Side-Channel Attack Evaluation of Post-Quantum Cryptographic Algorithms and Architectures

PI: Mehran Mozaffari Kermani REUs: Trevor Ammons, Trent Callahan

Why Post-Quantum Cryptography?

1. **With the potential advent of quantum computers, public-key cryptographic algorithms will be broken.**
2. **Post-quantum cryptography ensures security and feasible implementation in post-quantum era.**
3. **The steady progress in quantum computing has motivated standardization by the NIST (Round2: March 2019).**

Side-Channel Attacks

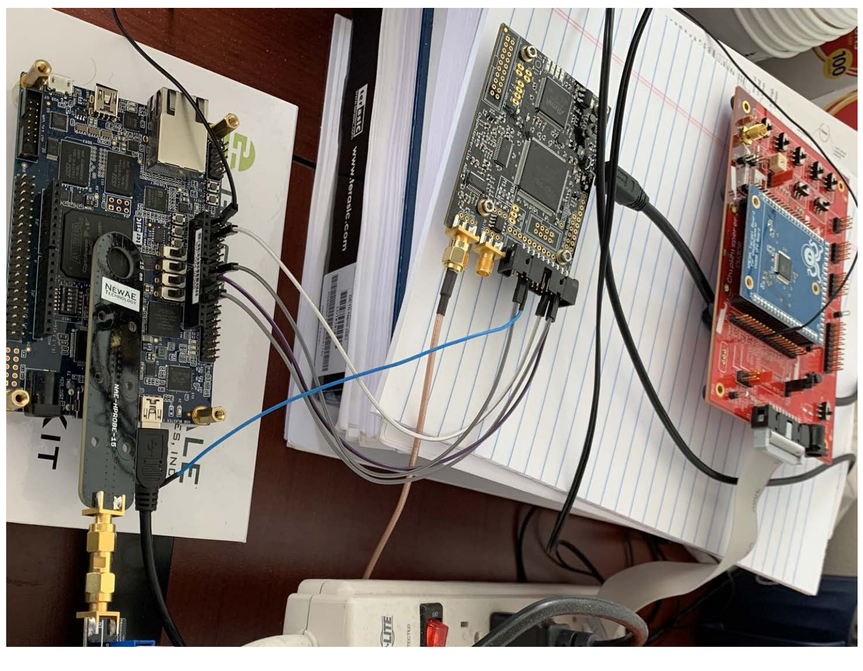
1. **Side channel attacks are indisputably much easier to mount and much more difficult to protect against compared to any algorithmic attacks based on special-purpose hardware.**
2. **Hardware implementation and side-channel attack analysis are generally not part of NIST standardization.**

As side-channel attacks are indisputably much easier to mount and much more difficult to protect against compared to any algorithmic attack, analyzing the vulnerability and providing solutions for post-quantum cryptographic algorithms is critical. This is important as such algorithms are not generally scrutinized in terms of such attacks in the standardization processes such as that of the NIST.

This project introduces another factor for scrutinizing the NIST candidates which is vulnerability to side-channel attacks and the cost of providing immunity to such attacks. Sixty-nine algorithms were proposed to NIST to find a replacement, now twenty-six remain. We hope that the results we provide help the next round of this competition.

The following steps are planned for the project:

1. EM waves and voltage analysis side-channel attacks measured by interfacing with the Chip Whisperer platform
2. H-Probe can measure EM waves and send the information to the Chip Whisperer
3. Each algorithm has C code that will be compiled to HEX code using the WinAVR compiler. The compiled HEX code will be implemented on the XMEGA board to run
4. The Chip Whisperer will be set up using Python code to interface with the XMEGA board. By running the same algorithm using random keys, any major variance observed in power consumption or EM waves can indicate information leakage



Broader Impacts:

(i) Since side-channel attacks for PQC are envisioned to be damaging, countermeasures are needed to thwart such attacks; we have developed in the past few months and plan to continue investigating various techniques to address this challenge for a variety of embedded systems, (ii) two female graduate students and a minority Hispanic Ph.D. student are involved in the project, (iii) two undergraduate students are involved in the project, (iv) work will be disseminated through well-known IEEE journals and conferences, and (v) research incorporated into course projects.