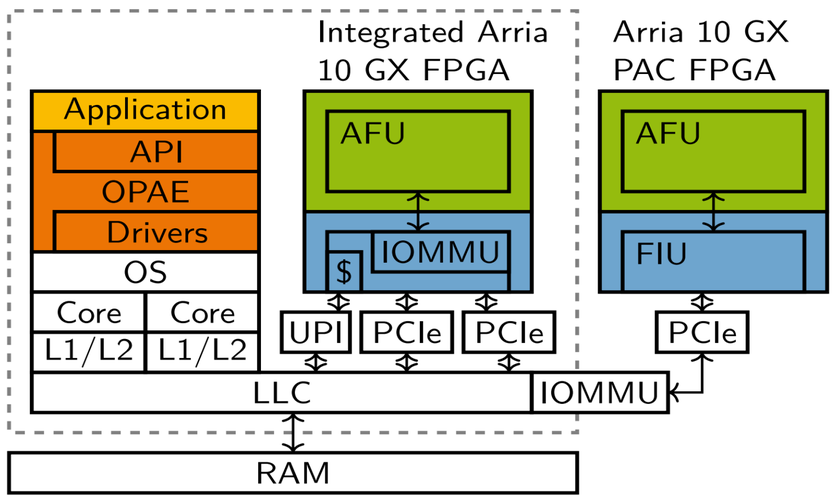
JackHammer: Rowhammer and Cache Attacks on Heterogeneous FPGA-CPU Platforms

Zane Weissman[1] **Thore Tiemann[2]** Daniel Moghimi[3],
Evan Custodio[4] Thomas Eisenbarth[2] Berk Sunar[1]
[1]Worcester Polytechnic Institute [2]University of Lübeck [3]UC San Diego [4]Amazon Web Services

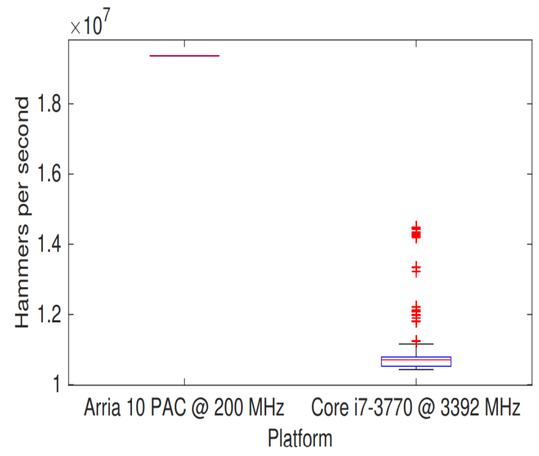
Abstract

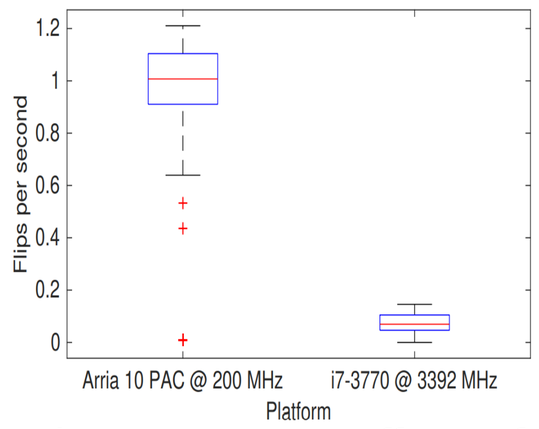
We studied two new **heterogeneous FPGA-CPU platforms** from Intel: the **integrated Arria 10 GX** which shares a chip with its host CPU, and the **Arria 10 GX PAC expansion card** which connects the FPGA to the CPU via a PCIe interface.



We show a **cache covert channel between FPGA and CPU** and **JackHammer**, which is a Rowhammer attack from FPGA against a host's main memory. It performs **twice as fast** as conventional CPU Rowhammer and causes **four times as many faults**.

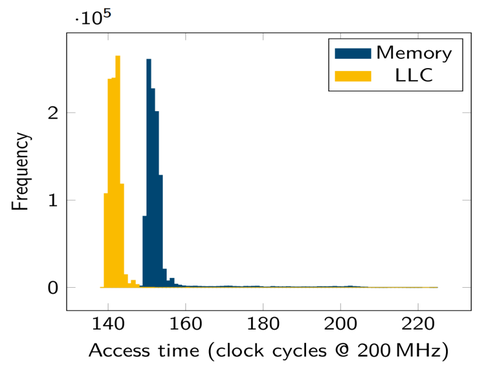
JackHammer

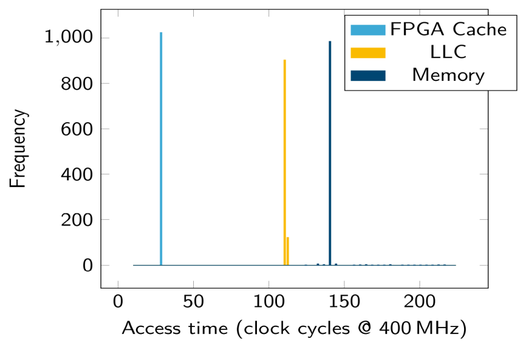




In the Rowhammer exploit, the electromagnetic effect of **repeated accesses to certain memory addresses causes stored bits in physically adjacent locations to flip their values**. JackHammer is our hardware Rowhammer implementation for Arria 10 GX FPGAs. It uses the PCIe interface to access the main memory. Compared to complicated modern CPUs, the Arria 10 GX has a **simpler memory access architecture**. **Memory reads bypass the CPU cache**, which eliminates the time-consuming flushing between memory accesses.

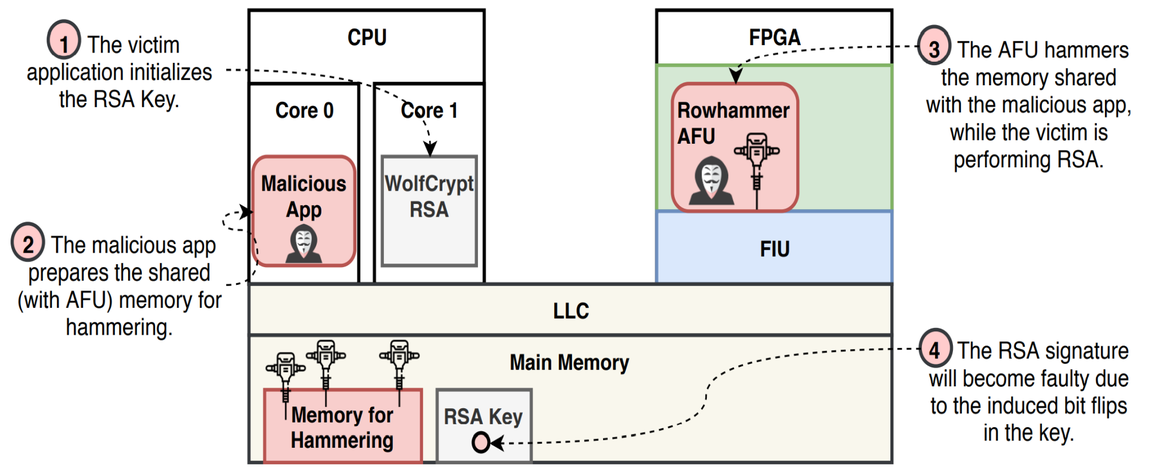
Caching Behavior





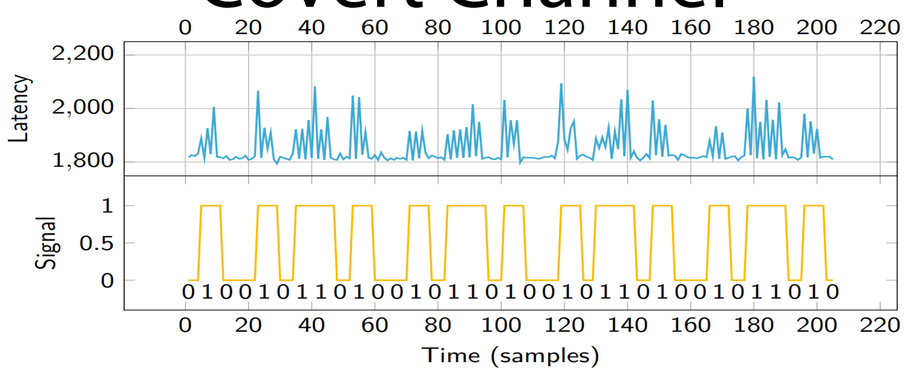
The **memory access latency** of the FPGA **depends on the location** answering a memory request. FPGA memory **reads do not alter the caching state** or location. FPGA memory **writes update the CPU's last level cache** state and data.

Fault Attack on WolfSSL RSA



We constructed a **fault injection attack against the RSA signing function in WolfSSL** [2], outlined in the figure above. When using JackHammer instead of a conventional CPU Rowhammer, **a key can be recovered an average of 17% faster**. With some typical defenses against Rowhammer exploits in place, JackHammer is **over three times more likely to cause a fault** than the same attack with CPU Rowhammer.

Covert Channel



We constructed a covert channel with the FPGA as the sender and a cooperative CPU program as receiver. The **FPGA sends binary messages by writing to a cache line** when transmitting a One and staying quiet otherwise. The **receiver continuously probes the cache set** to detect access latency fluctuations to receive the messages. While using heavily redundant encoding, we still achieve a **throughput of 94.98 kBit/s**.

References

[1] Weissman, Z., Tiemann, T., Moghimi, D., Custodio, E., Eisenbarth, T., & Sunar, B. (2020). JackHammer: Efficient Rowhammer on Heterogeneous FPGA-CPU Platforms. ***TCHES***, ***2020***(3), 169–195
[2] CVE-2019-19962. Available from MITRE, 2019.

Special thanks to Intel's Alpa Trivedi and Sayak Ray and former Intel's Evan Custodio for their guidance and support

Contact

Zane Weissman
zweissman@wpi.edu

Thore Tiemann
t.tiemann@uni-luebeck.de

UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR IT SECURITY

WPI