INTEL REQUEST FOR PROPOSALS

SUBJECT

Intel's University Research & Collaboration Office requests proposals for academic research on ***Secure Processor Assurance and Resilience (SPAR)***. At this point, we invite researchers in the European region. Teams in other geographies can propose research or join a proposal (if they have other funding that is compatible with our open IP approach), but they cannot be funded at this time.

KEY DATES

1. **March 13, 2023: Publication of this Call for Proposals**
2. **May 07, 2023: Submission Deadline (EoD AoE)**
3. **End of August 2023: Notifications**

OVERVIEW

Intel's University Research & Collaboration Office (URC) invites proposals to establish a new research center which will focus on the ***Secure Processor Assurance and Resilience (SPAR)***.

The goal of this research is to progress the state-of-the-art of RISC V platforms. More specifically, we aim to increase the resilience against malicious and accidental faults (RV-R) and develop new tools and methodologies to specify (RV-S) and validate (RV-P) the security of RISC V platforms. The research should contribute towards clean slate RISC-V IP that allows to build security-first processors that are simultaneously high-performance, provably correct, and resistant against advanced adversaries.

Academia has embraced RISC-V with research in instruction definition & tooling, memory models, security architectures, and implementations. However, we still see gaps that prevent academia from building a correct-by-construction RISC-V core focused on strong security guarantees with minimal reduction of performance.

PROGRAM SCOPE AND FUNDING

Intel intends to fund a new collaborative, multi-university research center addressing the Research Vectors (RVs) described in detail below. We suggest that each submitting organization focus their proposal on one or two research vectors (in line with their primary expertise) and identify key contributions that are expected.

RESEARCH VECTORS IN DETAIL

We are interested in sponsoring research that contributes to the following research vectors (in descending priority).

[RV-P] PROOF AUTOMATION & ASSURANCE

Our goal is to prove the complete functional correctness and end-to-end security properties of complex hardware designs such as RISC-V processors and Post-Quantum Cryptography (PQC) hardware accelerators. We also want to write provably correct and secure RISC-V firmware to run on top of these processors. Unfortunately, such proofs are currently beyond the capabilities of fully automated proof tools. While we aim at maximum automation, we accept that some level of interactive theorem proving is necessary. The goal of this RV is to enhance these proof frameworks such that

(1) we can formally reason about SystemVerilog designs that the hardware is written in,

(2) we can prove deep functional correctness and security properties about the RISC-V assembly code and/or C code the firmware is written in,

(3) SMT-based model checkers and other highly automated proof tools are integrated into the theorem provers in a trustworthy way such as having the tools generate proof certificates that are then checked by the theorem prover, and

(4) proof strategies for processors, RISC-V firmware, and PQC accelerators are developed that combine the automated tools in (3) with deductive reasoning so that the proof scripts are more robust to the continuing evolution of the hardware and software designs.

[RV-S] FORMAL SPECIFICATIONS

To gain practical assurance that a RISC-V processor is functionally correct and secure, we also need formal RISC-V instruction semantics that include a specification of the expected security-related behavior such as allowed timing dependencies within a sequence of instructions. This specification would then be used as input to a range of theorem provers such as ACL2 and Isabelle, as well as SystemVerilog-based validation tools such as Jasper that is used extensively within Intel and other hardware companies.

Furthermore, it is important that the translated output be close to its original source specification so that proof failures can be debugged interactively by formal verification engineers. Thus, translations are strongly preferred that avoid loop unrolling, function and expression in-lining, type erasure, etc. This may require that the translator make innovative use of the target language's higher-level features (loops, recursive functions, parameterized modules, datatypes, etc.) and automatically generate proofs that the recursive functions terminate, bit vector expressions have the correct bit-widths, and other well-formedness requirements.

[RV-R] RESILIENCE

This research vector aims to increase the resilience against attacks and faults. This includes security, reliability, and real-time guarantees in the presence of malicious adversaries. We primarily aim to protect against software-exploitable hardware bugs where an adversary can execute arbitrary code (isolated or unprivileged) to affect secrecy/integrity/availability of workloads of other users.

Our goal is to shape a science of resilience, i.e., the proposals should have precise definitions of what resilience requires for a well-defined adversary model and propose mechanisms that provide quantifiable contributions towards those specifications. Example mitigations that can be investigated include (but are not limited to)

- **Detection, containment, and recovery for advanced attacks** including SW-based fault injection or side-channel leakage
- Novel RISC-V security HW/SW architectures to **support resilience in real time**
- New paradigms for **dynamic reconfiguration** to allow in-field improvement of the security of a given SoC
- Architectures that allow **full crypto agility**, i.e. modification of cryptographic operations to address changing new threats (e.g. PQC), improved standards, or new weaknesses in deployed crypto algorithms

SUBMISSION AND EVALUATION PROCESS

The key dates are listed earlier in this document. Note that we encourage engaging before submission. This includes contacting us to share and discuss draft ideas to maximize the mutual benefits of the envisioned joint research.

PROPOSAL FORMAT

Proposals should be 4-5 pages, not including citations or cost volume. We slightly prefer proposals that define a project for one Principal Investigator (PI) for up to three years. Collaborative proposals between two Principal Investigators with complementary domain expertise are also encouraged; for example, one PI with expertise in silicon circuit design may collaborate with another PI on hardware architecture and performance optimization to fully evaluate a resilient approach. Researchers can be part of only one proposal.

Each proposal should comprise the following sections:

- **Proposal cover page (max 1/2 page)**
  - **Organization**
  - **List of PIs and the main contact person**
  - **List one or at most two targeted research vectors**
  - **Executive summary** including intended outcomes. Summarize the key elements of the proposal.

- **High-level motivation, preliminary results, approach, and proposed goals for the research questions (<= 2 pages)**. Briefly describe the motivation for the proposed project, preliminary results, techniques (especially novel ones) that underpin the approach, and the plan of tackling the proposed research questions. Summarize what will have been accomplished after 3 years if all goes according to plan. Be sure to explain the current state-of-the-art for the proposed technology (or nearest related technologies). This section must also include an explicit statement of the Intellectual Property (IP) status for all background IP related to this technology (i.e., are the property rights to this technology protected, and if so, who owns those rights).
- **Personnel plan and expertise statement (max. 1/4 page per Researcher).** Include a list of key personnel (at most 3) plus a statement on each person's role and time commitment. For each person, please add a brief bio or web page link and list their 6 most relevant prior publications (within the last 8 years) for the selected research questions.
- **Student plan (<1/4 page).** Please provide information about the PhD students and postdocs you envision to assign to this project (if known).
- **Diversity and Inclusion (<1/4 page)**. In light of Intel's strong commitment to diversity and creating an inclusive environment, please address your organization's commitment to diversity and inclusion with respect to gender, disabilities, and nationality. Provide a brief summary of your performance in this area and any initiatives you are pursuing.
- **Budget and Financials (1/4 page).** Typical grants are USD$70-140K per year for three years. We plan to work under an Open Intellectual Property model (results are published, code is open sourced). Our goal is to maximize the available research ideas for our fixed amount of total funding. Universities may propose how to achieve this. Please also indicate how many researchers (FTE) can contribute their research for the proposed funding.
- **IP-compatible funds amplification (no limit).** Describe funds you are committing to be applied towards this proposal from other compatible sources (including the University). See also below "Potential for Co-funding" under "Evaluation Criteria". If parts of the team can obtain funding for related work from other sources (including the University or government grants) and the sponsor commits to follow an OpenIP/public dedication approach for that project or provide Intel with non-exclusive, royalty-free **research and commercial** licenses to any IP, the team may list funding that would be considered to amplify the proposed project. Proposers are encouraged to simultaneously apply for public funding of their proposals through existing public funding instruments. Intel may support relevant proposal submissions via Letters of Support.
- **Citations {max 10}.**
- **Cost volume {<=1 page}**. Cost proposal in Excel or another format as appropriate.

EVALUATION CRITERIA

In order of importance, the evaluation criteria for this solicitation are as follows:

- **Potential contribution and relevance to Intel and the broader industry**: The proposed research should directly support a technology solution that addresses the RVs outlined above, leading to technological advances with the potential for ongoing technology transfer in collaboration with Intel and the broader industry.

- **Technical innovation**: Proposed solutions of interest should clearly push the boundaries of technical innovation and advancement. Research that is not of interest in this program includes incremental advancements to state-of-the-art and current design practices. Feasibility of new algorithms/techniques should be demonstrated through SW/HW implementations.
- **Potential for co-funding**: Proposals which clearly specify significant (actual or planned) cost-sharing and scope amplification (as measured, for example, by the number of engaged students and/or researchers; the utilization of high-value research infrastructure; the absorption of operational and administrative running costs) through the incorporation/sharing of compatible public matching grants will be given significant priority. To this end, we encourage proposers to apply for or incorporate existing related funding from other sources. Researchers from all countries are encouraged to apply to relevant national, multi-national and international funding instruments. Intel will support relevant applications, including applications for funding to the recent NSF-DFG joint DCL (NFS link and DFG link) for Secure and Trustworthy Cybersecurity.
- **Clarity of overall objective and success criteria**: The proposed Research Plan should clearly convey that the PIs have the knowledge and capability to achieve the stated research goals. It is understood that any research program will have uncertainties and unanswered questions at the proposal stage, but a clear path forward in key challenge areas must be identified and justified. Teams are expected to demonstrate progress toward project goals at quarterly milestones and monthly project status updates. As detailed in "Program Scope and Funding" section, the proposal should explicitly point out which RV is being addressed, the synergy among them if more than one RV, the plan and milestones towards building research prototypes, plan for ongoing technology transfers, and the anticipated proof of concept outcome. Strength of project management will also be considered.
- **Qualification of participating researchers:** The extent to which expertise and prior experience bear on the problem at hand. Please elaborate on track records of building research prototypes (e.g., open-source research code/collaterals on GitHub) and resulting publications from past relevant projects.
- **Cost effectiveness and cost realism**: The extent to which the proposed work is both feasible and impactful within the proposed resource levels will be examined.
- **Potential for broader impact:** As an industry leader, Intel pushes the boundaries of technology to make amazing experiences possible for every person on earth. From powering the latest devices and the cloud you depend on to driving policy, diversity, sustainability, and education, we create value for our stockholders, customers, and society. Intel expects the academic community to be strong partners in making Intel successful through support of Intel's goals and commitments to diversity, sustainability, and education. Intel supports the advancement of computing education and diverse participation in STEM. Significant consideration will be given to proposals in which the outcome of the research can influence the development of new curriculum initiatives

impacting undergraduate or graduate education at the respective universities (e.g., exposure to latest industry technologies/tools in classroom setting). Proposals are encouraged to elaborate on how the proposed work is anticipated to impact student education on campus and/or the broader academic community.

PI MEETINGS AND COLLABORATION STRUCTURE

Intel will be deeply engaged with the center and will assign partner technologists/collaborators across RVs to interact with the academic community to produce a stream of innovation proof-points, publications, demonstrations, and technology transfers into Intel and the broader industry throughout the duration of the program. We aim for the interaction to be bi-directional where Intel collaborators are part of the research team. Not only will they provide research feedback, but they will also actively contribute and co-develop the research to amplify the center outcome and enable continuous technology transfers into Intel and the broader industry.

It is expected the PI and student researchers will collaborate daily or weekly. Monthly PI, student and Intel collaborator meetings will be used to review research results, present significant updates, and provide feedback.

Semi-annual face-to-face or virtual meetings will be held to facilitate center-wide information exchange, review, and discussion of research. Researchers should anticipate one annual face-to-face meeting to be held at an Intel site in the US or Europe and one annual face-to-face meeting to be held at a university associated with this center. Associated travel costs for two annual meetings should be considered and included in the proposed budget. In the event unexpected travel restrictions prohibit a face-to-face meeting, a virtual meeting will be held.

To aid in collaboration across projects within the center and communication of research findings to the public, it is anticipated that a center website will be established, hosted, and maintained and Intel requests the right to host the associated website link on their respective university program websites.

Intel will offer free access to Intel’s Academic Compute Environment, a resource for academia researchers in the center to exercise their workloads on Intel’s latest hardware.

For researchers already funded and seeking collaboration opportunities with Intel and other researchers in this RFP, please tell us. One option is to participate in center activities (e.g., seminars, workshops, and hardware access) without Intel funding.

ELIGIBILITY

This RFP is open to academic researchers and institutions specifically invited to participate in the proposal process. Invitees may invite academic collaborators.

If you would like us to invite a given academic to submit an independent proposal, feel free to email us a nomination for consideration. We will review the proposal and will decide whether to invite the given academic.

INTELLECTUAL PROPERTY

This solicitation affords proposers the choice of submitting complete program proposals for the award of a grant, a Sponsored Research Agreement, or other agreement as appropriate. Intel reserves the right to negotiate the final choice of agreement. Intel prefers that university research in the program be placed in the public domain (patentable inventions dedicated to the public and source code distributed under an open-source license like the Apache, BSD or MIT license).
The final award terms are expected to follow a public dedication model. This means that either (1) Intel and the university will jointly agree that IP developed under an award will be placed in the public domain, including offering software under an open source license (Intel's preference as referenced above), or (2) if IP is not placed in the public domain, then all parties (the university, Intel and all third parties) will be afforded equivalent non-exclusive no-fee royalty-free rights to the research results for any commercial or non-commercial purposes, preferably with the right to sublicense third parties under such rights.

INTEL CONTACT INFORMATION

The following individuals from Intel Labs are actively involved with the creation of this center.

Richard Chow, Program Director (richard.chow@intel.com)
Matthias Schunter, Co-Principal Investigator (matthias.schunter@intel.com)
John Matthews, Co-Principal Investigator (john.matthews@intel.com)
Anand Rajan, Managing Sponsor (anand.rajan@intel.com)

Please submit proposals using the website:
https://academic-rfp.intel-research.net/cur-rfp/SPAR.

Please send any inquiries to Matthias Schunter and John Matthews and copy Richard Chow.
Please include "Submission for SPAR" in the Subject of your email.

FAQ

WHAT IS THE TYPICAL GRANT AND PROPOSAL TEAM SIZE?

Proposals generally request grants in the range of $70-140K per year. This would typically support 1 or 2 graduate students advised by 1 or 2 PIs.

WHAT IS THE ENVISAGED PROJECT DURATION?

Three years (there is a renewal process each year, but proposals should outline all 3 years with more details on year 1).

DO YOU CONSIDER PROPOSALS PRIMARILY CONCENTRATING ON THEORY/ALGORITHMS?

Proposals without a strong implementation/validation component are of interest, although it is strongly encouraged to provide evidence that the theory/algorithms will have use in practical systems. However, significant theoretical advances that will lead to practical solutions in the future are also welcome.

CAN YOU SPECIFY WHICH RESEARCHERS HAVE BEEN INVITED TO THIS RFP?

We do not release the names of invited researchers. Keep in mind that if you are seeking to partner with a specific academic PI, your partners do not have to be invited; you can choose to partner with any PI and share the RFP with them.

ARE WE ENCOURAGED TO SEEK CO-FUNDING OPPORTUNITIES?

Co-funding is strongly encouraged. A proposal with co-funding or matching funding would be a strong plus. Feel free to reach out to us to discuss what types of co-funding have worked in the past.

CAN TEAMS OUTSIDE THE EUROPEAN REGION PARTICIPATE IN THIS RFP?

For this RFP, we envision primarily sponsoring research teams based in the European region. We welcome affiliated researchers from other locations if they are interested in collaborating while obtaining funding from other sources.