Predicting Electromagnetic Vulnerabilities of Embedded Cryptography

Ali Yilmaz, Associate Professor, ECE

Abstract: Embedded computing systems and Internet-of-Things (IoT) devices have an increasing role in transportation, health care, defense, manufacturing, and critical infrastructure. Cryptographic techniques are deployed to secure these systems, e.g., to prevent unauthorized access to information, protect privacy, and authenticate other nodes. Because embedded systems are by their nature out in the world and physically accessible to adversaries, they are vulnerable to attacks in ways that traditional information-processing systems are not. Securing them requires countermeasures for not just remote (software) vulnerabilities but also local (hardware) vulnerabilities of their physical implementations. While cryptographic techniques are a cornerstone of modern (software) security, traditional techniques assume that cipher systems would be implemented in a closed, reliable computing environment that does not leak any sensitive information, i.e., the implementations are regarded as black boxes that only have an input and an output interface. This is far from the case in embedded cryptography; e.g., a particularly acute vulnerability arises from the so-called side-channel attacks that infer sensitive information by exploiting (unintended) information leakage from computing devices. Among the many possible attack modalities, those based on capturing EM emanations are particularly potent; indeed, EM emanations have been shown to leak information that is not available in other side channels; in part because (i) they are due to complex and subtle factors that fall under the radar of circuit designers, who typically ignore them. Even designs of chips, packages, and boards that attempt to minimize EM interference and meet EM compatibility standards are vulnerable because these attacks can be performed using near-field probes to sense local information-bearing EM fields that decay quickly (inversely proportional to the distance, square of the distance, or cube of the distance) and fall below the levels required to ensure EM compatibility and immunity with other components. EM side-channels remain a problem also because (ii) existing techniques for analyzing EM vulnerabilities are almost entirely experimental and can only be used after an electronic design has been fabricated. Simulation-based approaches for rapidly analyzing the vulnerabilities of embedded system designs to EM vulnerabilities are sorely needed to develop countermeasures early in the design process.

The primary objective of this project is to develop and validate computational methods and software that enable simulation-based prediction of EM side-channel vulnerabilities of embedded cryptographic modules. In this project, the PI will pursue two activities: (i) Develop software to accurately calculate transient EM fields near an electronic chip at-scale, from the layout of the chip interconnect network and the current distribution on it; (ii) Validate simulation-based predictions with experiments. Proper validation requires the design and fabrication of test chips, carefully controlled and instrumented measurements of EM side-channel emanations, 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.