INTEL REQUEST FOR PROPOSALS (RFP)

SUBJECT

Intel Corporation, through its University Research & Collaboration Office (“URC”) requests proposals for academic research in the area of Resilient Architectures and Robust Electronics (RARE).

KEY DATES

Proposal Submission Deadline (PIs): May 5, 2021

Proposal Responses from Intel: August 2021

Planned Research Start: September 2021

OVERVIEW

Intel invites proposals to establish a new research center which will focus on assessing and improving the resiliency, reliability, and security of silicon die. This is an invitation for proposals from academic researchers to innovate and develop new capabilities in the area of secure and resilient computing.

Intel would like to expand our collaboration with academia in the area of resilience of Intel platforms. This includes systematic mitigation of error conditions and faults, and associated impacts on future CPU architectures and implementations. We will consider faults caused by any reason, be it natural radiation, aging, random effects, or intentionally caused, such as fault injection. Faults are considered for data, control, and other logical paths.

PROGRAM SCOPE AND FUNDING

Intel intends to fund a new collaborative, multi-university research center addressing the four 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

RV1: ERROR CHARACTERISTICS OF SILICON COMPUTING

GOAL

The goal of this research vector is to identify silicon failure mechanisms which result in compute errors of various types and provide mitigations of and responses to these conditions.

Examples of desirable outcomes for this RVs and desirable impact are e.g.:

- New circuit, logic, and system analysis of methodologies and framework to assess and categorize more compute failures.
- Identify and show new circuit/logic environmental conditions which may impact correct operation of the circuit or logic.

BACKGROUND

Fault Injection Attacks (FIA) are classes of attacks which distort the device operating environment to cause incorrect operation. This includes both control flow and data disruption. Defects are classes of similar failures which result in incorrect operation of the device for no apparent reason. This RV attempts to understand incorrect circuit, logic, and system operation by proposing research into the area of errors from sources such as transient local voltage, temperature, and frequency conditions. Research should also include and evaluate impacts from other sources such as defects, radiation, laser, electromagnetic exposure, etc. We seek to have results which will characterize a wide variety of systems, logic and circuits and their impact to the user to identify the highest impact areas to improve the reliability of the device and to improve resilience.

RESEARCH QUESTION

Research Mission: Research silicon characteristics when parts operate outside the verified range or experience degradation because of intrinsic properties (e.g. manufacturing variation, aging). Identify characteristics that make a device susceptible to faults and fault inducing conditions, study how faults manifest and propagate beyond the device, and possibly propose mitigations tailored to the specific vulnerability. Evolve methodology to identify local areas that operate outside the specified range or experience an intrinsic degradation when the device is set up to operate in the verified range.

Example Research Questions: Example research questions that are in scope for RV1 are:

- Develop and demonstrate methodologies to assess and show the impacts of faults and mitigations in areas of the architecture, micro-architecture, and circuits
- Characterize the conditions which cause incorrect computation, assess their impact and manifestation to the user, and propose mitigations tailored to the observed behavior
- Develop mitigations to fault injection attacks with tools which measure susceptibility

RV2: NEW SOLUTIONS, TECHNIQUES, AND MECHANISMS TO DETECT COMPUTE FAILURE CONDITIONS

GOAL:

This RV aims to improve the handling of compute failures by providing new detection and mitigation mechanisms.

Examples of desirable outcomes for this RVs:

- Circuits which detect and signal a marginal computing condition in time to prevent an error.
- Guidance on placement of detection circuits based on metrics such as power draw, temperature, local voltage, significance to the user experience, etc.
- Circuits which require little or no manufacturing calibration to detect potentially error inducing conditions.
- Architecture and microarchitecture mechanisms which facilitate error recovery without user intervention.

BACKGROUND

To increase reliability and fault resilience, new techniques are required to identify when the device's results may be unreliable. This RV goes along with RV1 to provide insight and understanding around the improvements needed to increase resiliency and reliability in the face of errors.

Research circuits, logic, and architecture that detect voltage, frequency, timing, and thermal margins that may be leveraged to detect deviations from expected behavior that may then be applied to ensure reliability, reduce tester time, eliminate guard band, and predict aging characteristics. Research may also identify improved on-die local detection circuits, logic, and architecture solutions including increasing the robustness of the circuit itself to remain reliable when exposed to a fault.

RESEARCH QUESTION

Research Mission:

Research low-overhead circuits, logic, architecture, and micro-architecture features that enhance and augment real-time error detection mechanisms with autonomous recovery to increase reliability and availability. Expand the span of circuits and logic that are protected from failures through automation that identifies high-impact designs and implements or suggests efficient approaches to increase robustness.

Example research questions: Example research questions that are in scope for RV2:

- Detect local conditions leading to compute failure.
- Mitigate local conditions leading to a compute failure.
- Mitigate compute failures through advanced automatic recovery mechanism and concepts.

RV3: RESEARCH AND TOOLS FOR SIDE-CHANNEL-FREE AND FAULT-TOLERANT PROCESSORS

GOAL

This RV advances research related to speculative execution and other security issues such as fault injection attacks.

Examples of desirable outcomes for this RV:

- Solutions to reduce or eliminate timing leakage from cache accesses or memory transactions inside the processor
- Performant solutions to various Spectre attacks with proof of security properties
- Architecture solutions to expand protections for sandboxing
- Tools to detect and reason about circuits which are susceptible to faults at design time
- Methodologies and frameworks to reliably and holistically assess side-channel leakage and quantify effectiveness of mitigations at design and verification time

BACKGROUND

Previous research has shown promising results and produced promising approaches to many side-channel attacks. This includes areas as secure caches and Spectre mitigations. Research will be directed at general purpose computing, but we intend to extend those findings to other compute elements in the future.

RESEARCH QUESTION

Research Mission: side-channel-free and fault-tolerant mitigations for general purpose computing. Investigate novel architecture, micro-architecture, software, and tools that result in resilient designs as well as software with adjustable security/performance.

Researchers are encouraged to revisit all current assumptions. Explore new micro-architecture techniques that improve performance without introducing side channels and offer trade-offs in design complexity, area, power, or performance. To provide timely security insights for designers, there is a strong need for tools and methodology that can holistically assess and accurately quantify the leakage of a design and the effectiveness of a mitigation before the full set of traces is collected.

Example Research Questions: Example research questions that are in scope for RV3 are:

- Tools and methods to identify, detect, quantify, and prove absence of security issues
- Tools for detecting speculative state not correctly cleared
- Designs which obfuscate timing measurements

RV4: NOVEL HARDWARE MITIGATIONS

GOAL

Advance state of secure, confidential computing with new concepts learned from starting with a clean slate processor design. This design focuses on providing confidentiality and integrity in computing to remove leakages and increase resiliency.

Examples of desirable outcomes for this RV:

- Side-channel free data center (server) processor design
- Processor which is resilient to power-based and electromagnetic radiation side-channel attacks
- Performant data center processor without speculation

BACKGROUND

Traditionally vulnerabilities have been addressed through patches. Patches can be to software or RTL changes in a larger design. This retrofitting of previous designs to patch vulnerabilities limits the scope of fixes such that more robust and fundamental approaches are not entertained. This RFP would like to remove the legacy issues and focus on the best, most robust methods, and mechanisms to fix what are often described as systemic classes of security problems. How robust, secure, and performant will a clean slate design be when security is the main goal of the effort? The goal is to provide a secure but still performant design for a data center class processor unit.

RESEARCH QUESTION

Research Mission: Explore novel micro-architectural and architectural solutions to avoid inherent security vulnerabilities. Explore designs that avoid software side-channels, speculative side channels, and power side channels. Explore techniques which provide protection of user data at all points where user data transits or resides. Develop a security first design with performance options.

Example Research Questions: Example research questions that are in scope for RV4 are:

- Clean-slate microarchitecture design which is provably free from side channels and software attacks. Can include ISA enhancements.
- What are the performance characteristics of a secure processor design?
- What is the silicon area impact of differential power analysis resistant (DPA) design?

WILDCARD RESEARCH VECTOR

GOAL: IMPACTFUL RESEARCH TOWARDS OUR GOAL NOT COVERED IN RV1-4.

It is possible that we overlooked an essential research question for reaching the goals of this program. If you have a strong belief (and ideally also some evidence) that a major research question has been overlooked, you can submit a research question as “wild card”. In this case, the burden is higher and you need to argue that the research that you plan to pursue (a) is a promising approach to reach the goals stated above and (b) that your research does not fit into the research vectors documented above.

PROPOSAL FORMAT

Please note that Intel is unable to receive proposals under an obligation of confidentiality. All proposals submitted should therefore include only public information.

Proposals should be 4-8 pages, not including citations or cost volume. We slightly prefer proposals that aim at defining a proposal 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 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 (<= 3 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 detail 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).
- **Statement of work, schedule, milestones, success criteria and deliverables (<=3/4 page).** For each of the goals addressed, outline the 3-year scope of the effort including tasks to be performed, schedule, milestones, deliverables, and success criteria. It is understood that aspects of this research effort may be exploratory in nature and schedules/deliverables reflect intentions rather than a firm commitment.
- **Personnel plan and expertise statement (max. 1/4 page per Researcher).** Include a list of key personnel (at most 6) 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 page).** Please provide information about the PhD students and postdocs you envision to assign to this project (if known). Outline the approach and plan whereby PhD students will be recruited and incorporated into the team, and any plans for encouraging/supporting those students in collaborations with Intel (e.g., availability for Internships should a mutually interesting opportunity arise). If the PIs have a pre-existing relationship and history of student hiring by Intel please discuss issues/plans/ideas to continue or strengthen that connection.
- **Diversity and Inclusion (<1 page)**. In light of Intel's strong commitment to diversity and creating an inclusive environment, please address: (a) your organization's commitment to diversity and inclusion with respect to race, national origin, gender, veterans, individuals with diverse abilities and LGBTQ, and (b) a summary of your performance in this area and any initiatives you are pursuing.
- **Prior Intel Collaborations (max 1/3 page per project).** If you collaborated with Intel in the past, please list the project/institute, the year, and the main contact(s) at Intel. Furthermore, add a short abstract outlining the scope.
- **Past Successful Technology Transfers (<=1 page).** Evidence of past successful industry collaborations and technology transfers. Examples include startups, products, and other evidence of tangible business impact of the involved academics.
- **Budget and Financials (1/3 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).** If the team can obtain funding for related work from other sources (including the University) and the sponsor commits to follow a 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.
- **Citations {unlimited}.**
- **Cost volume {unlimited}**. Cost proposal in Excel or another format as appropriate.

EVALUATION CRITERIA

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

1. **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.

2. **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 include incremental advancements to state-of-the-art and current design practices. Feasibility of new algorithms/techniques should be demonstrated through SW/HW implementations.

3. **Clarity of overall objectives, intermediate milestones 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.

4. **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.

5. **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.

6. **Potential for co-funding:** Opportunity for closely synergistic matching grants and co-funding with other funding entities, such as SRC, NSF, DARPA, NSERC, etc. will be given significant consideration.

7. **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 on a daily or weekly basis. 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 request 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 those researchers who are already funded and seek collaboration opportunities with Intel and other researchers in the area of this RFP, please let us know. One option is to participate in center activities (e.g., seminars, workshops, and hardware access) without Intel funding.

ELIGIBILITY

This RFP is open only to academic researchers and institutions that have been specifically invited to participate in the proposal process. However, invitees may freely select additional academic collaborators. Any questions regarding eligibility should be directed to Richard Chow and Frank McKeen (contact info below).

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 reserve 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 similar to 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 TEAM CONTACT INFO

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

Richard Chow, Program Director (richard.chow@intel.com)
Frank McKeen, Co-Principal Investigator (frank.mckeen@intel.com)
Cameron McNairy, Co-Principal Investigator (cameron.mcnairy@intel.com)
Carlos Rozas, Co-Principal Investigator (carlos.v.rozas@intel.com)
Anand Rajan, Managing Sponsor (anand.rajan@intel.com)

Please send proposal submissions and related inquiries to Richard Chow and copy Frank McKeen, Cameron McNairy, and Carlos Rozas. Please include "Submission for RARE" 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 don't 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?

While co-funding is not required, a proposal with co-funding or matching funding would be a strong plus.