2019-2020 Grand Challenge Award Final Report

Awardee: **Ali Yilmaz, Professor**
Electrical and Computer Engineering

Research Award Title: **Predicting Electromagnetic Vulnerabilities of Embedded Cryptography**

Research Summary

The primary objective of this project was to develop and validate computational methods and software that enable simulation-based prediction of electromagnetic (EM) side-channel vulnerabilities of embedded cryptographic modules. To this end, I proposed to leverage the state-of-the-art petascale EM simulation tools recently developed at Oden Institute by my group. These tools are based on petascale boundary-integral algorithms for solving Maxwell's equations; these algorithms, which rely on FFT acceleration, efficient and scalable parallelization algorithms, and sparse preconditioners, had been successfully used to quantify EM scattering from aerospace platforms and radiation from antennas near complex objects. They had to be adapted, however, for predicting EM side-channel vulnerabilities; specifically, domain reduction and transient analysis features, integration with circuit simulators, and parallel algorithms suitable for multi and many core architectures are needed to combat the large density of on-chip and on-package interconnects and perform predictive simulations. I also proposed validating simulation-based predictions with experiments using the equipment and space that the ECE department provided to my research group in the new EER building. Proper validation requires design and fabrication of test chips, carefully controlled and precisely instrumented measurements, modeling and simulation of the specific chip and the cryptographic implementation, and statistical comparison of information leakage in the measurements to those predicted by simulations. To this end, I proposed to explore collaboration opportunities with researchers at Sandia National Labs who had expressed particular interest in our work on side-channel EM measurements and simulations.

In this project, my students and I advanced reduced-domain layered-medium integral-equation solvers [C5]-[C7],[J1],[J2] that can be used to efficiently simulate EM radiation from interconnects and can be easily coupled with circuit solvers. We also embarked on an ambitious simulation-informed experimental campaign to collect large datasets by near-field EM measurements over cryptographic chips. We quickly realized that before these datasets can be used to validate simulation-based predictions, the data collection and analysis process to reveal EM side-channel vulnerabilities had to be improved as the brute-force measurement approach turned out to be infeasible for the level of fidelity needed (requiring months-long campaigns for each configuration). We developed theories and novel methods to focus and therefore accelerate the measurements to information-leaking locations and configurations [C1],[C2]. We also started implementing design-stage countermeasures and strategies against such EM side-channel attacks [C3],[C4].

The COVID-19 pandemic that started in the middle of the Grand Challenge award period severely disrupted presentations, planned mutual site visits with Sandia researchers, and measurement campaigns in EER due to university lab closures. Although this inevitably translated to reduced my students' and my productivity and delayed outcomes, there were still several significant achievements: The research I performed during this project contributed to the publication of seven conference [C1]-[C7] and two journal [J1],[J2] papers. Our work was recognized by two awards [A1],[A2]. I was also able to pursue collaborations with various ECE faculty (J. P. Kulkarni, M. Orshanksy, and A. Gerstleur) with experience in circuits, cryptography, and computer architecture. I also submitted a grant proposal to Sandia National Labs that was funded [G1].

Presentations Made/Papers Published/Awards & Recognitions/Proposals

As a result of the Grand Challenge award, I was able to visit the Michigan Institute for Computational Discovery and Engineering before the COVID-19 pandemic started and gave a seminar presentation:

P1. A. E. Yılmaz, "Using (super)computers judiciously for higher fidelity electromagnetic analysis," MICDE Seminar Series, University of Michigan, Ann Arbor, MI, Oct. 2019.

The award allowed me to work on the following journal papers and conference papers which are in various stages of publication:

J1. C. Liu, K. Aygun, and A. E. Yılmaz, "A parallel FFT-accelerated layered-medium integral-equation solver for electronic packages," in Special Issue of Int. J. Num. Model.: Electron. Networks, Dev., Fields, vol. 33, no. 2, Mar./Apr. 2020.

J2. C. Liu and A. E. Yılmaz, "An accelerated reduced-domain layered-medium integral-equation method for the analysis of high-fidelity full-size electronic packages," IEEE Trans. CPMT, in preparation.

C1. V. V. Iyer and A. E. Yılmaz, "Using the ANOVA F-statistic to isolate information-revealing near-field measurement configurations for embedded systems," IEEE EMC Symp., submitted Feb. 2021, accepted.

C2. V. V. Iyer and A. E. Yılmaz, "Using the ANOVA F-statistic to rapidly identify near field vulnerabilities of cryptographic modules," IEEE Int. Microw. Symp., submitted Dec. 2020, accepted.

C3. M. Wang, V. V. Iyer, S. Xie, G. Li, S. K. Mathew, R. Kumar, M. Orshansky, A. E. Yılmaz, and J. P. Kulkarni, "Physical design strategies for mitigating fine-grained electromagnetic side-channel attacks," IEEE CICC Conf., submitted Dec. 2020, accepted.

C4. M. Wang, S. Xie, P. N. Li, A. Sayal, G. Li, V. V. Iyer, A. Thimmaiah, M. Orshansky, A. E. Yılmaz, and J. P. Kulkarni, "Galvanically isolated, power and electromagnetic side-channel attack resilient secure AES core with integrated charge pump based power management," IEEE CICC Conf., submitted Dec. 2020 accepted.

C5. C. Liu and A. E. Yılmaz, “A shielded-block preconditioner for reduced-domain layered-medium integral-equation methods,” IEEE EPEPS Conf., Nov. 2020.

C6. Y.-R. Jeong and A. E. Yılmaz, “A comparison of finite vs. infinite plane models of reference conductors in electronic packages,” IEEE EPEPS Conf., Nov. 2020.

C7. C. Liu and A. E. Yılmaz, “A reduced-domain layered-medium integral-equation method for electronic packages,” in Proc. IEEE EPEPS, Oct. 2019.

Our work enabled by the Grand Challenge Award received the following recognitions:

A1. 2019 IEEE EPEPS Conference Best Student Paper Award, First Place Winner, for the conference paper [C7].

A2. Intel 2020 Outstanding Researcher Award “for exceptional contributions made through Intel university-sponsored research”.

The award also enabled me to pursue collaboration with Sandia National Labs and submit the following grant proposal:

G1. A. E. Yılmaz, “Coupled electromagnetic/micromagnetic simulations,” Sandia National Labs, $78,950, funded, 10/2020.