WE INTEGRATE
HARDWARE, SOFTWARE, AI ALGORITHMS, AND DATA FOR SCALABLE MACHINE LEARNING AND SECURITY

REAL-TIME DATA ANALYTICS
Hardware, software and algorithm co-design for real-time data analytics. Our customized performance optimization engine is automated and works across platforms, from low-power sensors to data centers and the cloud. Our solutions integrate adaptive data collection processes with training, learning, and inference in real-time and streaming applications.

PARADIGM SHIFT IN DEEP LEARNING
Automated acceleration and adaptive retraining of deep learning. Our framework allows for training of deep learning networks that are platform independent, and scale from sensors to mobile to data centers. We introduced a paradigm shift when we built and demonstrated the first training of deep learning on Edge devices.

SECURITY AND PRIVACY FOR CYBER-PHYSICAL SYSTEMS
To secure cyber-physical systems, we fully consider hardware, software, algorithms and data – and their isolation and interactions. We offer new approaches to security and privacy. Safe machine learning / defense against adversarial attacks, secure embedded medical devices, and privacy-preserving computing (DNA, learning, biometrics) are examples.
Our work is crucial for developing scalable and secure machine intelligence for cloud computing, data centers, Internet of Things, drone-based search and rescue, imaging systems, low-power sensor networks, and many other applications.

**CENTER LEADERSHIP**

Farinaz Koushanfar  
Center Co-Director
Accelerated and domain-specific machine learning (ML), safe and secure ML, private ML, embedded and hardware systems, security and trust

Tara Javidi  
Center Co-Director
Practical solutions with theoretical guarantees for information acquisition, processing, and communication

**CENTER FACULTY**

Ilkay Altintas  
Makes computational data science more reusable, scalable and reproducible through methods and tools for workflows for problem solving

Kamalika Chaudhuri  
Trustworthy machine learning, learning and active learning theory

Pamela Cosman  
Image and video compression, processing, and wireless communications

Hadi Esmaeilzadeh  
Immersive machine intelligence, full-stack solutions

Andrew Kahng  
Physical design of VLSI

Ryan Kastner  
Embedded security, hardware and FPGA acceleration; FPGAs; reconfigurable computing

Duygu Kuzum  
In-memory computing with emerging non-volatile memory devices, neuromorphic computing, brain interfaces

Siavash Mirarab  
Scalable analysis of large-scale biological datasets

Truong Nguyen  
Image and video processing on low-power, low-cost systems

Alon Orlitsky  
Estimation, learning, and speech processing

Piya Pal  
High dimensional statistical signal processing, high resolution imaging

Bhaskar Rao  
Signal processing, estimation theory, speech processing

Tajana Simunic Rosing  
Embedded system design and software optimization, power management

Deian Stefan  
Systems, security, and programming languages

Behrouz Touri  
Dynamics and controls over complex networks, distributed optimization and computation

Nuno Vasconcelos  
Statistical signal processing, computer vision, machine learning, multimedia

Jishen Zhao  
Memory and storage architecture and systems, domain-specific acceleration, software/hardware co-design

**BENEFITS OF PARTNERSHIP**

- Develop Masters and PhD talent pipeline
- Partner-only recruiting events
- Industry-faculty-student research teams
- Embed a Visiting Industry Fellow
- Influence research priorities
- First look at new discoveries
- Research portfolio management
- Center Advisory Board membership
- Fast-track research agreements
- Research Summits, workshops, and more

**CONTACT**

Luciana Xavier  
Director for Corporate Research Partnerships  
lxavier@eng.ucsd.edu

**Partners**

Cubic  
Leidos  
Qualcomm