MASSACHUSETTS INSTITUTE OF TECHNOLOGY

MIT Campus

The **Massachusetts Institute of Technology (MIT)** community is driven by a shared purpose: to make a better world through education, research, and innovation. Our graduates have invented fundamental technologies, launched new industries, and created millions of American jobs. Through teaching, research, and innovation, MIT's exceptional community pursues its mission of service to the nation and the world.

The Electrical Engineering and Computer Science (EECS) Department at MIT is where the future is invented. EECS brings the world's most brilliant faculty and students together to innovate and explore foundational hardware and software systems, cutting-edge machine learning models and computational methods to address critical societal problems.

DESIGNATIONS

- **CAE-Research**

CONTACT INFORMATION

Srini Devadas
devadas@mit.edu

Jeremy Kepner
kepner@mit.edu

www.mit.edu | www.eecs.mit.edu

EECS research in security and cryptography is focused on making future computer systems more secure, and protecting the privacy of data and individuals. We employ cross-cutting techniques from theoretical cryptography and programming-language ideas, to low-level hardware and operating-systems security, to overall system designs and empirical bug-finding. These techniques are applied to a wide range of application domains, such as blockchains, cloud systems, Internet privacy, machine learning, and Internet-of-Things devices.

Cybersecurity researchers at MIT are supported by a wide range of laboratories, centers, and institutes that develop techniques for securing tomorrow's global information infrastructure by exploring theoretical foundations, near-term practical applications, and long-range speculative research. Seeking to understand the theoretical power of cryptography and the practical engineering of secure information systems, from appropriate definitions and proofs of security, through cryptographic algorithm and protocol design, to implementations of real applications with easy-to-use security features.

We research, develop, evaluate, and deploy tools and systems designed to ensure objectives despite cyber-attacks. We have deep connections to other computing fields through complexity theory, quantum computing, algorithms, machine learning, and cryptographic policy. Our work provides global policymakers with technically grounded guidance for cybersecurity, Internet privacy, and more.