Confidential Computing Consortium Research Fund

Confidential Computing Consortium Research Call for Proposals

About

The Confidential Computing Consortium (CCC) is pleased to invite university faculty to respond to this call for research proposals on Confidential Computing; up to 2 awards are available. We are interested in making awards on a wide range of Confidential Computing research, including, but not limited to:

- Formal verification of trusted execution environments (TEEs), secure enclaves, and related components.
- New approaches to attestation and trusted boot in Confidential Computing environments.
- Novel cryptographic techniques and protocols for data privacy and integrity in Confidential Computing.
- Secure software development life cycles (SDLC) for confidential applications.
- Performance and scalability analysis of Confidential Computing solutions, including overheads and optimization techniques.
- Threat modeling and security analysis of Confidential Computing platforms and use cases.
- Integration of Confidential Computing with emerging technologies like AI/ML, blockchain, and federated learning.
- Confidential computing in cloud-native environments, including containers and serverless functions.
- Hardware-software co-design for future Confidential Computing architectures.
- Novel use cases and applications of Confidential Computing in various sectors (e.g., healthcare, finance, government).
- Approaches to improving developer experience and tooling for Confidential Computing.
- Policy-based access control and data governance in Confidential Computing.
- Confidential Computing in multi-party computation (MPC) and homomorphic encryption (HE) contexts.
- Approaches to addressing side-channel attacks and other TEE vulnerabilities.
- Techniques for secure data sharing and collaboration between organizations using Confidential Computing.
- Scalable methods of employing and benefiting from CC in and across the breadth of the software supply chain.
- Reference designs for various attestation models

- Composite attestation processes
- Geofencing and Confidential Computing
- Mitigation for availability and DoS attacks TEEs
- Time and attestation - ephemeral vs long-lived attestation strategies as combined with systems such as Certificate Authorities and IDMs
- Constant time cryptography and TEEs
- Trust models and TCB options for Confidential VMs

To Apply

Applicants should submit the contents mentioned under the requirements section to research@confidentialcomputing.org considering the timelines mentioned below. Funding will range from $25,000 to $50,000 per proposal, depending on the specific requirements.

Application Timeline

[Timeline information to be inserted here]

Requirements

Proposals should include:

- A summary of the project (2 pages maximum) explaining the area of focus, a description of techniques, any relevant prior work, and a timeline with milestones and expected outcomes.
- A draft budget description (1 page) including an approximate cost of the award and an explanation of how funds would be spent.
- Curriculum Vitae for all project participants.
- Organization details including tax information and administrative contact details.

Eligibility

- Awards must comply with applicable U.S. and international laws, regulations and policies.
- Applicants must be current full-time faculty at an accredited academic institution that awards research degrees to PhD students or at a reputed research institute.
- Applicants must be the Principal Investigator on any resulting award.

Additional Information

Payment will be made to the proposer’s host university as an unrestricted gift. Because of its nature, salary/headcount could be included as part of the budget presented for the RFP. Since

the award/gift is paid to the university, they will be able to allocate the funds to that winning project and have the freedom to use as they need. Award funds can be used to cover a researcher's salary. Typically research funds ideally cover graduate or post-graduate students' employment/tuition and other research costs (e.g., equipment, laptops, incidental costs).

Expected Outcomes - This is not in the eBPF doc.

An emphasis should be placed on open collaboration and community benefit. Therefore, we expect successful proposals to produce outcomes that contribute to the broader Confidential Computing ecosystem. This includes, but is not limited to, the publication of research findings in a public forum, the release of open source code under a permissive license, and the contribution of new features or improvements to existing open-source projects within the Confidential Computing Consortium. Awardees will be encouraged to present their work at relevant industry conferences and to engage with the community to ensure their research has a lasting and positive impact.

Terms & Conditions

By submitting a proposal, you are authorizing the Confidential Computing Consortium to evaluate the proposal for a potential award, and you agree to the terms herein.

- You agree that the Confidential Computing Consortium will not be required to treat any part of the proposal as confidential or protected by copyright.
- You agree and acknowledge that personal data submitted with the proposal, including name, mailing address, phone number, and email address of you and other named researchers in the proposal may be collected, processed, stored and otherwise used by the Confidential Computing Consortium for the purposes of evaluating the contents of the proposal.
- You acknowledge that neither party is obligated to enter into any business transaction as a result of the proposal submission, the Confidential Computing Consortium is under no obligation to review or consider the proposal, and neither party acquires any intellectual property rights as a result of submitting the proposal.

List of potential Program Committee / Topic Review members

- falder@nvidia.com
- mingshen.sun@tiktok.com
- Mona Vij
- Mike Bursell
- Dan Middleton
- Caroline Perez-Vargas
- SIG chairs