Title: Investigation of COTS NVM Technologies from a Reliability and Security Perspective

Supriya Chakraborty
Department of Electrical Engineering,
Indian Institute of Technology Delhi

Abstract

Emerging Non-Volatile Memory (NVM) technologies are a significant contender for next generation memory applications including both standalone and embedded memory usage. In addition, there are significant advancements in NVM technologies beyond storage applications. This includes in-memory computing, neuromorphic applications, security primitives, approximate computing, etc. Since emerging NVM technologies are used in mainstream memory applications, it is high time to investigate their reliability aspects. With the advancement of modern electronic systems and integrated circuits, hardware security has become one of the crucial concerns. Hardware security threats may arise at any stage of the life cycle of the electronic systems/devices ranging from the device specifications to fabrication including recycling. In addition, data processing within the electronic system is also subject to various threats such as unauthorized access, side channel attack, fault injection, data corruption, DoS, etc.

In this work we investigate two aspects of Commercial-Off-The-Shelf (COTS) NVM chips i) reliability, and ii) security. We show that the unique characteristics of NVM technologies can act as two sides of the same coin: i) one related to the exploitation of vulnerabilities leading to threats and other ii) related to exploitation for building innovative hardware security primitives. The key contributions of this work include characterization of NVM chips for i) latency, ii) current consumption, and iii) endurance. Different soft-techniques are experimentally validated on FPGA to enhance the performance of the chips beyond datasheet specifications. We significantly reduce the

number of bit flips by ~26%. The unique current consumption signature of the chips is further exploited for efficient NVM programming. The reliability aspect is investigated by exposing MRAM chips to the external magnetic field. Both static and dynamic stress analyses are performed while exposing the external magnetic field to the chip from different directions. We observed that exposure to external magnetic field results in increase in chip read and chip write current. Furthermore, the intrinsic properties of COTS NVM chips are exploited for hardware security applications including PUF, TRNG, and IC anti-counterfeiting. The proposed methodology leverages the latency and variability of COTS NVM chips for security primitives. The randomness of the generated bitstream is evaluated using the industry standard NIST SP 800-22 statistical test suite, and all 15 tests are passed. The obtained results validate the reliability and robustness of the extracted TRNG. Utilization of the existing NVM chips and no requirement for additional specialized hardware makes the proposed technique highly advantageous and cost-effective. A dedicated dataset through experimental characterization is also developed for conventional and emerging NVM technologies to train the ML classifier to high accuracy for detecting IC origin.