - Continues	Istinye University, Doğa Bilimleri ve Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü
Professor 2022 - Continues	University of Tartu, Institute of Computer Science, Chair of Security and Theoretical Computer Science
Professor 2022 - 2024	Ondokuz Mayis University, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü

Associate Professor 2016 - 2022	Ondokuz Mayis University, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü
Assistant Professor 2012 - 2016	Ondokuz Mayis University, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü
2014 - 2015	Technische Universitaet Darmstadt, Computer Science, Computer Algebra And Cryptography
Research Assistant 2005 - 2011	Middle East Technical University, Uygulamalı Matematik Enstitüsü, Kriptografi (Dr)

Supported Projects

1. Akleylek S., Homomorfik Şifreleme Algoritmaları için Verimli Önyükleme Metotları, 2022 - Continues
2. Akleylek S., Project Supported by Higher Education Institutions, THE SECOND INTERNATIONAL WORKSHOP ON CRYPTOGRAPHY AND ITS APPLICATIONS (2IWCA), 2018 - Continues
3. Akleylek S., TUBITAK Project, ETSI TS 102 640 Standardına ve Türk Mevzuatına Uyumlu Güvenli ve Yüksek Performanslı İletişim Protokolüne Dayalı Kayıtlı Elektronik Posta Sistemi Yönetim Yazılımının Geliştirilmesi, Continues
4. TUBITAK Project, Açık Anahtar Altyapı Konusunda Araştırma Geliştirme ve Uygulamalar, Continues
5. Akleylek S., Finite Geometry Coding Theory and Cryptography, Continues
6. Akleylek S., Çok Seviyeli Güvenliğe Uygun Kriptografik Algoritmaların Uygulanması, Continues
7. Akleylek S., Kriptografik Algoritmaların Çalışma Ortamlarındaki Gereksinimleri Üzerine, Continues
8. Akleylek S., Özgün Eliptik Eğri Tasarlanması ve Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi, Continues
9. Akleylek S., TUBITAK Project, Eğri Tabanlı Kriptografiye Matematiksel Bakış, Continues
10. Akleylek S., Project Supported by Other Private Institutions, ASELSAN - Siber Güvenlik Araştırma ve Geliştirme Projesi, 2022 - 2023
11. Akleylek S., TÜBİTAK International Multi-Cooperation Project, Kuantum Sonrası Kriptografik Protokollerin Biçimsel Analizi ve Doğrulanması (FAVPQC), 2021 - 2023
12. Akleylek S., Project Supported by Higher Education Institutions, Kuantum sonrası güvenli yeni anahtar değişim protokolü, 2021 - 2023
13. Akleylek S., Project Supported by Higher Education Institutions, The Third International Conference on Applications of Mathematics and Informatics in Natural Sciences and Engineering (Workshop on Practical and Theoretical Aspects of Cryptography and Information Security), 2017 - 2023
14. Akleylek S., Şahin D. Ö., Project Supported by Higher Education Institutions, Android Kötücül Yazılımların Tespit Edilmesini Sağlayan Mobil/Web Tabanlı Uygulamanın Geliştirilmesi, 2022 - 2022
15. 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
16. Akleylek S., Other International Funding Programs, Multicast Group Key Management in IoT using Post-quantum Cryptography and Zero-Knowledge Authentication, 2020 - 2021
17. Akleylek S., NTRU Tabanlı Kriptosistemlerin Tasarımı ve Biçimsel Yöntemler Ile Analizi, 2019 - 2021
18. Akleylek S., Project Supported by Other Private Institutions, Akıllı İş/İşçi Güvenliği Tespit Platformu Tasarımı ve Uygulaması, 2019 - 2021
19. Akleylek S., Kılıç E., Ergün E., Akıllı Siber Güvenlik ve Kriptografi Çözümleri: Mobil Cihazlar İçin Kötücül Yazılım ve

Güvenlik Açığı Tespit Etme Yazılımı, 2018 - 2020

20. Akleylek S., Kafes Tabanlı Güvenilir Kriptografik Protokol Tasarımı Ve Verimli Uygulamaları, 2018 - 2020
21. Ergün E., Akleylek S., Akıllı Aktif Satış ve Rota Yönetim Sistemi, 2018 - 2019
22. Akleylek S., Project Supported by Higher Education Institutions, Siber Güvenlik ve Kriptoloji Laboratuvarı, 2017 - 2019
23. Akleylek S., Kuantum Sonrası Kriptografik Protokol Bileşenlerinin Verimlilik Analizi Ve Yazılım/Donanım Uygulamaları, 2017 - 2019
24. Akleylek S., Project Supported by Higher Education Institutions, V. International Scientific Conference of Students and Young Scientists, Theoretical and Applied Aspects of Cybernetics (TAAC-2015), 2015 - 2016
25. Akleylek S., Project Supported by Higher Education Institutions, Boolean Fonksiyonlarının Kriptografik Ölçütlere Göre Değerlendirilmesi ve Sınıflandırılması, 2014 - 2016
26. Akleylek S., TUBITAK Project, Bazı Kriptografik Fonksiyonlar ve Verimli Uygulamalar TÜBİTAK 113F249, 2014 - 2014
27. Akleylek S., TUBITAK Project, Cebirsel Eğriler Ve Onların Bazı Kriptografik Ve Kodlama Teorisindeki Problemlerdeki Uygulamaları, 2010 - 2013
28. Akleylek S., Eşleme Tabanlı Kripto Sistemleri Araştırma Geliştirme Projesi Pairing Based Cryptosystems Research and Development, 2008 - 2009
29. Akleylek S., Project Supported by Other Private Institutions, Eşleme Tabanlı Kripto Sistemleri Araştırma Geliştirme Projesi, 2008 - 2009

Published journal articles indexed by SCI, SSCI, and AHCI

1. **A new lattice-based password authenticated key exchange scheme with anonymity and reusable key**
   Seyhan K., Akleylek S.
   PEERJ COMPUTER SCIENCE, 2024 (SCI-Expanded)
2. **Formal Analysis of Post-Quantum Hybrid Key Exchange SSH Transport Layer Protocol**
   Tran D. D., Ogata K., Escobar S., Akleylek S., Otmani A.
   IEEE ACCESS, vol.12, pp.1672-1687, 2024 (SCI-Expanded)
3. **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)
4. **Modified graph-based algorithm to analyze security threats in IoT**
   Arat F., Akleylek S.
   PEERJ COMPUTER SCIENCE, vol.9, pp.1-22, 2023 (SCI-Expanded)
5. **A new method for vulnerability and risk assessment of IoT**
   Arat F., Akleylek S.
   Computer Networks, vol.237, 2023 (SCI-Expanded)
6. **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)
7. **Kyber, Saber, and SK-MLWR Lattice-Based Key Encapsulation Mechanisms Model Checking with Maude**
   Tran D. D., Ogata K., Escobar S., Akleylek S., Otmani A., Haines T.
   IET INFORMATION SECURITY, 2023 (SCI-Expanded)
8. **Attack Path Detection for IIoT Enabled Cyber Physical Systems: Revisited**
   Arat F., Akleylek S.
   COMPUTERS & SECURITY, vol.128, 2023 (SCI-Expanded)
9. **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)

10. **Security enhancement in cellular networks employing D2D friendly jammer for V2V communication**
Kumar J. S., Gupta A., Tanwar S., Kumar N., Akleylek S.
CLUSTER COMPUTING-THE JOURNAL OF NETWORKS SOFTWARE TOOLS AND APPLICATIONS, vol.26, no.2, pp.865-878, 2023 (SCI-Expanded)
11. **A novel permission-based Android malware detection system using feature selection based on linear regression**
Şahin D. Ö., Kural O. E., Akleylek S., Kılıç E.
NEURAL COMPUTING & APPLICATIONS, vol.35, no.7, pp.4903-4918, 2023 (SCI-Expanded)
12. **A survey of quantum secure group signature schemes: Lattice-based approach**
Sahin M., Akleylek S.
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, vol.73, 2023 (SCI-Expanded)
13. **Automatic delay-sensitive applications quality of service improvement with deep flows discrimination in software defined networks**
Mohammadi R., Akleylek S., Ghaffari A., Shirmarz A.
CLUSTER COMPUTING-THE JOURNAL OF NETWORKS SOFTWARE TOOLS AND APPLICATIONS, vol.26, no.1, pp.437-459, 2023 (SCI-Expanded)
14. **A novel Android malware detection system: adaption of filter-based feature selection methods**
Şahin D. Ö., Kural O. E., Akleylek S., Kılıç E.
JOURNAL OF AMBIENT INTELLIGENCE AND HUMANIZED COMPUTING, vol.14, pp.1243-1257, 2023 (SCI-Expanded)
15. **Modelling and verification of post-quantum key encapsulation mechanisms using Maude**
García V., Escobar S., Ogata K., Akleylek S., Otmani A.
PeerJ Computer Science, vol.9, 2023 (SCI-Expanded)
16. **A new hybrid method combining search and direct based construction ideas to generate all 4 × 4 involutory maximum distance separable (MDS) matrices over binary field extensions**
Tuncay G., Sakallı F. B., KURT PEHLİVANOĞLU M., Yılmazgüç G. G., Akleylek S., SAKALLI M. T.
PeerJ Computer Science, vol.9, 2023 (SCI-Expanded)
17. **SDN-IoT: SDN-based efficient clustering scheme for IoT using improved Sailfish optimization algorithm**
Mohammadi R., Akleylek S., Ghaffari A.
PeerJ Computer Science, vol.9, 2023 (SCI-Expanded)
18. **On the Construction of New Lightweight Involutory MDS Matrices in Generalized Subfield Form**
KURT PEHLİVANOĞLU M., BÜYÜKSARAÇOĞLU SAKALLI F., Akleylek S., Sakalli M. T.
IEEE ACCESS, vol.11, pp.32708-32715, 2023 (SCI-Expanded)
19. **Group Key Management in Internet of Things: A Systematic Literature Review**
Samiullah F., Gan M. L., Akleylek S., Aun Y.
IEEE Access, vol.11, pp.77464-77491, 2023 (SCI-Expanded)
20. **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)
21. **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)
22. **Taxonomy of traffic engineering mechanisms in software-defined networks: a survey**
Mohammadi R., Akleylek S., Ghaffari A., Shirmarz A.
TELECOMMUNICATION SYSTEMS, vol.81, no.3, pp.475-502, 2022 (SCI-Expanded)

23. **GOALALERT: A novel real-time technical team alert approach using machine learning on an IoT-based system in sports**
Karakaya A., ULU A., Akleylek S.
MICROPROCESSORS AND MICROSYSTEMS, vol.93, 2022 (SCI-Expanded)
24. **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)
25. **A new lattice-based authentication scheme for IoT**
Akleylek S., Soysald M.
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, vol.64, 2022 (SCI-Expanded)
26. **Quantum Secure Communication Between Service Provider and Sim**
Karacan E., Karakaya A., Akleylek S.
IEEE ACCESS, vol.10, pp.69135-69146, 2022 (SCI-Expanded)
27. **Module learning with rounding based key agreement scheme with modified reconciliation**
Akleylek S., Seyhan K.
COMPUTER STANDARDS & INTERFACES, vol.79, 2022 (SCI-Expanded)
28. **LinRegDroid: Detection of Android Malware Using Multiple Linear Regression Models-Based Classifiers**
Şahin D. Ö., Akleylek S., Kılıç E.
IEEE ACCESS, vol.10, pp.14246-14259, 2022 (SCI-Expanded)
29. **Permission-based Android malware analysis by using dimension reduction with PCA and LDA**
Şahin D. Ö., Kural O. E., Akleylek S., Kılıç E.
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, vol.63, 2021 (SCI-Expanded)
30. **Efficient Nyberg-Rueppel type of NTRU digital signature algorithm**
Elverdi F., Akleylek S., Kırlar B. B.
TURKISH JOURNAL OF MATHEMATICS, no.1, pp.59-70, 2021 (SCI-Expanded)
31. **A NOVEL NIEDERREITER-LIKE CRYPTOSYSTEM BASED ON THE (u vertical bar u plus v)-CONSTRUCTION CODES**
Mahdjoubi R., Cayrel P. L., Akleylek S., Kenza G.
RAIRO-THEORETICAL INFORMATICS AND APPLICATIONS, vol.55, 2021 (SCI-Expanded)
32. **Efficient Implementations of Sieving and Enumeration Algorithms for Lattice-Based Cryptography**
SATILMIŞ H., Akleylek S., Lee C.
MATHEMATICS, vol.9, no.14, 2021 (SCI-Expanded)
33. **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)
34. **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)
35. **Parallel implementation of Nussbaumer algorithm and number theoretic transform on a GPU platform: application to qTESLA**
Lee W., Akleylek S., Wong D. C., Yap W., Goi B., Hwang S.
JOURNAL OF SUPERCOMPUTING, vol.77, no.4, pp.3289-3314, 2021 (SCI-Expanded)
36. **A novel IoT-based health and tactical analysis model with fog computing**
Karakaya A., Akleylek S.
PEERJ COMPUTER SCIENCE, vol.7, pp.1-34, 2021 (SCI-Expanded)
37. **MaTRU-KE revisited: CCA2-secure key establishment protocol based on MaTRU**
Akleylek S., Çevik N.
International Journal of Communication Systems, vol.33, no.7, 2020 (SCI-Expanded)

38. **On the automorphisms and isomorphisms of MDS matrices and their efficient implementations**
Sakalli M. T., Akleylek S., AKKANAT K., Rijmen V.
TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, vol.28, no.1, pp.275-287, 2020 (SCI-Expanded)
39. **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)
40. **A new matrix form to generate all 3 x 3 involutory MDS matrices over F-2(m)**
Guzel G. G., SAKALLI M. T., Akleylek S., Rijmen V., ÇENGELLENMİŞ Y.
INFORMATION PROCESSING LETTERS, vol.147, pp.61-68, 2019 (SCI-Expanded)
41. **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)
42. **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)
43. **Generalisation of Hadamard matrix to generate involutory MDS matrices for lightweight cryptography**
KURT PEHLİVANOĞLU M., SAKALLI M. T., Akleylek S., DURU N., Rijmen V.
IET INFORMATION SECURITY, vol.12, no.4, pp.348-355, 2018 (SCI-Expanded)
44. **A Modified Parallel Learning Vector Quantization Algorithm for Real-Time Hardware Applications**
Alkim E., Akleylek S., Kılıç E.
JOURNAL OF CIRCUITS SYSTEMS AND COMPUTERS, vol.26, no.10, 2017 (SCI-Expanded)
45. **Efficient methods to generate cryptographically significant binary diffusion layers**
Akleylek S., Rijmen V., SAKALLI M. T., ÖZTÜRK E.
IET INFORMATION SECURITY, vol.11, no.4, pp.177-187, 2017 (SCI-Expanded)
46. **Generating binary diffusion layers with maximum/high branch numbers and low search complexity**
Akleylek S., SAKALLI M. T., ÖZTÜRK E., Mesut A. S., Tuncay G.
SECURITY AND COMMUNICATION NETWORKS, vol.9, no.16, pp.3558-3569, 2016 (SCI-Expanded)
47. **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)
48. **New methods for public key cryptosystems based on XTR**
Akleylek S., KIRLAR B. B.
SECURITY AND COMMUNICATION NETWORKS, vol.8, no.18, pp.3682-3689, 2015 (SCI-Expanded)
49. **On the arithmetic operations over finite fields of characteristic three with low complexity**
Akleylek S., ÖZBUDAK F., Ozel C.
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, vol.259, pp.546-554, 2014 (SCI-Expanded)
50. **On the Construction of 20 x 20 and 24 x 24 Binary Matrices with Good Implementation Properties for Lightweight Block Ciphers and Hash Functions**
SAKALLI M. T., Akleylek S., ASLAN B., BULUŞ E., Sakalli F. B.
MATHEMATICAL PROBLEMS IN ENGINEERING, vol.2014, 2014 (SCI-Expanded)
51. **Efficient interleaved Montgomery modular multiplication for lattice-based cryptography**
Akleylek S., Tok Z. Y.
IEICE ELECTRONICS EXPRESS, vol.11, no.22, 2014 (SCI-Expanded)
52. **A New Representation of Elements of Binary Fields with Subquadratic Space Complexity Multiplication of Polynomials**
ÖZBUDAK F., Akleylek S., CENK M.
IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS COMMUNICATIONS AND COMPUTER SCIENCES, vol.E96A, no.10, pp.2016-2024, 2013 (SCI-Expanded)

53. **On the generalisation of special moduli for faster interleaved montgomery modular multiplication**
Akleylek S., CENK M., ÖZBUDAK F.
IET INFORMATION SECURITY, vol.7, no.3, pp.165-171, 2013 (SCI-Expanded)
54. **On the Polynomial Multiplication in Chebyshev Form**
Akleylek S., Cenk M., ÖZBUDAK F.
IEEE TRANSACTIONS ON COMPUTERS, vol.61, no.4, pp.584-587, 2012 (SCI-Expanded)
55. **Modified Redundant Representation for Designing Arithmetic Circuits with Small Complexity**
Akleylek S., ÖZBUDAK F.
IEEE TRANSACTIONS ON COMPUTERS, vol.61, no.3, pp.427-432, 2012 (SCI-Expanded)

Articles Published in Other Journals

1. **Preface**
Akleylek S., Koç Ç. K.
Handbook of Formal Analysis and Verification in Cryptography, 2023 (Scopus)
2. **Bulut Bilişim Güvenliği İçin Kullanılan Makine Öğrenimi Yöntemleri Üzerine Bir Derleme**
YAZAR B. K., AKLEYLEK S., KILIÇ E.
Düzce Üniversitesi Bilim ve Teknoloji Dergisi, vol.10, no.2, pp.893-913, 2022 (Peer-Reviewed Journal)
3. **Proceedings of FAVPQC 2022**
Escobar S., Otmani A., Akleylek S., Ogata K.
CEUR Workshop Proceedings, vol.3280, 2022 (Scopus)
4. **On the Effect of k Values and Distance Metrics in KNN Algorithm for Android Malware Detection**
ŞAHİN D. Ö., AKLEYLEK S., KILIÇ E.
Advances in Data Science and Adaptive Analysis, 2021 (Peer-Reviewed Journal)
5. **A Review of Machine Learning and Deep Learning Models Used for IoT Security**
SATILMIŞ H., AKLEYLEK S.
Bilişim Teknolojileri Dergisi, vol.14, no.4, pp.457-481, 2021 (Peer-Reviewed Journal)
6. **A Review on Deep Learning Based Intrusion Detection Systems for Ensuring Security of Controller Area Network**
AKŞEHİR Z. D., AKLEYLEK S.
Avrupa Bilim ve Teknoloji Dergisi, vol.0, no.27, pp.1038-1049, 2021 (Peer-Reviewed Journal)
7. **KAPALI MEKAN KONUMLANDIRMA ÜZERİNE BİR ÇALIŞMA**
AKLEYLEK S., KILIÇ E., SÖYLEMEZ B., ARUK E., ÇAVUŞ YILDIRIM A.
Mühendislik Bilimleri ve Tasarım Dergisi, vol.8, no.5, pp.90-105, 2020 (Peer-Reviewed Journal)
8. **NESNELERİN İNTERNETİ TABANLI SAĞLIK İZLEME SİSTEMLERİ ÜZERİNE BİR ÇALIŞMA**
AKLEYLEK S., KILIÇ E., SÖYLEMEZ B., ARUK E., AKSAÇ C.
Mühendislik Bilimleri ve Tasarım Dergisi, vol.8, no.5, pp.80-89, 2020 (Peer-Reviewed Journal)
9. **Parola Tabanlı SIMSec Protokolü**
AKLEYLEK S., KARACAN E.
Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi, vol.11, no.3, pp.1021-1030, 2020 (Peer-Reviewed Journal)
10. **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)
11. **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)
12. **Efficient GeMSS Based Ring Signature Scheme**
DEMİRCİOĞLU M., AKLEYLEK S., CENK M.

Malaysian Journal of Computing and Applied Mathematics, vol.3, no.2, 2020 (Peer-Reviewed Journal)

13. **New Signature Algorithm Based on Concatenated Rank Codes**
    Mahdjoubi R., AKLEYLEK S., Kenza G.
    Malaysian Journal of Computing and Applied Mathematics, vol.2, no.2, pp.25-31, 2019 (Peer-Reviewed Journal)
14. **İş Sağlığı ve Güvenliği Sektöründe Bayes Ağları Uygulaması**
    AKŞEHİR Z. D., PEKEL E., oruç y., AKLEYLEK S., KILIÇ E.
    Bilgisayar Bilimleri ve Mühendisliği Dergisi, vol.12, no.1, pp.47-59, 2019 (Peer-Reviewed Journal)
15. **A Survey on Security Threats and Solutions in the Age of IoT**
    ATAÇ C., AKLEYLEK S.
    Avrupa Bilim ve Teknoloji Dergisi, vol.0, no.15, pp.36-42, 2019 (Peer-Reviewed Journal)
16. **IoT Çağında Güvenlik Tehditleri ve Çözümleri Üzerine Bir Araştırma**
    Ataç C., AKLEYLEK S.
    Avrupa Bilim ve Teknoloji Dergisi, vol.15, pp.36-42, 2019 (Peer-Reviewed Journal)
17. **E-Kitap Ödünç Alma Yönetim Sistemi İçin Yeni Model**
    KARAKAYA A., AKLEYLEK S., ERZURUMLU K., KILIÇ E.
    ACADEMIC PLATFORM-JOURNAL OF ENGINEERING AND SCIENCE, vol.6, no.3, pp.49-57, 2018 (Peer-Reviewed Journal)
18. **ÜÇ TERİMLİ POLİNOMLAR İÇİN KARATSUBA BENZERİ ÇARPMA YÖNTEMLERİNİN ARAŞTIRILMASI**
    AKLEYLEK S., Kaya N.
    ULUSLARARASI BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ DERGİSİ, vol.3, no.2, pp.22-32, 2017 (Peer-Reviewed Journal)
19. **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)
20. **A New Short Signature Scheme with Random Oracle from Bilinear Pairings**
    AKLEYLEK S., KIRLAR B. B., Sever Ö., Yüce Z.
    Journal of Telecommunications and Information Technology, vol.5, no.1, pp.5-11, 2011 (Peer-Reviewed Journal)
21. **Open Source UTM Alternative ClearOS**
    AKLEYLEK S., EMMUNGİL L., NURIYEV U.
    Proceeding of the third International Conference "Problems of Cybernetics and Informatics, PCI' 2010, vol.1, pp.211-212, 2010 (Peer-Reviewed Journal)
22. **Security Analysis and Proposed Solutions About Wireless Campus Networks of Universities in Türkiye**
    EMMUNGİL L., AKLEYLEK S., NURIYEV U.
    Proceeding of the 3-th International conference on Information Technologies and Telecommunication (IT T C 2007), pp.38-44, 2007 (Peer-Reviewed Journal)
23. **A note on Knapsack Cryptosystems**
    AKLEYLEK S., EMMUNGİL L., NURIYEV U.
    Proceeding of the International scientific conference "Information Technologies and Telecommunications in Education and Science" (IT T ES'2007), pp.152-153, 2007 (Peer-Reviewed Journal)
24. **A modified algorithm for peer-to-peer security**
    Akleylek S., Emmungil L., Nuriyev U.
    Applied and Computational Mathematics, vol.7, no.1, pp.1-14, 2007 (Peer-Reviewed Journal)
25. **Securty of online Learning**
    NURIYEV U., ÖZARSLAN S., AKLEYLEK S.
    Proceeding o the fInternational scientific conference "Information Technologies and Telecommunications in Education and Science" (IT T ES'2005), pp.194-196, 2005 (Peer-Reviewed Journal)

Books & Book Chapters

1. **Handbook of Formal Analysis and Verification in Cryptography**

AKLEYLEK S., Dundua B.
Taylor Francis CRC Press, 2023

2. **On the Android Malware Detection System Based on Deep Learning**
ŞAHİN D. Ö., YAZAR B. K., AKLEYLEK S., KILIÇ E., Giri D.
in: Smart Applications with Advanced Machine Learning and Human-Centred Problem Design, D. Jude Hemanth , Utku Kose , Junzo Watada , Bogdan Patrut, Editor, Springer Cham, pp.453-466, 2023
3. **A New Hybrid Method for Indoor Positioning**
AKŞEHİR Z. D., AKLEYLEK S., KILIÇ E., AKSAÇ C., Ghaffari A.
in: Smart Applications with Advanced Machine Learning and Human-Centred Problem Design, , Editor, Springer International Publishing, pp.441-451, 2023
4. **Collecting Health Information with LoRa Technology**
AKŞEHİR Z. D., AKLEYLEK S., KILIÇ E., ŞİRİN B., CENGİZ K.
in: Smart Applications with Advanced Machine Learning and Human-Centred Problem Design, , Editor, Springer International Publishing, pp.429-439, 2023
5. **Siber Güvenlik ve Savunma: Siber Güvenlik Ontolojisi, Tehditler ve Çözümler**
SAĞIROĞLU Ş., AKLEYLEK S.
NOBEL AKADEMİK YAYINCILIK EĞİTİM DANIŞMANLIK TİC. LTD. ŞTİ., 2022
6. **Havacılık Sistemlerinde Siber Güvenlik**
Çevik N., AKLEYLEK S.
in: Siber Güvenlik ve Savunma: Siber Güvenlik Ontolojisi, Tehditler ve Çözümler, Sağıroğlu Şeref, Akleylek Sedat, Editor, NOBEL AKADEMİK YAYINCILIK EĞİTİM DANIŞMANLIK TİC. LTD. ŞTİ., pp.293-324, 2022
7. **A Review of Resource Allocation and Management Methods in IoT**
KARAKAYA A., AKLEYLEK S.
in: A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems, Pardeep Kumar, Ahmed Jabbar Obaid, Korhan Cengiz, Ashish Khanna, Valentina Emilia Balas, Editor, Springer, Cham, pp.409-429, 2022
8. **Siber Güvenlik ve Savunma: Blokzincir ve Kriptoloji**
SAĞIROĞLU Ş., AKLEYLEK S.
NOBEL AKADEMİK YAYINCILIK EĞİTİM DANIŞMANLIK TİC. LTD. ŞTİ., Ankara, 2021
9. **PROCEEDINGS OF 14TH INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND CRYPTOLOGY**
SAĞIROĞLU Ş., AKLEYLEK S., KARAÇUHA E., ALKAN M., ÖZBUDAK F., CANBAY Y., SELÇUK A. A.
IEEE, Ankara, 2021
10. **Kafes Tabanlı Grup İmzalama Şemalarının Özellikleri Ve Değerlendirilmesi**
SOYSALDI ŞAHİN M., AKLEYLEK S.
in: Siber Güvenlik ve Savunma: BlokZincir ve Kriptoloji, Sağıroğlu Şeref, Akleylek Sedat, Editor, Nobel Akademik Yayıncılık Eğitim Danışmanlık Ltdi. Şti., Ankara, pp.491-541, 2021
11. **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
12. **PROCEEDINGS OF 13TH INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND CRYPTOLOGY**
AKLEYLEK S., SAĞIROĞLU Ş., CANBAY Y., ÖZBUDAK F.
IEEE, New York, 2020
13. **proceedings of the 13th international conference on information security and cryptography**
ÖZBUDAK F., sağıroğlu ş., AKLEYLEK S., CANBAY Y.
ieee, 2020
14. **SİBER GÜVENLİK VE SAVUNMA : BİYOMETRİK VE KRİPTOGRAFİK UYGULAMALAR**
SAĞIROĞLU Ş., AKLEYLEK S.
NOBEL AKADEMİK YAYINCILIK EĞİTİM DANIŞMANLIK TİC. LTD. ŞTİ., Ankara, 2020
15. **Sis Bilişimi ve Uygulamalarında Veri Güvenliği**

KARAKAYA A., AKLEYLEK S.
in: Siber Güvenlik ve Savunma Biyometrik ve Kriptografik Uygulamalar, Sağıroğlu Şeref, Akleylek Sedat, Editor, NOBEL AKADEMİK YAYINCILIK EĞİTİM DANIŞMANLIK TİC. LTD. ŞTİ., Ankara, pp.1-28, 2020

16. **Kafes Tabanlı Kriptografide Kullanılan Zor Problemlerin Kriptanalizi ve Yazılım Kütüphaneleri**
SATILMIŞ H., AKLEYLEK S.
in: SİBER GÜVENLİK VE SAVUNMA:Biyometrik ve Kriptografik Uygulamalar, Sağıroğlu Şeref, Akleylek Sedat, Editor, NOBEL AKADEMİK YAYINCILIK EĞİTİM DANIŞMANLIK TİC. LTD. ŞTİ., Ankara, pp.233-256, 2020
17. **SİBER GÜVENLİK VE SAVUNMA : PROBLEMLER ÇÖZÜMLER**
SAĞIROĞLU S.
GRAFİKER, Ankara, 2019
18. **12. ULUSLARARASI BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI BİLDİRİ KİTABI**
SAĞIROĞLU Ş., AKLEYLEK S., CANBAY Y., ALKAN M., KARAÇUHA E., ÖZBUDAK F.
BİLGİ GÜVENLİĞİ DERNEĞİ, Ankara, 2019
19. **Lightweight Block Ciphers with Applications in IoT**
KURT PEHLİVANOĞLU M., SAKALLI M. T., AKLEYLEK S., DURU N.
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.153-180, 2019
20. **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
21. **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 Sağıroğlu, Mustafa Şenol, Editor, Grafiker Yayınları, Ankara, pp.137-168, 2019
22. **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
23. **Algoritmalara Giriş (Introduction to Algorithms kitabınının çevirisi)**
ÖNER T., TOPAL S., BERBERLER M. E., ŞENTÜRK İ., ORDİN B., KUTUCU H., AKLEYLEK S., NASİBOĞLU E., NURİYEV U., PEKTAŞ B., et al.
PALME YAYINCILIK, Ankara, 2017
24. **Şifrelerin Matematiği Kriptografi**
AKLEYLEK S., AKYILDIZ E., Çimen C.
ODTÜ Geliştirme Vakfı Yayıncılık, 2015

Refereed Congress / Symposium Publications in Proceedings

1. **QUANTUM SECURE INSTANT MESSAGING: REVISITED**
DURSUN A. F., SEYHAN K., AKLEYLEK S.
INFORMATION SECURITY: PROBLEMS AND PROSPECTS, Baku, Azerbaijan, 25 - 26 November 2022
2. **Post-Quantum Cryptography: A Snapshot of Standardization Efforts**
AKLEYLEK S., SEYHAN K.
Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, NATO Science for Peace and Security Series, Azerbaijan, 5 - 09 September 2022, pp.90-99
3. **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

4. **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
5. **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
6. **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
7. **CODE-BASED CRYPTOSYSTEMS MCNIE REVISITED**
   AKLEYLEK S., AYDOĞMUŞ E., SINAK A.
   Applications of Computer Algebra (ACA), SCALE, GEBZE, Turkey, 15 August 2022
8. **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
9. **On the Construction Structures of 3x3 Involutory MDS Matrices over F_2^m**
   KURT PEHLİVANOĞLU M., DEMİR M. A., BÜYÜKSARAÇOĞLU SAKALLI F., AKLEYLEK S., SAKALLI M. T.
   ICNDA 2022 International Conference on Nonlinear Dynamics and Applications, Majitar, India, 9 - 12 March 2022
10. **Challenges and Opportunities in Cryptography**
    AKLEYLEK S.
    The 6th International Conference of Reliable Information and Communication Technology, Saudi Arabia, 22 - 23 December 2021
11. **On the Construction Structures of 3 × 3 Involutory MDS Matrices over F2m**
    KURT PEHLİVANOĞLU M., Ali Demir M., Büyüksaraçoğlu Sakallı F., Akleylek S., Tolga Sakallı M.
    International Conference on Nonlinear Dynamics and Applications, ICNDA 2022, Virtual, Online, 9 - 11 March 2022, pp.587-595
12. **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
13. **Formal specification and model checking of lattice-based key encapsulation mechanisms in Maude**
    Tran D. D., Ogata K., Escobar S., Akleylek S., Otmani A.
    2022 International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols, FAVPQC 2022, Madrid, Spain, 24 October 2022, vol.3280, pp.16-31
14. **Formal specification and model checking of Saber lattice-based key encapsulation mechanism in Maude**
    Tran D. D., Ogata K., Escobar S., Akleylek S., Otmani A.
    34th International Conference on Software Engineering and Knowledge Engineering, SEKE 2022, Pennsylvania, United States Of America, 1 - 10 July 2022, pp.382-387
15. **IMPLEMENTATION OF LATTICE-BASED IDENTIFICATION SCHEMES IN C**
    Murzaeva A., AKLEYLEK S.
    INFORMATION SECURITY: PROBLEMS AND PROSPECTS, Baku, Azerbaijan, 29 October 2021, pp.81-84
16. **CHALLENGES AND OPPORTUNITIES IN CRYPTOGRAPHY: LATTICE-BASED AND CODE-BASED CRYPTOGRAPHY IN THE QUANTUM ERA WITH FORMAL ANALYSIS**
    AKLEYLEK S.
    International Conference on INFORMATION SECURITY: PROBLEMS AND PROSPECTS, Baku, Azerbaijan, 22 October 2021, pp.9-12

17. **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
18. **Binary finite field extensions for diffusion matrices over the finite field F2m F2msonlu cismi üzerindeki yayilim matrisleri için ikili sonlu cisim genişlemeleri**
KURT PEHLİVANOĞLU M., Buyuksaracoglu Sakalli F., Akleylek S., Sakalli M. T.
29th IEEE Conference on Signal Processing and Communications Applications, SIU 2021, Virtual, Istanbul, Turkey, 9 - 11 June 2021
19. **On the Construction of $$4 \times 4$$ Lightweight Involutory MDS Matrices Over $$\mathbb {F}_{2^{8}}$$**
KURT PEHLİVANOĞLU M., BÜYÜKSARAÇOĞLU SAKALLI F., AKLEYLEK S., SAKALLI M. T.
Proceedings of the Seventh International Conference on Mathematics and Computing ICMC 2021, 02 March 2021
20. **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
21. **Support Vector Machines: From Classical Version to Quantum**
Decadjevi G., AKLEYLEK S., Abdiu G., Halabi O.
4th International Students Science Congress, İzmir, Turkey, 15 January 2021, pp.207-216
22. **Keystroke Dynamics Based Authentication System**
Çevik N., Akleylek S., Koç K. Y.
6th International Conference on Computer Science and Engineering, UBMK 2021, Ankara, Turkey, 15 - 17 September 2021, pp.644-649
23. **A Brief Review on Deep Learning Based Software Vulnerability Detection**
Alagoz Z. I., Akleylek S.
14th International Conference on Information Security and Cryptology, ISCTURKEY 2021, Ankara, Turkey, 2 - 03 December 2021, pp.143-148
24. **Apk2Img4AndMal: Android Malware Detection Framework Based on Convolutional Neura Network**
Kural O. E., Şahin D. Ö., Akleylek S., Kılıç E., Ömüral M.
6th International Conference on Computer Science and Engineering, UBMK 2021, Ankara, Turkey, 15 - 17 September 2021, pp.731-734
25. **PQ-FLAT: A New Quantum-Resistant And Lightweight Authentication Approach for M2M Devices**
Karacan E., Akleylek S., Karakaya A.
9th International Symposium on Digital Forensics and Security (ISDFS), Elazığ, Turkey, 28 - 29 June 2021
26. **A Systematic Survey on Mobile Internet of Things Security**
Arat F., Akleylek S.
14th International Conference on Information Security and Cryptology, ISCTURKEY 2021, Ankara, Turkey, 2 - 03 December 2021, pp.116-120
27. **DDOS Attack Detection Accuracy Improvement in Software Defined Network (SDN) Using Ensemble Classification**
Shirmarz A., Ghaffari A., Mohammadi R., Akleylek S.
14th International Conference on Information Security and Cryptology, ISCTURKEY 2021, Ankara, Turkey, 2 - 03 December 2021, pp.111-115
28. **GPU implementation of quantum secure ABC cryptosystem on CUDA**
Akleylek S., Koyutürk R., Kutucu H.
2nd International Workshop on Intelligent Information Technologies and Systems of Information Security, IntellTSIS 2021, Khmelnytskyi, Ukraine, 24 - 26 March 2021, vol.2853, pp.309-316
29. **Efficient Implementations of Gauss-Based Sieving Algorithms Gauss Tabanli Eleme Algoritmalarinin Verimli Uygulamalari**
SATILMIŞ H., Akleylek S.
28th Signal Processing and Communications Applications Conference, SIU 2020, Gaziantep, Turkey, 5 - 07 October 2020

30. **Comparison of Regression Methods in Permission Based Android Malware Detection**
Şahin D. Ö., Kural O. E., Akleylek S., Kılıç E.
28th Signal Processing and Communications Applications Conference (SIU), ELECTR NETWORK, 5 - 07 October 2020
31. **Efficient Implementation of HashSieve Algorithm for Lattice-Based Cryptography**
SATILMIŞ H., Akleylek S.
International Conference on Information Security and Cryptology (ISCTURKEY), ELECTR NETWORK, 3 - 04 December 2020, pp.75-79
32. **Efficient Implementations of Gauss-Based Sieving Algorithms**
Satılmış H., Akleylek S.
28th Signal Processing and Communications Applications Conference (SIU), ELECTR NETWORK, 5 - 07 October 2020
33. **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
34. **Stocks Prices Prediction with Long Short-term Memory**
Akşehir Z. D., Kılıç E., Akleylek S., Dongul M., Coskun B.
5th International Conference on Internet of Things, Big Data and Security (IoTBDS), Prague, Czech Republic, 7 - 09 May 2020, pp.221-226
35. **Kuantum Sonrası Güvenilir ABC Şifreleme Sisteminin Farklı Platformlardaki Uygulamaları**
AKLEYLEK S., Koyutürk R.
12th International Conference on Information Security and Cryptology, Ankara, Turkey, 16 - 17 October 2019, pp.24-29
36. **Efficient GeMSS Based Ring Signature Scheme**
Demircioğlu M., AKLEYLEK S., CENK M.
The Second International Workshop on Cryptography and its Applications – 2'IWCA'19, Oran, Algeria, 18 - 19 June 2019
37. **New Signature Algorithm Based on Concatenated Rank Codes**
Mahdjoubi R., AKLEYLEK S., Kenza G.
Second International Workshop on Cryptography and its Applications, Oran, Algeria, 18 - 19 June 2019, pp.221-224
38. **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
39. **Parameter Estimation for Lattice-Based Cryptosystems By Using Sieving Algorithms**
Akleylek S., SATILMIŞ H.
4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11 - 15 September 2019, pp.372-377
40. **Accelerating Number Theoretic Transform in GPU Platform for qTESLA Scheme**
Lee W., Akleylek S., Yap W., Goi B.
15th International Conference on Information Security Practice and Experience (ISPEC), Kuala-Lumpur, Malaysia, 26 - 28 November 2019, vol.11879, pp.41-55
41. **Permission Weighting Approaches in Permission Based Android Malware Detection**
Kural O. E., Şahin D. Ö., Akleylek S., Kılıç E.
4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11 - 15 September 2019, pp.134-139
42. **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

43. **Formal Analysis of MaTRU Cryptosystem**
Akleylek S., Cevik N.
4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11 - 15 September 2019, pp.403-408

44. **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

45. **A Bayesian Networks Application in Occupational Health and Safety**
PEKEL E., AKŞEHİR Z. D., meto b., AKLEYLEK S., KILIÇ E.
International Conference on Computer Science and Engineering, 20 - 23 September 2018

46. **Kuantum Sonrası Güvenilir Yeni Kimlik Doğrulama Şeması**
AKLEYLEK S., SOYSALDI ŞAHİN M.
SAVTEK 2018, 9. SAVUNMA TEKNOLOJİLERİ KONGRESİ, 27 June 2018

47. **GUI Based Ring Signature Scheme**
AKLEYLEK S., Demircioğlu M., CENK M.
18th Central European Conference on Cryptology (CECC 2018), Smolenice, Slovakia, 6 - 08 June 2018, pp.1-3

48. **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

49. **An Automated Vulnerable Website Penetration**
Murzaeva A., AKLEYLEK S.
International Conference on Advanced Technologies, Computer Engineering and Science (ICATCES 2018), Karabük, Turkey, 11 - 13 May 2018, pp.297-301

50. **An Overview for the National Cyber Security Strategy**
Ataç C., AKLEYLEK S.
International Conference on Advanced Technologies, Computer Engineering and Science (ICATCES 2018), Karabük, Turkey, 11 - 13 May 2018, pp.603-609

51. **A study on the use of quantum computers, risk assessment and security problems**
ARSLAN B., Ulker M., Akleylek S., SAĞIROĞLU Ş.
6th International Symposium on Digital Forensic and Security, ISDFS 2018, Antalya, Turkey, 22 - 25 March 2018, vol.2018-January, pp.1-6

52. **New Results on Permission Based Static Analysis for Android Malware**
Şahin D. Ö., Kural O. E., Akleylek S., Kılıç E.
6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22 - 25 March 2018, pp.340-343

53. **On the Analysis of Work Accidents Data by Using Data Preprocessing and Statistical Techniques**
Akşehir Z. D., Oruc Y., Elibol A., Akleylek S., Kılıç E.
2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Kizilcahamam, Turkey, 19 - 21 October 2018, pp.649-654

54. **New Quantum Secure Key Exchange Protocols Based on MaTRU**
Akleylek S., Kaya N.
6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22 - 25 March 2018, pp.260-264

55. **TRCyberLab: An Infrastructure for Future Internet and Security Studies**
ÖZÇELİK İ., Akleylek S., ÖZÇELİK İ.
6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22 - 25 March 2018, pp.431-435

56. **Work Accident Analysis with Machine Learning Techniques**

Şahin D. Ö., Sirin B., Akleylek S., Kılıç E.
3rd International Conference on Computer Science and Engineering (UBMK), Sarajevo, Bosnia And Herzegovina, 20 - 23 September 2018, pp.215-219

57. **Generating MDS Matrices in Toeplitz Form by Using Generalised Hadamard Form**
KURT PEHLİVANOĞLU M., Akleylek S., Sakalli M. T., Duru N.
International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 3 - 04 December 2018, pp.81-86

58. **A Bayesian Network Application in Occupational Health and Safety**
Pekel E., Akşehir Z. D., Meto B., Akleylek S., Kılıç E.
3rd International Conference on Computer Science and Engineering (UBMK), Sarajevo, Bosnia And Herzegovina, 20 - 23 September 2018, pp.239-243

59. **A Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks**
Karakaya A., Akleylek S.
6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22 - 25 March 2018, pp.359-362

60. **Fast NTRU Encryption in GPU for Secure IoP Communication in Post-quantum Era**
Lee W., Goi B., Wong D. C., Yap W., Akleylek S.
IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 7 - 11 November 2018, pp.1923-1928

61. **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

62. **Computing Square Roots in Prime Fields via Singular Elliptic Curves**
AKLEYLEK S., KIRLAR B. B.
The Third International Conference on Applications of Mathematics and Informatics in Natural Sciences and Engineering (AMINSE 2017), 6 - 09 December 2017

63. **Reducing Key Sizes in Rainbow: Partially Hadamard-Rainbow**
AKLEYLEK S., ENGİN E.
The 3rd International Conference on Applications of Mathematics and Informatics in Natural Sciences and Engineering, Tiflis, Georgia, 6 - 09 December 2017, vol.3, pp.68

64. **A Reliable and Energy-Efficient Routing Protocol for Wireless Sensor Networks in Large Scale**
AKLEYLEK S., KARAGÖL S., KUTUCU H., MOHAMMADI R.
8 th International Advanced Technologies Sympoium, Elazığ, Turkey, 19 - 22 October 2017, pp.3733-3738

65. **Üç Terimli Polinomlar için Karatsuba Benzeri Çarpma Yöntemlerinin Araştırılması**
AKLEYLEK S., Kaya N.
10th International Conference on Information Security and Cryptology, 20 - 21 October 2017, vol.10, pp.1-7

66. **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

67. **An artificial bee colony algorithm for solving the weapon target assignment problem**
Durgut R., Kutucu H., Akleylek S.
7th International Conference on Information Communication and Management, ICICM 2017, Moscow, Russia, 28 - 30 August 2017, vol.Part F131202, pp.28-31

68. **Optimizing Reliability and Energy in Wireless Sensor Networks with an Effective Topology**
AKLEYLEK S., KUTUCU H., MOHAMMADI R.
International Conference on Theoretical and Application Problems of Mathematics, 25 - 26 May 2017, vol.1, pp.21

69. **Strassen-like 2x2 Matrix Squaring Revisited**
AKLEYLEK S., ŞAHİN D. Ö., KURAL O. E.

3rd International Conference on Engineering and Natural Sciences (ICENS 2017), Budapest, Hungary, 3 - 07 May 2017, pp.421

70. **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

71. **On the Design Strategies of Diffusion Layers and Key Schedule in Lightweight Block Ciphers**
KURT PEHLİVANOĞLU M., Akleylek S., SAKALLI M. T., DURU N.
2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 5 - 08 October 2017, pp.456-461

72. **A Novel Identicication 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

73. **The Trend of Business Intelligence Adoption and Maturity**
Bin Qushem U., Zeki A. M., Abubakar A., Akleylek S.
2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 5 - 08 October 2017, pp.532-537

74. **Some Results on MDS Matrices**
AKLEYLEK S., SAKALLI M. T.
9th International Conference on Information Security and Cryptology (ISCTURKEY 2016), Turkey, 25 - 26 October 2016, vol.35

75. **Speeding up Number Theoretic Transform Lazy Reductions Explained**
AKLEYLEK S., ALKIM E.
9th International Conference on Information Security and Cryptology (ISCTURKEY 2016), Turkey, 25 - 26 October 2016, vol.9, pp.115-119

76. **A Reliable and Energy Efficient Routing Protocol for Wireless Sensor Networks**
AKLEYLEK S., Mohammadi R.
International Conference on Computer Science and Engineering, Turkey, 20 - 23 October 2016, vol.75

77. **Efficient Methods for Lattice based Cryptography**
AKLEYLEK S.
The 5th International Workshop on Cryptography and its Applications - IWCA' 2016, Algeria, 26 - 27 April 2016

78. **Efficient Interleaved Montgomery Modular Multiplication Method for Sparse Polynomials for Lattice Based Cryptography**
AKLEYLEK S.
3rd International Conference on "Converging Technologies & Management (CTM-2016), India, 1 - 02 April 2016

79. **Post Quantum Cryptography An Introduction**
AKLEYLEK S.
3rd INTERNATIONAL CONFERENCE ON CONVERGENCE TECHNOLOGY MANAGEMENT (CTM-2016), India, 1 - 02 April 2016

80. **On the efficiency of polynomial multiplication for lattice-based cryptography on GPUs using CUDA**
Akleylek S., Dağdelen Ö., Tok Z. Y.
2nd International Conference on Cryptography and Information Security in the Balkans, BalkanCryptSec 2015, Koper, Slovenia, 3 - 04 September 2015, vol.9540, pp.155-168

81. **An efficient lattice-based signature scheme with provably secure instantiation**
Akleylek S., Bindel N., Buchmann J., Krämer J., Marson G. A.
8th International Conference on the Theory and Application of Cryptographic Techniques in Africa, AFRICACRYPT 2016, Fes, Morocco, 13 - 15 April 2016, vol.9646, pp.44-60

82. **Arithmetic Operations in Lattice Based Cryptography**
AKLEYLEK S.
International Scientific Conference of Students and Young Scientists Theoretical and Applied Aspects of

Cybernetics, Kiev, Ukraine, 23 - 27 November 2015

83. **Data Storage of Electronic Exams**
Ölçüoğlu L. T., AKLEYLEK S.
Proceedings of 8th International Conference on Information Security and Cryptology (ISCTURKEY 2015), Ankara, Turkey, 30 - 31 October 2015

84. **Multiplication in a Galois Ring**
Akleylek S., ÖZBUDAK F.
7th International Workshop on Signal Design and Its Applications in Communications (IWSDA), Bengaluru, India, 13 - 19 September 2015, pp.28-32

85. **Efficient Arithmetic for Lattice Based Cryptography on GPU Using CUDA**
AKLEYLEK S., Yüce Tok Z.
IEEE 22nd Signal Processing and Communications Applications Conference, Trabzon, Turkey, 23 - 25 April 2014, pp.854-857

86. **EFFICIENT ARITHMETIC FOR LATTICE-BASED CRYPTOGRAPHY ON GPU USING THE CUDA PLATFORM**
Akleylek S., Tok Z. Y.
22nd IEEE Signal Processing and Communications Applications Conference (SIU), Trabzon, Turkey, 23 - 25 April 2014, pp.854-857

87. **Kriptoloji ve Uygulama Alanları Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta**
AKLEYLEK S., YILDIRIM H. M., Yüce Z.
Akademik Bilişim 2011, Malatya, Turkey, 2 - 04 February 2011, pp.723-728

88. **Polynomial multiplication over binary fields using charlier polynomial representation with low space complexity**
Akleylek S., CENK M., ÖZBUDAK F.
11th International Conference on Cryptology in India, INDOCRYPT 2010, Hyderabad, India, 12 - 15 December 2010, vol.6498 LNCS, pp.227-237

89. **Faster Montgomery modular multiplication without pre-computational phase for some classes of finite fields**
Akleylek S., CENK M., ÖZBUDAK F.
25th International Symposium on Computer and Information Sciences, ISCIS 2010, London, England, 22 - 24 September 2010, vol.62 LNEE, pp.405-408

90. **The Third International Conference onProblems of Cybernetics and Informatics**
NURIYEV U., EMMUNGİL L., AKLEYLEK S.
Problems of Cybernetics and Informatics, PCI' 2010, Baku, Azerbaijan, 08 September 2010, pp.211-212

91. **Open Source UTM Alternative ClearOS**
AKLEYLEK S., EMMUNGİL L., NURIYEV U.
Proceeding of the third International Conference "Problems of Cybernetics and Informatics, 08 September 2010

92. **Substitution Boxes of the Third Generation GSM and Advanced Encryption Standard Ciphers**
AKLEYLEK S., Diker Yücel M.
Information Security and Cryptology Conference, 13 - 15 December 2007, pp.157-163

93. **A note on Knapsack Cryptosystems**
AKLEYLEK S., EMMUNGİL L., NURIYEV U.
International scientific conference "Information Technologies and Telecommunications in Education and Science, 06 October 2007

94. **Security Analysis and Proposed Solutions About Wireless Campus Networks of Universities in Türkiye**
EMMUNGİL L., AKLEYLEK S., NURIYEV U.
Proceeding of the 3-th International conference on Information Technologies and Telecommunication (IT T C 2007), 06 October 2007

95. **Steganography and new implementation of steganography Steganografi ve steganografinin yeni bir uygulamasi**
Akleylek S., NURİYEV U.

IEEE 13th Signal Processing and Communications Applications Conference, SIU 2005, Kayseri, Turkey, 16 - 18 May 2005, vol.2005, pp.64-67

96. **Securty of online Learning**
NURIYEV U., ÖZARSLAN S., AKLEYLEK S.
International scientific conference "Information Technologies and Telecommunications in Education and Science" (IT T ES'2005), 22 May 2005

Academic and Administrative Experience

2023 - Continues	**Program Koordinatörü**	University of Tartu, Institute of Computer Science, Chair of Security and Computer Science
2022 - Continues	**Director of the Center**	Ondokuz Mayis University, Siber Güvenlik ve Bilişim Teknolojileri Uygulama ve Araştırma Merkezi
2017 - Continues	**Head of Department**	Ondokuz Mayis University
2019 - 2022	**Head of Department**	Ondokuz Mayis University
2016 - 2021	**Head of Department**	Ondokuz Mayis University
2014 - 2014	**Head of Department**	Ondokuz Mayis University

Courses

SONLU CİSİM ARİTMETİĞİ VE UYGULAMALARI, Postgraduate, 2015 - 2016, 2013 - 2014, 2012 - 2013
Bilgisayar Mühendisliğinde Matematiksel Teknikler, Undergraduate, 2015 - 2016
AYRIK MATEMATİK, Undergraduate, 2015 - 2016, 2013 - 2014, 2012 - 2013
KRİPTOGRAFİ MÜHENDİSLİĞİNE GİRİŞ, Postgraduate, 2015 - 2016, 2013 - 2014, 2012 - 2013
Mesleki İngilizce 1, Undergraduate, 2015 - 2016
Doğrusal Cebir, Undergraduate, 2013 - 2014, 2012 - 2013
Bilgisayar Mühendisliğinde Özel Konular, Undergraduate, 2013 - 2014, 2012 - 2013
Sayılar Teorisi ve Uygulamaları, Undergraduate, 2013 - 2014
Özdevinirler Kuramı, Undergraduate, 2013 - 2014, 2012 - 2013
Sayısal Çözümleme, Undergraduate, 2013 - 2014, 2012 - 2013
Doğrusal Cebir, Undergraduate, 2011 - 2012
Sayısal Çözümleme, Undergraduate, 2011 - 2012
Kriptografi Mühendisliğine Giriş, Postgraduate, 2011 - 2012
Özdevinirler Kuramı, Undergraduate, 2011 - 2012
Ayrık Matematik, Undergraduate, 2011 - 2012

Advising Theses

, Akleylek S., SERVİS SAĞLAYICI VE SIM KART ARASINDA KUANTUM SONRASI GÜVENLİ HABERLEŞME İÇİN YENİ BİR MODEL, Doctorate, E.KARACAN(Student), 2023
Akleylek S., Blokzincirde Akıllı Sözleşmeler ve Güvenli E-Cüzdan Uygulaması, Postgraduate, E.ALBAYRAK(Student), 2023
Akleylek S., Quality of service and DDos attacks detection improvement with deep flows discrimination in SDNS, Doctorate, R.MOHAMMADI(Student), 2022
Akleylek S., Quantum secure lattice-based group signature and encryption schemes, Doctorate, M.SOYSALDI(Student),

2022
Sedat A., Efficient multivariate-based ring signature schemes, Doctorate, M.DEMİRCİOĞLU(Student), 2022
Akleylek S., Sis bilişim ve IoT tabanlı sağlık ve taktik analiz izleme modeli, Doctorate, A.KARAKAYA(Student), 2021
Sedat A., Çok değişkenli polinom sistemlerine dayanan kuantum sonrası güvenilir şifreleme sistemleri ve açık kaynak kodlu uygulamaları, Postgraduate, R.KOYUTÜRK(Student), 2020
Akleylek S., Kafes tabanlı yeni kimliği doğrulanmış anahtar değişim protokolü ve uzlaşma mekanizmaları, Postgraduate, K.SEYHAN(Student), 2020
Akleylek S., Çok değişkenli polinom sistemlerine dayalı kuantum bilgisayarlar sonrası güvenilir yeni kimlik doğrulama ve imzalama şemaları, Postgraduate, M.SOYSALDI(Student), 2018
Sedat A., On the efficiency of lattice-based cryptographic schemes on graphical processing unit, Doctorate, Z.YÜCE(Student), 2016
Sedat A., Secure electronic exam, Doctorate, L.TARKAN(Student), 2016
Sedat A., Results on the multiplication in finite fields of characteristic three using modified polynomial representation and normal elements in binary fields, Doctorate, C.ÖZEL(Student), 2013

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
Akleylek S., SİMETRİK ANAHTARLI ŞİFRELERDE İKİLİ DOĞRUSAL DÖNÜŞÜM GELİŞTİRİLMESİ İÇİN BİR YÖNTEM, Patent, CHAPTER B Implementation of Operations; Transport, The Invention Registration Number: TR2015 05618 B , Standard Registration, 2021

Activities in Scientific Journals

PEERJ COMPUTER SCIENCE, Assistant Editor/Section Editor, 2019 - Continues
IEEE ACCESS, Editor, 2019 - Continues
TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, Editor, 2017 - Continues
INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, First Editor, 2012 - Continues

Research Areas

Information Theory, Complexity Theory, Information Security and Reliability, Cryptography, Quantum Cryptography, Software Security, Quantum Calculation, Software, Software Engineering, Computer Science, Field Theory and Polynomials, Number Theory