



IEEE International Symposium on Secure and Private Execution  
Environment Design (SEED)

Worldwide Virtual Event, September 20-21, 2021

Web: <https://seed-symposium.org>

Contact: [seed21chairs@gmail.com](mailto:seed21chairs@gmail.com)

## CALL FOR PAPERS

The IEEE International Symposium on Secure and Private Execution Environment Design (SEED) is a forum which brings together researchers from the computer architecture and computer security communities into one venue that focuses on the design of architectural and system primitives which provide secure and private execution environments for applications, containers, or virtual machines.

SEED primarily focuses on research topics spanning across the boundaries of computer architecture, systems, and security. Papers are solicited on a range of topics, including (but not limited to):

- Architecture, operating systems, and programming models and language for supporting secure and private execution
- Novel Designs for secure and private execution environments for GPUs, accelerators, and FPGAs
- Architectural support for new security primitives
- Novel cryptographic hardware designs for secure and private execution
- Models and analysis of performance-security trade-offs in the design of a secure execution environment
- Evaluation of security vulnerabilities in post-Moore's Law technologies, e.g. persistent memory, quantum computing
- Demonstration and mitigation of architectural side channels, covert channels and other security vulnerabilities
- Metrics for measuring architecture-related security vulnerabilities
- Compiler and code generation techniques for mitigating architecture-induced side and covert channels and other vulnerabilities

## PAPER TYPES

SEED will accept one of four types of papers: (1) regular papers of 11 pages, (2) SoK papers of 11 pages, (3) Seeds of SEED papers of 6 pages, or (4) WiP paper of 6 pages. The primary focus of the regular papers should be to describe new research ideas overlapping computer architecture/systems and security, supported by experimental implementation and evaluation of the proposed research ideas. Systemization of Knowledge (SoK) papers are also welcome and should be submitted as regular papers. The primary focus of "Seeds of SEED" should be to describe the promising designs, initial development, and preliminary evaluation of new ideas critical to the security of future architecture/systems. Contributions from industry, that bring awareness to a new security problem and/or lay vision for sound architecture/systems security principles, are especially encouraged for Seeds of SEED papers. Additionally, we accept Work-in-Progress (WiP) papers that should describe novel secure systems designs supported by experiments. For papers accepted under WiP category, the authors will make a presentation and include the title and a brief abstract on the conference website.

## **IMPORTANT DATES**

Combined Abstract and Full Paper Deadline: June 14, 2021 at 11:59 PM AoE

Rebuttal Period: TBD

Author Notification: July 31, 2021

Camera-ready Submission: August 15, 2021

Conference Dates: September 20-21, 2021

## **ORGANIZATION**

General Chairs: Jakub Szefer (Yale Univ.) and Yan Solihin (Univ. of Central Florida)

Program Chairs: Guru Venkataramani (George Washington Univ.) and Yinqian Zhang (SUSTech)

## **STEERING COMMITTEE**

Todd Austin (U. of Michigan)

David Kaeli (Northeastern U.)

Ruby Lee (Princeton)

Milos Prvulovic (Ga. Tech)

Deborah Shands (SRI)

Yan Solihin - Chair (U. of Central Florida)

Guru Venkataramani (GWU)