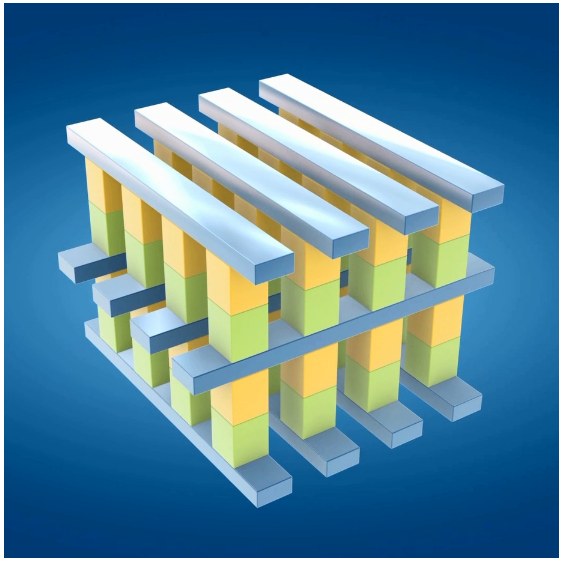
NVCool: When Non-Volatile Caches Meet Cold Boot Attacks

Xiang Pan[†], Anys Bacha[‡], Spencer Rudolph, Li Zhou, Yinqian Zhang, and Radu Teodorescu

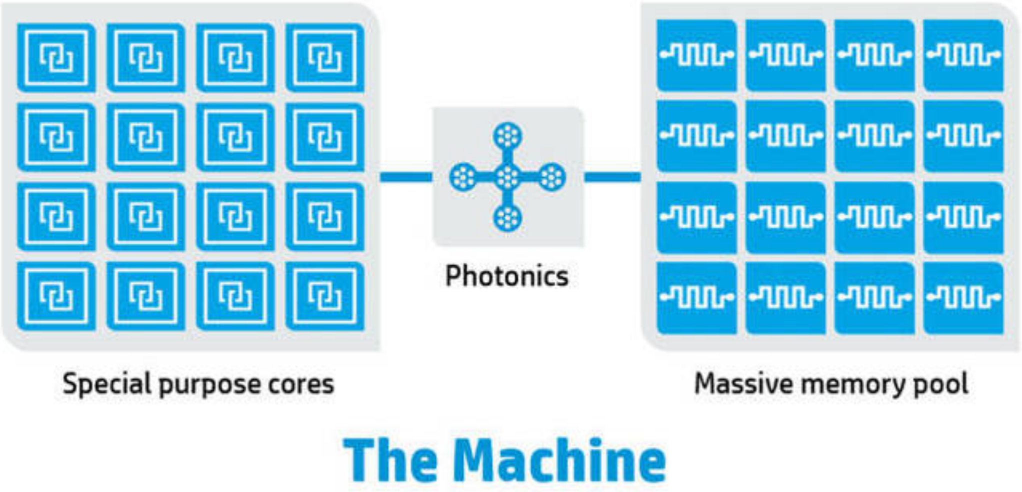
The Ohio State University, Uber[†], University of Michigan[‡]

Non-Volatile Memory is Coming

- Low power, high density, and good scalability make NVM attractive to industry companies
- 3D XPoint from Intel and Micron



- The Machine from HPE



- Crossbar and Everspin also make and sell NVM products

Cold Boot Attack on DRAM

- Cooling DRAM to a certain low temperature can preserve its data for a short duration of time even without power supply

Halderman et al., Lest We Remember: Cold Boot Attacks on Encryption Keys, citp.princeton.edu/research/memory

- Plug in the frozen DRAM DIMMs to a pre-prepared machine and run key search program to get secret keys
- Successfully conducted on both laptop and mobile computer systems

Cold Boot Attack on NVM

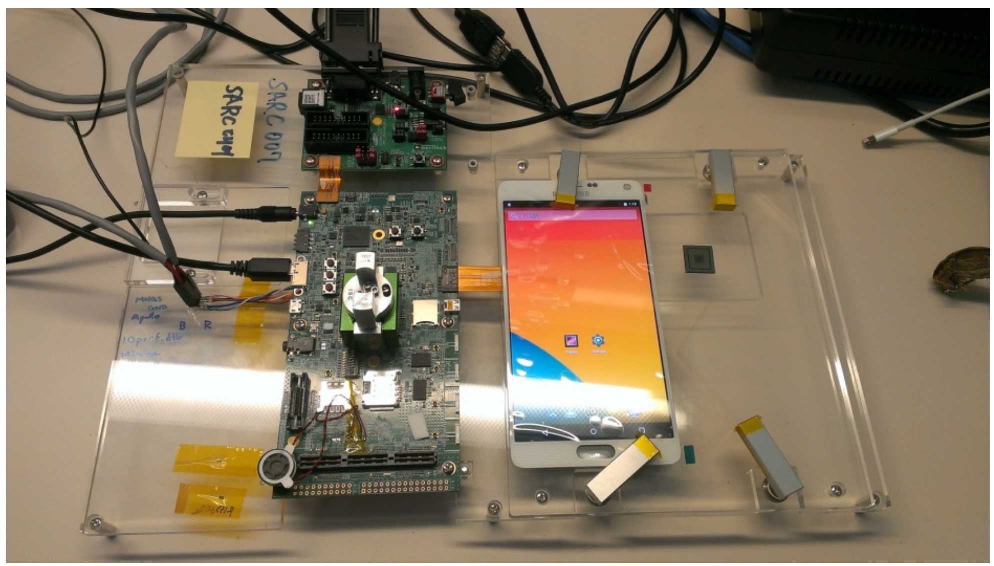
- Trivial for NVM main memory but we focus on NVM caches
- NVM caches are vulnerable to cold boot attacks in a way SRAM caches are not
    - A few ms data retention time without power supply at cold temperatures
- Challenges
    - Caches only store a subset of data
    - Cache structure (set-associative) is very different from main memory (page)
    - Can we really find secrets from NVM caches?

Outline

- **Threat Model**
- Cache-Aware AES Key Search
- Methodology
- Attack Analysis
- Countermeasure
- Conclusions

Threat Model

- Attacker has physical access to the victim device
- Attacker has necessary equipments and knowledge to extract data from CPU caches



Threat Model

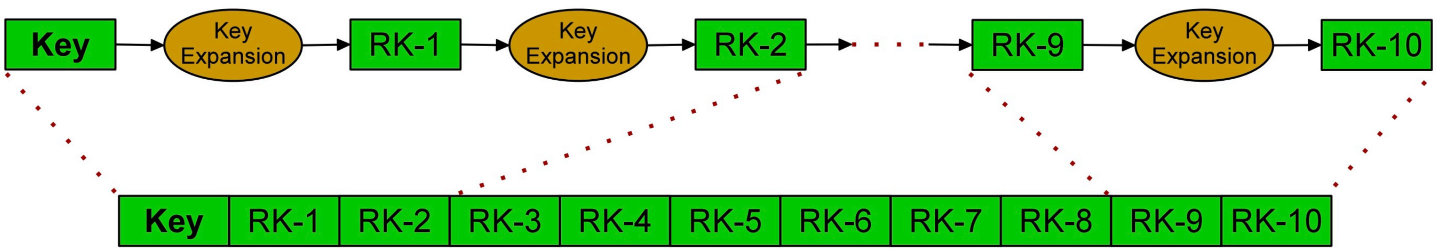
- What secrets can be found from cache?
  - Photos, emails, messages, disk encryption keys, ssh keys…
  - Anything stored in cache and useful to attacker
  - This work focuses on disk encryption keys as an example

Outline

- Threat Model
- **Cache-Aware AES Key Search**
- Methodology
- Attack Analysis
- Countermeasure
- Conclusions

AES Key Schedule

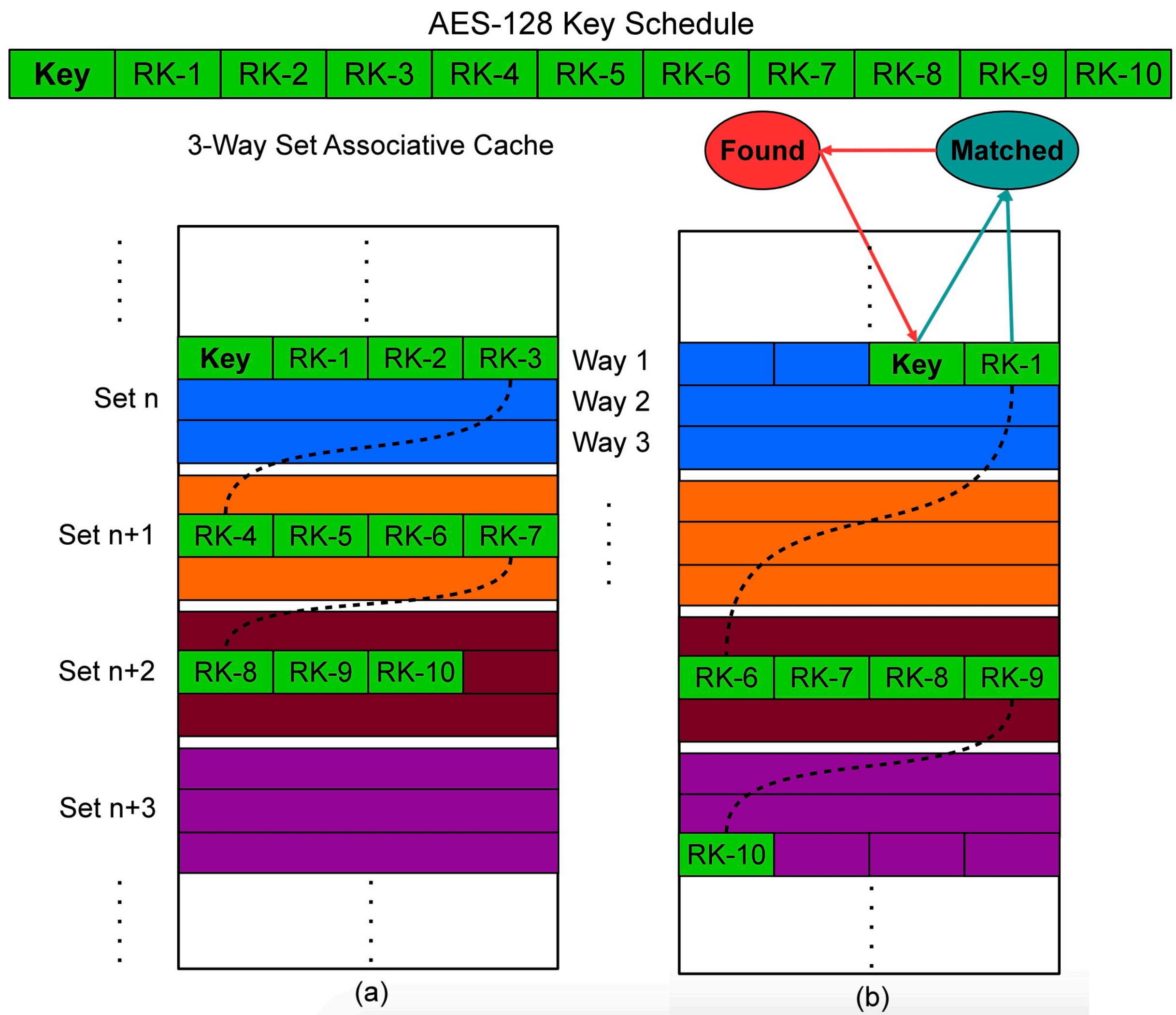
- AES key search:
  - Original key needs to be expanded before encryption/decryption operations



  - Current round key is deterministically computed from the previous round key
  - Scanning memory image sequentially can find the key if exists
- Challenges in cache-based approach:
  - Non-contiguous memory space
  - Incomplete key schedules

Cache Aware AES Key Search

- Non-contiguous memory space
- Incomplete key schedules



Outline

- Threat Model
- Cache-Aware AES Key Search
- **Methodology**
- Attack Analysis
- Countermeasure
- Conclusions

Experimental Methodology

Software Configuration	
Simulator	gem5
OS	Ubuntu Trusty 14.04 64-bit
Disk Encryption Module	dm-crypt + LUKS
Encryption Algorithm	AES-XTS with 128-bit key
Application	SPEC CPU2006
Execution	1B insts to run
	1M insts to sample

Hardware Configuration	
Cores	8 (out-of-order)
ISA	ARMv8 (64-bit)
Frequency	3GHz
IL1/DL1 Size	32KB
IL1/DL1 Block Size	64B
IL1/DL1 Associativity	8-way
IL1/DL1 Latency	2 cycles
Coherence Protocol	MESI
L2 Size	2, 4, 8 (default), and 128MB
L2 Block Size	64B
L2 Associativity	16-way
L2 Latency	20 cycles
Memory Type	DDR3-1600 SDRAM [27]
Memory Size	2GB
Memory Page Size	4KB
Memory Latency	300 cycles
Disk Type	Solid-State Disk (SSD)
Disk Latency	150us

Outline

- Threat Model
- Cache-Aware AES Key Search
- Methodology
- **Attack Analysis**
- Countermeasure
- Conclusions

Attack Scenarios

- Random Attack
  - Execution can be stopped at any given time to extract secrets from CPU caches
  - Due to power failures, disk failures, system crashes…

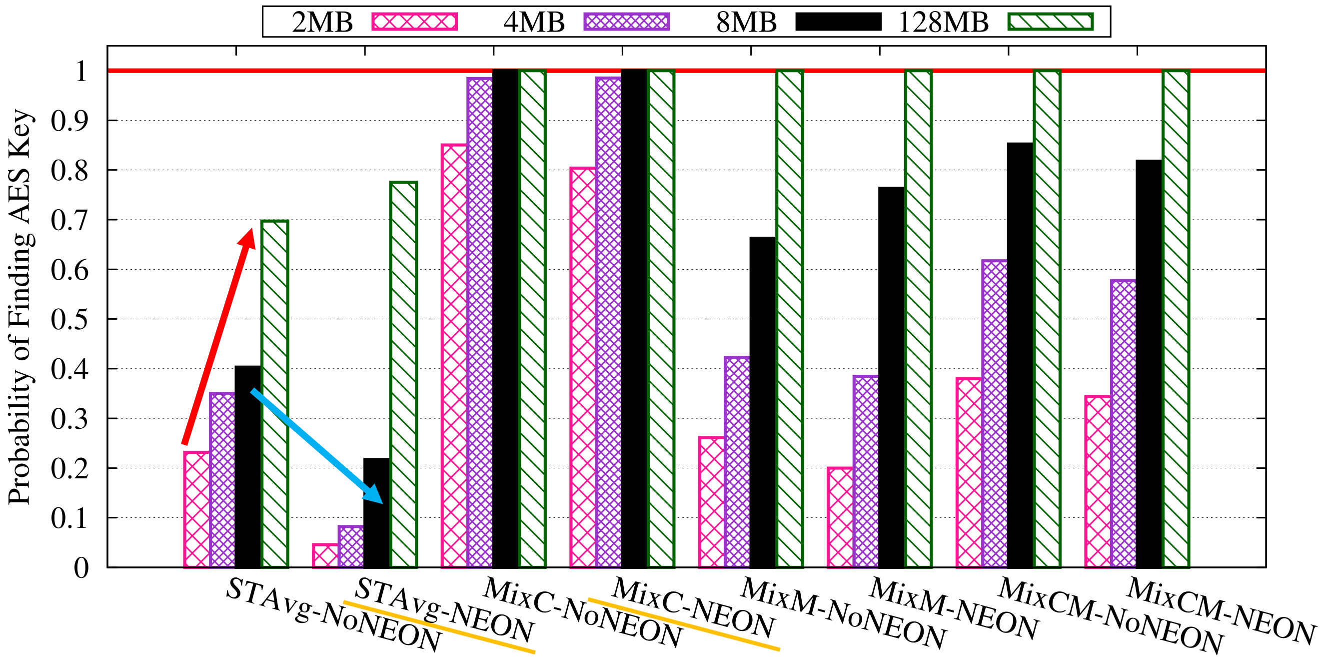
- Targeted Power-Off Attack
  - Conduct power-off operation on victim systems and extract secrets from CPU caches
  - Can be a normal power-off or a forced power-off

Experiments and Benchmarks

NVCool Experiments	
NoNEON	System without ARM's cryptographic acceleration support
NEON	System with ARM's cryptographic acceleration support
STAvg	Geometric mean of single-threaded benchmarks from SPEC CPU2006

Mixed Benchmark Groups		
mixC	compute-bound	*calculix, dealII, gamess, gromacs, h264ref, namd, perlbench, povray*
mixM	memory-bound	*astar, cactusADM, GemsFDTD, lbm, mcf, milc, omnetpp, soplex*
mixCM	compute/memory	*dealII, gamess, namd, perlbench, astar, cactusADM, lbm, milc*

Random Attack Analysis

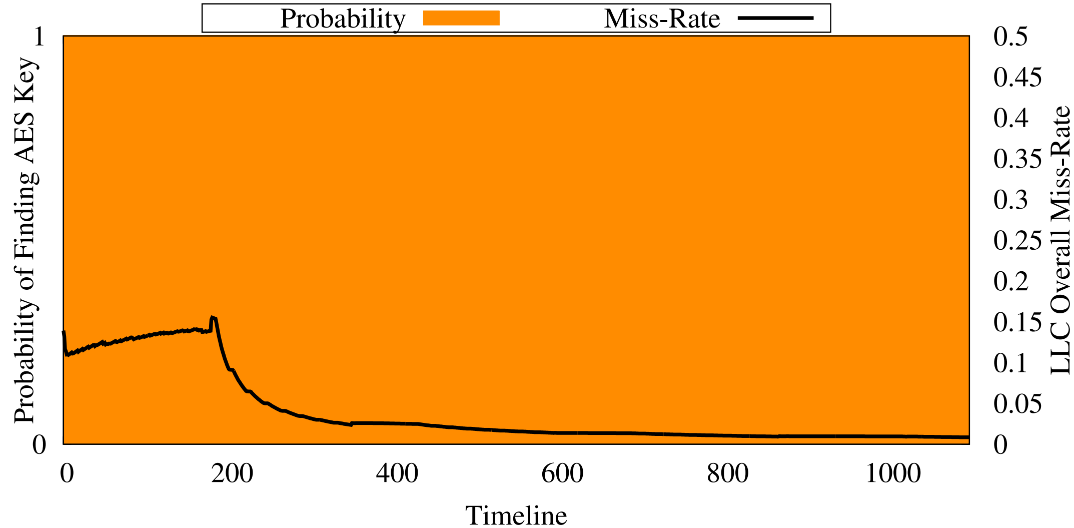


- Overall probability of finding AES keys in systems with different LLC sizes
- Larger caches increase the system vulnerability to random attack
- Systems running multi-programs are more vulnerable
- NoNEON systems are generally more vulnerable than NEON systems

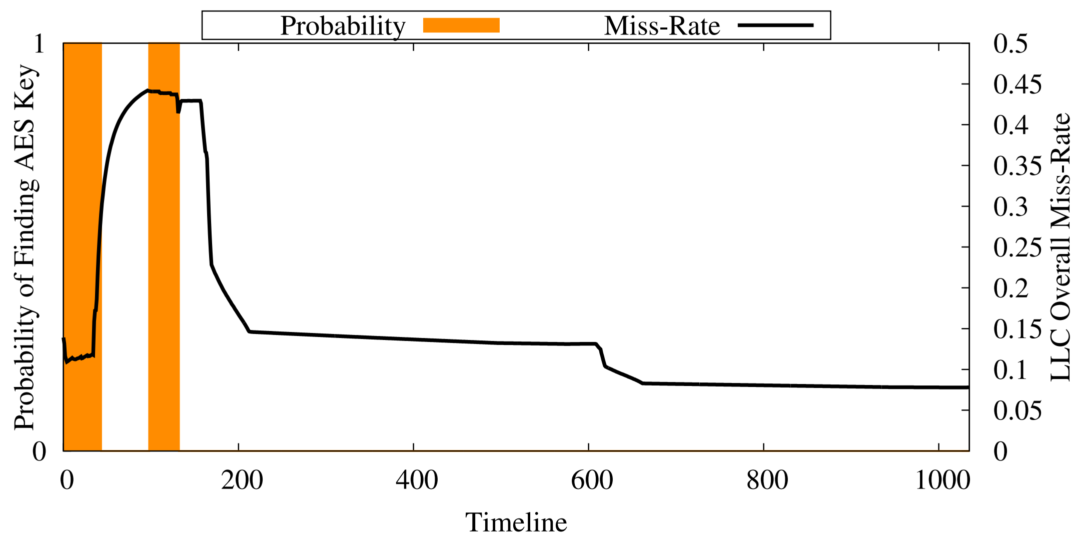
Random Attack Analysis

- Two factors:
  - Encryption disk accesses
  - Cache evictions

computation-bound: dealII



memory-bound: bzip2



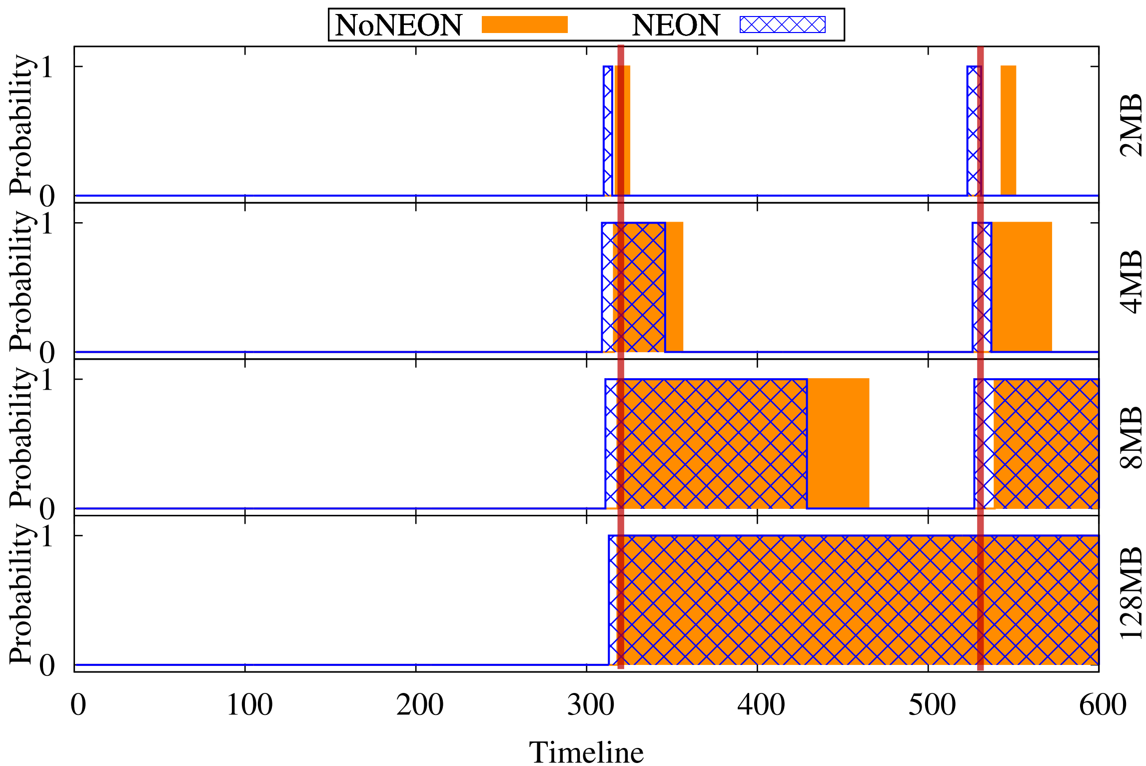
Power-Off Attack Analysis

- Two modes:
  - Normal Power-Off: poweroff (-p)
  - Force Power-Off: poweroff -f

```
root@aarch64-gem5:/# poweroff
Session terminated, terminating shell...exit
 ...terminated.
 * Stopping rsync daemon rsync
      [ OK ] // 1
 * Asking all remaining processes to terminate...
      [ OK ] // 2
 * All processes ended within 1 seconds...
      [ OK ] // 3
 * Deactivating swap...
      [ OK ] // 4
 * Unmounting local filesystems...
      [ OK ] // 5
 * Stopping early crypto disks...
      [ OK ] // 6
 * Will now halt // 7
[  604.955626] reboot: System halted
```

Power-Off Attack Analysis

Mode	Command	Keys exist in cache after power-off?			
		2MB	4MB	8MB	128MB
Normal Power-off	poweroff (-p)	N	N	Y	Y
Forced Power-off	poweroff -f	Y	Y	Y	Y



Outline

- Threat Model
- Cache-Aware AES Key Search
- Methodology
- Attack Analysis
- **Countermeasure**
- Conclusions

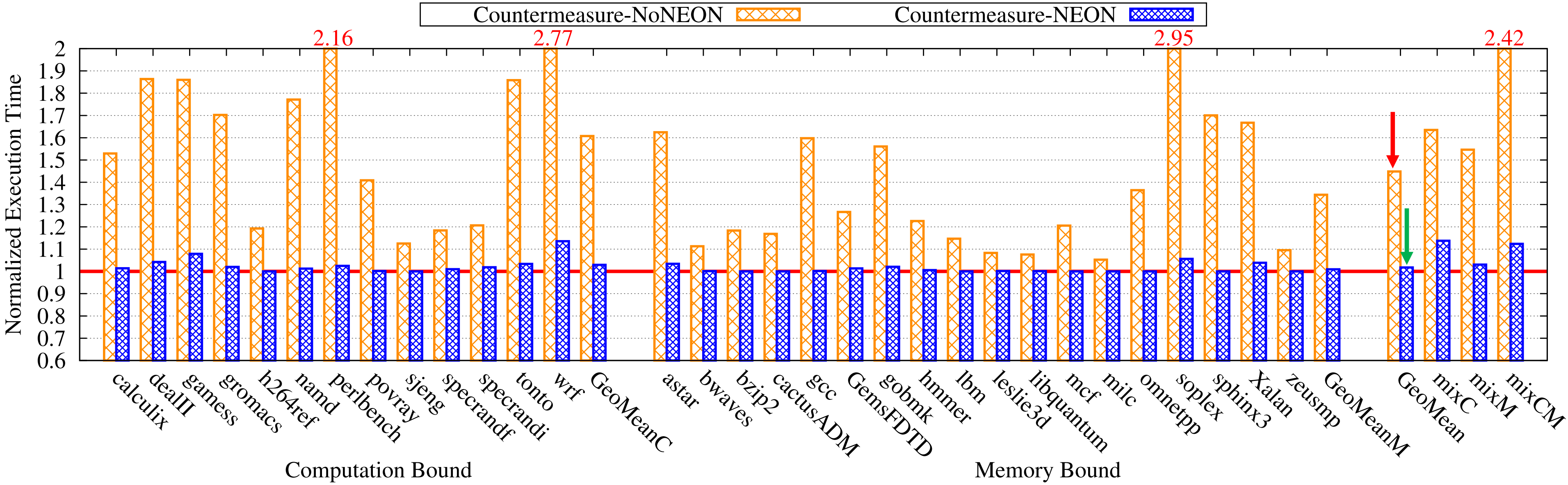
Software-based Countermeasure

- Key idea: marking secret information as uncacheable
  - Walk through page table at kernel space; mark sensitive pages as uncacheable
- Effectiveness

	NoNEON	NEON	Countermeasure
Single-threaded Benchmark	23 - 70%	5 - 77%	**0%**
mixC	85 - 100%	80 - 100%	**0%**
mixM	26 - 100%	20 - 100%	**0%**
mixCM	38 - 100%	34 - 100%	**0%**
Normal Power-off	0 - 100%	0 - 100%	**0%**
Forced Power-off	100%	100%	**0%**

Performance Analysis

- Performance Overhead



- NoNEON systems show high performance overhead
- NEON systems show less than 3% average performance overhead
- Performance optimizations are discussed in the paper

Outline

- Threat Model
- Cache-Aware AES Key Search
- Methodology
- Attack Analysis
- Countermeasure
- **Conclusions**

Conclusions

- Non-volatile caches are vulnerable to cold boot attacks
- Two attacks on disk encryption keys are successfully conducted — random attacks and targeted power-off attacks
- A software-based countermeasure that allocates sensitive information into uncacheable memory pages is developed and shown effective
- We hope this work will serve as a starting point for future studies on the security vulnerabilities of NVM caches and their countermeasures

Questions?

Thank you!