Muslum Ozgur Ozmen

✉ moozmen@asu.edu Brickyard Engineering 396, 699 S Mill Ave, Tempe, AZ 85281
https://ozgurozmen.github.io/ · Google Scholar

Education

Jan 2020 — Aug 2024	**Ph.D. in Computer Science** Advisor: Prof. Z. Berkay Celik Purdue University	West Lafayette, IN, USA
Sept 2016 — June 2018	**MS in Computer Science** Advisor: Prof. Attila Altay Yavuz Oregon State University	Corvallis, OR, USA
Sept 2012 — June 2016	**BS in Electrical and Electronics Engineering** Bilkent University	Ankara, Turkey

Research Interests

My research interests broadly lie in the area of **system security**. Through **system design**, **formal methods**, **machine learning**, and **applied cryptography**, my research seeks to improve the security and privacy guarantees in emerging computing platforms and their interactions with physical spaces. My research approach is best illustrated by my work in IoT and CPS safety and security.

Research and Professional Experience

Assistant Professor **Aug 2024 - Present**
School of Computing and Augmented Intelligence, Arizona State University

Lead Graduate Student **2022 - 2024**
Prof. Celik's Research Group, Purdue University

Cyber-Physical Systems Research Intern **2023**
Toyota Research Institute North America, Supervisors: Dr. Georgios Fainekos and Dr. Bardh Hoxha

Publications

Peer-reviewed conference publications:

C32 Doguhan Yeke, Kartik A. Pant, **Muslum Ozgur Ozmen**, Hyungsub Kim, James M. Goppert, Inseok Hwang, Antonio Bianchi, and Z. Berkay Celik. *Automated Discovery of Semantic Attacks in Multi-Robot Navigation Systems.* USENIX Security Symposium 2025.

C31 Edwin Kayang, Mishel Jyothis Paul, Eric Jahns, **Muslum Ozgur Ozmen**, Milan Stojkov, Kevin Rudd, and Michel A. Kinsy. *R-Visor: An Extensible Dynamic Binary Instrumentation and Analysis Framework for Open Instruction Set Architectures.*ACM SIGPLAN/SIGBED International Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES) 2025.

C30 Thea U. Kjeldsmark, Hui Zhuang, Habiba Farrukh, and **Muslum Ozgur Ozmen**. *Intermittent Power, Continuous Protection: Security and Privacy for Batteryless Devices in IoT.* International Workshop on Security and Privacy of Sensing Systems 2025.

C29 **Muslum Ozgur Ozmen**, Mehmet Oguz Sakaoglu, Jackson Bizjak, Jianliang Wu, Antonio Bianchi, Dave Jing Tian, and Berkay Celik. *Why Am I Seeing Double? An Investigation of Device Management Flaws in Voice Assistant Platforms.* PoPETs 2025. (Acceptance Rate: 28%)

C28 Arjun Arunasalam, Jason Tong, Habiba Farrukh, **Muslum Ozgur Ozmen**, Koustuv Saha, and Z. Berkay Celik. *Deceptive Sound Therapy on Online Platforms: Do Mental Wellbeing Tracks Conform to User Expectations?* International AAAI Conference on Web and Social Media (ICWSM) 2025.

C27 **Muslum Ozgur Ozmen**, Habiba Farrukh and Z. Berkay Celik. *Physical Side-Channel Attacks against Intermittent Devices.* PoPETs 2024. (Acceptance Rate: 19.5%)

C26 Syed Ghazanfar Abbas, **Muslum Ozgur Ozmen**, Abdulellah Alsaheel, Arslan Khan, Z. Berkay Celik and Dongyan Xu. *SAIN: Improving ICS Attack Detection Sensitivity via State-Aware Invariants.* Usenix Security 2024. (Acceptance Rate: 18.3%)

C25 Hyungsub Kim, Rwitam Bandyopadhyay, **Muslum Ozgur Ozmen**, Z. Berkay Celik, Antonio Bianchi, Yongdae Kim and Dongyan Xu. *A Systematic Study of Physical Sensor Attack Hardness.* IEEE S&P 2024. (Acceptance Rate: 17.8%)

C24 Arjun Arunasalam, Andrew Chu, **Muslum Ozgur Ozmen**, Habiba Farrukh, and Z. Berkay Celik. *The Dark Side of E-Commerce: Dropshipping Abuse as a Business Model.* Network and Distributed System Security Symposium (NDSS) 2024. (Acceptance Rate: 20.2%)

C23 **Muslum Ozgur Ozmen**, Ruoyu Song, Habiba Farrukh and Z. Berkay Celik. *Evasion Attacks and Defenses on Smart Home Physical Event Verification.* Network and Distributed System Security Symposium (NDSS) 2023. (Acceptance Rate: 16.2%)

C22 Habiba Farrukh*, **Muslum Ozgur Ozmen***, Kerem Ors and Z. Berkay Celik. *One Key to Rule Them All: Secure Group Pairing for Heterogeneous IoT Devices.* IEEE S&P 2023. – equally contributed. (Acceptance Rate: 17%)

C21 **Muslum Ozgur Ozmen***, Habiba Farrukh*, Hyungsub Kim, Antonio Bianchi and Z. Berkay Celik. *Rethinking Secure Pairing in Drone Swarms.* VehicleSec 2023. – equally contributed.

C20 Ruoyu Song, **Muslum Ozgur Ozmen**, Hyungsub Kim, Raymond Muller, Z. Berkay Celik, and Antonio Bianchi. *Discovering Adversarial Driving Maneuvers against Autonomous Vehicles.* Usenix Security 2023. (Acceptance Rate: 29%)

C19 Hyungsub Kim, **Muslum Ozgur Ozmen**, Z. Berkay Celik, Antonio Bianchi and Dongyan Xu. *PatchVerif: Discovering Faulty Patches in Robotic Vehicles.* Usenix Security 2023. (Acceptance Rate: 29%)

C18 Khaled Serag, Rohit Bhatia, Akram Faqih, **Muslum Ozgur Ozmen**, Vireshwar Kumar, Z. Berkay Celik, Dongyan Xu. *ZBCAN: A Zero-Byte CAN Defense System.* Usenix Security 2023. (Acceptance Rate: 29%)

C17 **Muslum Ozgur Ozmen**, Xuansong Li, Andrew Chu, Z. Berkay Celik, Bardh Hoxha and Xiangyu Zhang. *Discovering IoT Physical Channel Vulnerabilities.* ACM Conference on Computer and Communications Security (ACM CCS) 2022. (Acceptance Rate: 22%)

C16 Hyungsub Kim, **Muslum Ozgur Ozmen**, Z. Berkay Celik, Antonio Bianchi and Dongyan Xu. *PGPATCH: Policy-Guided Logic Bug Patching for Robotic Vehicles.* IEEE S&P 2022. (Acceptance Rate: 14.5%)

C15 Andrew Chu, Arjun Arunasalam **Muslum Ozgur Ozmen** and Z. Berkay Celik. *Behind the Tube: Exploitative Monetization of Content on YouTube.* Usenix Security 2022. (Acceptance Rate: 17.2%)

C14 Hyungsub Kim, **Muslum Ozgur Ozmen**, Antonio Bianchi, Z. Berkay Celik and Dongyan Xu. *PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles.* Network and Distributed System Security Symposium (NDSS) 2021. (Acceptance Rate: 15.2%)

C13 Furkan Goksel*, **Muslum Ozgur Ozmen***, Michael Reeves, Basavesh Shivakumar and Z. Berkay Celik. *On the Safety Implications of Misordered Events and Commands in IoT Systems.* IEEE Workshop on the Internet of Safe Things (SafeThings) 2021. – equally contributed.

C12 Rouzbeh Behnia, Attila Yavuz, **Muslum Ozgur Ozmen** and Tsz Hon Yuen. *Compatible Certificateless and Identity-Based Cryptosystems for Heterogeneous IoT.* International Conference on Information Security (ISC) 2020.

C11 Efe U. A. Seyitoglu, Attila Yavuz and **Muslum Ozgur Ozmen**. *Compact and Resilient Cryptographic Tools for Digital Forensics.* IEEE Conference on Communications and Network Security (IEEE CNS) 2020. **(Best Paper Award Finalist)**

C10 **Muslum Ozgur Ozmen**, Attila Yavuz and Rouzbeh Behnia. *Energy-Aware Digital Signatures for Embedded Medical Devices.* IEEE Conference on Communications and Network Security (IEEE CNS) 2019.

C9 Rouzbeh Behnia, **Muslum Ozgur Ozmen** and Attila Yavuz. *ARIS: Authentication for Real-Time IoT Systems.* International Conference on Communications (IEEE ICC) 2019.

C8 **Muslum Ozgur Ozmen**, Rouzbeh Behnia and Attila Yavuz. *Fast Authentication from Aggregate Signatures with Improved Security.* Financial Cryptography and Data Security (FC) 2019. (Acceptance Rate: 21.9%)

C7 Thang Hoang, **Muslum Ozgur Ozmen**, Yeongjin Jang and Attila Yavuz. *Hardware-Supported ORAM in Effect: Practical Oblivious Search and Update on Very Large Dataset.* PoPETs, 2019. (Acceptance Rate: 22%)

C6 Rouzbeh Behnia, **Muslum Ozgur Ozmen**, Attila Yavuz and Mike Rosulek. *TACHYON: Fast Signatures from Compact Knapsack.* ACM Conference on Computer and Communications Security (ACM CCS) 2018. (Acceptance Rate: 16.6%)

C5 **Muslum Ozgur Ozmen** and Attila Yavuz. *Dronecrypt-An Ultra-Low Energy Cryptographic Framework for Small Aerial Drones.* IEEE MILCOM 2018.

C4 **Muslum Ozgur Ozmen**, Rouzbeh Behnia and Attila Yavuz. *Compact Energy and Delay-Aware Authentication.* IEEE Conference on Communications and Network Security (IEEE CNS) 2018.

C3 **Muslum Ozgur Ozmen**, Thang Hoang and Attila Yavuz. *Forward-Private Dynamic Searchable Symmetric Encryption with Efficient Search.* International Conference on Communications (IEEE ICC) 2018.

C2 **Muslum Ozgur Ozmen** and Attila Yavuz. *Low-Cost Standard Public Key Cryptography Services for Wireless IoT Systems.* Workshop on Internet of Things Security and Privacy (IoT S&P) 2017 (Affiliated with ACM CCS).

C1 Rouzbeh Behnia, Attila Yavuz and **Muslum Ozgur Ozmen**. *High-Speed High-Security Public Key Encryption with Keyword Search.* IFIP Annual Conference on Data and Applications Security and Privacy (DBSec) 2017.

Peer-reviewed journal publications:

J3 Luigi Mastromauro, Dhiego Souto Andrade, **Muslum Ozgur Ozmen**, and Michel Kinsy. *Survey of Attacks and Defenses on Consensus Algorithms for Data Replication in Distributed Systems.* IEEE Access 2025.

J2 Attila Yavuz and **Muslum Ozgur Ozmen**. *Ultra Lightweight Multiple-time Digital Signature for the Internet of Things Devices.* IEEE Transactions on Services Computing (IEEE TSC), 2019.

J1 Rouzbeh Behnia, **Muslum Ozgur Ozmen** and Attila Yavuz. *Lattice-Based Public Key Encryption with Keyword Search from Experimental Perspectives.* IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), 2018.

Patents

P4 **Muslum Ozgur Ozmen**, Rouzbeh Behnia and Attila Yavuz. *Algebraic proof-of-work algorithm for blockchains*, US Patent 12,231,568

P3 Rouzbeh Behnia, **Muslum Ozgur Ozmen** and Attila Yavuz. *Efficient Identity-Based and Certificateless Cryptosystems*, US Patent 10,673,625

P2 Attila Yavuz, **Muslum Ozgur Ozmen** and Rouzbeh Behnia. *Energy-aware Digital Signatures*, US Patent 10,547,455

P1 Thang Hoang, **Muslum Ozgur Ozmen**, and Attila Yavuz *Forward-Private Dynamic Searchable Symmetric Encryption with Efficient Search*, US Patent 10,922,273

Teaching Experience

Instructor:

- CSE230 - Computer Organization and Assembly Language, Arizona State University — Fall 2025
- CSE230 - Computer Organization and Assembly Language, Arizona State University — Fall 2024

Guest Lecturer:

- CS390 - Great Issues in Computer Science, Purdue University — Fall 2023
- CS426 - Computer Security, Purdue University — Spring 2023
- CS590 - IoT & CPS Security, Purdue University — Spring 2022

Invited Talks

I3 *Discovering IoT Physical Channel Vulnerabilities.* CCI Workshop on Privacy-Preserving and Trustworthy Ubiquitous Computing, Virginia Tech, May 2024.

I2 *Compositional Safety and Security Reasoning in IoT Environments.* University of California Santa Cruz. Virtual, February 2023.

I1 *Lightweight, Delay-Aware and Scalable Cryptographic Services for Smart-Grid Systems.* Cyber Resilient Energy Delivery Consortium (CREDC) Pacific Northwest Industry Workshop. Richland, WA, USA, November 2017.

Current Students

Argha Dhar	PhD Computer Science, Arizona State University
Yaphet Weldegebriel (Co-advised)	PhD Computer Science, Arizona State University
Aniruddha Sawant	PhD Computer Engineering, Arizona State University
Scott Mountjoy	PhD Computer Science, Arizona State University
Hui Zhuang (FURI-funded)	BS Computer Science, Arizona State University
Andrew Postik (FURI-funded)	BS Computer Science, Arizona State University

Past Students

Aniruddha Sawant	MS Computer Science, ASU → PhD ASU	2024 - 2025
Leo Lin	MS Computer Science, Purdue → Ph.D. Purdue	2024 - 2025
Ben Chen	MS Computer Science, Purdue → Ambient Security	2022 - 2024
Andrew Chu	BS Computer Science, Purdue → Ph.D. University of Chicago	2020 - 2021
Ruoyu Song	BS Computer Science, Purdue → Ph.D. Purdue	2020

Furkan Goksel	BS Computer Science, METU → Picus Security	Summer 2020
Kerem Ors	BS Computer Science, Sabanci Uni → Ph.D. Purdue	Summer 2020

Services

Organizing Committee Member:

- Security and Privacy in Cyber-Physical Systems and Smart Vehicles (SmartSP) 2025, 2026

Program Committee Member:

- ACM Conference on Computer and Communications Security (ACM CCS) 2026
- Network and Distributed System Security (NDSS) Symposium 2026
- Privacy Enhancing Technologies (PETs) 2026
- IEEE Symposium on Security and Privacy (S&P) 2025, 2026
- International Symposium on Research in Attacks, Intrusions and Defenses (RAID) 2025
- IEEE Computer Security Foundations (CSF) 2025
- IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2025
- ACM Conference on Data and Application Security and Privacy (CODASPY) 2024
- Symposium on Vehicle Security and Privacy (VehicleSec) 2024, 2025
- IEEE International Conference on Smart Grid Communications (SmartGridComm) 2023, 2024
- IEEE/ACM Workshop on the Internet of Safe Things (SafeThings) 2023, 2024, 2025

Reviewer:

- NSF Review Panel 2024, 2025
- IEEE Transactions on Dependable and Secure Computing (TDSC) - 2024, 2025
- IEEE Transactions on Automation Science and Engineering (TASE) - 2024, 2025
- ACM Transactions on Internet Technology (TOIT) - 2024
- ACM Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/Ubicomp) - 2023
- IEEE Transactions on Information Forensics and Security (TIFS) - 2023, 2024
- ACM Transaction on Internet of Things (TIOT) - 2023
- IEEE Internet of Things Journal (IoT-J) - 2022, 2024
- IEEE Transactions on Services Computing (TSC) - 2020

External Reviewer:

- IEEE Symposium on Security and Privacy (S&P) 2023, 2024
- Usenix Security 2022, 2023, 2024
- Network and Distributed System Security Symposium (NDSS) 2022, 2023, 2024, 2025
- ACM Conference on Computer and Communications Security (CCS) 2021
- Annual Computer Security Applications Conference (ACSAC) 2017, 2018, 2019, 2022
- International World Wide Web Conference (WWW) 2019

Awards and Honors

- Diamond Award for academic excellence from the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University, 2024.
- Purdue CS Department's merit recognition award, 2024.
- Served at the Student Advisory Council of *NSF AI Institute for Agent-based Cyber Threat Intelligence and Operation (ACTION)*, 2023-2024.
- Invited as a panelist to *NSA's Center of Academic Excellence in Cybersecurity Research Symposium 2023* to present my dissertation research on IoT/CPS security to practitioners and government agencies for real-world adoption.
- IEEE CNS 2020 Best Paper Award Finalist