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

Zane Weissman
Thore Tiemann
Daniel Moghimi

October 2, 2020

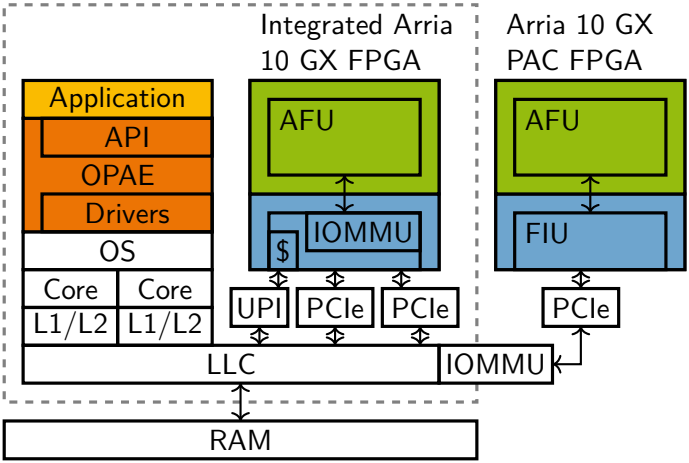
UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR IT SECURITY

Motivation

Motivation

Microsoft
Azure

Motivation



Motivation

Important Considerations

- Address spaces: physical, virtual, I/O virtual

Motivation

Important Considerations

- Address spaces: physical, virtual, I/O virtual
- Pages (4 KB) and hugepages (2 MB)

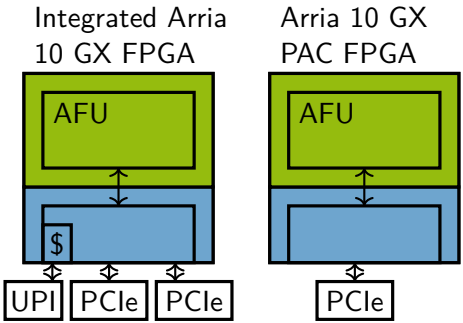
Motivation

Important Considerations

- Address spaces: physical, virtual, I/O virtual
- Pages (4 KB) and hugepages (2 MB)
- Which caches are/aren't modified by CPU/FPGA reads/writes/flushes

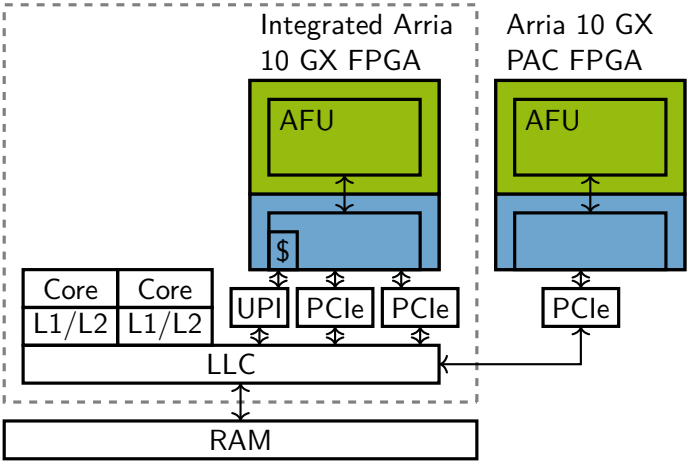
Background

Intel Acceleration Stack



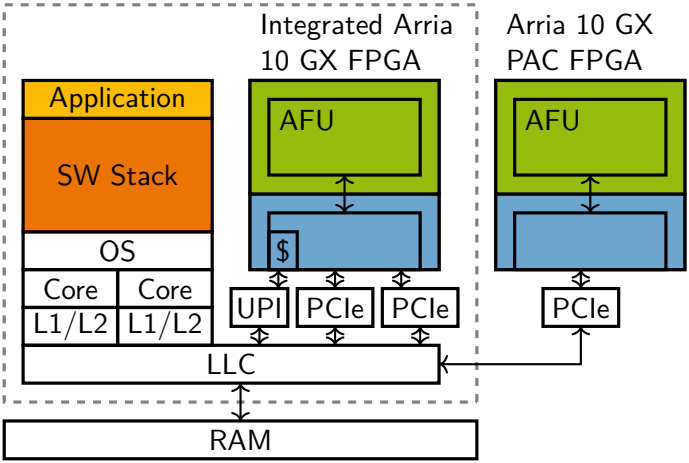
Background

Intel Acceleration Stack



Background

Intel Acceleration Stack



Background

Core Cache Interface Port

- MMIO
- DMA
  - Communication channels

Background

Core Cache Interface Port

- MMIO
- DMA
  - Communication channels
  - Physical addressing of (huge)pages

Background

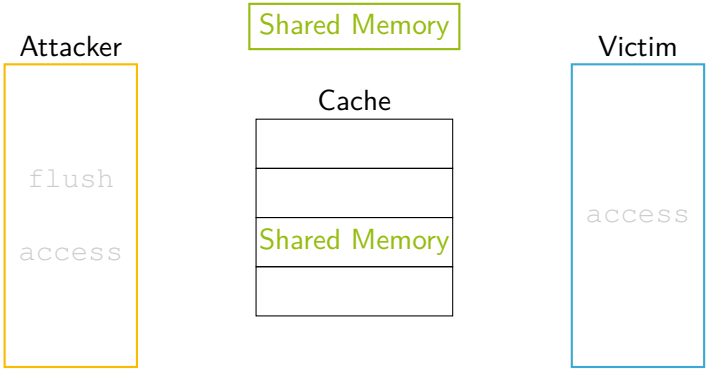
Core Cache Interface Port

- MMIO
- DMA
  - Communication channels
  - Physical addressing of (huge)pages
  - Caching hints

```
RdLine_I  WrLine_I
RdLine_S  WrLine_M
          WrPush_I
```

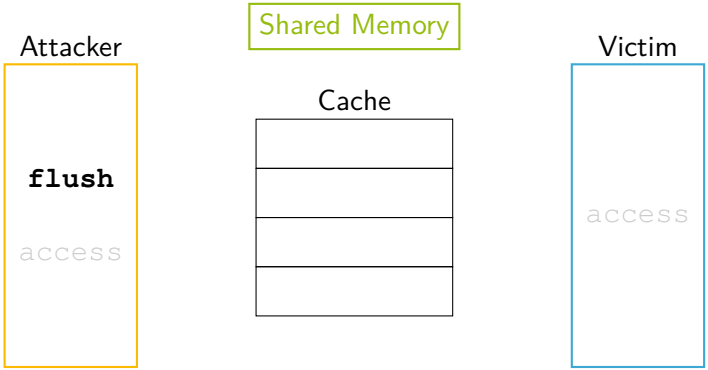
Cache Attacks

Background – Flush+Reload



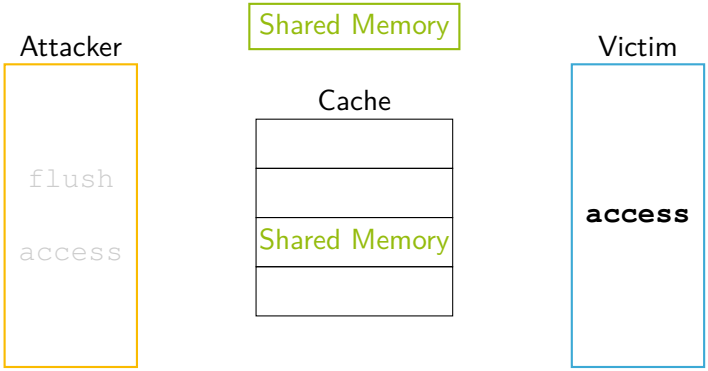
Cache Attacks

Background – Flush+Reload



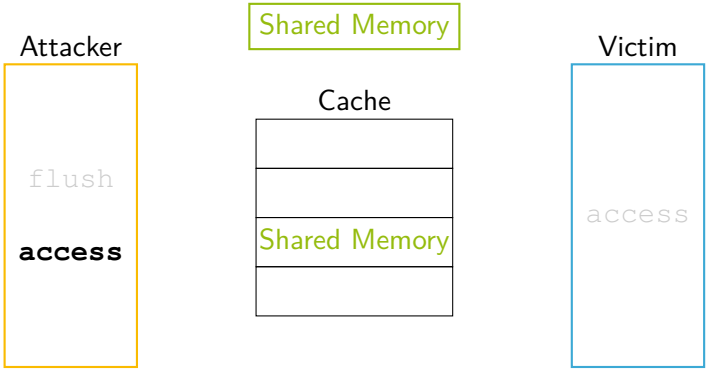
Cache Attacks

Background – Flush+Reload



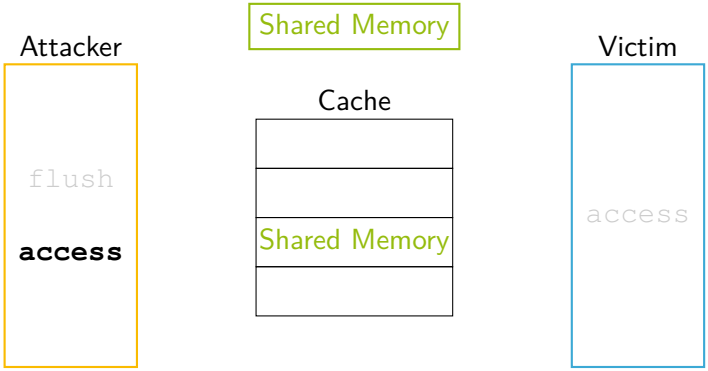
Cache Attacks

Background – Flush+Reload



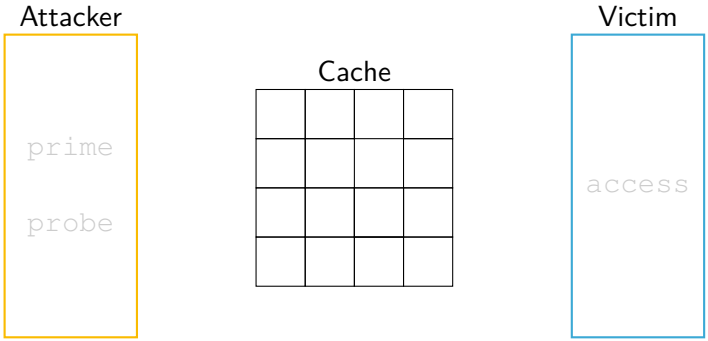
Cache Attacks

Background – Flush+Reload



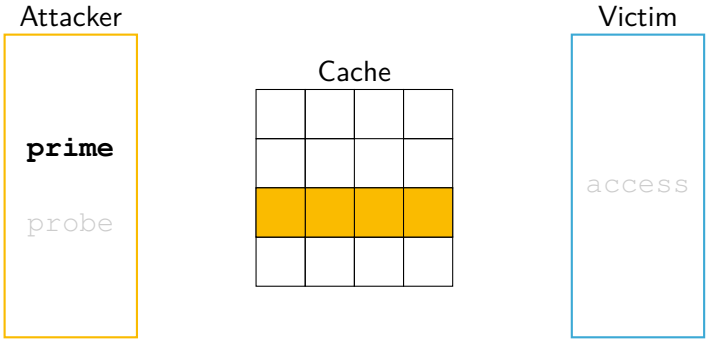
Cache Attacks

Background – Prime+Probe



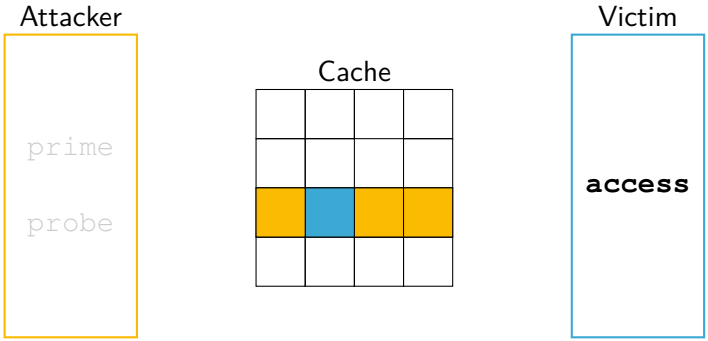
Cache Attacks

Background – Prime+Probe



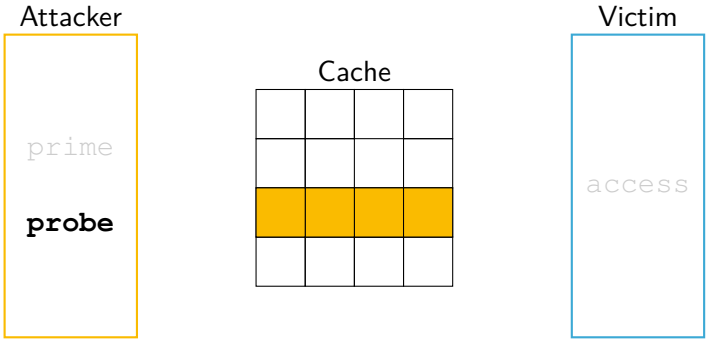
Cache Attacks

Background – Prime+Probe



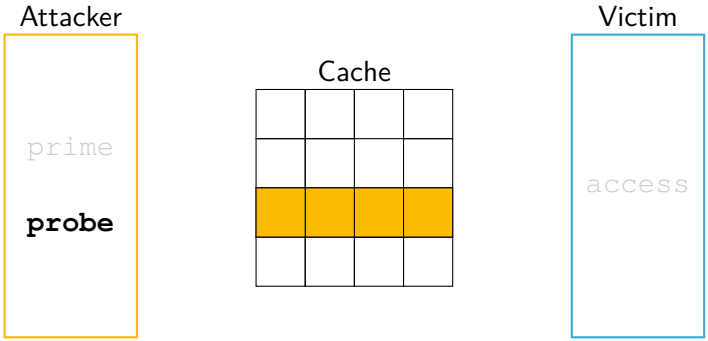
Cache Attacks

Background – Prime+Probe



Cache Attacks

Background – Prime+Probe

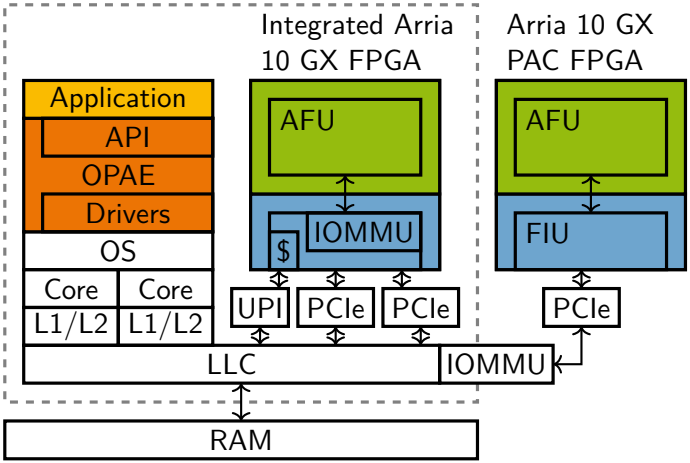


fast
Victim did not accessed

slow
Victim accessed

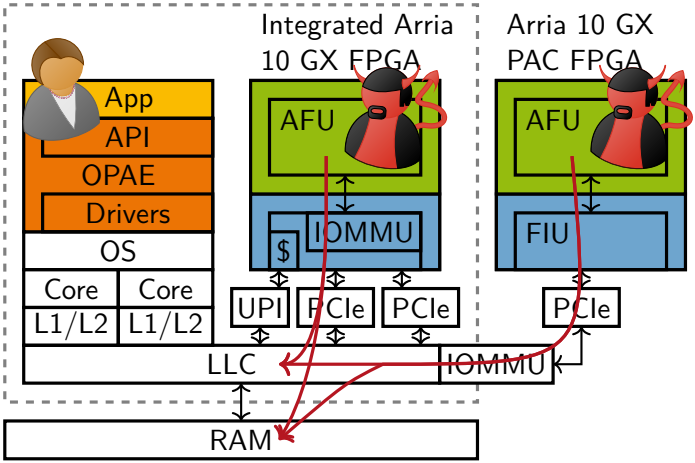
Cache Attacks

Attack Vectors – PCIe



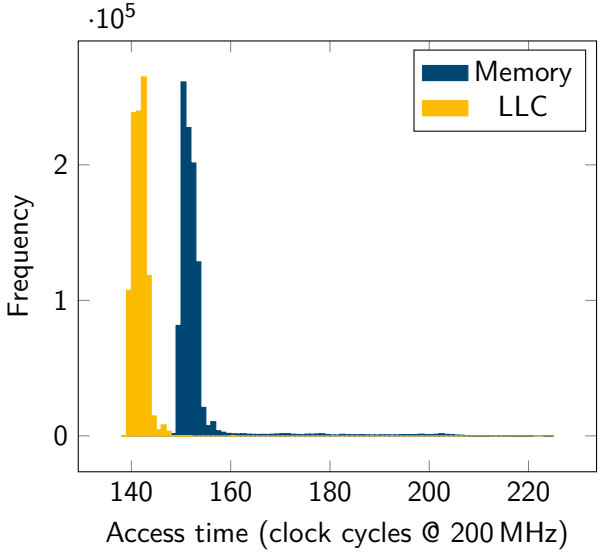
Cache Attacks

Attack Vectors – PCIe



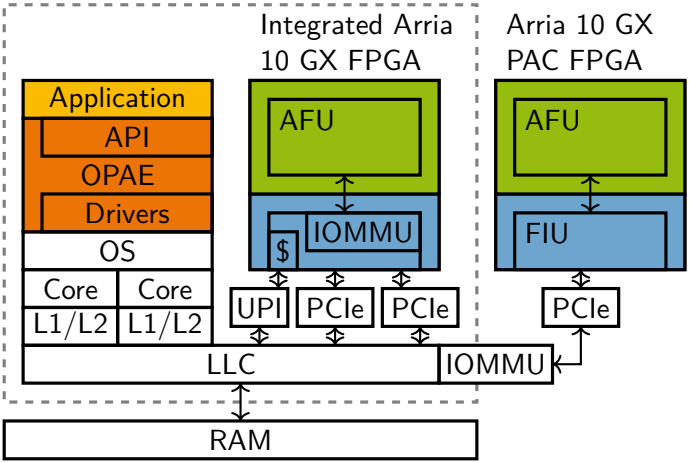
Cache Attacks

Attack Vectors – PCIe



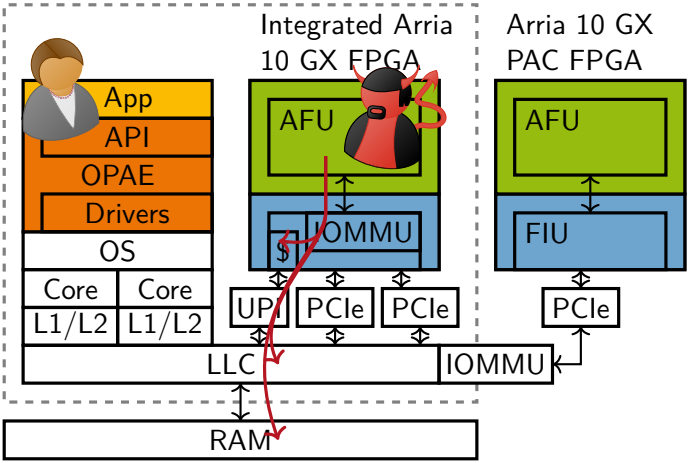
Cache Attacks

Attack Vectors – UPI



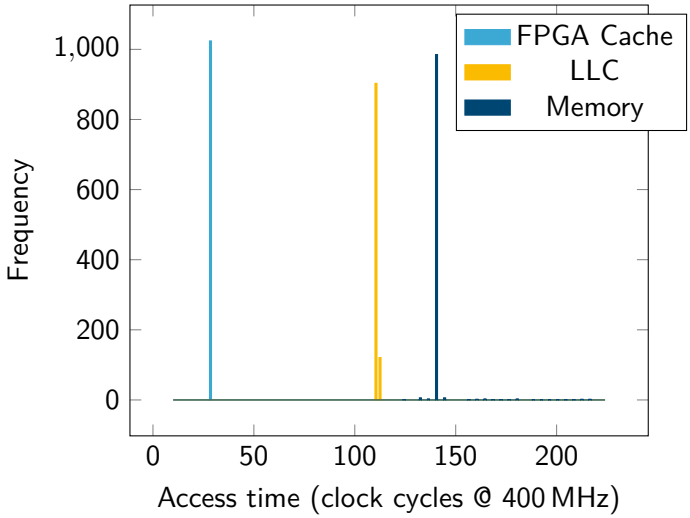
Cache Attacks

Attack Vectors – UPI



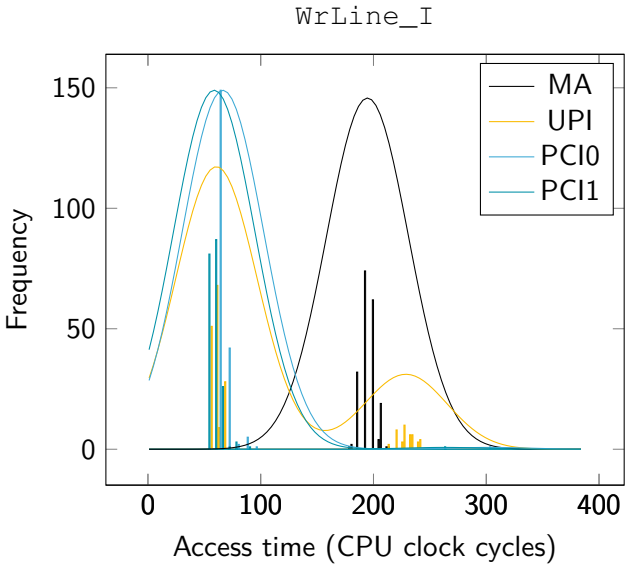
Cache Attacks

Attack Vectors – FPGA/UPI



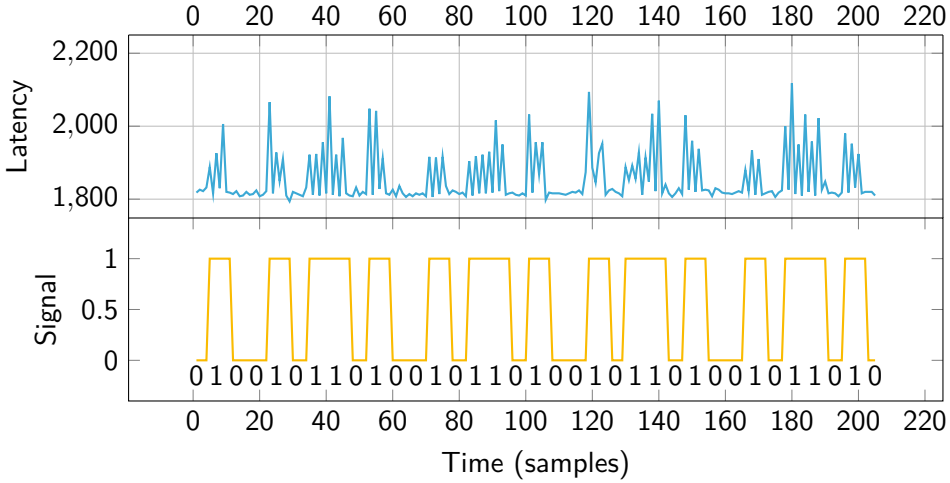
Cache Attacks

Attack Vectors – Caching Hints



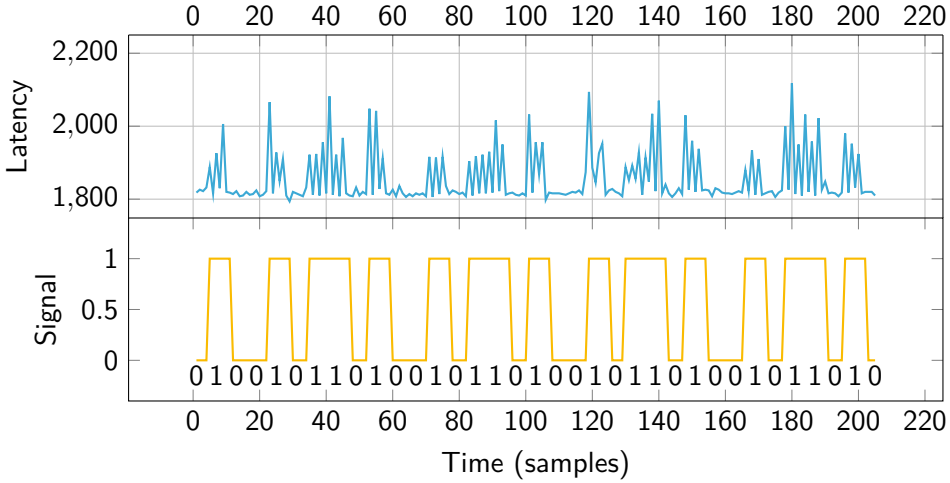
Cache Attacks

Covert Channel



Cache Attacks

Covert Channel



Throughput: 94.98 kBit/s

Cache Attacks

Summary of Cache Attack Analysis

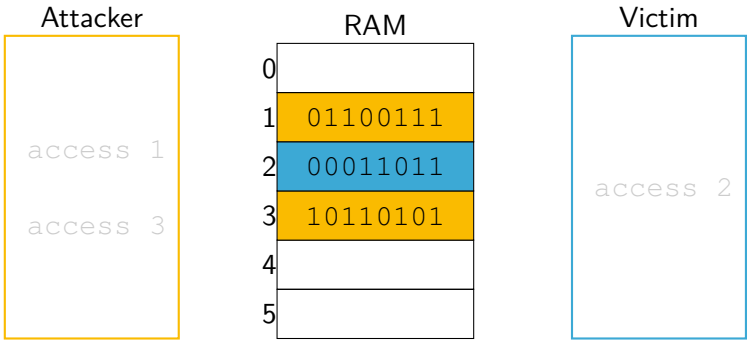
Attacker	Target	Channel	Attack
FPGA PAC AFU	CPU LLC	PCIe	E+T, E+R, P+P
Integrated FPGA AFU	CPU LLC	UPI	E+T, E+R, P+P
Integrated FPGA AFU	CPU LLC	PCIe	E+T, E+R, P+P
CPU	FPGA Cache	UPI	F+R, F+F
Integrated FPGA AFU	FPGA Cache	CCI-P	E+T, E+R, P+P

JackHammer

Background – Rowhammer

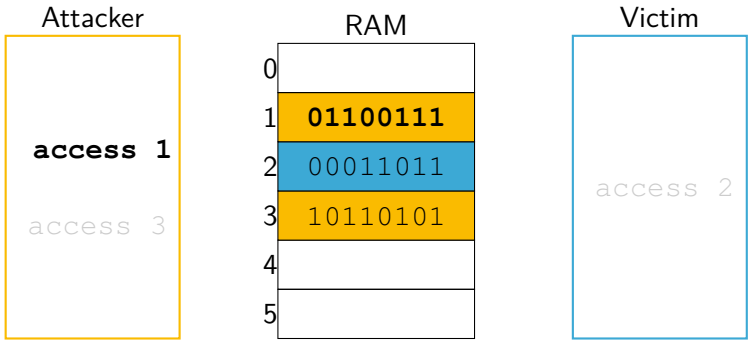
JackHammer

Background – Rowhammer



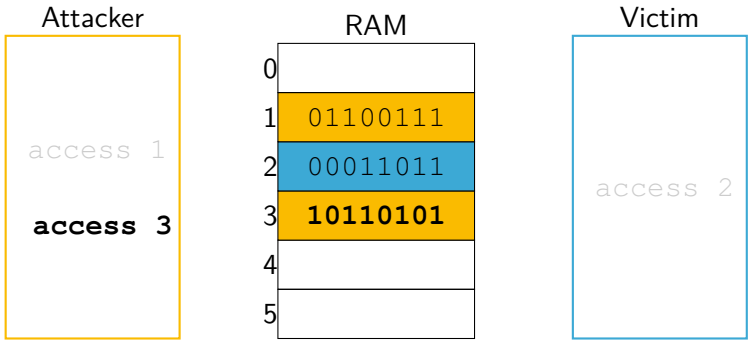
JackHammer

Background – Rowhammer



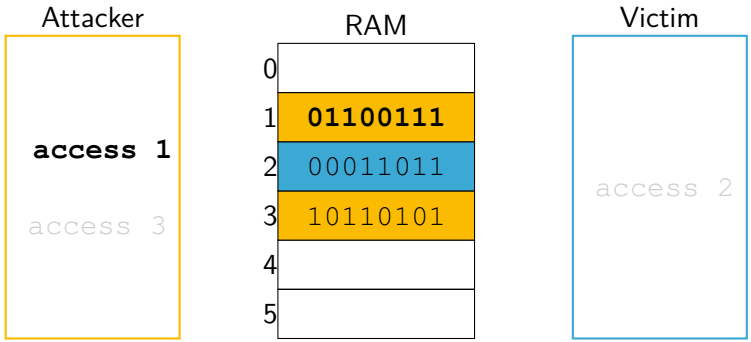
JackHammer

Background – Rowhammer



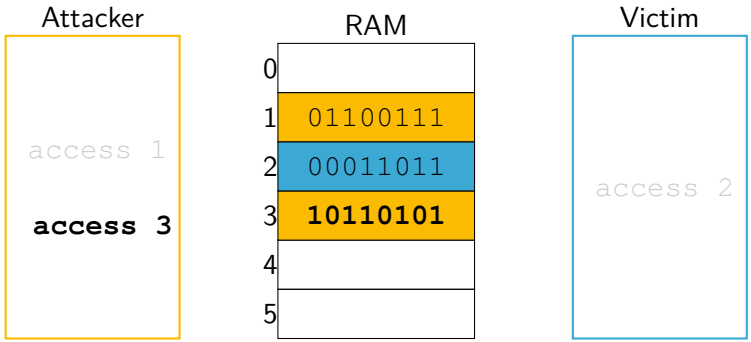
JackHammer

Background – Rowhammer



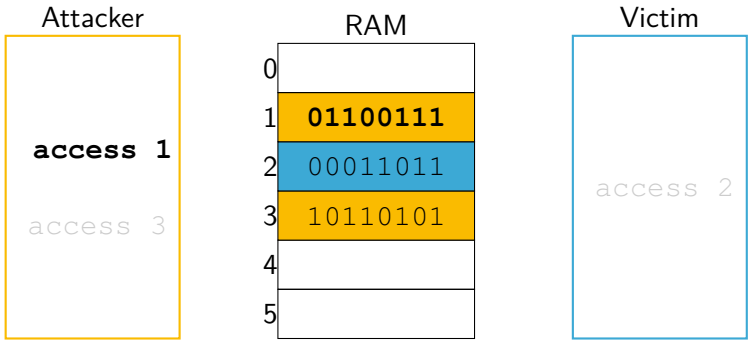
JackHammer

Background – Rowhammer



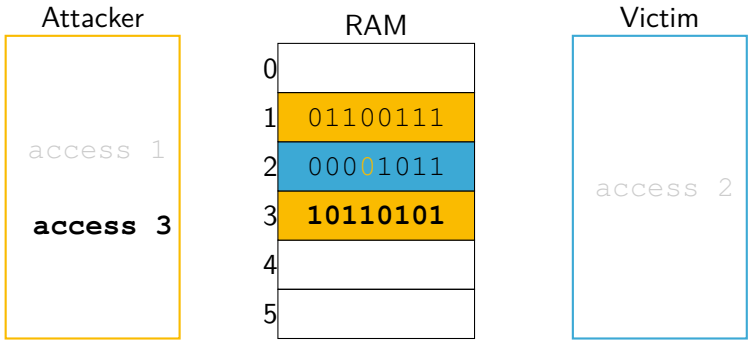
JackHammer

Background – Rowhammer



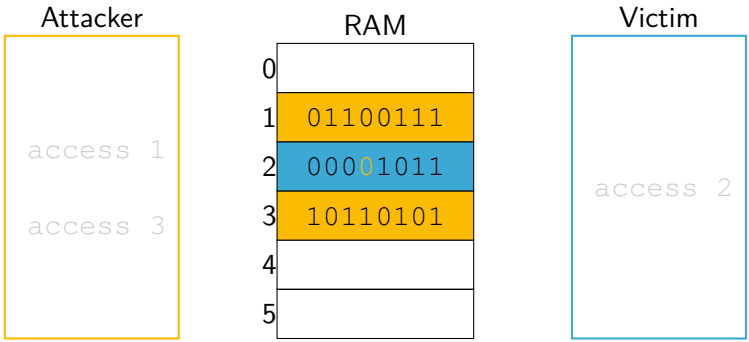
JackHammer

Background – Rowhammer



JackHammer

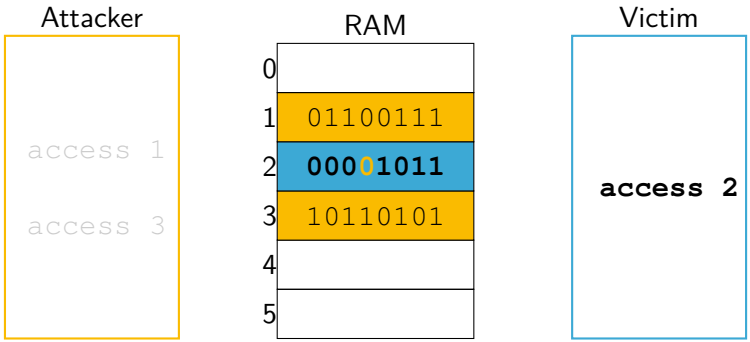
Background – Rowhammer



Z. Weissman,
T. Tiemann,
D. Moghimi

JackHammer

Background – Rowhammer



JackHammer

Background – Rowhammer

JackHammer

Background – Rowhammer

- **Aggressor rows** accessed by the attacker must be near **victim rows**

JackHammer

Background – Rowhammer

- **Aggressor rows** accessed by the attacker must be near **victim rows**
- Rows mapped by XORing bits of the physical address on most modern CPUs (desktop, server, mobile) - see “DRAMA” by Pessl et al.

JackHammer

Background – Rowhammer

- **Aggressor rows** accessed by the attacker must be near **victim rows**
- Rows mapped by XORing bits of the physical address on most modern CPUs (desktop, server, mobile) - see “DRAMA” by Pessl et al.
- Attack probably relies on electromagnetic effects

JackHammer

Background – Rowhammer

- **Aggressor rows** accessed by the attacker must be near **victim rows**
- Rows mapped by XORing bits of the physical address on most modern CPUs (desktop, server, mobile) - see “DRAMA” by Pessl et al.
- Attack probably relies on electromagnetic effects
- Simplest defense: increase automatic DRAM row refresh rate

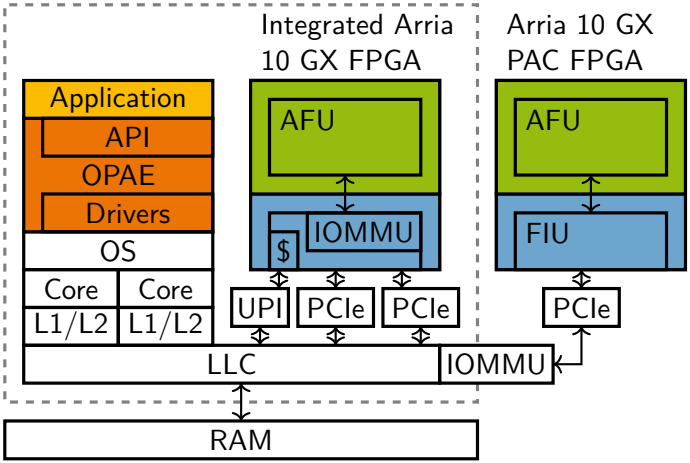
JackHammer

Background – Rowhammer

- **Aggressor rows** accessed by the attacker must be near **victim rows**
- Rows mapped by XORing bits of the physical address on most modern CPUs (desktop, server, mobile) - see “DRAMA” by Pessl et al.
- Attack probably relies on electromagnetic effects
- Simplest defense: increase automatic DRAM row refresh rate
- Shown to work on many DDR3, some DDR4, some ECC

JackHammer

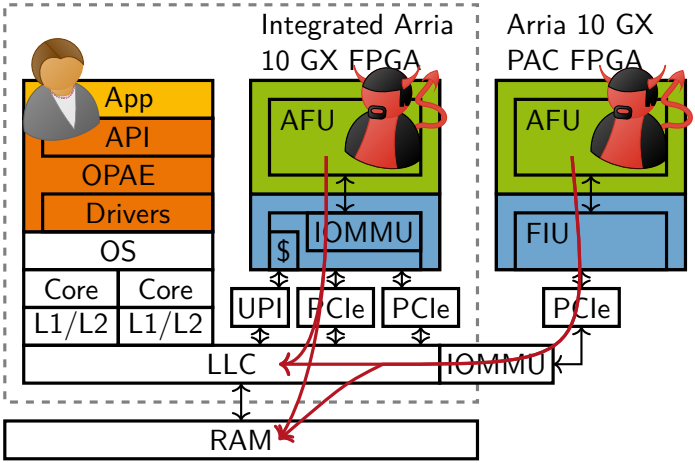
Background – Scenario



Z. Weissman,
T. Tiemann,
D. Moghimi

JackHammer

Background – Scenario

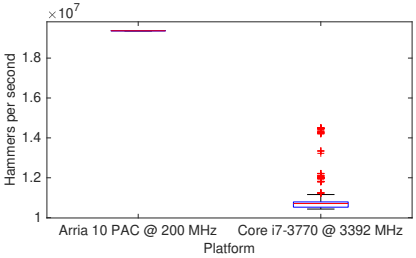


Z. Weissman,
T. Tiemann,
D. Moghimi

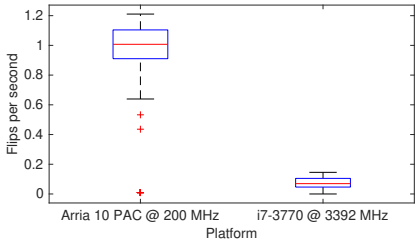
JackHammer

Performance

Hammering Rate



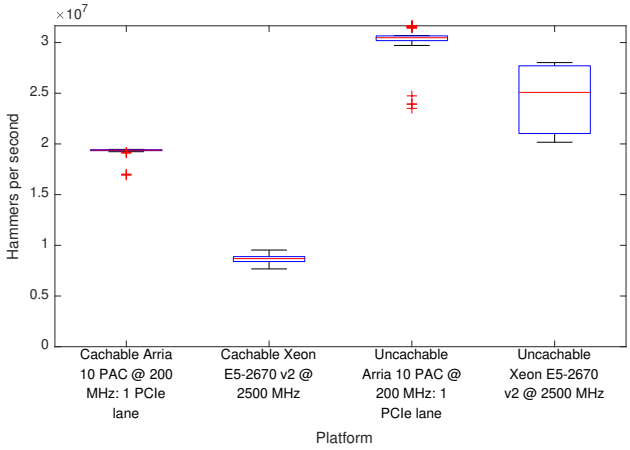
Flip Rate



JackHammer

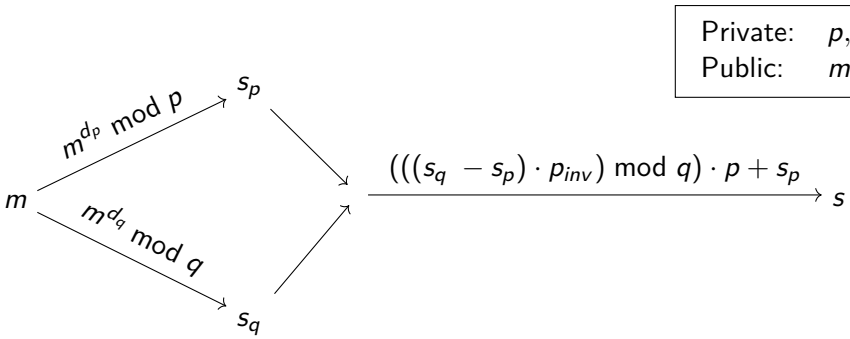
Caching and Rowhammer

Hammering rates with and without memory caching



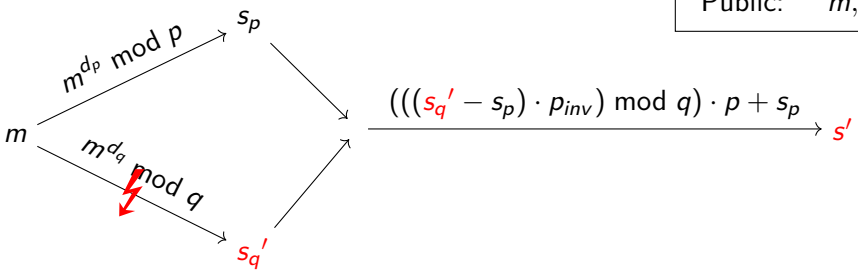
JackHammer

RSA-CRT Fault Injection



JackHammer

RSA-CRT Fault Injection



JackHammer

RSA-CRT Fault Injection

Private:	p, q, d_p, d_q
Public:	$m, s, N = pq$

$$
\begin{aligned}
& (((s'_q - s_p) \cdot p_{inv}) \bmod q) \cdot p + s_p \\
- \quad & (((s_q - s_p) \cdot p_{inv}) \bmod q) \cdot p + s_p \\
= \quad & (((s'_q - s_q) \cdot p_{inv}) \bmod q) \cdot p
\end{aligned}
$$

JackHammer

RSA-CRT Fault Injection

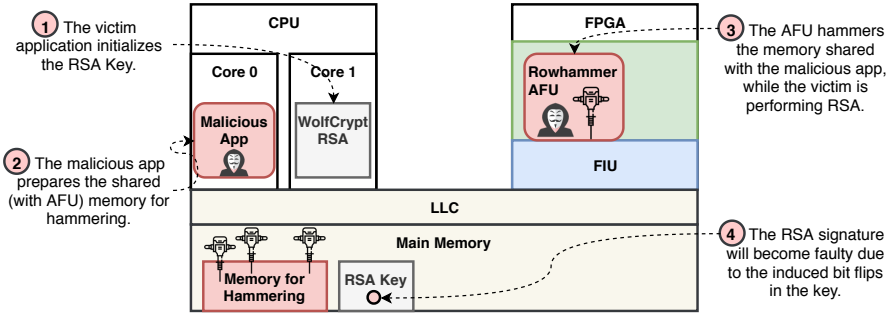
Private:	p, q, d_p, d_q
Public:	$m, s, N = pq$

$$
\begin{aligned}
& (((s'_q - s_p) \cdot p_{inv}) \bmod q) \cdot p + s_p \\
- \quad & (((s_q - s_p) \cdot p_{inv}) \bmod q) \cdot p + s_p \\
= \quad & (((s'_q - s_q) \cdot p_{inv}) \bmod q) \cdot p
\end{aligned}
$$

Bellcore Attack:
$\Rightarrow \gcd(s' - s, N) = p$

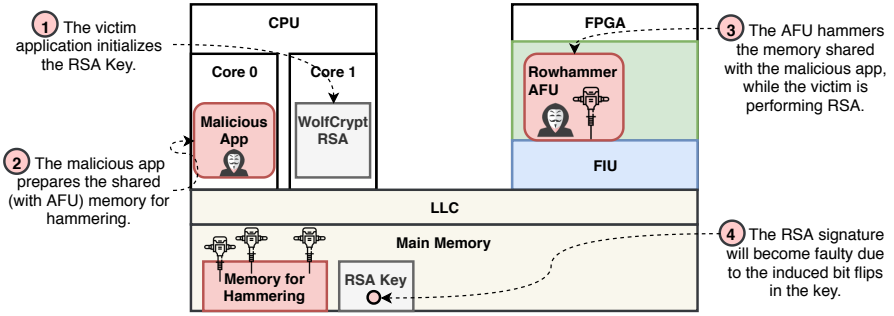
JackHammer

End-to-End Fault Injection Attack (WolfSSL CVE-2019-19962)



JackHammer

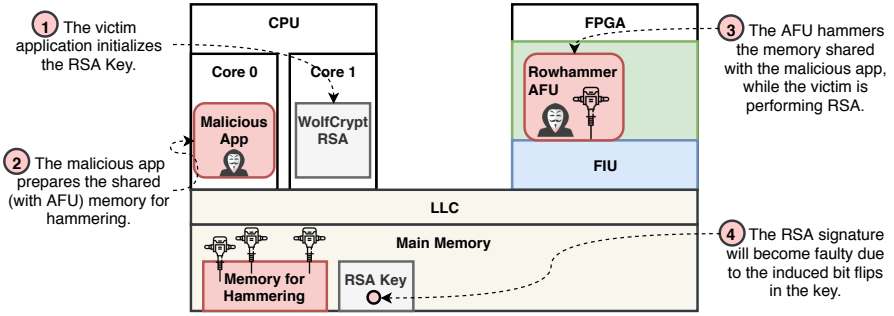
End-to-End Fault Injection Attack (WolfSSL CVE-2019-19962)



- Best case: JackHammer causes a fault 25% faster than CPU Rowhammer

JackHammer

End-to-End Fault Injection Attack (WolfSSL CVE-2019-19962)



- Best case: JackHammer causes a fault 25% faster than CPU Rowhammer
- With doubled DRAM row refresh rate: 185% faster than CPU

Conclusions

- Systematic verification of timing leakages

Conclusions

- Systematic verification of timing leakages
- Caching hint analysis

Conclusions

- Systematic verification of timing leakages
- Caching hint analysis
- Covert channel of 94.98 kBit/s

Conclusions

- Systematic verification of timing leakages
- Caching hint analysis
- Covert channel of 94.98 kBit/s
- Rowhammer performance acceleration by 25%

Conclusions

- Systematic verification of timing leakages
- Caching hint analysis
- Covert channel of 94.98 kBit/s
- Rowhammer performance acceleration by 25%
- CVE-2019-19962

Acknowledgements

- Berk Sunar @ WPI
- Thomas Eisenbarth @ UzL
- Evan Custodio @ ex-Intel
- Alpa Trivedi @ Intel

Thanks for your attention!

zweissman@wpi.edu t.tiemann@uni-luebeck.de

@danielmgmi @ThoreTiemann

Sponsors: