Project Summary

Making Analog Side Channels a First-Class Consideration  
in Architecture-Level Design

Milos Prvulovic, Alenka Zajic, and Rakesh Kumar

Analog side-channels (power, electromagnetic, acoustic, etc.) have long been a potential source of attacks that circumvent traditional protections and security measures. Many such attacks have been demonstrated over the past several decades, followed by countermeasures that prevent specific attacks by modifying the software that has been demonstrated to leak sensitive information. However, recent analog side channel attacks have shown that both attacks and mitigations are becoming increasingly dependent on microarchitectural behavior and potentially fragile to future microarchitectural changes. Ideally, the potential for information leakage through analog side channels and “breaking” existing software mitigation approaches would be considered in early stages of design for both hardware and software, guided by tools that can predict the impact a specific design has on analog side channels. This would be analogous to how performance and power consumption are predicted by cycle-accurate simulators, which allows the tradeoff between performance, power, and cost to be investigated at design time, years before the first prototype of that processor is fabricated.

However, early-design tools such as cycle-accurate simulators do not model analog side channel signals, so these side channels can only be considered when they can be physically measured on already-fabricated chips. At that time, however, time-to-market concerns prevent introduction of overall design changes that would adjust the design tradeoffs in a more desirable direction. Additionally, most software developers have neither the know-how nor the equipment to assess their software’s potential vulnerability to analog side channels, so such considerations are typically either absent or qualitative/abstract when software is designed, giving first-mover advantage to attackers, and resulting in mitigation via localized patches, which themselves are becoming increasingly microarchitecture-dependent. Hence we propose to:

**Proposed Work** Develop 1) techniques that allow architecture-level simulators to efficiently generate estimated side channel signals, to help computer architects, researchers, and software developers assess the impacts of microarchitectural and software changes on the tradeoff between performance, power, and side channel leakage, 2) methods for efficient circuit-level exploration of caches and functional units that can be integrated into architecture-level simulators, analogous to how Cacti and McPat are used to obtain per-event latency and power estimates in cycle-accurate simulators, and 3) methods for “calibration” of simulation parameters against measured signals from real systems.

**Intellectual Merit** Our work will demonstrate the feasibility of modeling analog side-channels at the microarchitectural level and provide proof-of-concept integration of such modeling into a cycle-accurate simulator. This will allow analog side channels to become a first-class consideration, along with performance and power, in processor designs, allowing computer architects to avoid introducing significant new vulnerabilities and “breaking” existing software mitigations, and possibly even to reduce leakage and/or enable new mitigations. It would also allow programmers and even compilers to include analog side channel considerations in their tradeoff space during design and/or optimization.

**Broader Impact** We expect that our results will help the inclusion of analog side channels among early design considerations and will help reduce the cost of side-channel resistant designs by addressing side-channel-related problems early in the design process, when side-channel resilience may be improved (or preserved) with little or no sacrifice in performance, power, cost, weight, etc. The proposal also includes 1) developing an interactive demonstrator to educate and raise awareness about analog side channels 2) visits and activities in local schools to improve K-12 education and participation of women and minorities in STEM, and 3) course and curriculum development activities at the undergraduate and graduate level.

**Keywords:** cycle accurate simulation, analog side channels, microarchitecture

Material for Broadening participation in Computing (<https://bpcnet.org>). Needed for medium proposals

https://www.nsf.gov/cise/bpc.

1. **Context**: Describes the problem the plan addresses using institutional or local data, and the goals of the proposed activities;
2. **Intended population(s)**: Specifically identifies the demographics of the participants, including school level(s) (e.g., African-American undergraduates or female high-school students);
3. **Strategy**: Outlines the plan of activities with specific intended outcomes, corresponding to the elements in (1) and (2) and with a role for each PI and co-PI;
4. **Preparation**: Describes any past engagement with BPC activities and/or intended preparation/training activities to implement proposed work; and
5. **Measurement**: Describes plans for the measurement of outcomes for the proposed activities.

**Supplementary Documents:**

In the Supplementary Documents Section, upload the following:

*1. A list of Project Personnel and Partner Institutions (Note: In collaborative proposals, the lead institution should provide this information for all participants):*

Provide current, accurate information for all personnel and institutions involved in the project. NSF staff will use this information in the merit review process to manage reviewer selection. The list must include all PIs, co-PIs, Senior Personnel, paid/unpaid Consultants or Collaborators, Subawardees, Postdocs, and project-level advisory committee members. This list should be numbered and include (in this order) Full name, Organization(s), and Role in the project, with each item separated by a semi-colon. Each person listed should start a new numbered line. For example:

1. Mary Smith; XYZ University; PI
2. John Jones; University of PQR; Senior Personnel
3. Jane Brown; XYZ University; Postdoc
4. Bob Adams; ABC Community College; Paid Consultant
5. Susan White; DEF Corporation; Unpaid Collaborator
6. Tim Green; ZZZ University; Subawardee

*2. Collaboration Plans:*

Collaboration Plans for Medium projects (if applicable): 9 Note: In collaborative proposals, the lead organization should provide this information for all participants. Since the success of collaborative research efforts are known to depend on thoughtful coordination mechanisms that regularly bring together the various participants of the project, all Medium proposals that include more than one investigator must include a Collaboration Plan of up to two pages, even when the investigators are affiliated with the same institution. The length of and degree of detail provided in the Collaboration Plan should be commensurate with the complexity of the proposed project. Where appropriate, the Collaboration Plan might include: 1) the specific roles of the project participants in all organizations involved; 2) information on how the project will be managed across all the investigators, organizations, and/or disciplines; 3) identification of the specific coordination mechanisms that will enable cross-investigator, cross-organization, and/or cross-discipline scientific integration (e.g., yearly conferences, graduate student exchange, project meetings at conferences, video conferences, software repositories, etc.); and 4) specific references to the budget line items that support collaboration and coordination mechanisms. If a Medium proposal with more than one investigator does not include a Collaboration Plan of up to two pages, that proposal will be returned without review.

*3. Data Management Plan (required):*

Proposals must include a Supplementary Document of no more than two pages labeled "Data Management Plan." The data management plan must be substantive and specific to the project and should address all project-relevant aspects of data privacy and security. In addition to addressing how the project will conform to NSF's policy on the dissemination and sharing of research results, the Data Management Plan should address the following topics if they are relevant to the project:

* **Handling of sensitive data**: sensitivity of the data to be collected, ethics of data collection and identification of harms that could arise from its collection or inadvertent dissemination, techniques that will be used to protect the privacy of individuals and organizations associated with the data; and plans to request Institutional Review Board (IRB) approval for data collection, aggregation, and analysis.
* **Data sharing:** methods for providing other researchers with controlled access to datasets and the time period during which data will be available. If the project will develop software or hardware, the Data Management Plan should discuss not only what access other researchers will have to source code or hardware design artifacts (e.g., specific open source licenses) and the physical location of the data repository (e.g., commercial cloud, private server, campus server), but also the method by which other researchers may access these products of the project (e.g., GitHub repository).
* **Authorization for data access and protection of data:** policies for authorizing access to the data and techniques (including security protections) that will be used to prevent the unauthorized dissemination of the data.

See Chapter II.C.2.j of the [PAPPG](https://www.nsf.gov/publications/pub_summ.jsp?ods_key=pappg) for full policy implementation.

For additional information on the Dissemination and Sharing of Research Results, see: <https://www.nsf.gov/bfa/dias/policy/dmp.jsp>.

*4. Broadening Participation in Computing (BPC) Plans for Medium and Large projects:*

Each Medium or Large project that with a lead or nonlead organization (department, school, or institute) that primarily carries out research and education in computer science, computer engineering, information science, and/or other closely-related field, must, by the time of award, have in place an approved BPC plan. In this ongoing pilot phase, CISE will work with each PI team prior to making an award to ensure that plans are meaningful and include concrete metrics for success. CISE will also provide opportunities for PIs to share BPC experiences and innovations through program PI meetings. PIs of Medium or Large proposals are therefore strongly encouraged to consider this eventual requirement as they develop their proposals, and to include descriptions (of one to three pages) of their planned BPC activities under Supplementary Documents in their submissions. Feedback will be provided on such plans.

***No other Supplementary Documents, except as permitted by the NSF Proposal & Award Policies & Procedures Guide, are allowed.***

**Single Copy Documents:**

**Collaborators and Other Affiliations Information:** Proposers should follow the guidance specified in [Chapter II.C.1.e](https://www.nsf.gov/pubs/policydocs/pappg20_1/pappg_2.jsp#IIC1e) of the NSF PAPPG.

Note the distinction to item (1) under Supplementary Documents above: the listing of all project participants is collected by the project lead and entered as a Supplementary Document, which is then automatically included with all proposals in a project. The Collaborators and Other Affiliations are entered for each participant within each proposal and, as Single Copy Documents, are available only to NSF staff.

**Submission Checklist:**

In an effort to assist proposal preparation, the following checklists are provided as a reminder of the items that should be checked before submitting a proposal to this solicitation. These are a summary of the requirements described above. For the items marked with (RWR), the proposal will be returned without review if the required item is non-compliant at the time of proposal submission. Note that there are multiple lists: (1) for all proposals, unique to this solicitation; (2) additional requirements for Small and OAC Core proposals; and (3) additional requirements for Medium proposals. For all proposals, regardless of size: The last line of the Overview section of the Project Summary must consist of the word "Keywords" followed by a colon and between 3-6 10 keyword sets, separated by semi-colons. If REU supplements are requested, then a supplementary document describing the REU activity must be included, and REU supplement costs must be specified in the Participant Support Costs section of the proposal budget. The proposal title should comply with the requirements under Proposal Preparation Instructions above. If requesting public cloud resources through CloudBank, a supplementary document of up to two pages must be provided, and the "CloudAccess" keyword should be specified in the Project Summary. For Small proposals and OAC Core proposals: (RWR) The total budget must not exceed $600,000, excluding funds for any embedded REU supplements. For separately-submitted collaborative proposals, this is the total across all participating organizations. (RWR) For proposals submitted to the OAC Core Research program only, the Project Description should include a validation or transition-topractice plan. For proposals submitted to the CSR and NeTS programs only, the Project Description should include an evaluation plan. A Collaboration Plan (up to two pages) may be provided as a Supplementary Document. If provided, the Collaboration Plan should include all organizations participating, not a separate plan for each organization. For Medium proposals: (RWR) The total budget must be $600,001 to $1,200,000, excluding funds for any embedded REU supplements. For separately-submitted collaborative proposals, this is the total across all participating organizations. For proposals submitted to the CSR and NeTS programs only, the Project Description should include an evaluation plan. (RWR) If there is more than one investigator, a collaboration plan (up to two pages) must be provided as a Supplementary Document, even if all investigators are affiliated with the same organization. The Collaboration Plan should include all organizations participating, not a separate plan for each organization. (RWR) A BPC plan is required as a Supplementary Document with a title clearly identifying it as such. Collaborative proposals should submit one BPC plan, as described in the proposal preparation instructions.

For Medium proposals, reviewers will be asked to: Comment on the extent to which the project scope justifies the level of investment requested, and the degree to which the Collaboration Plan (if required) adequately demonstrates that the participating investigators will work synergistically to accomplish the project objectives. Comment on whether key personnel, and especially lead PIs, have allocated adequate time for both their individual technical contributions and the leadership of collaborative activities necessary to realize the synergistic effects of larger-scale research. Comment on whether the Broadening Participation in Computing (BPC) plan meaningfully addresses the five elements of a BPC Plan: (1) the goal and context of the proposed activity, (2) intended population(s), (3) strategy, (4) measurement, and (5) PI engagement.