ObfusMem: A Low-Overhead Access Obfuscation for Trusted Memories

Amro Awad [1], Yipeng Wang [2], Deborah Shands [3], Yan Solihin [2]

[1] Sandia National Laboratories

[2] North Carolina State University

[3] National Science Foundation

ISCA 2017

Presented by Andrew Loveless and Alex Kisil

Motivation: Hiding Information

- Attackers rely on information
- Consider a heist movie

High Tech Vault

New Security

- *Ocean's Eleven*. (2001). [film] Directed by S. Soderbergh. Warner Bros.
- *Ocean's Thirteen*. (2007). [film] Directed by S. Soderbergh. Warner Bros.

Motivation: Hiding Information

- Attackers rely on information
- Consider a heist movie

Study the Blueprints

Infiltrate the Casino

- *Ocean's Eleven*. (2001). [film] Directed by S. Soderbergh. Warner Bros.
- *Ocean's Thirteen*. (2007). [film] Directed by S. Soderbergh. Warner Bros.

Motivation: Hiding Information

- Attackers rely on information
- Consider a heist movie

Steal the Money

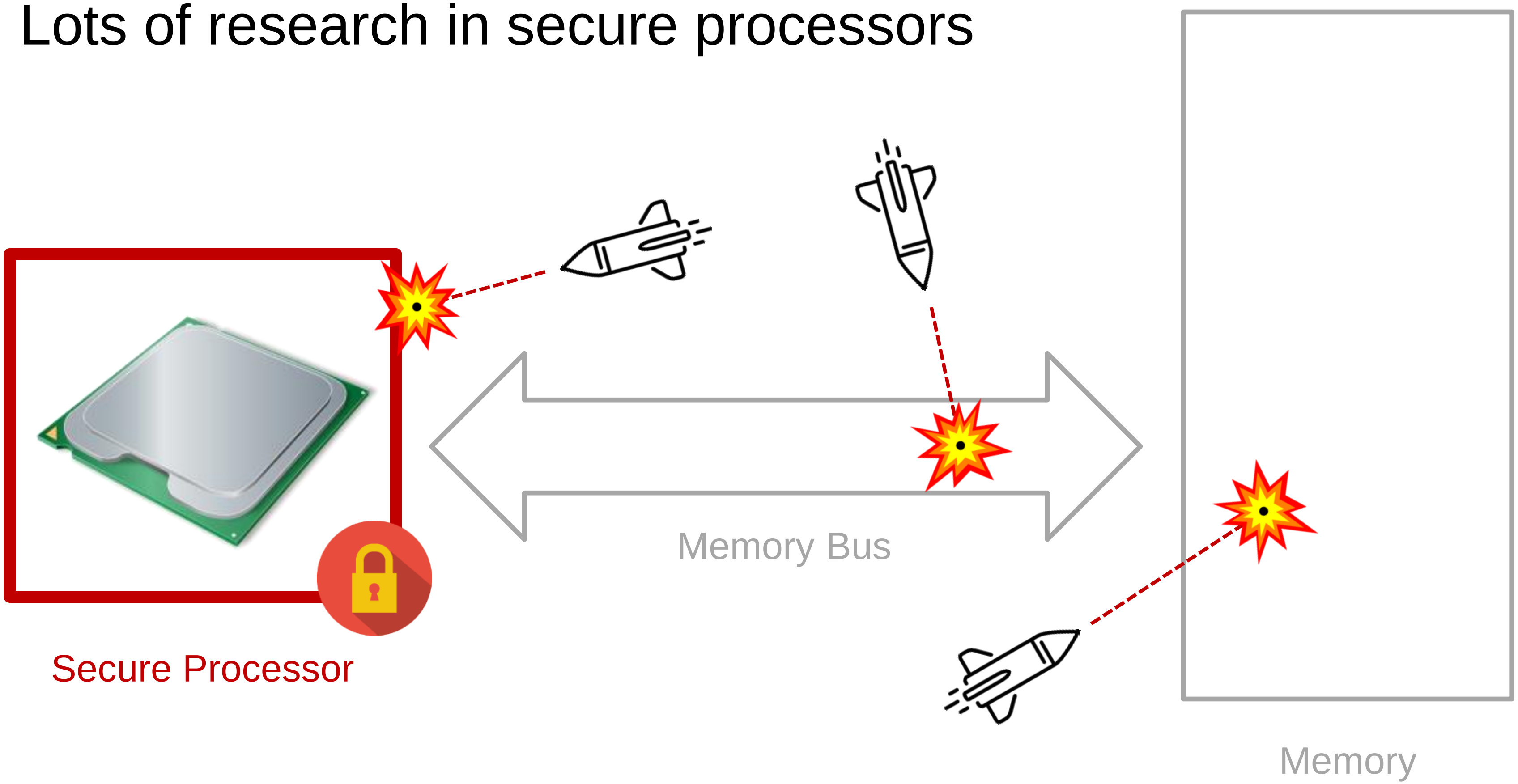
Rig the Games

- *Ocean's Eleven*. (2001). [film] Directed by S. Soderbergh. Warner Bros.
- *Ocean's Thirteen*. (2007). [film] Directed by S. Soderbergh. Warner Bros.

Hide any information an attacker could exploit

Secure Hardware

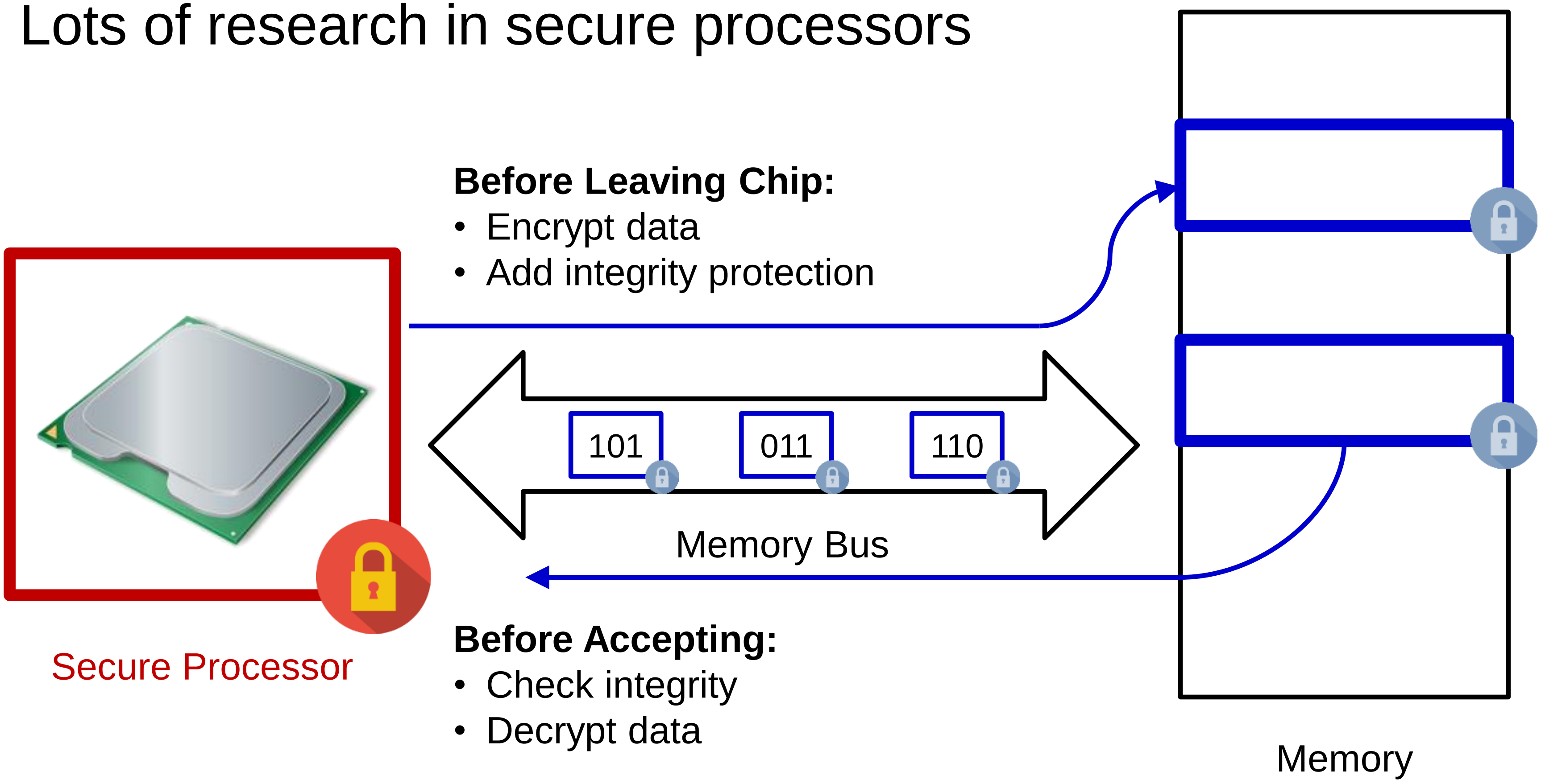
- Secure systems rely on secure hardware
- Lots of research in secure processors



- Zlatko Najdenovski. “Missile.” *Flaticon Basic License.* https://www.flaticon.com/free-icon/missile_182414
- OpenClipartVectors. “Explosion.” *CC Zero*. https://commons.wikimedia.org/wiki/File:Explosion-155624_icon.svg
- Double-J Design. “CPU Icon.” *CC Attribution 4.0*. http://www.doublejdesign.co.uk.
- GraphicLoads. “Lock Icon.” Freeware.

Secure Hardware

- Secure systems rely on secure hardware
- Lots of research in secure processors



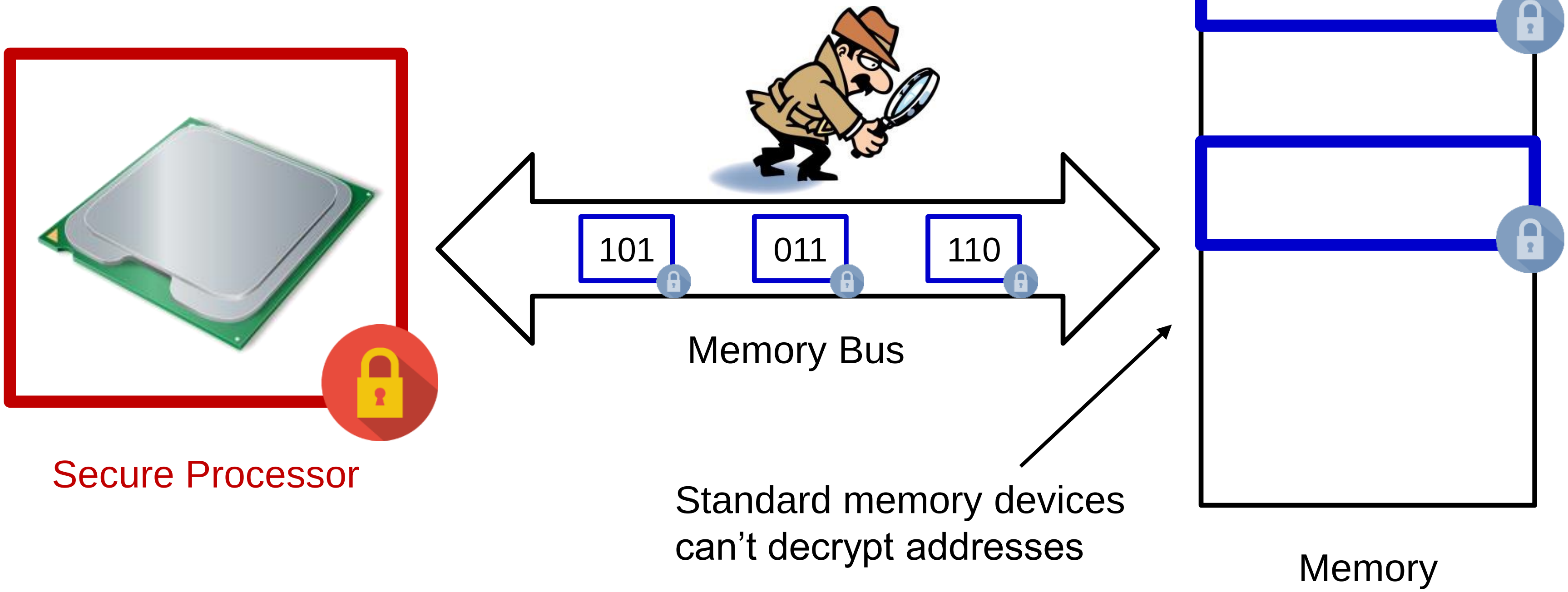
Before Leaving Chip:
- Encrypt data
- Add integrity protection

Before Accepting:
- Check integrity
- Decrypt data

- Double-J Design. “CPU Icon.” *CC Attribution 4.0*. http://www.doublejdesign.co.uk.
- GraphicLoads. “Lock Icon.” Freeware.

Memory Bus: An Easy Target

- Memory bus is vulnerable to snooping
- Addresses are still transmitted plainly
- Can still determine request type



Memory Bus

Secure Processor

Standard memory devices can’t decrypt addresses

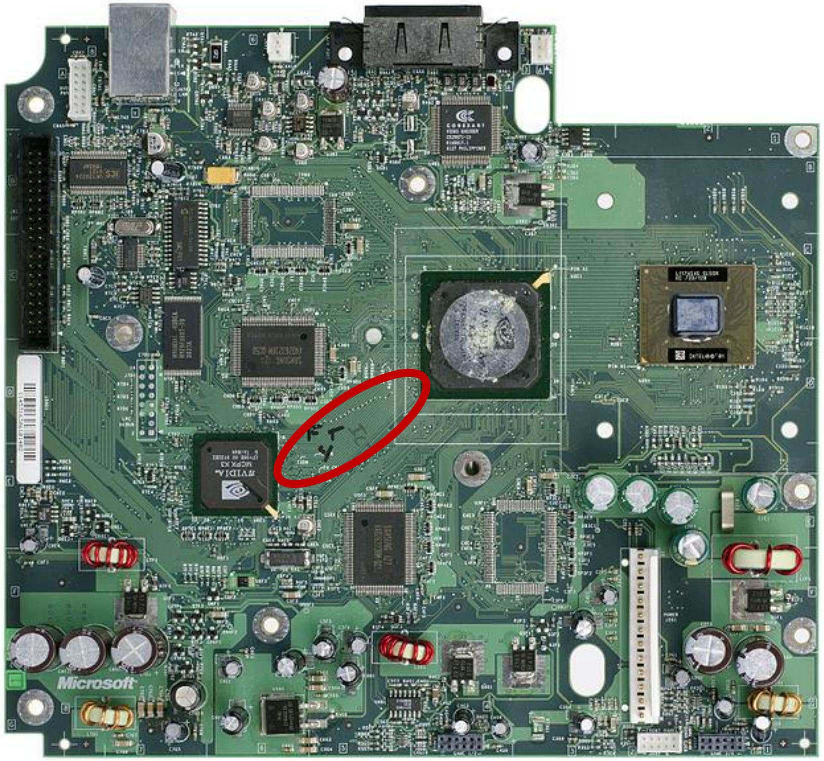
Memory

- Double-J Design. “CPU Icon.” *CC Attribution 4.0*. http://www.doublejdesign.co.uk.
- GraphicLoads. “Lock Icon.” Freeware.
- ClipartXtras. “Inspector Clipart.” https://clipartxtras.com

What’s the Harm?

- Steal important information
- Prevent system from working
- Enable a future attack

- Xbox Case Study (2002)
  - Probed HyperTransport bus
  - Identified boot code
  - Found decryption algorithm
  - Isolated key in boot code
  - Accessed boot loader

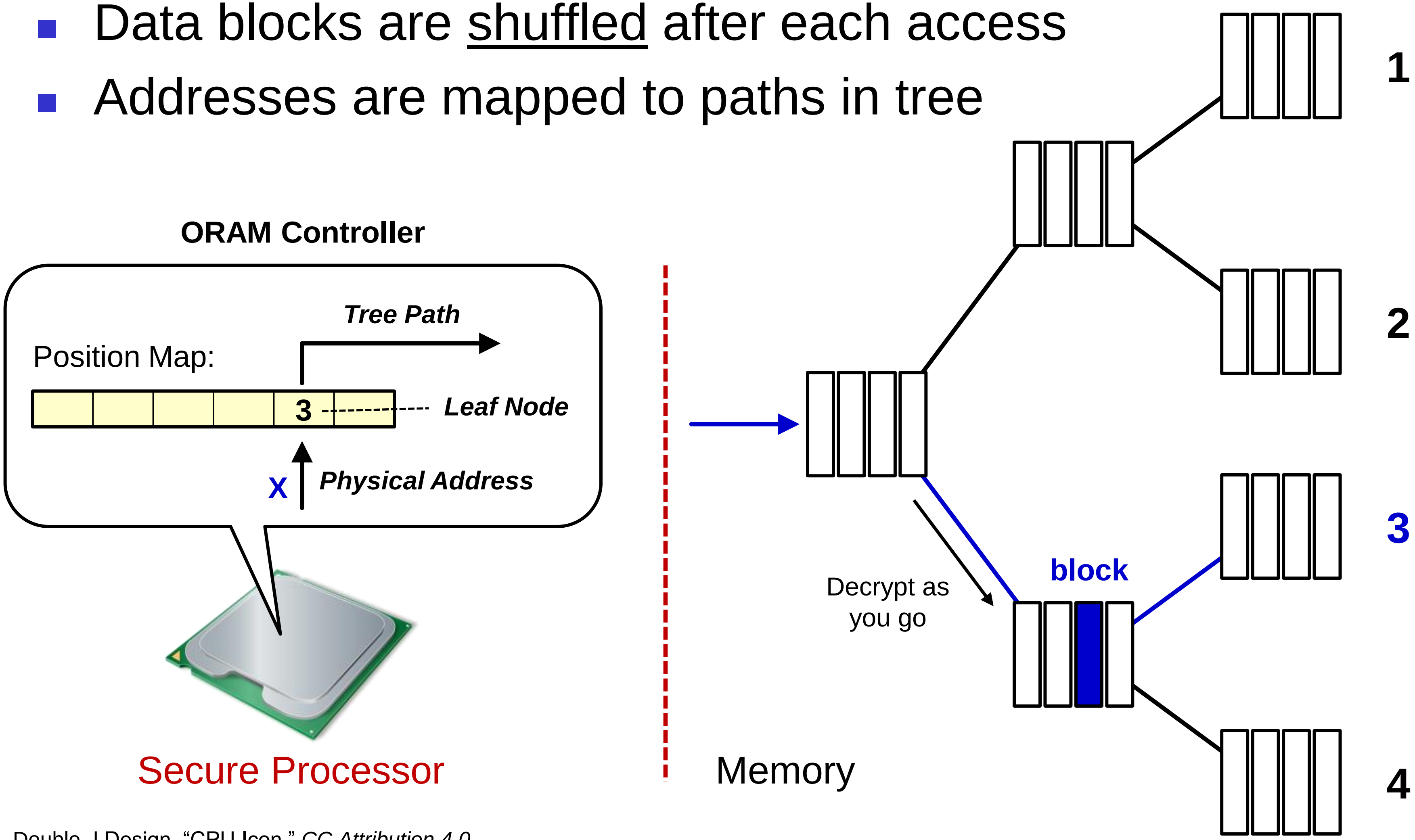


- A. Huang. “Breaking the Physical Security.” Keeping Secrets in Hardware: the Microsoft Xbox^{TM} Case Study. https://dspace.mit.edu/bitstream/handle/1721.1/6694/AIM-2002-008.pdf?sequence=2 .

- Evan-Amos. “Xbox-Motherboard-Rev1.” Public Domain. https://commons.wikimedia.org/wiki/File:Xbox-Motherboard-Rev1.jpg

Oblivious RAM (ORAM)

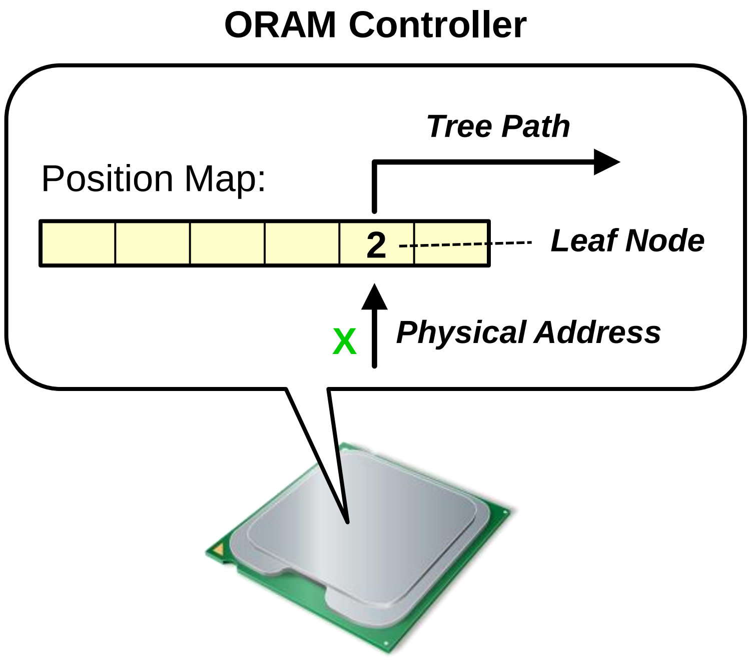
- Data blocks are shuffled after each access
- Addresses are mapped to paths in tree



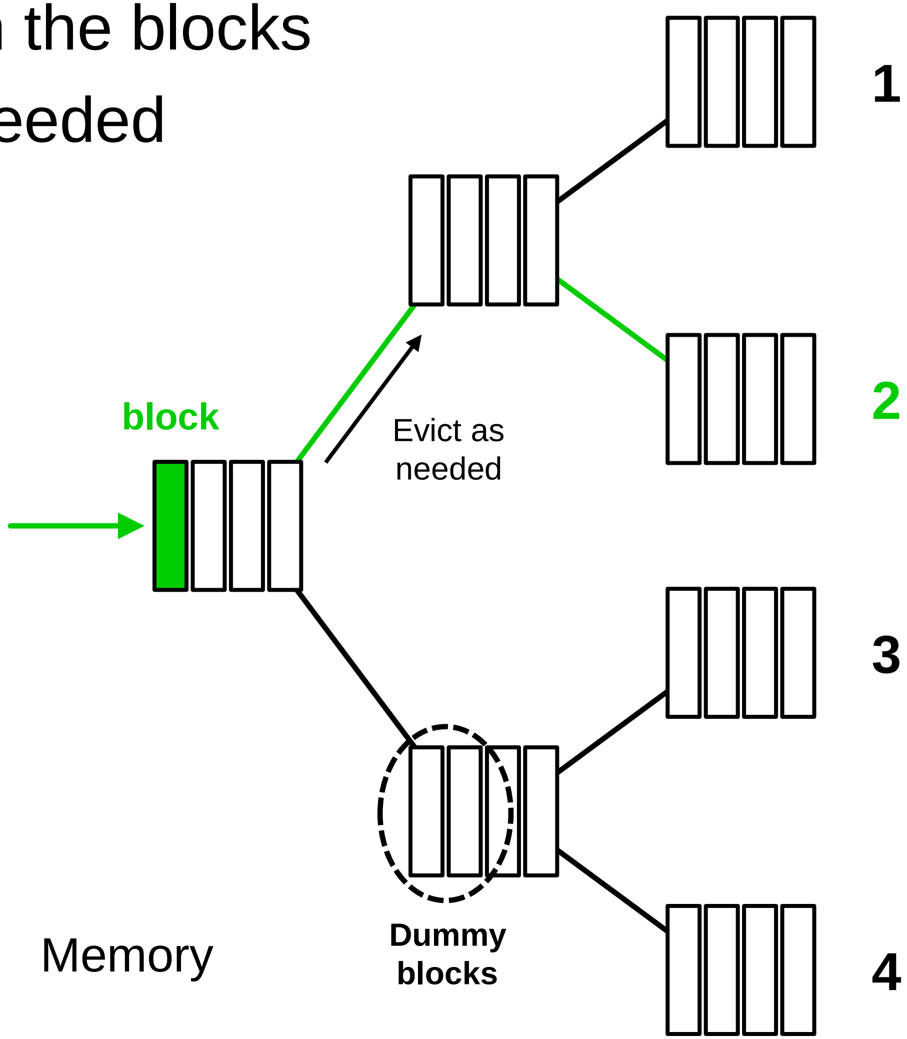
- Double-J Design. "CPU Icon." *CC Attribution 4.0*. http://www.doublejdesign.co.uk.

Oblivious RAM (ORAM)

- Different ways to reassign the blocks
- Dummy blocks are also needed



Secure Processor

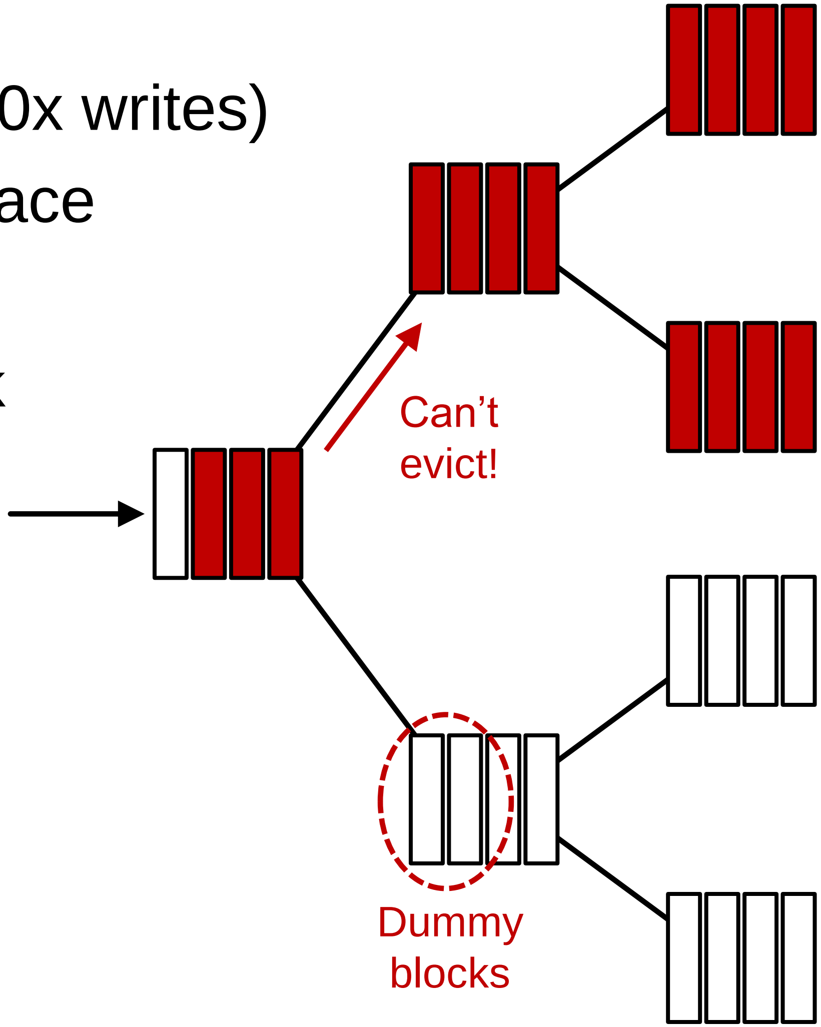


Memory

- Double-J Design. “CPU Icon.” *CC Attribution 4.0*. http://www.doublejdesign.co.uk.

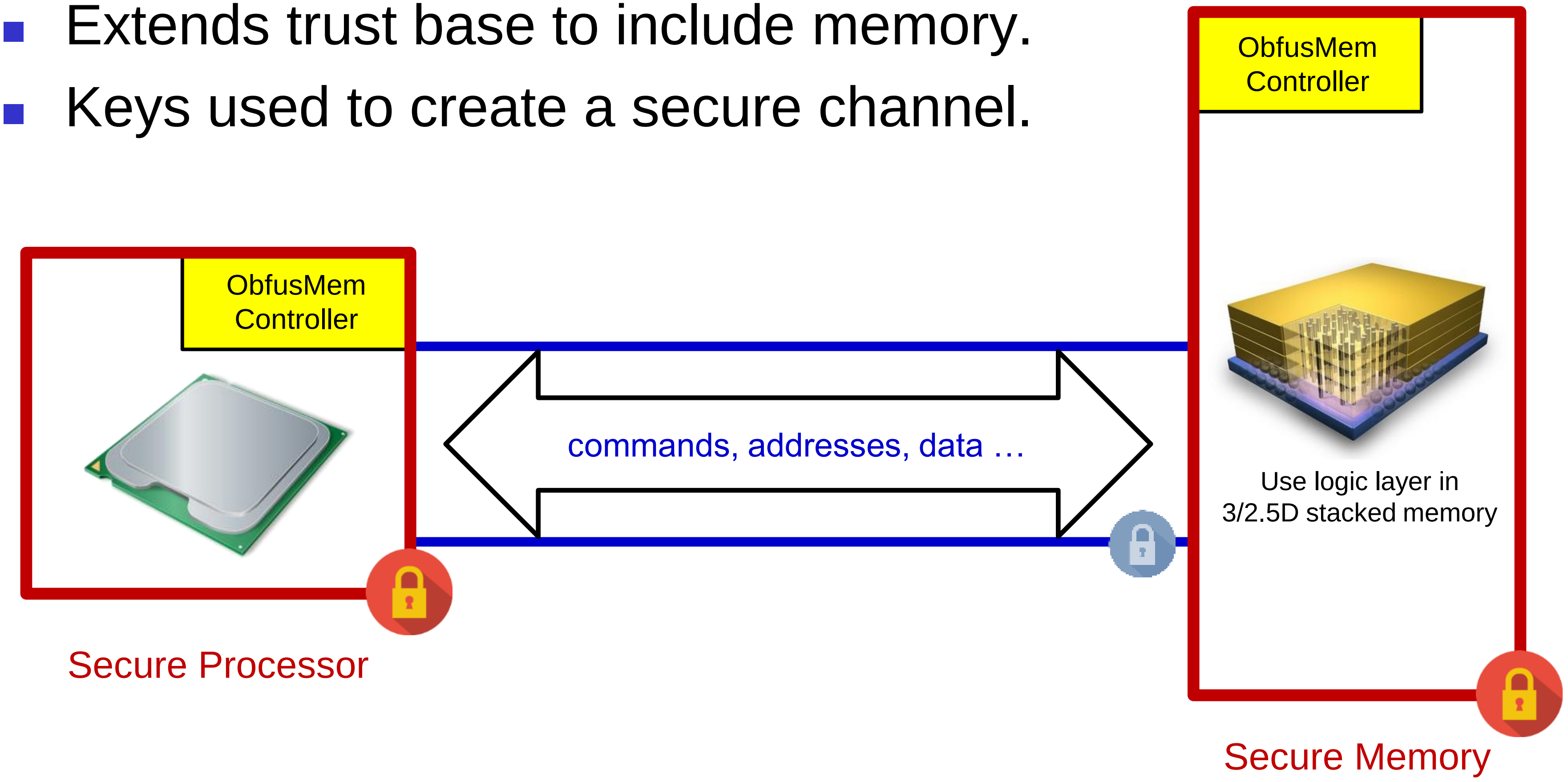
Oblivious RAM (ORAM): Downsides

- High bandwidth overhead
- Early device wear-out (100x writes)
- Dummy blocks require space
- Slow performance
- Possible system deadlock



ObfusMem Architecture

- CPU and memory have ObfusMem controller.
- Extends trust base to include memory.
- Keys used to create a secure channel.

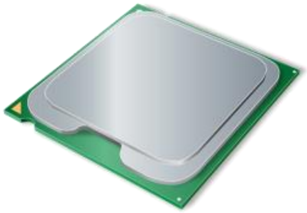


ObfusMem Controller
ObfusMem Controller
commands, addresses, data …
Use logic layer in 3/2.5D stacked memory
Secure Processor
Secure Memory

- Double-J Design. “CPU Icon.” *CC Attribution 4.0*. http://www.doublejdesign.co.uk.
- GraphicLoads. “Lock Icon.” Freeware.
- Flickr “3D DRAM” http://farm8.staticflickr.com/7013/6436525561_27bf9b4eaf.jpg.

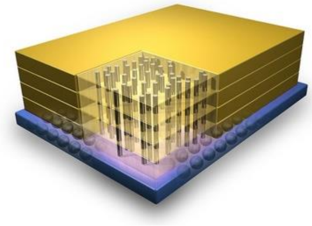
ObfusMem: Key Exchange

Keys burned in by manufacturer



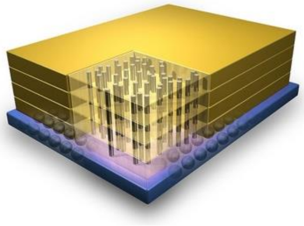
Public Private

Processor



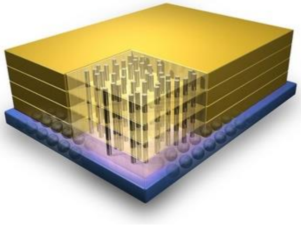
Memory

Public Private



Memory

Public Private



Memory

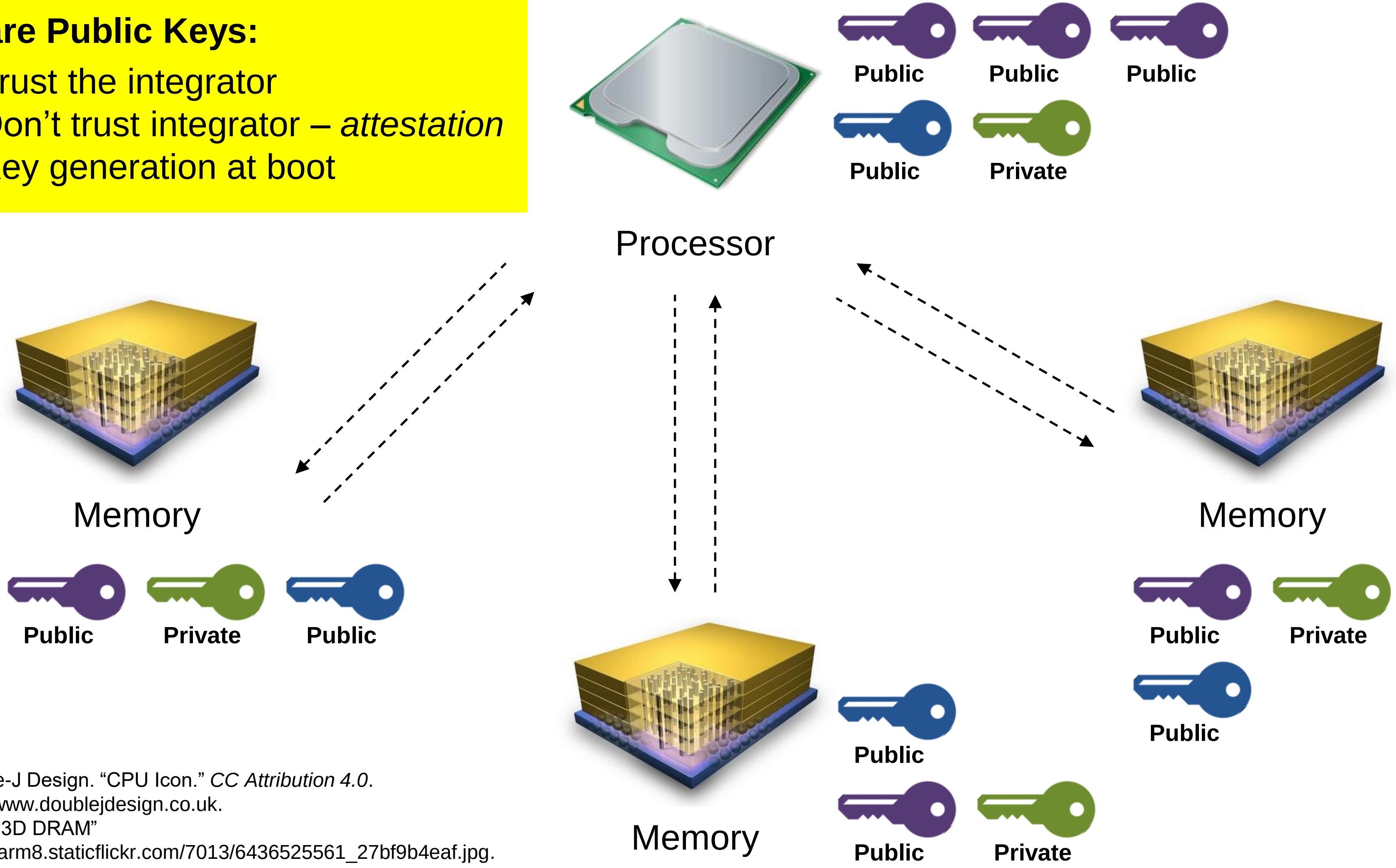
Public Private

- Double-J Design. “CPU Icon.” *CC Attribution 4.0*. http://www.doublejdesign.co.uk.
- Flickr “3D DRAM” http://farm8.staticflickr.com/7013/6436525561_27bf9b4eaf.jpg.
- IconFinder. “Key Icon.” *MIT License*. https://www.iconfinder.com/icons/298808/key_icon.

ObfusMem: Key Exchange

Share Public Keys:

1. Trust the integrator
2. Don’t trust integrator – *attestation*
3. Key generation at boot

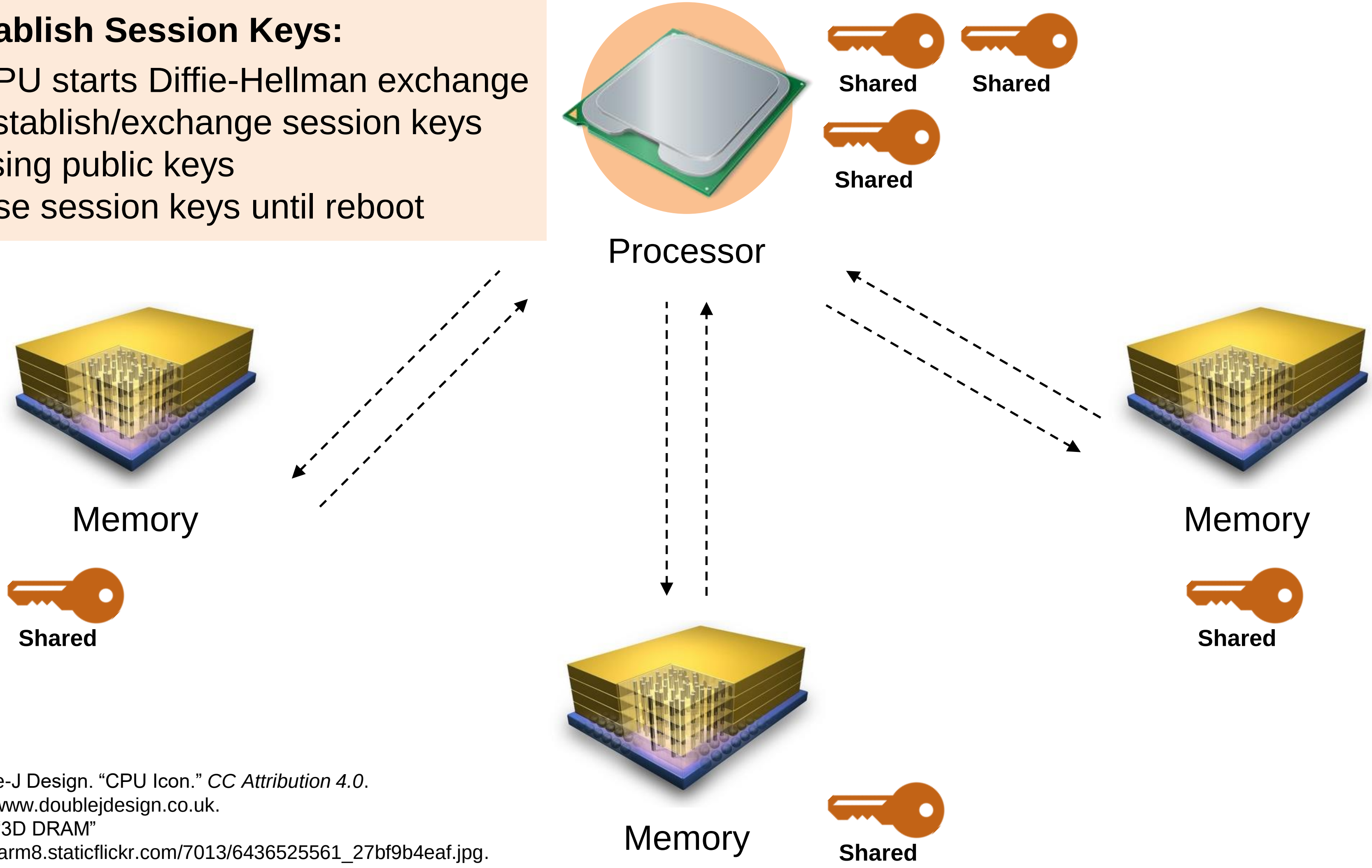


- Double-J Design. “CPU Icon.” *CC Attribution 4.0*. http://www.doublejdesign.co.uk.
- Flickr “3D DRAM” http://farm8.staticflickr.com/7013/6436525561_27bf9b4eaf.jpg.
- IconFinder. “Key Icon.” *MIT License*. https://www.iconfinder.com/icons/298808/key_icon.

ObfusMem: Key Exchange

Establish Session Keys:

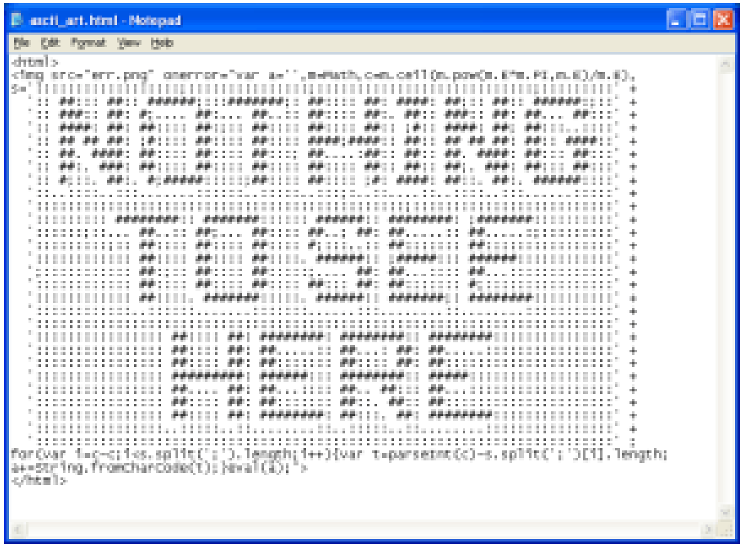
- CPU starts Diffie-Hellman exchange
- Establish/exchange session keys using public keys
- Use session keys until reboot



- Double-J Design. “CPU Icon.” *CC Attribution 4.0*. http://www.doublejdesign.co.uk.
- Flickr “3D DRAM” http://farm8.staticflickr.com/7013/6436525561_27bf9b4eaf.jpg.
- IconFinder. “Key Icon.” *MIT License*. https://www.iconfinder.com/icons/298808/key_icon.

Access Pattern Obfuscation

- Patterns to obfuscate
  - Spatial
  - Temporal
  - Command
  - Memory Footprint

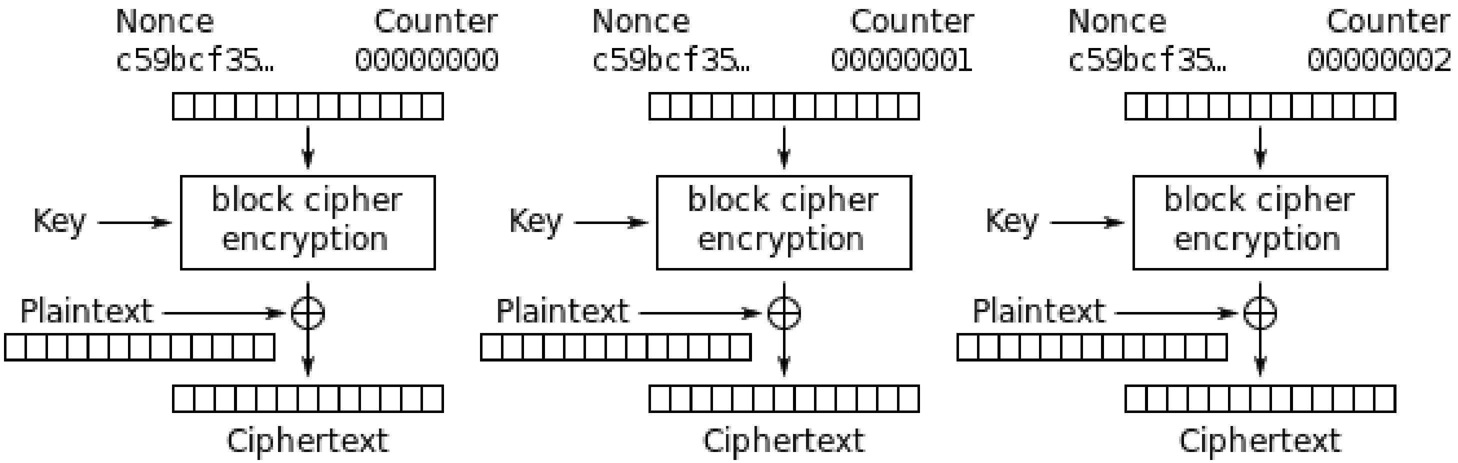


```
<html>
<img src="err.png" onerror="var a='',m=Math,c=m.ceil(m.pow(m.E*m.PI,m.E)/m.E),
s='[illegible]
for(var i=c-c;i<s.split(';').length;i++){var t=parseInt(c)-s.split(';')[i].length;
a+=String.fromCharCode(t);}eval(a);'">
</html>
```

- Ou, Elaine. “Obfuscated Obfuscation.” *Elaine’s Idle Mind*. https://elaineou.com/2016/06/07/obfuscated-obfuscation/.

Access Pattern Obfuscation

- Method: use counter mode encryption
  - ...twice

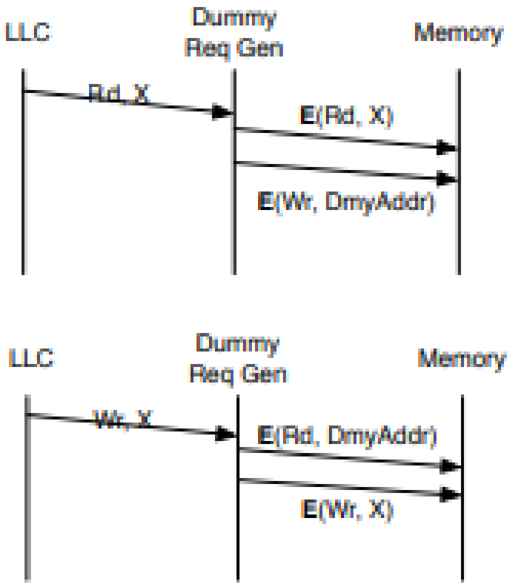


Counter (CTR) mode encryption

- WhiteTimberwolf. “CTR encryption 2.” *Wikimedia Commons*. https://commons.wikimedia.org/wiki/File:CTR_encryption_2.svg.

Pattern Obfuscation: Command

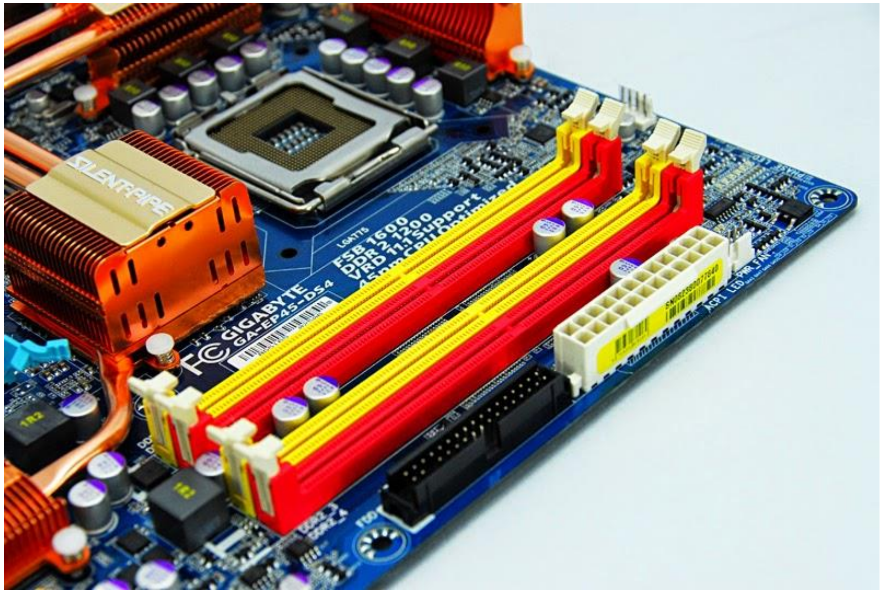
- Method: pair each read with a dummy write, and vice versa
- A fixed location in memory is used for the dummy address
  - CTR mode encryption ensures it'll never look the same



- A. Awad et al. "Illustration of dummy request generation." Obfusmem. *ACM Digital Library*. https://dl.acm.org/citation.cfm?id=3080230.

Pattern Obfuscation: Inter-Channel

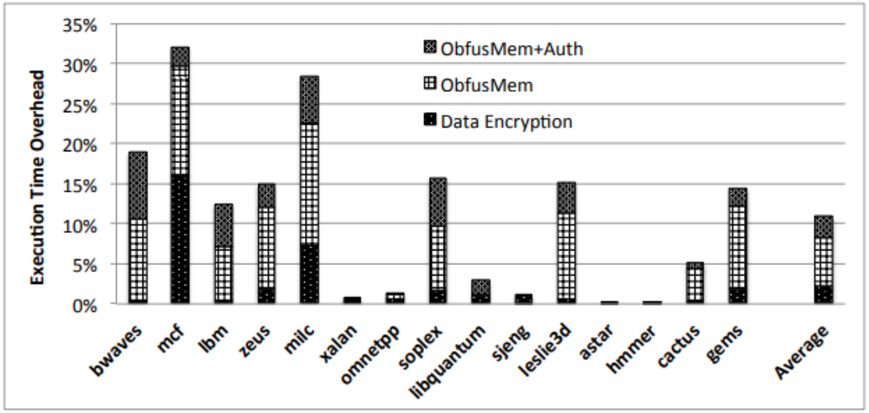
- Method: idle channel dummy replication
- Fake a request on any idle channel during a real one

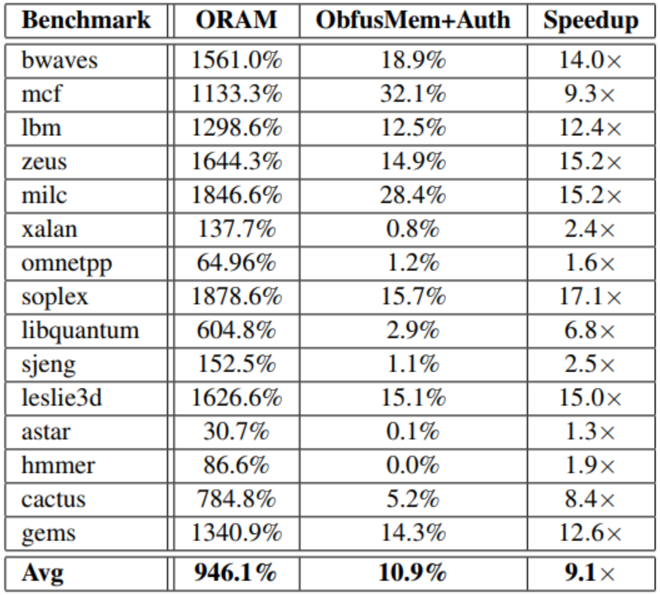


- PhoneProject. “Multi-Channel Memory.” *An Overview of Storage Devices - CompTIA A+ 220-801: 1.5*. http://studyforyourcerts.blogspot.com/2015/01/.

Analysis: Performance Overhead

- ORAM adds 946.1% to execution time and 100% memory overhead
- ObfusMem adds 10.9% on average and 32.1% worst case with 0-2% memory overhead



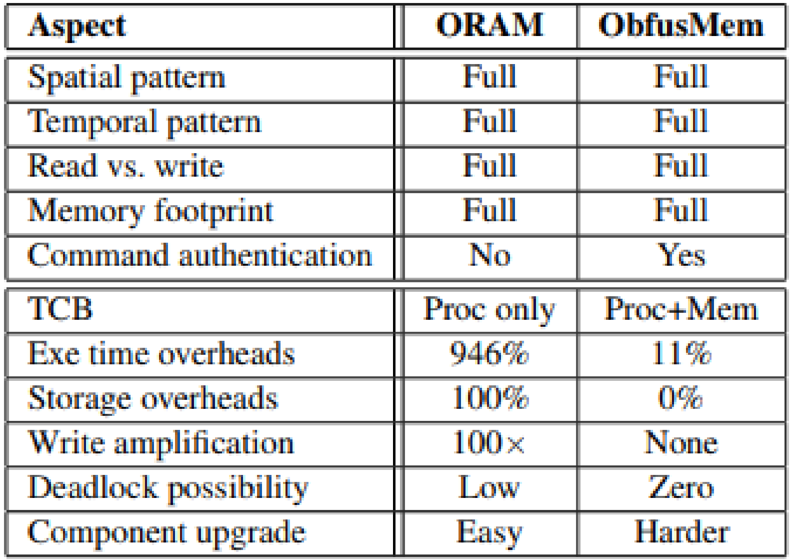


Benchmark	ORAM	ObfusMem+Auth	Speedup
bwaves	1561.0%	18.9%	14.0×
mcf	1133.3%	32.1%	9.3×
lbm	1298.6%	12.5%	12.4×
zeus	1644.3%	14.9%	15.2×
milc	1846.6%	28.4%	15.2×
xalan	137.7%	0.8%	2.4×
omnetpp	64.96%	1.2%	1.6×
soplex	1878.6%	15.7%	17.1×
libquantum	604.8%	2.9%	6.8×
sjeng	152.5%	1.1%	2.5×
leslie3d	1626.6%	15.1%	15.0×
astar	30.7%	0.1%	1.3×
hmmer	86.6%	0.0%	1.9×
cactus	784.8%	5.2%	8.4×
gems	1340.9%	14.3%	12.6×
Avg	**946.1%**	**10.9%**	**9.1**×

- A. Awad et al. “5.1 Performance Overhead.” Obfusmem. *ACM Digital Library*. https://dl.acm.org/citation.cfm?id=3080230.

Analysis: Challenges

- Multiprocessor systems’ cache coherence protocols require processor-processor protection
- ObfusMem remains susceptible to thermal and timing side-channel attacks



Aspect	ORAM	ObfusMem
Spatial pattern	Full	Full
Temporal pattern	Full	Full
Read vs. write	Full	Full
Memory footprint	Full	Full
Command authentication	No	Yes
TCB	Proc only	Proc+Mem
Exe time overheads	946%	11%
Storage overheads	100%	0%
Write amplification	100×	None
Deadlock possibility	Low	Zero
Component upgrade	Easy	Harder

- A. Awad et al. “6.1 Security Analysis.” Obfusmem. *ACM Digital Library*. https://dl.acm.org/citation.cfm?id=3080230.

Discussion

- Is it a problem that ObfusMem does not protect from side-channel attacks?

Discussion

- Is it feasible to assume the memory is not vulnerable to physical attacks?

Discussion

- Is ObfusMem strictly better than ORAM?