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

Zane Weissman Thore Tiemann Daniel Moghimi







JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS

CCI-P

Cache Attacks

Background Attack Vectors

PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer RSA-CRT Fault Injection

RSA-CRT Fault Injection End-to-End Fault Injection

Attack

Conclusions









Microsoft **Azure**

JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS

CCI-P

Cache Attacks

Background
Attack Vectors
PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection

Conclusions

Conclusions











JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

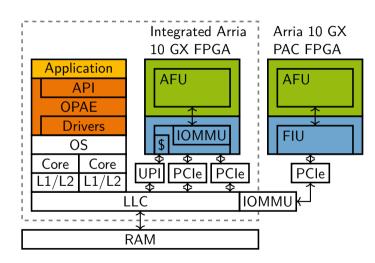
Performance
Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection

. .

Conclusions

Attack



JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

Backgroun

CCI-P

Cache Attacks

Background Attack Vectors

PCIe

UPI Covert Channel

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection

Conclusions

Important Considerations

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

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

CCI-I

Cache Attacks Background

Attack Vectors PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance Caching and Rowh

Caching and Rowhammer RSA-CRT Fault Injection End-to-End Fault Injection

. . .

Conclusions

Attack

Important Considerations

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

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

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

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors PCIe

PCle

Covert Channel

Summary of Cache Attack

Analysis

JackHammer Background

Performance

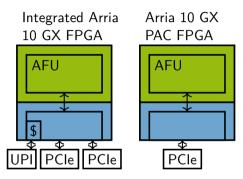
Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection

Conclusions

Attack

Intel Acceleration Stack



JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

CCI-

Cache Attacks

Background Attack Vectors

PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

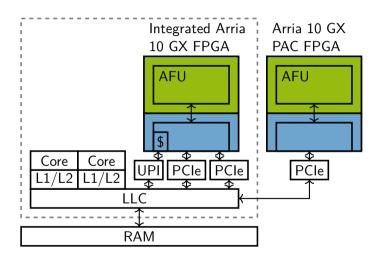
Performance
Caching and Rowhammer

RSA-CRT Fault Injection

End-to-End Fault Injection

Conclusions

Intel Acceleration Stack



JackHammer

Z. Weissman,

T. Tiemann, D. Moghimi

Motivation

Background

IAS

CCI-P

Cache Attacks

Background

Attack Vectors

PCIe UPI

Covert Channel

Summary of Cache Attack

Summary of Cache Att Analysis

JackHammer

Background Performance

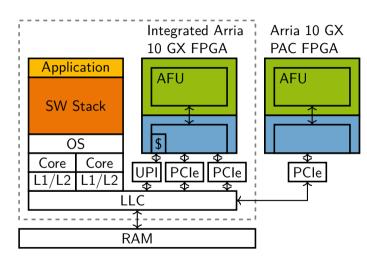
Caching and Rowhammer

RSA-CRT Fault Injection

End-to-End Fault Injection

Conclusions

Intel Acceleration Stack



JackHammer

Z. Weissman.

T. Tiemann. D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background

Attack Vectors

PCIe

HPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

Core Cache Interface Port

- ► MMIO
- ► DMA
 - Communication channels

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS

CCI-P

Cache Attacks

Background
Attack Vectors
PCIe
UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background Performance

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

Core Cache Interface Port

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

JackHammer

Z. Weissman, T. Tiemann,

D. Moghimi

Motivation

Background

IAS CCI-P

CCI-F

Cache Attacks

Background Attack Vectors PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance
Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection

Attack

Conclusions

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
```

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors PCIe

UPI Covert Channel

Covert Channel
Summary of Cache Attack
Analysis

JackHammer

Background Performance

Performance
Caching and Rowhammer

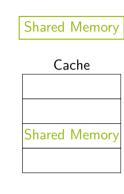
RSA-CRT Fault Injection
End-to-End Fault Injection

Conclusions

Attack

Background - Flush+Reload





Victim

JackHammer

Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background

Attack Vectors PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance Caching and Rowhammer

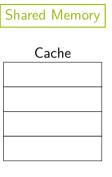
RSA-CRT Fault Injection End-to-End Fault Injection

Attack

Conclusions

Background - Flush+Reload

Attacker flush





JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

CCI-P

Cache Attacks

Background Attack Vectors

PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

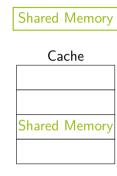
Caching and Rowhammer

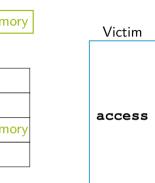
RSA-CRT Fault Injection End-to-End Fault Injection Attack

Conclusions

Background - Flush+Reload







JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance
Caching and Rowhammer

RSA-CRT Fault Injection
End-to-End Fault Injection

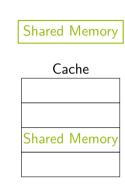
. . .

Conclusions

Attack

Background - Flush+Reload

Attacker access





JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background

Attack Vectors

PCIe UPI

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

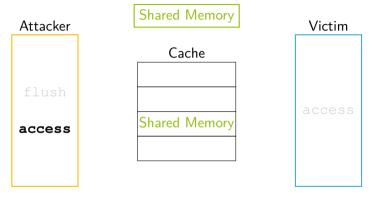
Performance

Caching and Rowhammer RSA-CRT Fault Injection

RSA-CRT Fault Injection End-to-End Fault Injection

Conclusions

Background – Flush+Reload



fast slow Victim accessed Victim did not access

JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

CCI-P

Cache Attacks

Background Attack Vectors

PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance
Caching and Rowhammer

RSA-CRT Fault Injection

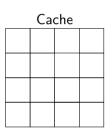
End-to-End Fault Injection

·----

Conclusions

Background - Prime+Probe







JackHammer

Z. Weissman,

T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

CCI-P

Cache Attacks

Background Attack Vectors

PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

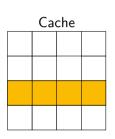
Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection

Conclusions

Background - Prime+Probe







JackHammer

Z. Weissman,

T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

CCI-P

Cache Attacks

Background Attack Vectors

PCle

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer

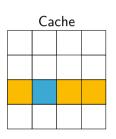
RSA-CRT Fault Injection End-to-End Fault Injection

Attack

Conclusions

Background - Prime+Probe







JackHammer

Z. Weissman,

T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

_

Cache Attacks
Background

Attack Vectors

PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer

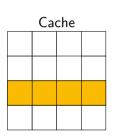
RSA-CRT Fault Injection End-to-End Fault Injection

Conclusions

Attack

Background - Prime+Probe







JackHammer

Z. Weissman,

T. Tiemann, D. Moghimi

Motivation

Background

IAS

CCI-P

Cache Attacks

Background Attack Vectors

PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

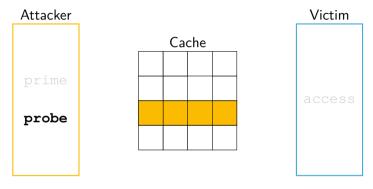
Performance
Caching and Rowhammer

RSA-CRT Fault Injection

End-to-End Fault Injection

Conclusions

Background - Prime+Probe



fast slow Victim did not accessed Victim accessed

JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

CCI-F

Cache Attacks

Background Attack Vectors

PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background Performance

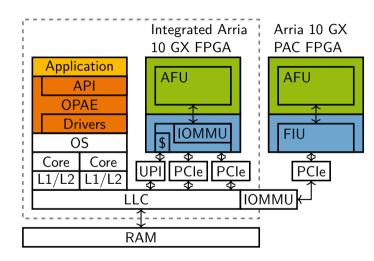
Caching and Rowhammer

RSA-CRT Fault Injection

End-to-End Fault Injection

Conclusions

Attack Vectors - PCIe



JackHammer

Z. Weissman,

T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background

Attack Vectors

UPI

Covert Channel

Summary of Cache Attack Analysis

Analysis Jack Hammer

Background

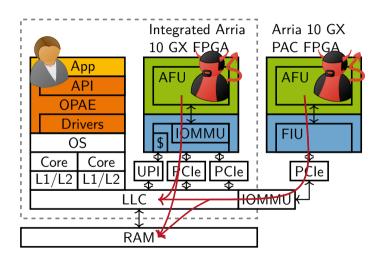
Performance

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection

Conclusions

Attack Vectors - PCIe



JackHammer

Z. Weissman.

T. Tiemann. D. Moghimi

Motivation

Background

IAS

CCI-P

Cache Attacks Background Attack Vectors

PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

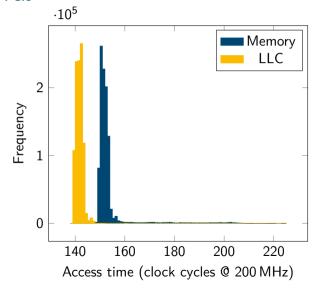
Background Performance

Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection Attack

Conclusions

Attack Vectors - PCle



JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

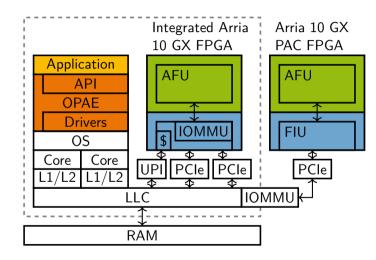
Background

Performance
Caching and Rowhammer
RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

Attack Vectors - UPI



JackHammer

Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe HPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

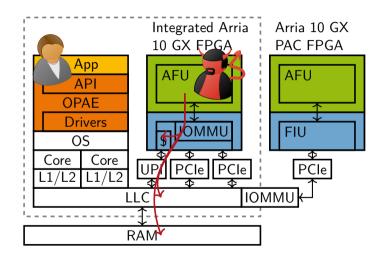
Porformanco

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

Attack Vectors - UPI



JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background Performance

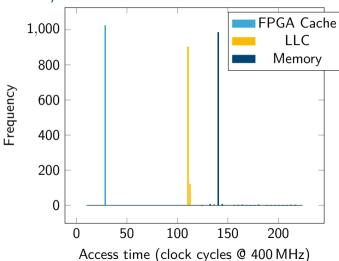
Performance
Caching and Rowhammer

RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

Attack Vectors - FPGA/UPI



JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe
UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

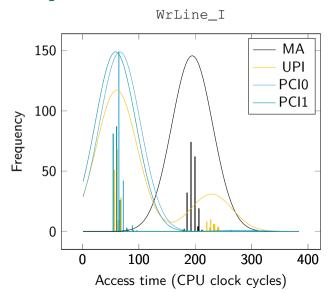
Background

Performance
Caching and Rowhammer

RSA-CRT Fault Injection
End-to-End Fault Injection

Attack Conclusions

Attack Vectors - Caching Hints



JackHammer

Z. Weissman. T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

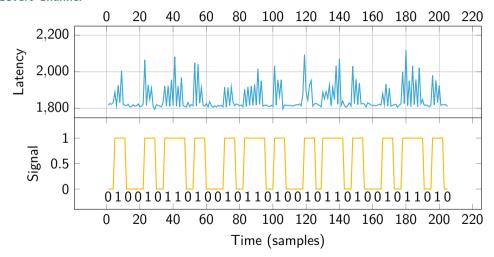
Background Performance

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

Covert Channel



JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background
Attack Vectors
PCIe

UPI

Covert Channel
Summary of Cache Attack

Analysis

JackHammer Background

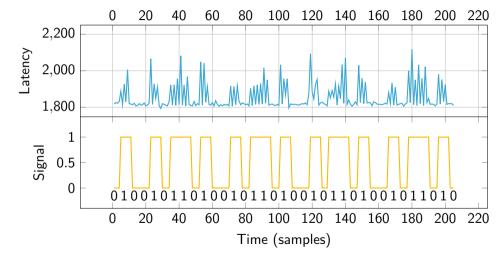
Performance
Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection

Conclusions

Attack

Covert Channel



Throughput: 94.98 kBit/s

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

CCI-P

Background

Cache Attacks

Background
Attack Vectors
PCIe

UPI Covert Channel

Covert Channel
Summary of Cache Attack
Analysis

JackHammer

Background
Performance
Caching and Rowhammer
RSA-CRT Fault Injection

.....

Conclusions

Acknowledgements

End-to-End Fault Injection

Summary of Cache Attack Analysis

| Attacker | Target | Channel | Attack |
|---------------------|------------|---------|--------------------|
| FPGA PAC AFU | CPU LLC | PCle | E+T, E+R, P+P |
| Integrated FPGA AFU | CPU LLC | UPI | E+T, $E+R$, $P+P$ |
| Integrated FPGA AFU | CPU LLC | PCle | 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

Z. Weissman, T. Tiemann,

D. Moghimi

Motivation

Background

IAS CCI-P

CCI-P

Cache Attacks

Background Attack Vectors

PCle UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance
Caching and Rowl

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

JackHammer

Background - Rowhammer

JackHammer

Z. Weissman, T. Tiemann,

D. Moghimi

Motivation

Background

IAS CCI-P

CCI-P

Cache Attacks

Attack Vectors

PCle UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

ackground

Performance

Caching and Rowhammer RSA-CRT Fault Injection

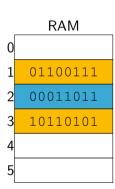
End-to-End Fault Injection Attack

Conclusions

JackHammer

Background - Rowhammer







JackHammer

Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer RSA-CRT Fault Injection End-to-End Fault Injection

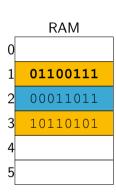
Attack

Conclusions

JackHammer

Background - Rowhammer







JackHammer

Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

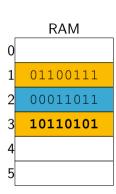
Caching and Rowhammer RSA-CRT Fault Injection End-to-End Fault Injection

Conclusions

Attack

Background - Rowhammer







JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

CCI-P

Cache Attacks

Background Attack Vectors

PCIe UPI

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Performance
Caching and Rowhammer

Caching and Rowhammer RSA-CRT Fault Injection End-to-End Fault Injection

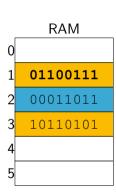
Conclusions

Attack

Conclusions

Background - Rowhammer







JackHammer

Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background

Attack Vectors PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

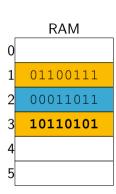
Performance Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection Attack

Conclusions

Background - Rowhammer







JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

CCI-P

Cache Attacks

Background Attack Vectors

PCIe UPI

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Performance
Caching and Rowhammer

Caching and Rowhammer RSA-CRT Fault Injection End-to-End Fault Injection

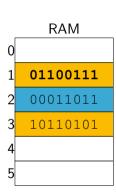
Conclusions

Attack

Conclusions

Background - Rowhammer







JackHammer

Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background

Attack Vectors PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

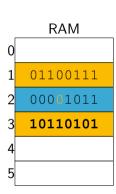
Performance Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection Attack

Conclusions

Background - Rowhammer







JackHammer

Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

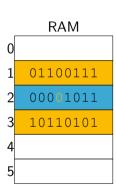
Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

Background - Rowhammer







JackHammer

Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

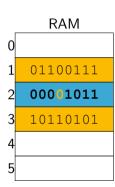
Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

Background - Rowhammer







JackHammer

Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer RSA-CRT Fault Injection End-to-End Fault Injection

Conclusions

Attack

Background - Rowhammer

JackHammer

Z. Weissman, T. Tiemann,

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection Attack

Conclusions

Background - Rowhammer

▶ Aggressor rows accessed by the attacker must be near victim rows

JackHammer

Z. Weissman, T. Tiemann. D. Moghimi

Motivation

Background

IAS CCI-P

Background

Cache Attacks

Attack Vectors

PCIe UPI

Covert Channel

Summary of Cache Attack

Analysis

JackHammer

Background

Performance

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

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

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS

CCI-P

Cache Attacks

Background Attack Vectors PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Background

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

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

Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors PCIe

HPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Porformanco

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

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

Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors PCIe

HPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Porformanco

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

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

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

CCI-P

Cache Attacks

Background Attack Vectors PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

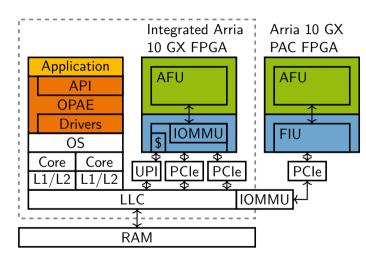
Performance

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

Background - Scenario



JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

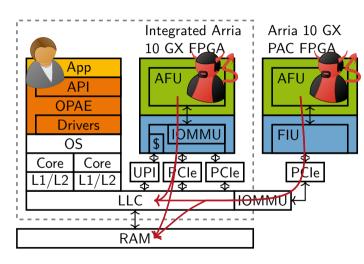
Performance

Caching and Rowhammer

End-to-End Fault Injection
Attack

Conclusions

Background - Scenario



JackHammer

Z. Weissman,

T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe UPI

Covert Channel

Summary of Cache Attack

Analysis

JackHammer Background

Performance

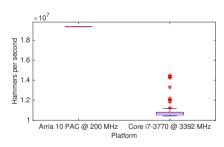
Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

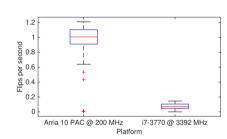
Conclusions

Performance

Hammering Rate



Flip Rate



JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCIe UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Attack

Background Performance

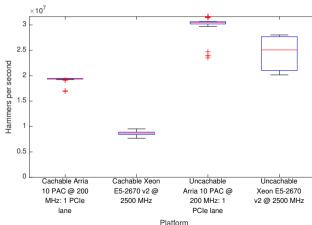
Performance
Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection

Conclusions

Caching and Rowhammer

Hammering rates with and without memory caching



JackHammer

Z. Weissman.

T. Tiemann. D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors PCIe UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background Performance

Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection

Attack

Conclusions

RSA-CRT Fault Injection



Z. Weissman. T. Tiemann.

D. Moghimi

Motivation

Background IAS

CCI-P

Cache Attacks Background

Attack Vectors PCIe UPI

Covert Channel Summary of Cache Attack

Analysis

JackHammer

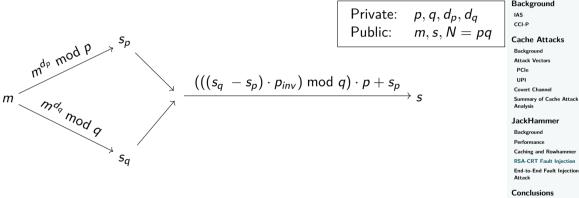
Background

Performance

Caching and Rowhammer RSA-CRT Fault Injection

Attack

Conclusions



RSA-CRT Fault Injection

JackHammer

Z. Weissman, T. Tiemann,

D. Moghimi

Motivation

Background

CCI-P

Cache Attacks

Background Attack Vectors PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

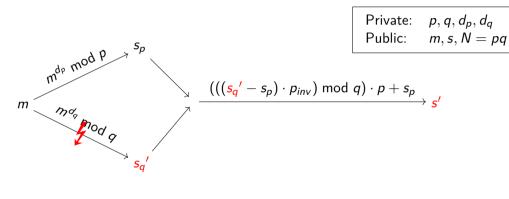
Background

Performance

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions



RSA-CRT Fault Injection

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

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

_....

Motivation

Background

IAS
CCI-P

Cache Attacks Background Attack Vectors

PCIe UPI Covert Channel

Covert Channel
Summary of Cache Attack
Analysis

JackHammer

Background Performance

Performance
Caching and Rowhammer
RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

RSA-CRT Fault Injection

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

$$\begin{aligned} & \left(\left(\left(s_{q}' - s_{p} \right) \cdot p_{inv} \right) \bmod q \right) \cdot p + s_{p} \\ - & \left(\left(\left(s_{q} - s_{p} \right) \cdot p_{inv} \right) \bmod q \right) \cdot p + s_{p} \\ = & \left(\left(\left(s_{q}' - s_{q} \right) \cdot p_{inv} \right) \bmod q \right) \cdot p \end{aligned}$$

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

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

CCI-P

Cache Attacks

IAS

Background Attack Vectors PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

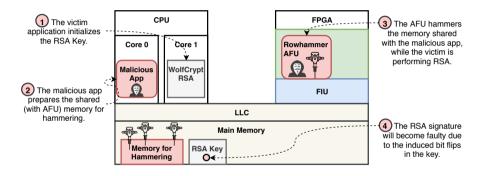
Background
Performance

Performance Caching and Rowhammer

RSA-CRT Fault Injection
End-to-End Fault Injection
Attack

Conclusions

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



JackHammer

Z. Weissman,

T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background
Attack Vectors

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

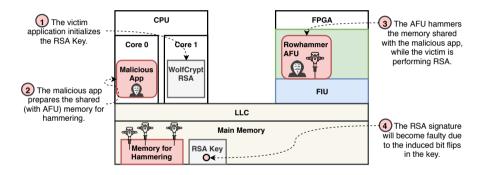
Background

Caching and Rowhammer

End-to-End Fault Injection Attack

Conclusions

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



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

JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS

CCI-P

Cache Attacks

Background Attack Vectors

Attack Vectors PCIe

UPI Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background Performance

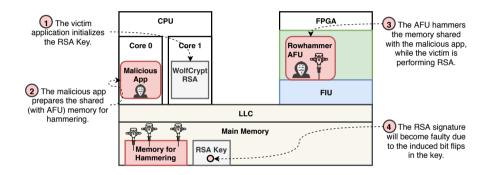
Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection

End-to-End Fault Attack

Conclusions

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

JackHammer

- Z. Weissman, T. Tiemann.
- D. Moghimi

Motivation

Background

Background

CCI-P

Cache Attacks

Background Attack Vectors

PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background Performance

Caching and Rowhammer

RSA-CRT Fault Injection

End-to-End Fault Injection

Conclusions

► Systematic verification of timing leakages

JackHammer

Z. Weissman. T. Tiemann. D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks Background

Attack Vectors PCIe UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer RSA-CRT Fault Injection End-to-End Fault Injection

Conclusions

Attack

- ► Systematic verification of timing leakages
- ► Caching hint analysis

JackHammer

Z. Weissman. T. Tiemann. D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks Background

Attack Vectors PCIe

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background Performance

Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection

Attack

Conclusions

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

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCle

UPI Covert Channel

Covert Channel Summary of Cache Attack

Analysis

JackHammer

Јаскпатте

Background Performance

Caching and Rowhammer

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

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

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

CCI-F

Cache Attacks

Background

Attack Vectors

PCle

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

skaraund

Background

Performance
Caching and Rowl

Caching and Rowhammer

End-to-End Fault Injection Attack

Conclusions

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

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks

Background Attack Vectors

PCle

UPI

Covert Channel

Summary of Cache Attack Analysis

JackHammer

Background

Performance

Caching and Rowhammer

End-to-End Fault Injection Attack

Conclusions

Acknowledgements

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

JackHammer

Z. Weissman, T. Tiemann, D. Moghimi

Motivation

Background

IAS CCI-P

Cache Attacks Background

Attack Vectors

PCle

UPI

Covert Channel Summary of Cache Attack

Analysis

JackHammer

JackHamme

Background Performance

Caching and Rowhammer RSA-CRT Fault Injection

End-to-End Fault Injection Attack

Conclusions

Thanks for your attention!

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

🍠 @danielmgmi @ThoreTiemann

Sponsors:





JackHammer

Z. Weissman, T. Tiemann.

D. Moghimi

Motivation

Background

IAS

CCI-P

Cache Attacks

Background
Attack Vectors
PCIe

UPI

Covert Channel

Summary of Cache Attack

Analysis

JackHammer Background

Performance

Performance
Caching and Rowhammer

RSA-CRT Fault Injection End-to-End Fault Injection

Attack Conclusions

Conclusion