Pin Tumbler Lock: A Shift based Encryption Mechanism for Racetrack Memory

Hongbin Zhang, Chao Zhang, Xian Zhang,
Guangyu Sun, Jiwu Shu

ASP-DAC2016
January 26, 2016

Executive Summary

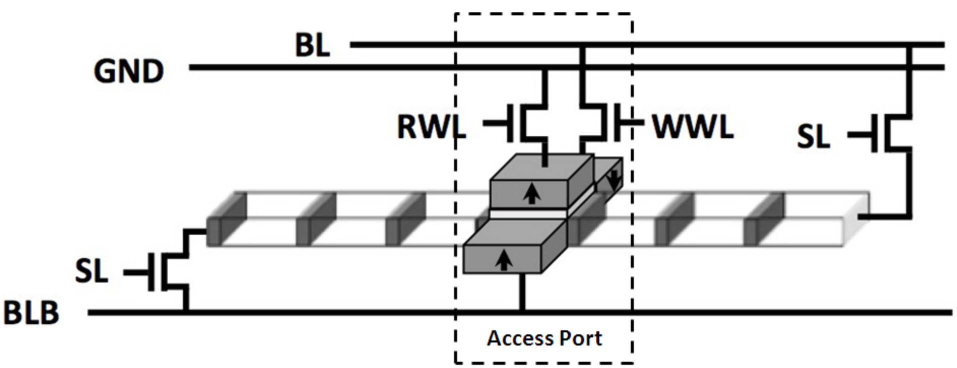
- Problem: Data security problem of NVM
  - Data retain in the NVM after power off or stolen
  - Traditional methods induce non-trivial timing overhead
- Observation: Racetrack memory read and write data through shift operation, which can be used as encrypt and decrypt schematic.
  - Shift operation make data encrypted, only right key can restore the data (like pin tumbler lock)
- Key Ideas:
  - (1) Data is encrypted by shift operation according to shift key
  - (2) Keys are generated from randomizer and stored in DRAM
  - (3) Encryption shift operation merger into R/W shift operation
- Results: PTL get the same security strength of AES-128 with 3.1% performance overhead and 3.7% energy overhead and 1.56% storage cost and 1.6% area cost.

Outline

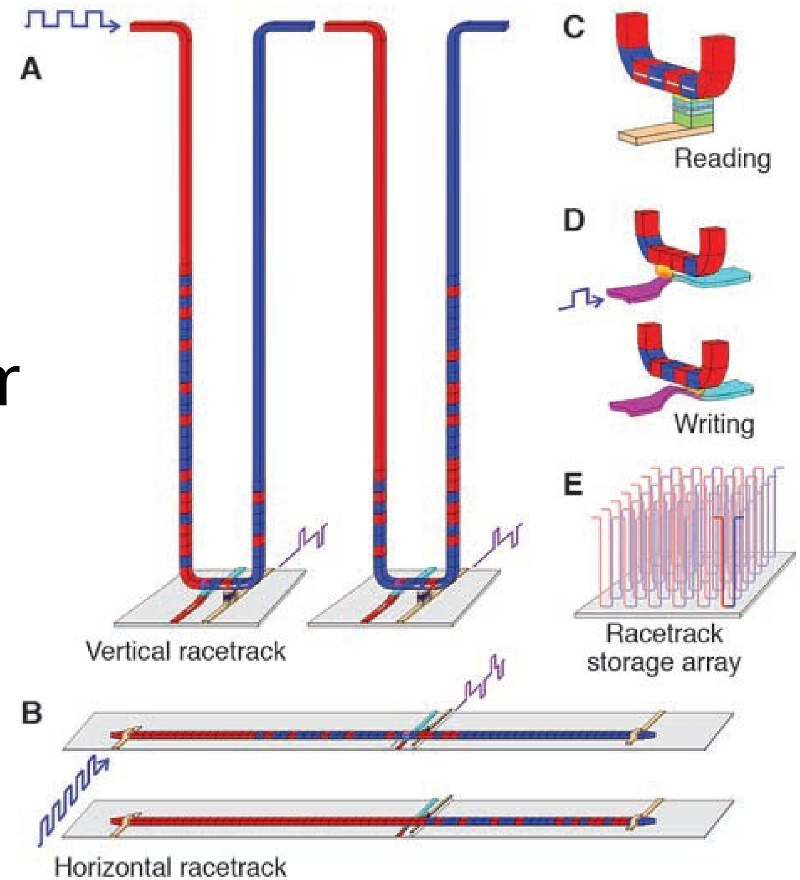
- Executive Summary
- Background
  - Racetrack memory
  - Problem
  - Existing proposals
  - Our proposal
- Design
- Evaluation
- Conclusion

Racetrack Memory

- Ultra-high density
- Comparable R/W latency
- Used as cache or memory
- Facing also security problem



Cell structure



Racetrack

Problem

- Data security
  - Data retain in NVM after power off
  - Data can be easy inspected after stolen
- Traditional methods
  - Existing methods try to encrypt data with software
  - Traditional methods can not protect data totally
  - Traditional methods induce non-trivial timing overhead
- How to better protect the data in racetrack memory?

Existing Proposals

- AES encryption: use AES to encrypt data before being stored in memory[DSN' 2010]
  - Solution: protect the data in main memory using AES algorithm
  - Problem: inducing large timing overhead
- i-NVMM: encrypt main memory incrementally [ISCA' 2011]
  - Solution: encrypt the working set of application dynamically
  - Problem: sensitive information in working set is not protected
- PAD-XOR: provide run-time protection through encrypting the main memory using sub-PAD [ICCAS' 2013]
  - Solution: run-time protection to all data using sub-pad
  - Problem: introduces extra sub-PAD tables for encryption

Our Proposal - PTL

- Encrypt the data using shift operation
- Only right key can decrypt the data
- Shift keys are stored in volatile memory
- Keys disappear when power off and data protected

a) With no key b) With wrong key c) With right key d) Unlocked

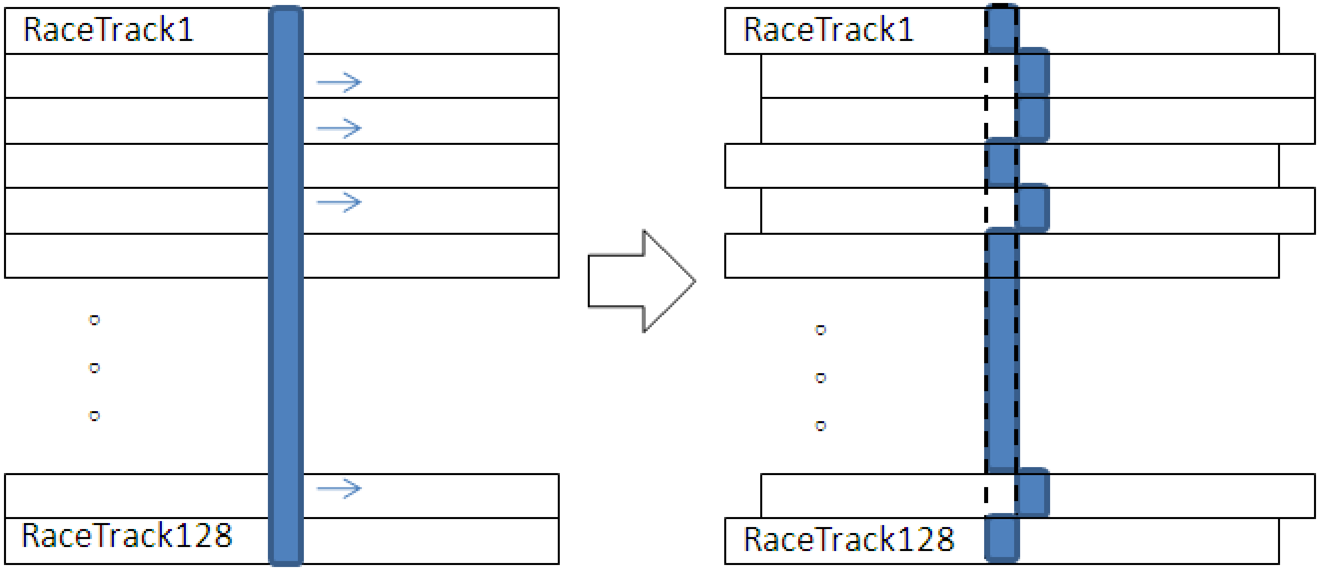
https://en/wikipedia.org/wiki/Pin_tumbler_lock.

Outline

- Executive Summary
- Background
- Design
  - Shift based encryption scheme
  - Key width and security strength
  - Redundant Domain Wall
  - Random Number Generator
  - System structure
- Evaluation
- Conclusion

Shift based encryption scheme

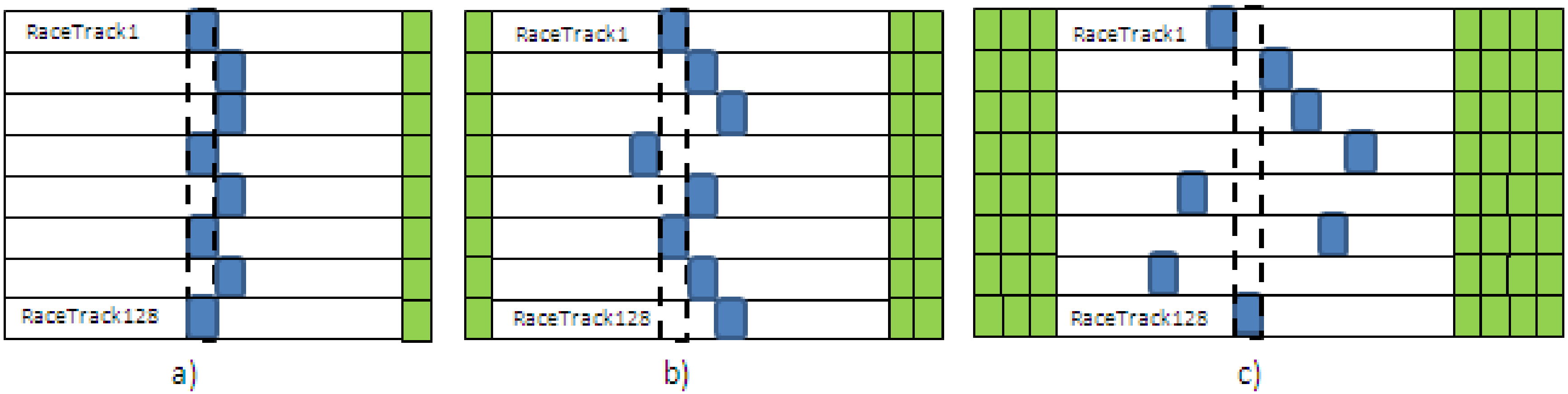
- Data is placed vertically
- Shift operation of racetrack encrypt the data



(a)Before encryption. (b)After encryption.

Key width and security strength

- Longer key brings higher security
- Longer key induces larger key storage cost



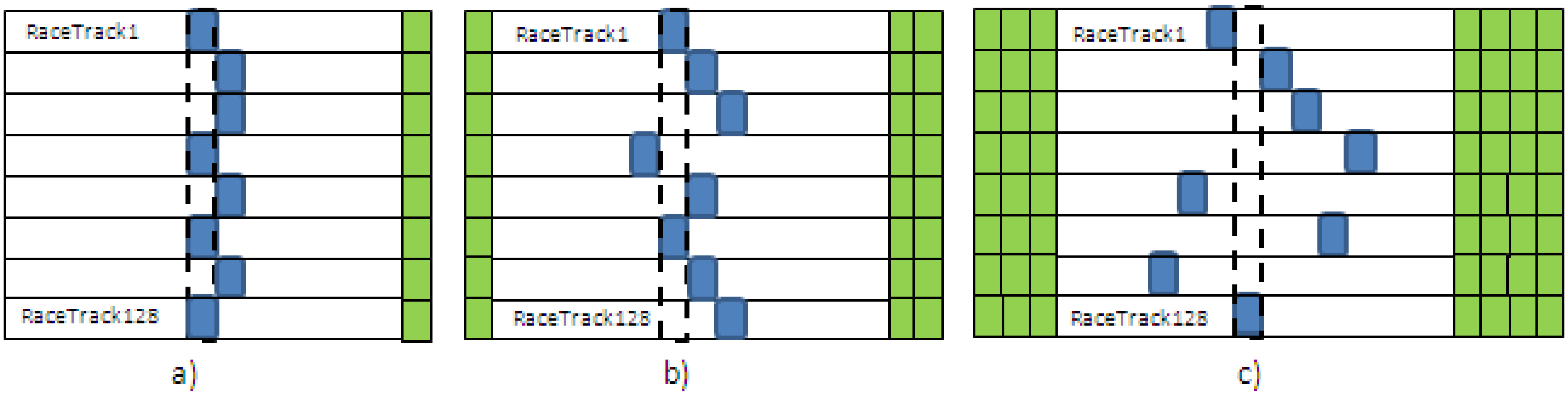
(a) Region with 128bit shift key (key-width is 1).

(b) Region with 256bit shift key (key-width is 2).

(c) Region with 384bit shift key (key-width is 3).

Redundant Domain Wall

- Longer key brings higher security
- Longer key induces larger area cost



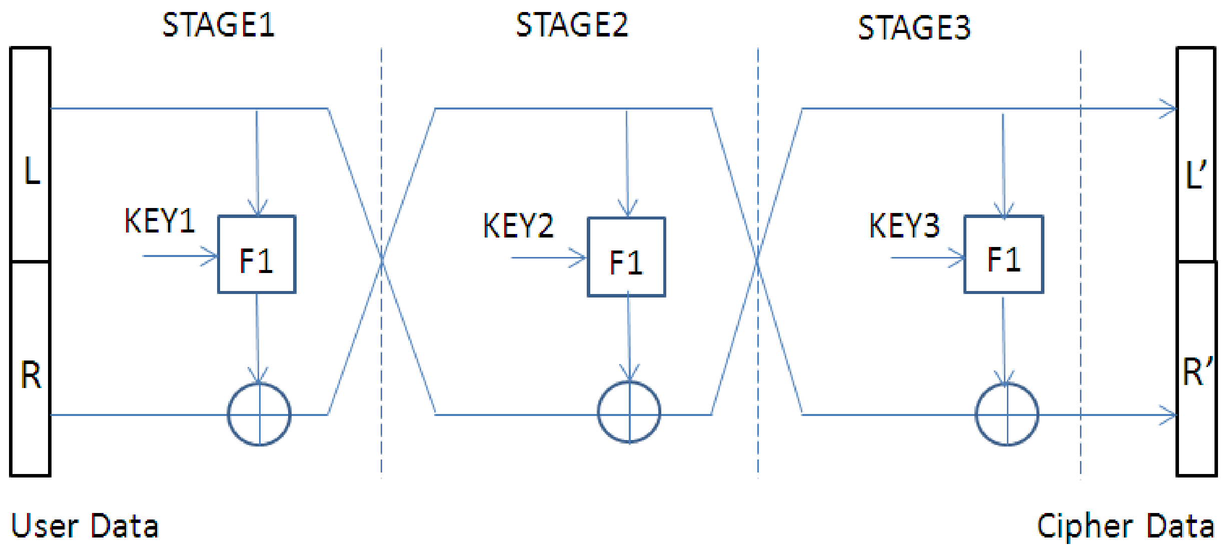
For the region with 128 bit key, 1 more stripe redundant bits.

For the region with 256 bit key, 3 more stripe redundant bits.

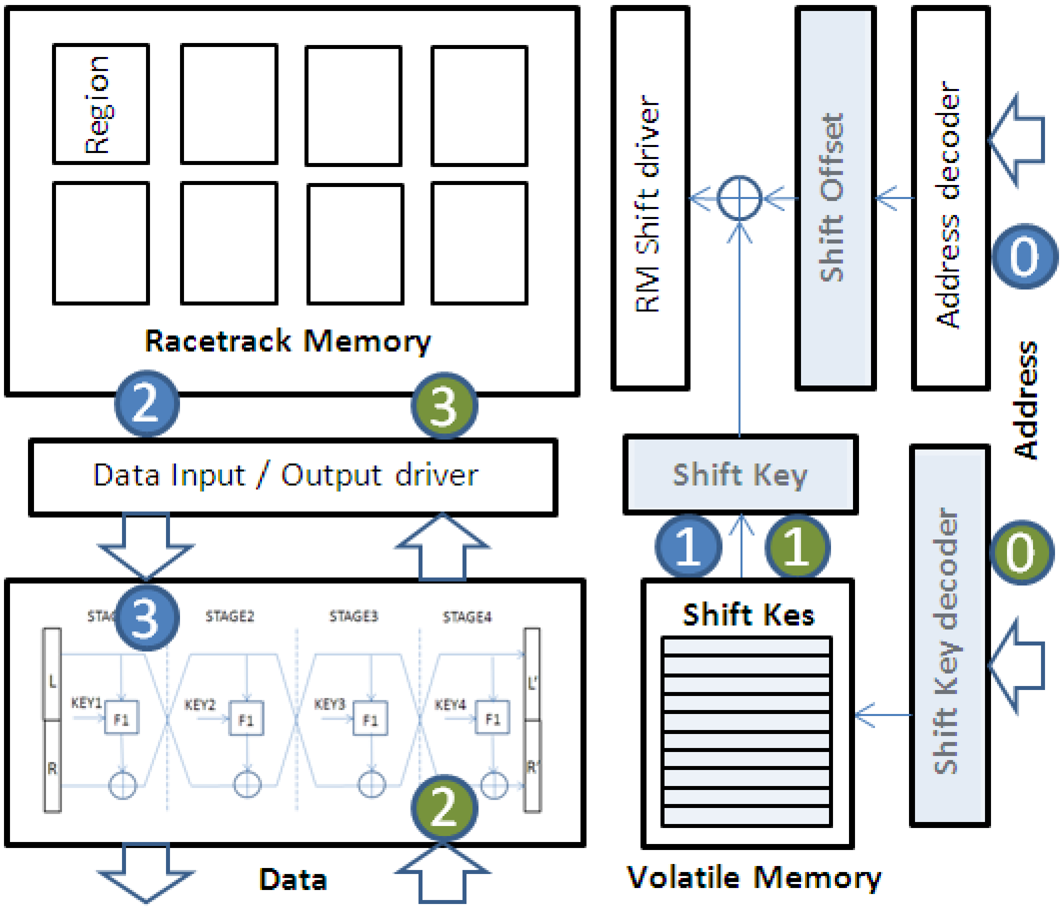
For the region with 384 bit key, 7 more stripe redundant bits.

Random Number Generator

- Using 4-stage FN to transform a data into a pseudo random number.
- In order to avoid the data with strong patterns being easily decrypted.



Structure of secure racetrack memory



Blue: read operation sequence.

Green: write operation sequence.

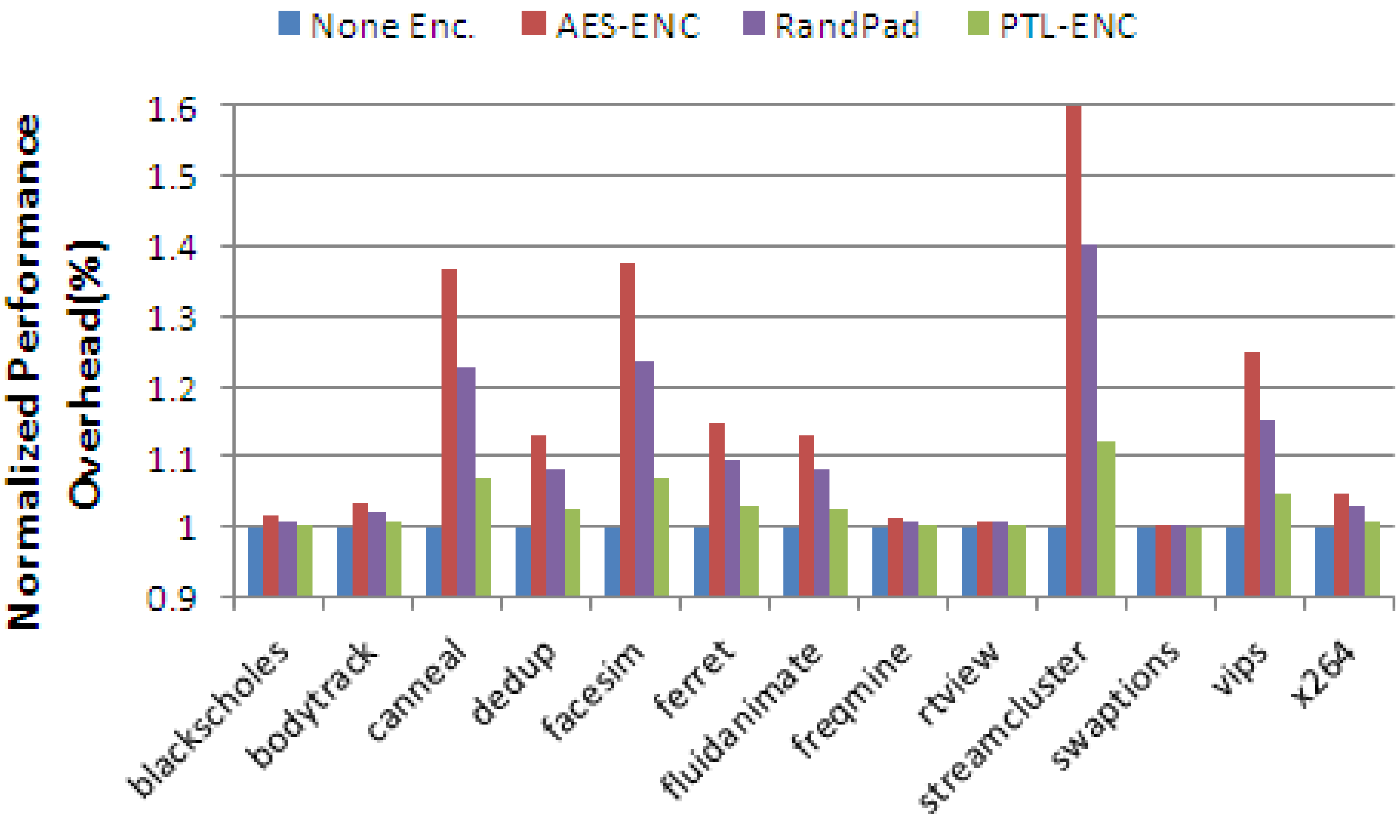
Outline

- Executive Summary
- Background
- Design
- Evaluation
  - Performance evaluation on methods
  - Performance evaluation on key-width
  - Energy evaluation
  - Storage cost
  - Area cost
- Conclusion

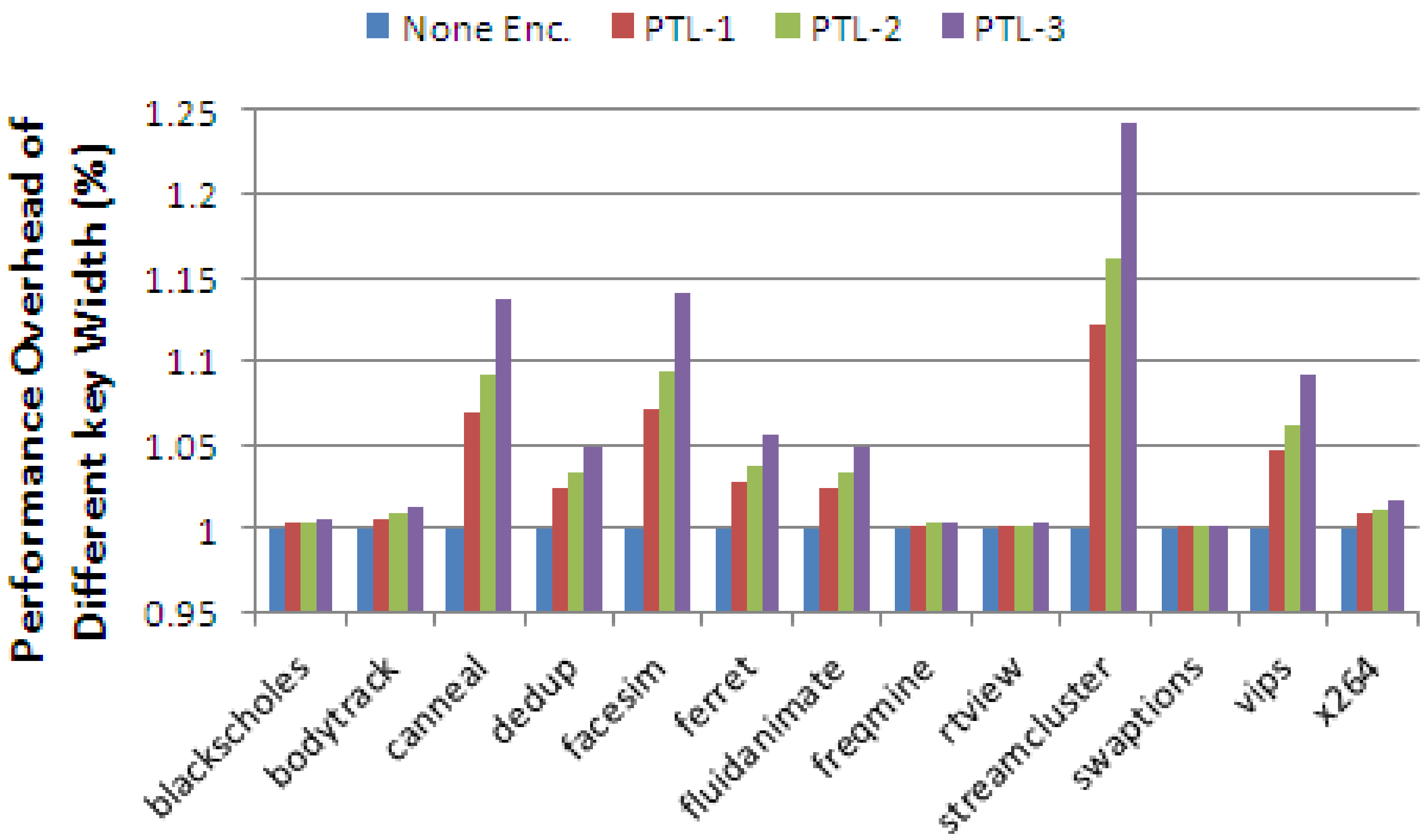
Evaluation Setup

- PTL based on CentOS
  - Compared with no-ENC, AES-ENC, Rand-Pad
- Platform
  - 4-core CPU,32KB L1,1MB L2,128MB racetrack L3 cache
- Workloads
  - 13 workloads from Parsec3 benchmarks
- Metrics
  - Performance: R/W latency
  - Energy: read, write, shift and static energy
  - Storage: shift key size
  - Area: redundant domain wall size

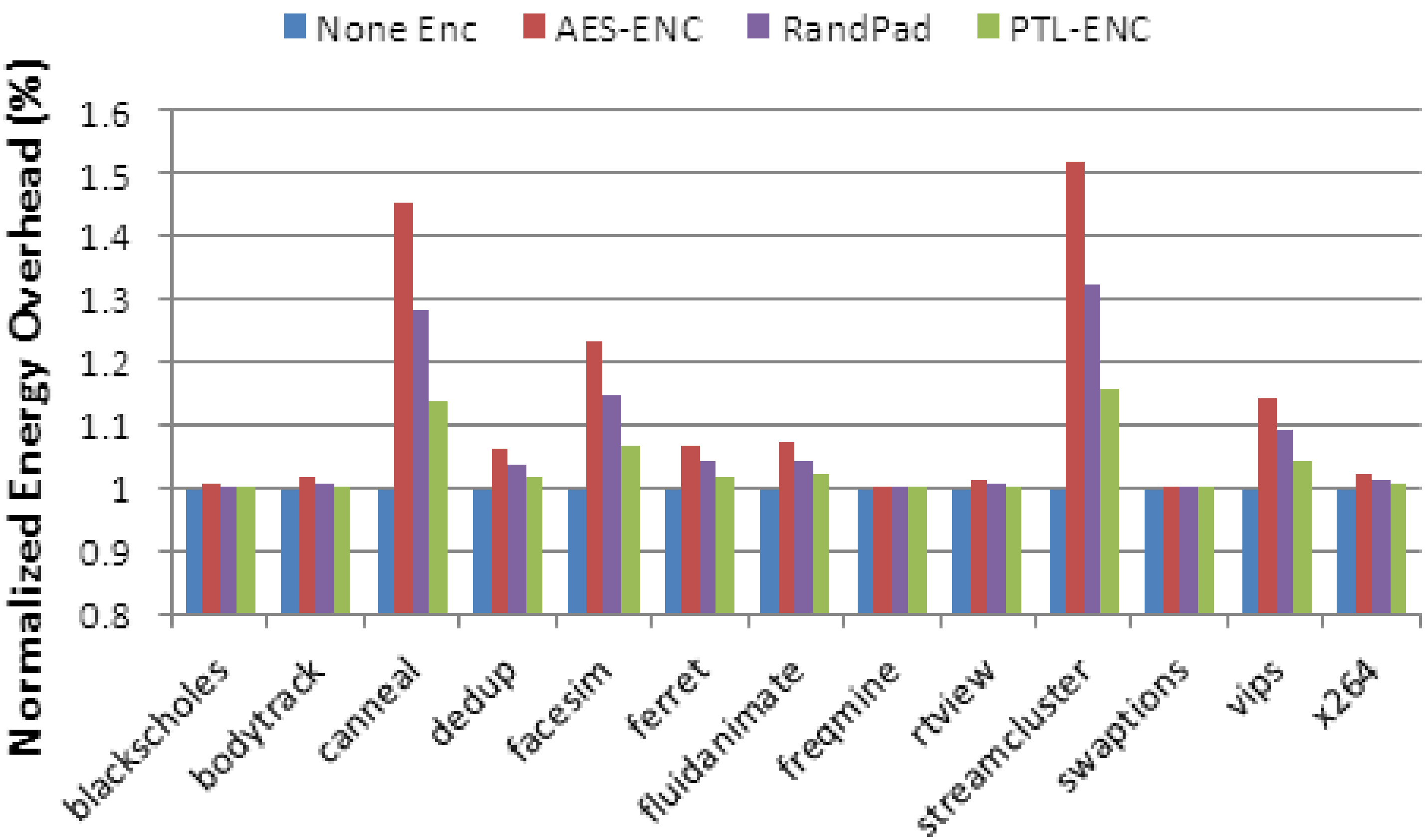
Performance evaluation on methods



Performance evaluation on key-width



Energy overhead evaluation



Storage and area cost

- For 128MB cache

Region Size	Key Num.	Key width	Key length	Key Storage	Storage Cost(%)	Redun. Area	Area Cost(%)
1KB	128K	1	128	2MB	1.56	2MB	1.6
2KB	64K	1	256	2MB	1.56	2MB	1.6
4KB	32K	1	512	2MB	1.56	2MB	1.6
1KB	128K	2	256	4MB	3.12	6MB	4.7
2KB	64K	2	512	4MB	3.12	6MB	4.7
4KB	32K	2	1024	4MB	3.12	6MB	4.7
1KB	128K	3	384	6MB	4.68	14MB	10.9
2KB	64K	3	768	6MB	4.68	14MB	10.9
4KB	32K	3	1536	6MB	4.68	14MB	10.9

Storage and area cost

- For 4GB main memory

Region Size	Key Num.	Key width	Key length	Key Storage	Storage Cost(%)	Redun. Area	Area Cost(%)
1KB	4M	1	128	64MB	1.56	64MB	1.6
2KB	2M	1	256	64MB	1.56	64MB	1.6
4KB	1M	1	512	64MB	1.56	64MB	1.6
1KB	4M	2	256	128MB	3.12	192MB	4.7
2KB	2M	2	512	128MB	3.12	192MB	4.7
4KB	1M	2	1024	128MB	3.12	192MB	4.7
1KB	4M	3	384	192MB	4.68	448MB	10.9
2KB	2M	3	768	192MB	4.68	448MB	10.9
4KB	1M	3	1536	192MB	4.68	448MB	10.9

Conclusion

- Security is one of the problems of NVM
  - Data retained in NVM when power off
  - Difficult to provide run time protecting
- Shift based PTL schematic solved this problem
  - Achieving the same security strength as AES
  - With less performance cost and energy consuming
  - With less storage and area cost
- PTL achieves the same security strength of AES-128 with 3.1% performance overhead and 3.7% energy overhead and 1.56% storage cost and 1.6% area cost.

Major contribution

- The first work that leverages the RM structure and shifting operations for NVM data encryption.
- Present a scheme achieving the same or higher security strength as prior works using AES.
- Our encryption mechanism is compatible with RM design for different levels of a memory hierarchy.
- Our work achieves less performance and energy overhead than existing approaches.

Thanks

Pin Tumbler Lock: A Shift based Encryption Mechanism for Racetrack Memory

Hongbin Zhang, Chao Zhang, Xian Zhang, Guangyu Sun, Jiwu Shu