

Moving Target Defense for Secure Hardware Design



Cyber Security Division 2012 Principal Investigators' Meeting

October 10, 2012

**Ruby B. Lee, PI
Professor
Princeton University
rblee@princeton.edu
609-258-1426**

Moving Target Defense for Secure Hardware Design

- TTA12: Moving Target Defense
- Team:
 - PI: Ruby B. Lee, Professor, Princeton University
 - 2-3 PhD students
 - Newcache simulation, performance and security
 - Subcontractor: Alan Rogers, President, Analog Bits
 - 4-5 Circuit, Mask design and Verification Engineers
 - test-chip design, fabrication and testing

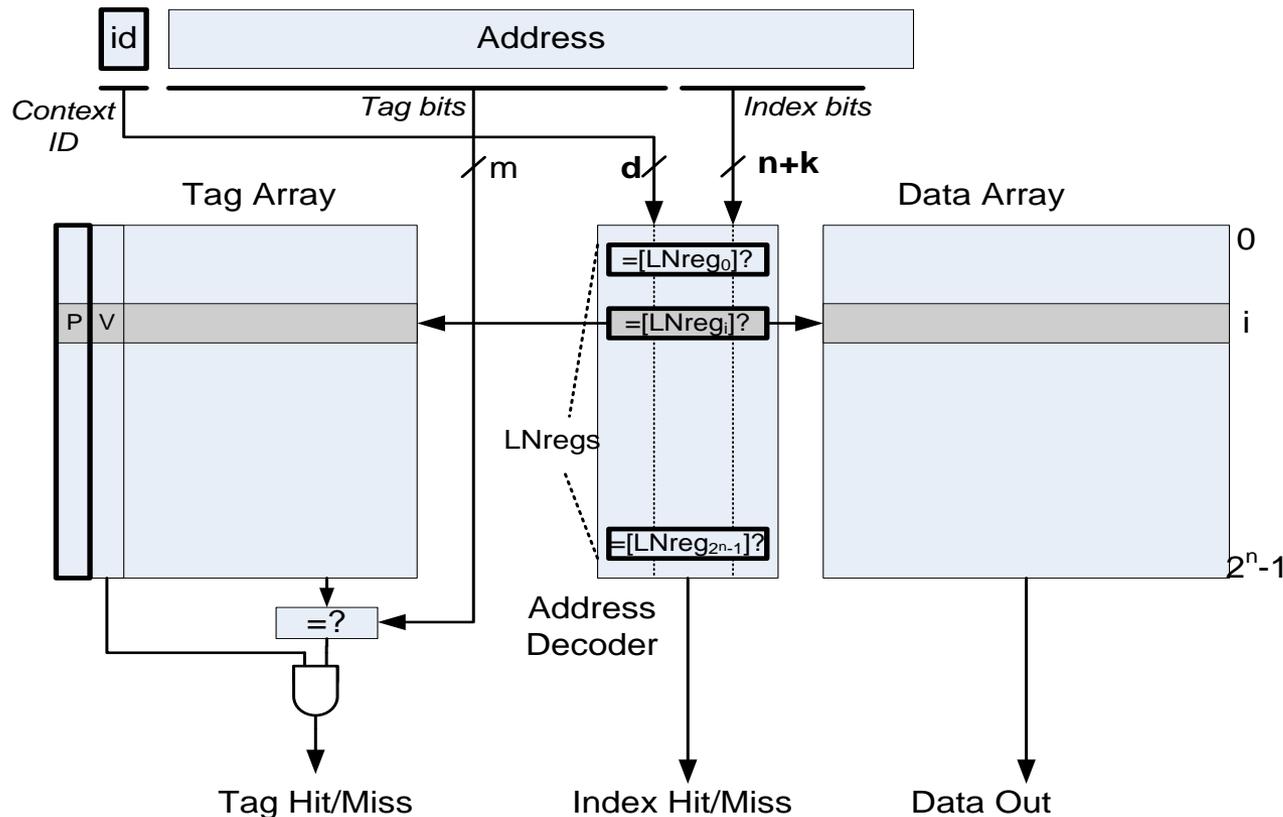
Motivation

- Problem:
 - Cache side-channels leak secret information, despite strong cryptography and software isolation mechanisms
 - Hardware caches essential for computer performance
 - HW problem - very hard for SW-only solutions
- Approach:
 - Secure Cache: thwart attacker, without performance hit
 - Fits in current ecosystem
- Benefits:
 - Built-in; software and performance transparent

Newcache: Technical Approach

Use Moving Target Defense to thwart cache side-channel attacks with performance comparable to current caches

Dynamic, random mapping of memory address to cache-line

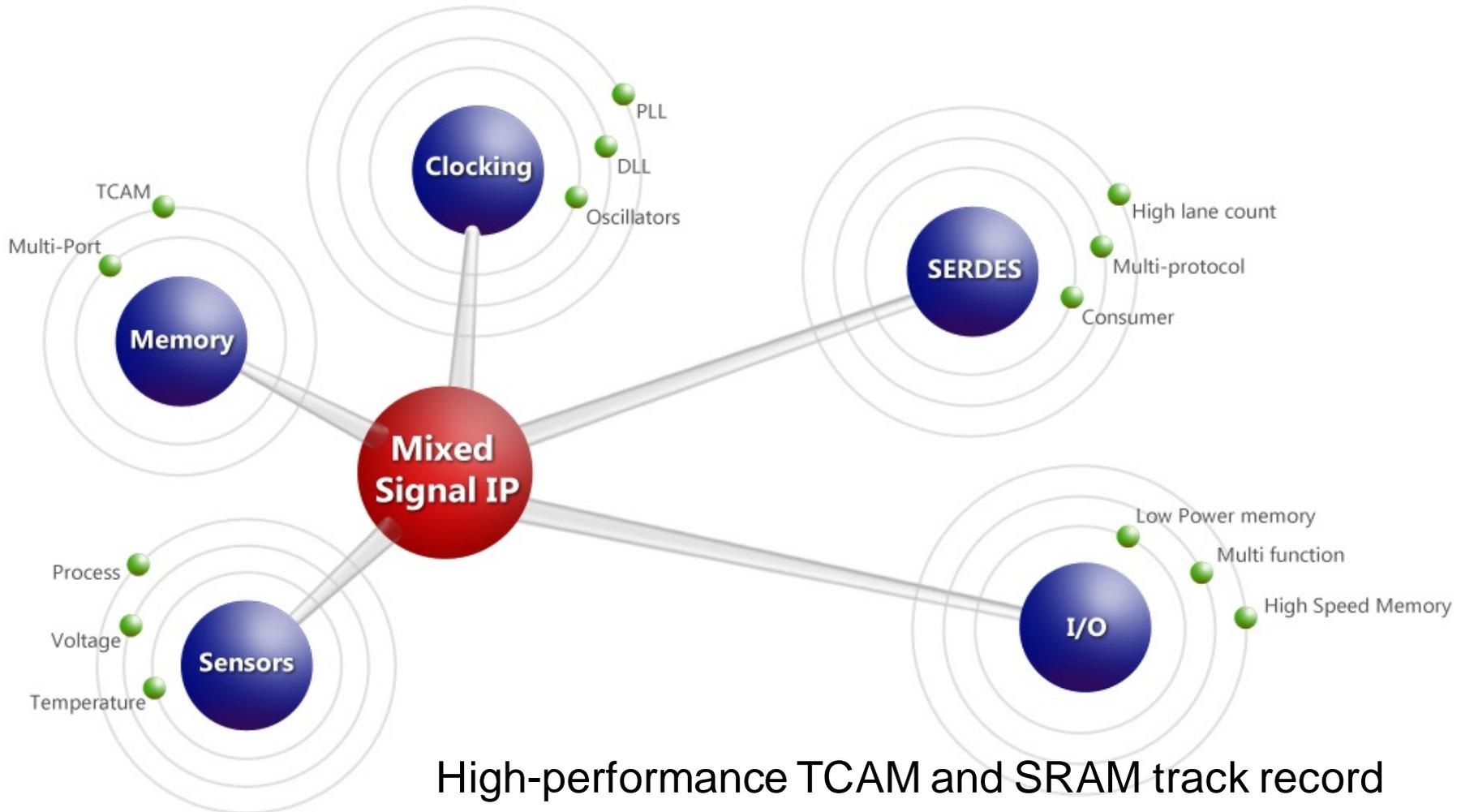


Novel secure,
leak-free
caches

Technical Approach

- Design and implement a simulation model of Newcache to get system performance characteristics (e.g., cache miss rates)
 - Challenge: latest representative benchmarks for each market, e.g., smartphone, cloud based server
- Verify the security enhancement of Newcache
 - Challenge: to gain access to attack test suite used and accepted by the defense industry
- Design and implement a test-chip to get physical performance characteristics (e.g., access speed, power and size)
 - Challenge: accurate comparison with conventional caches and availability of silicon shuttle run schedule to meet the given schedule.

Analog Bits: Subcontractor for Testchip

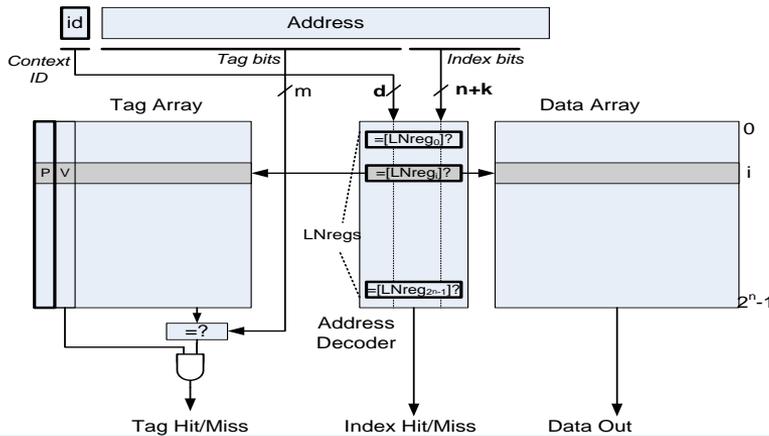


Milestones, Deliverables, Schedule

- Testchip: full chip specification / Datasheet 01/13
- Cycle-accurate Simulation of Newcache 07/13
- Testchip: Pre-Silicon Report / Tape-out 07/13
- Test-chip: Receive fabricated parts 09/13
- Initial Performance and Security Results 10/13
- Document of chip design, testing and evaluation 11/13
- Improvements / Testchip2 06/14
- Document of cache miss performance 10/14
- Document on security against cache side-channel attacks 10/14
- Final Report of Entire Project 10/14

Technology Transition Plan (working with Analog Bits)

- Increase Security with best Power & Performance balance
 - Market: Smartphones, Tablets and Intelligent Sensors via the SOC design suppliers
 - Key target: ARM architecture licensees for the mobile segment
 - Other target architectures: MIPs & ARM for the SOC segment
- Increase Security & Performance
 - Market: Servers, especially used in cloud based services
 - Key target: x86 suppliers
 - Other target: 64bit ARM v8 Architecture suppliers; SPARC
- Upgrade Security for Defense Industry
 - Target defense microprocessor suppliers that require utmost security capabilities



Novel leak-free cache design that also improves performance!

- **Proposed Technical Approach:**
- Novel cache design modifies a direct-mapped cache with:
 - Dynamic memory to cache mapping
 - Random replacement algorithm
 - Circuit re-design of address decoder
 - Longer cache index
- Proposed Tasks:
 - Demonstrate system performance improvement due to the use of Newcache via a behavior level simulation.
 - Demonstrate the security enhancement, overcoming the side channel attack vulnerability of all existing cache designs.
 - Design and fabricate a Newcache chip to show actual physical size, power and performance compared to existing offerings.
- Base technology and feasibility established at Princeton.
- World-class custom circuit designers, Analog Bits, Inc., for chip design.

- **Operational Capability:**
- Goal: To secure the processor's cache from information leakage through cache side-channel attacks.
- No software impact. No code changes required.
- Best-in-class performance: access time similar to direct-mapped cache designs with cache miss performance equal to set-associative caches.
- Physical die area and power similar to direct-mapped cache implementations of equal size.
- After initial design, no known impact to cost of ownership.
- **Uses Moving Target Defense to design secure, leak-free cache memories needed by all computing products**

- **Schedule, Cost, Deliverables, & Contact Information**
- Schedule: 24 months.
- Deliverables:
 - ✓ Behavioral model of Newcache
 - ✓ Document of cache miss performance for various applications
 - ✓ Test chip with custom circuit design of Newcache
 - ✓ Document of chip design, testing and evaluation.
- Contact Information: Prof. Ruby B. Lee
 - Dept. of Electrical Engineering,
 - Princeton University
 - Princeton, NJ 08544
 - Tel: 609.258.1426
 - E-mail: rblee@princeton.edu