CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

Using Moving Target Defense for Secure Hardware Design

Princeton University

Ruby B. Lee

September 16-18, 2013.

Homeland Security

Science and Technology

Team Profile

- **Princeton University (prime contractor)**
  - Prof. Ruby Lee, the PI, is known for her expertise in Hardware Security and Computer Architecture.
    - Princeton Architecture Lab for Multimedia and Security (PALMS) has designed architectures for secure processors, secure caches, secure cloud servers, secure embedded systems, etc.
  - Princeton team responsible for the behavioral model and simulation of the proposed secure cache, system performance, security assessment and overall design of the test-chips.
- **Carnegie Mellon University (sub-contractor)**
  - Prof. Ken Mai is known for his circuit design expertise.
  - CMU team responsible for the circuit design, layout, fabrication and testing of the secure cache test-chips.

Customer Need

- Customers need security
- Industry security solutions like TPM, ARM Trustzone, Intel SGX (emerging) can be defeated by side-channel attacks!
- Problem: Hardware optimization features, e.g., caches, can inadvertently leak secret information to attackers
  - Caches are essential for performance: they bridge the performance gap between fast processors and slow memories.
- But caches leak information through cache side-channel attacks, e.g., secret keys for encryption/decryption
- They nullify security provided by strong cryptography, or by software isolation techniques
- Easy to perform – locally or remotely.

Approach

- Our approach: re-design caches to thwart cache side-channel attacks, without impacting performance.
- Works for all cryptographic algorithms for all platforms, whether smartphones or cloud servers
  - i.e., any computing device that has a processor with a cache
- Holistic Moving Target Defense solution for hardware
  - Replace current fixed memory-to-cache mapping with a dynamic, randomized memory-to-cache mapping, so attacker cannot get information about which cache lines are used by the victim process
- Only hardware change required is in the address decoder, a small part of the cache structure

Current Status and Accomplishments

① Behavior model of Newcache in gem5 simulator (completed)

② Security evaluation of Newcache

- Unmodified real attacks (completed on gem5)
- Attacks specifically targeting Newcache (completed)
- Improved Newcache (completed – new result)

③ Performance evaluation of Newcache

- Smartphone benchmarks (completed)

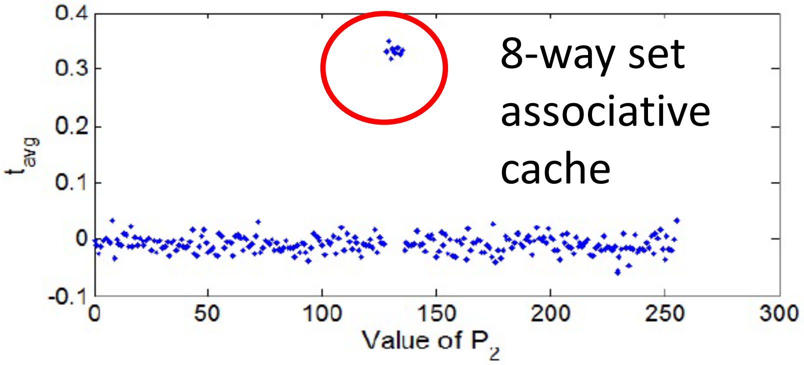
④ Test chip of Newcache – Physical characteristics

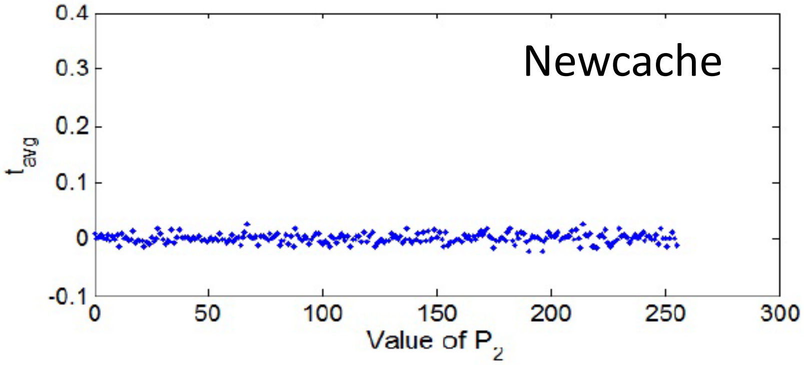
- First test-chip taped out (in fabrication, parts back in Oct 2013)

- On target for all milestones, deliverables and schedule.

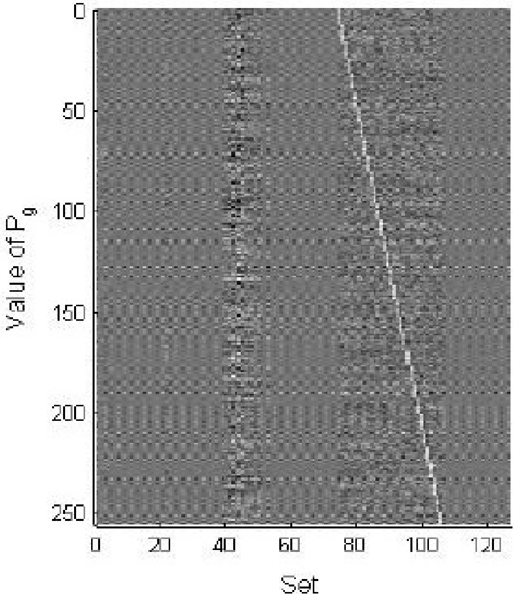
Security Testing: attacks succeed on current caches, but fail on Newcache

Evict and Time attack



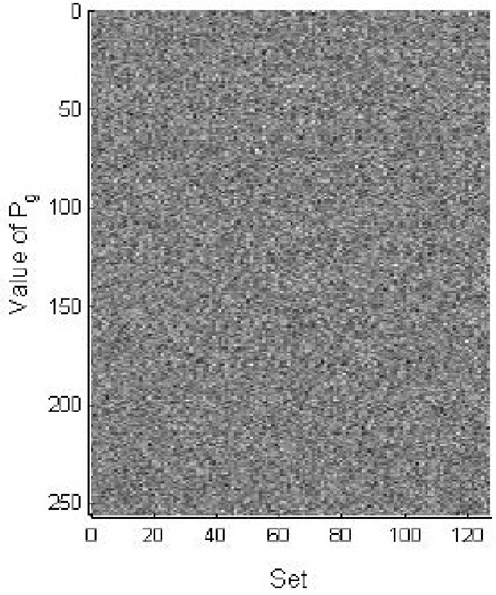


Prime and Probe attack



8-way set associative cache

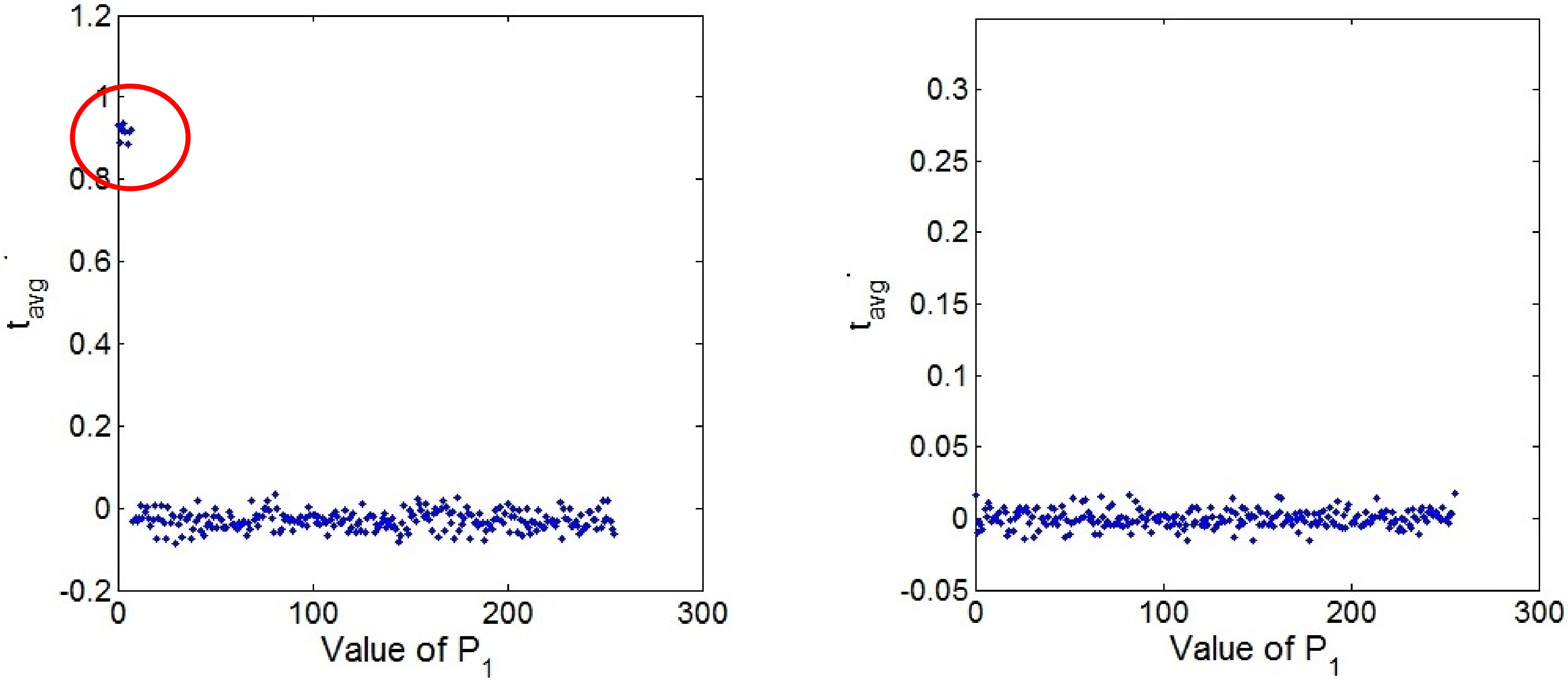
2^{20} samples
Key = all zero bytes



Newcache

We designed new attacks specially crafted for Newcache

New Evict and Time attack

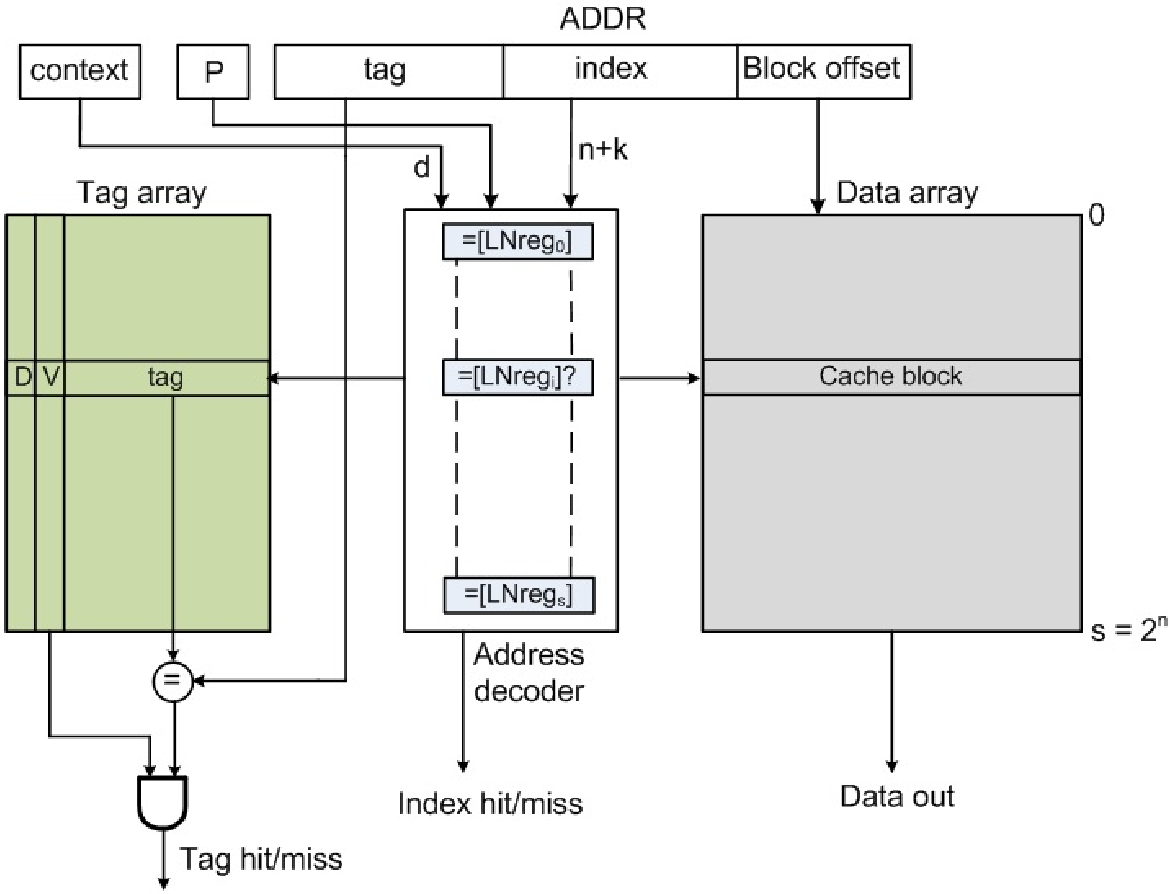

Original Newcache design

Improved Newcache design

- Very smart Attacker can still occupy a specific cache slot before victim process
- Minor change in Newcache design thwarts even this specially-crafted attack
- Similar result for Prime and Probe attacks

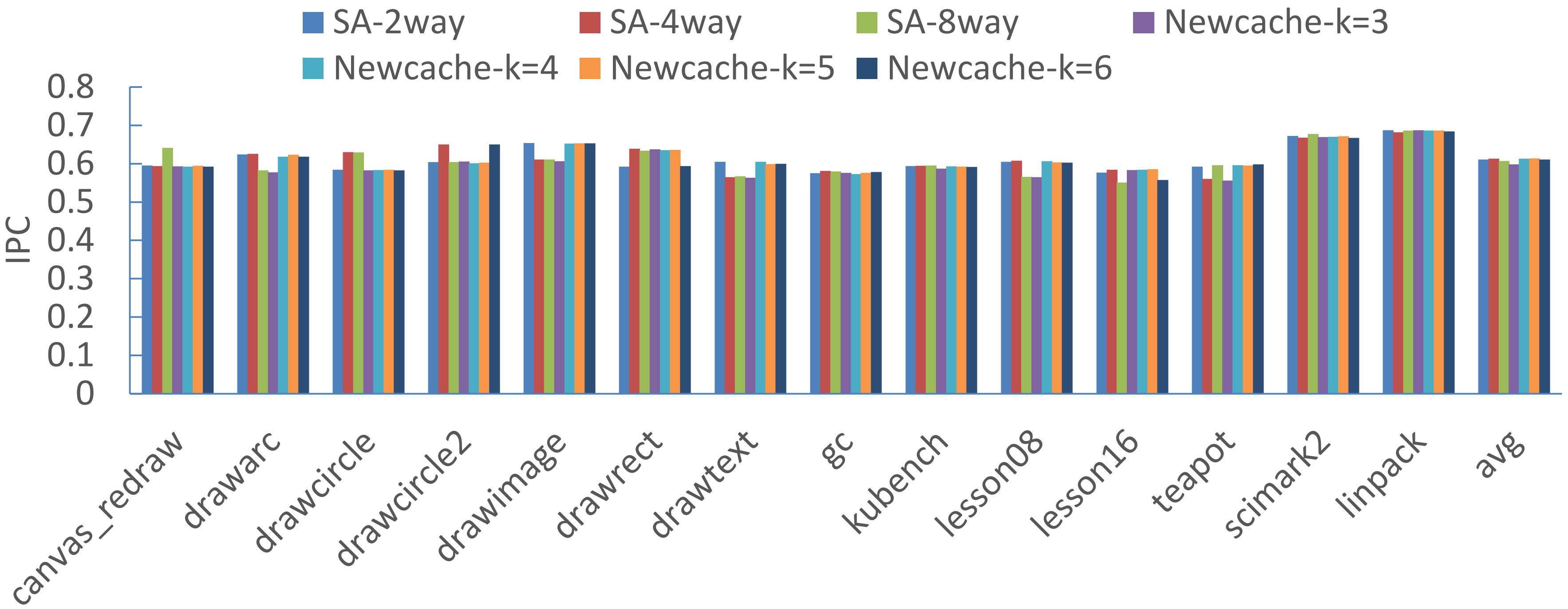
Improved Newcache
defeats even specially-crafted attacks

- Move P-bit from tag to LNregs

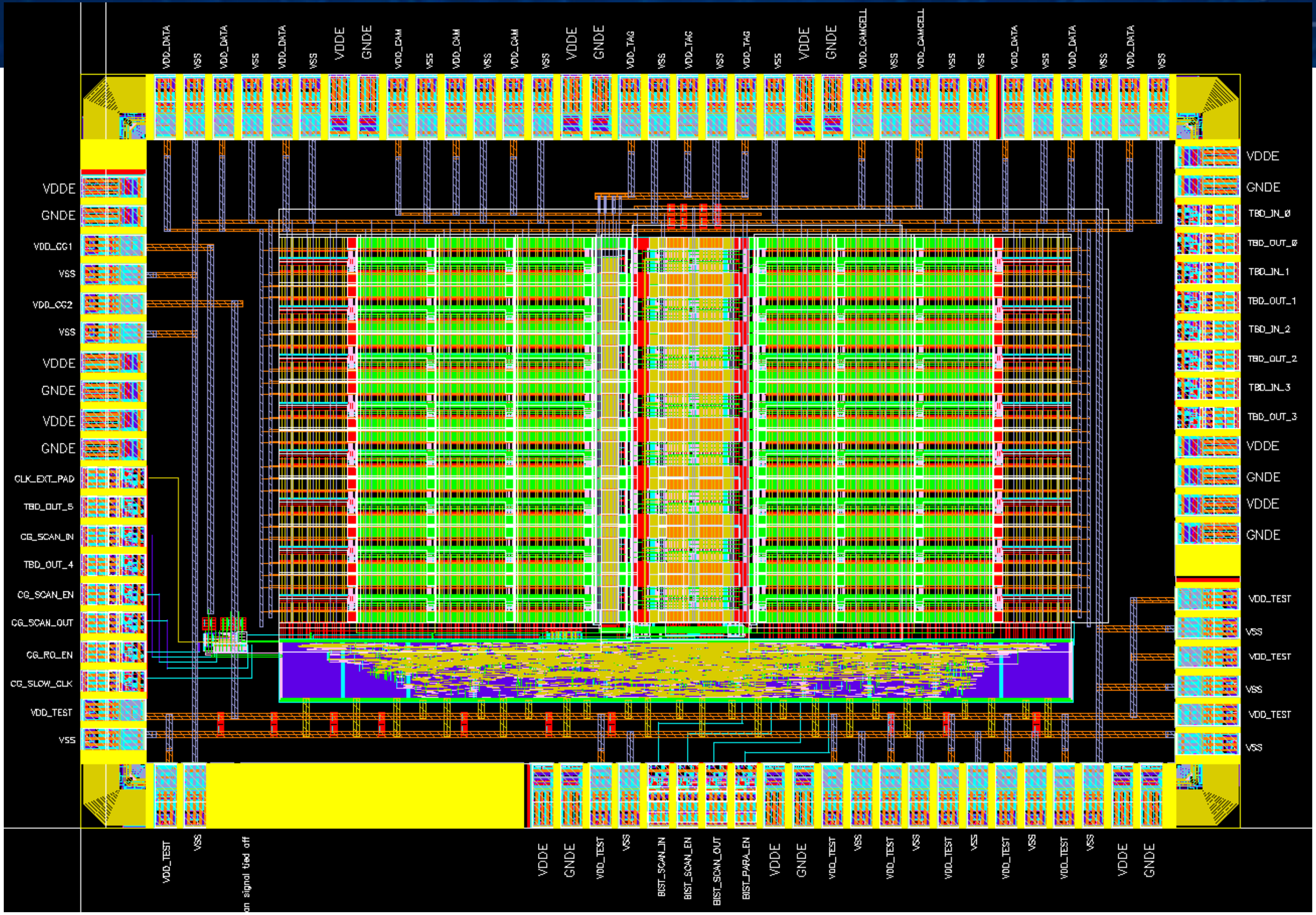


Performance on Smartphone benchmarks: no degradation in performance

- 0xbench is a comprehensive Open-source Android benchmark suite, available on the Android Market (e.g. Google Play)
- Overall performance, in Instructions Per Cycle (IPC) same for Newcache (k = 4,5,6) and conventional caches (Set-Associative) – Newcache sometimes better!



Newcache Testchip



- 32kB Newcache
- 65nm 7-metal bulk CMOS
- STMicroelectronics via CMP

- ❑ 2mm x 1.3mm die
- ❑ Taped out June 2013
- ❑ Chips expected Oct 2013

Benefits

- Built-in security
- Performance transparent
- Software transparent
- Cost transparent, once implemented in core
- Either lower power or faster than conventional caches
- Can be used for all types of caches
  - D-cache, I-cache, L2 cache, etc.
- Reusable for all future caches
- Fits in current ecosystem

Competition

- No hardware competition to date.
  - All existing hardware caches are insecure – they leak information through cache side-channel attacks
- Software solutions to mitigate cache side channel attacks incur huge performance degradation of 3X to 10X slowdown.
  - Furthermore, not completely secure since software cannot control hardware caches
  - Different changes (ad-hoc) required for each cryptographic program
- Separate hardware crypto module for each cipher
  - Does not prevent non-crypto information leaks

Next Steps

- Behavioral model simulation
  - Enhance gem5 to do dual-system simulation for server benchmarks
  - Model Newcache variations and other secure caches
- Performance
  - Performance of Newcache for L2 caches, I-cache
  - server benchmarks
- Security
  - Consider new attacks, and improve secure cache designs
- Physical Characteristics
  - Measure test-chip 1: access time and power consumption
  - Design and fabricate test-chips 2 and 3
  - Evaluate design tradeoffs
- Publish papers and write full Report
- Technology Transfer
  - Find DoD customers and potential commercial customers

Contact Information

- Technology is available for experimentation, implementation and licensing
- Contact:

Professor Ruby B. Lee
Department of Electrical Engineering
Princeton University
Princeton, NJ 08544
rblee@princeton.edu
609-258-1426