

# | Cohere+Reload

## Re-enabling High-Resolution Cache Attacks on AMD SEV-SNP

Lukas Giner (@redrabbbyte), Sudheendra Raghav Neela, and Daniel Gruss

DIMVA 2025

# Who am I?



**Lukas Giner**

PhD Candidate @ Graz University of Technology

🐦 @redrabbite

✉️ lukas.giner@tugraz.at

- Confidential Virtual Machine



- Confidential Virtual Machine
- Secure Memory Encryption (SME)



- Confidential Virtual Machine
- Secure Memory Encryption (SME)
- 1 key per CVM



- Confidential Virtual Machine
- Secure Memory Encryption (SME)
- 1 key per CVM
- Encryption bit 51



# Cache Addressing

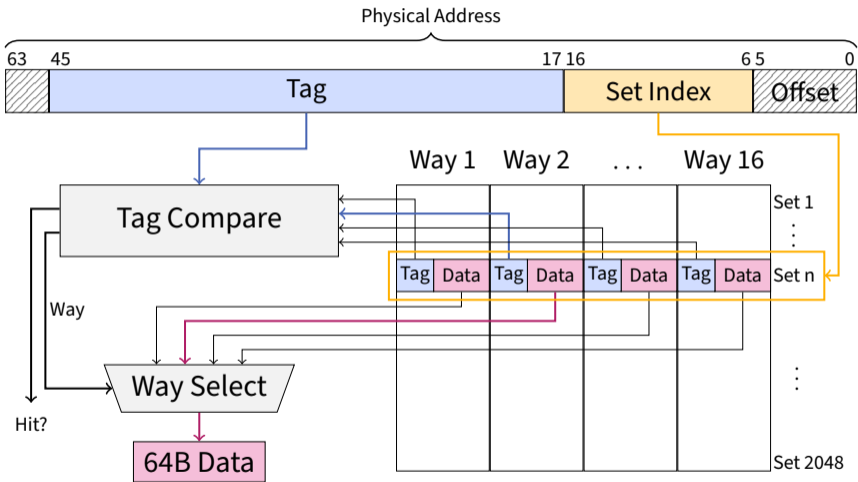
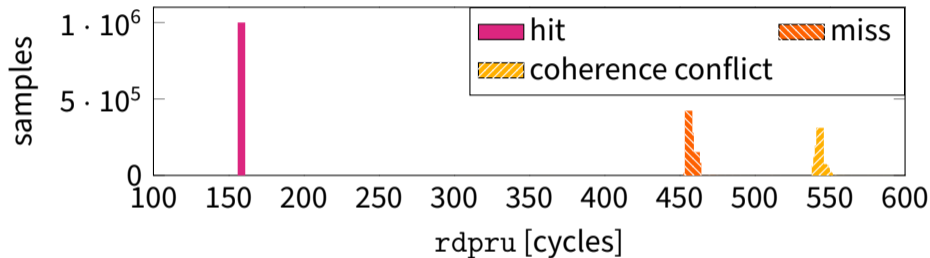
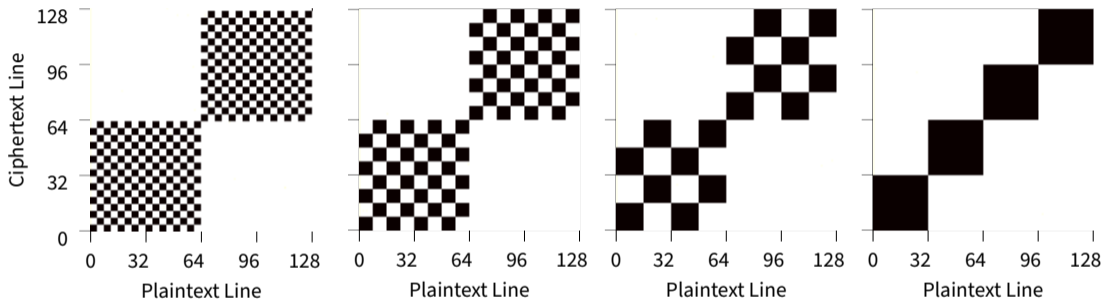


Figure: Cache addressing in a 16-way set-associative cache.



**Figure:** Access timing histogram for accesses that are hits, misses (flushed) or conflicts caused by SME (Secure Memory Encryption) coherence.

# Cohere+Reload Eviction Pattern



(a) 256B

(b) 512B

(c) 1024B

(d) 2048B

**Figure:** Eviction Pattern for different **DRAM interleaving size** setting over 8 KiB of physically contiguous memory.

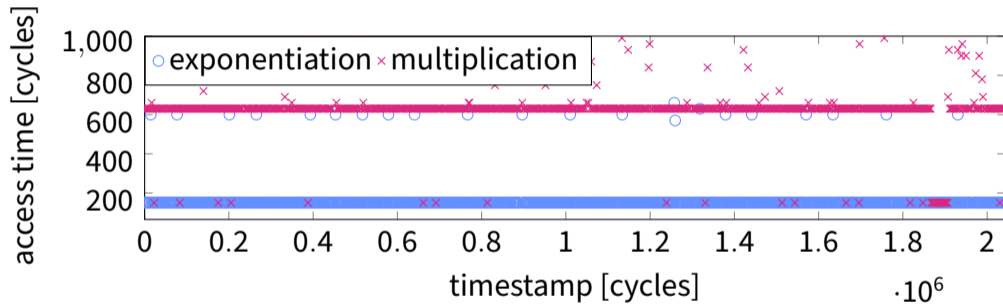


Figure: One-shot RSA encryption trace.

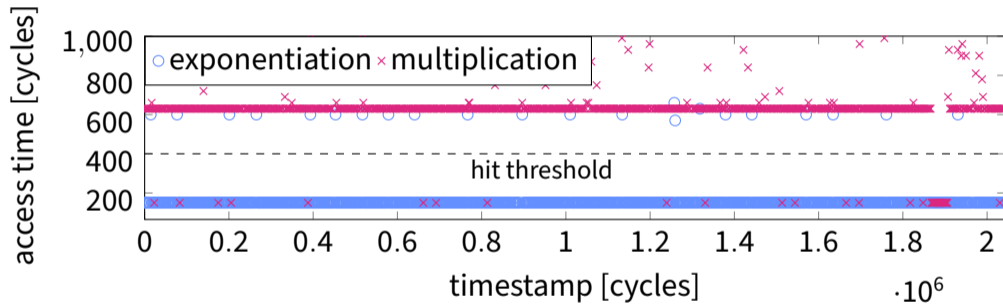


Figure: One-shot RSA encryption trace.

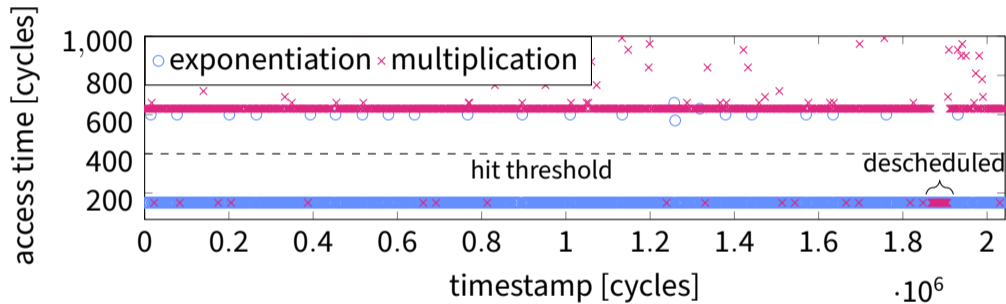


Figure: One-shot RSA encryption trace.

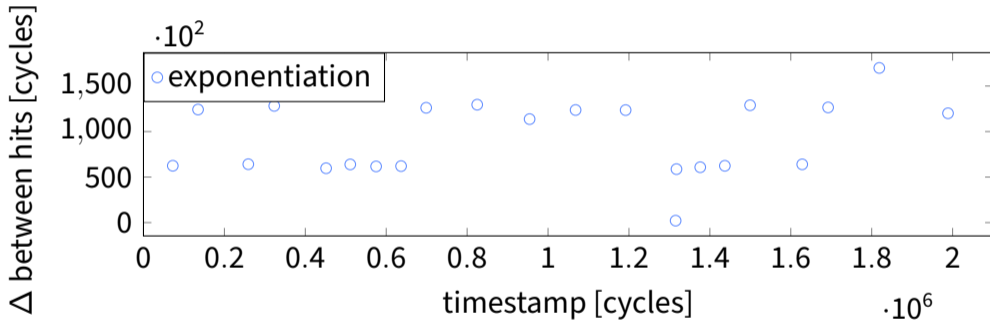


Figure: One-shot RSA encryption trace.

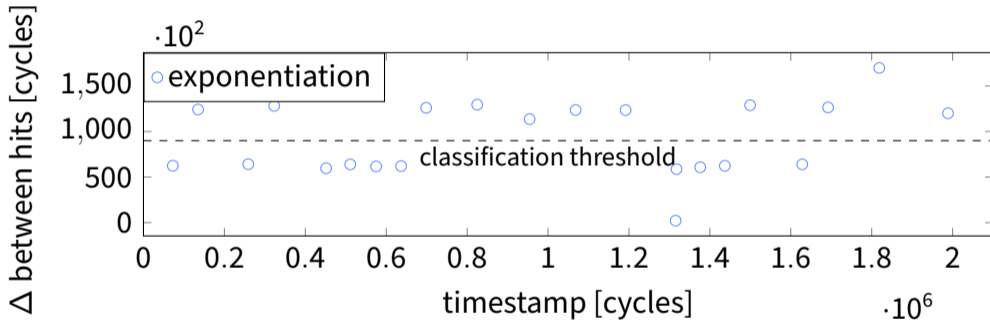


Figure: One-shot RSA encryption trace.

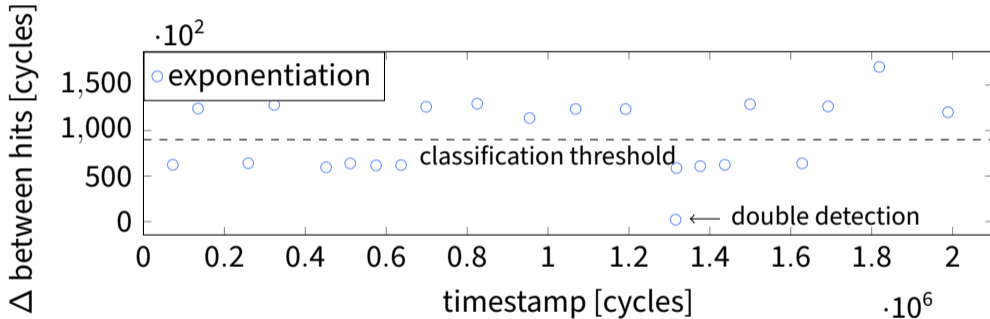


Figure: One-shot RSA encryption trace.

# AES Attack

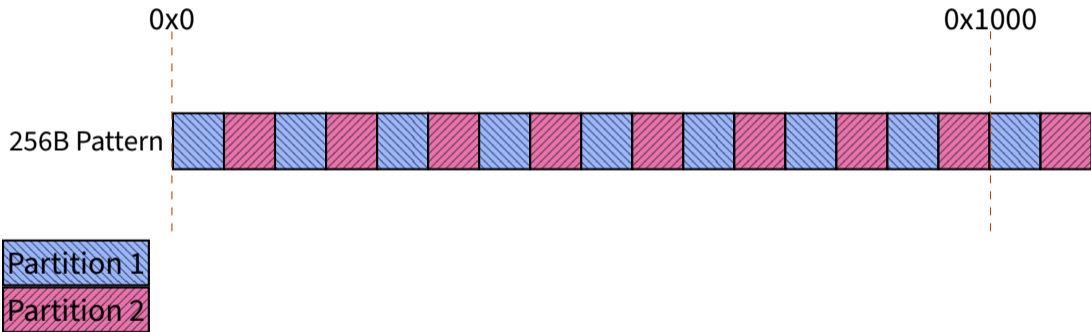


Figure: AES T-table memory alignment in OpenSSL.

# AES Attack

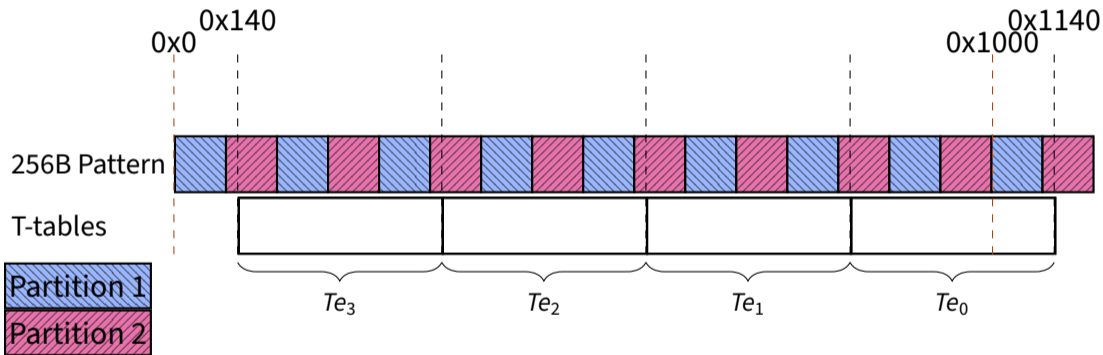


Figure: AES T-table memory alignment in OpenSSL.

# AES Attack

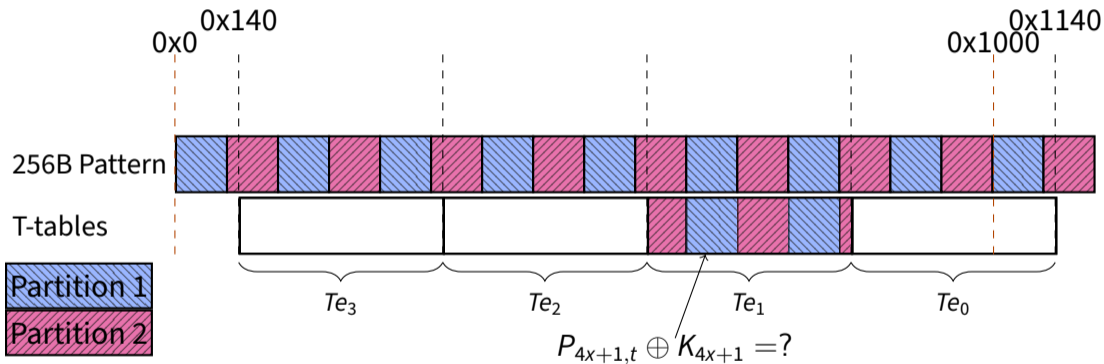


Figure: AES T-table memory alignment in OpenSSL.

# AES Attack

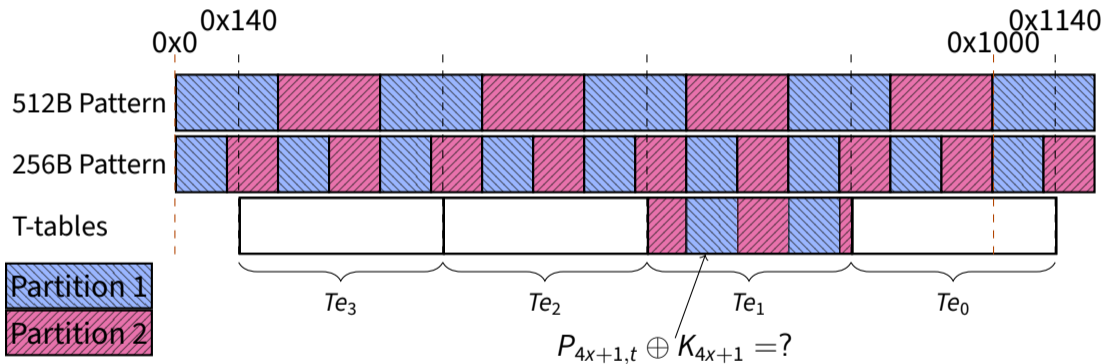
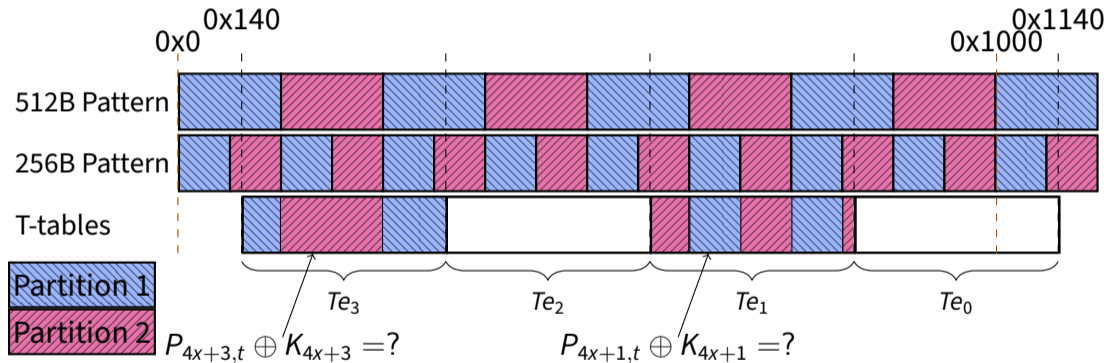


Figure: AES T-table memory alignment in OpenSSL.



**Figure:** AES T-table memory alignment in OpenSSL.

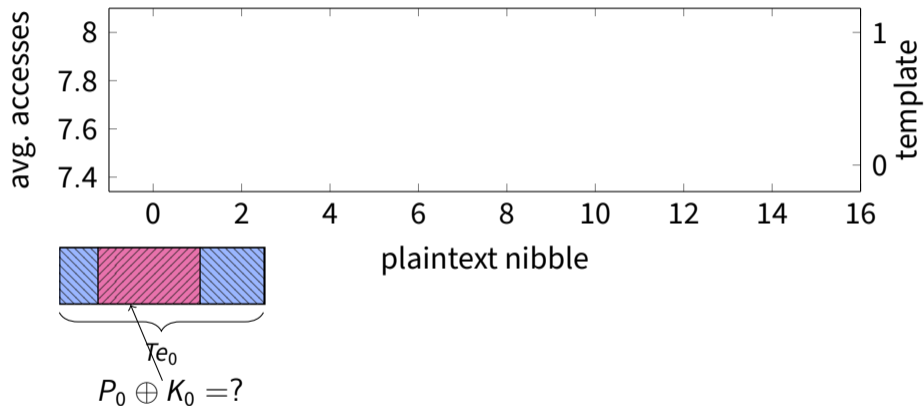


Figure: AES T-table memory alignment in OpenSSL.

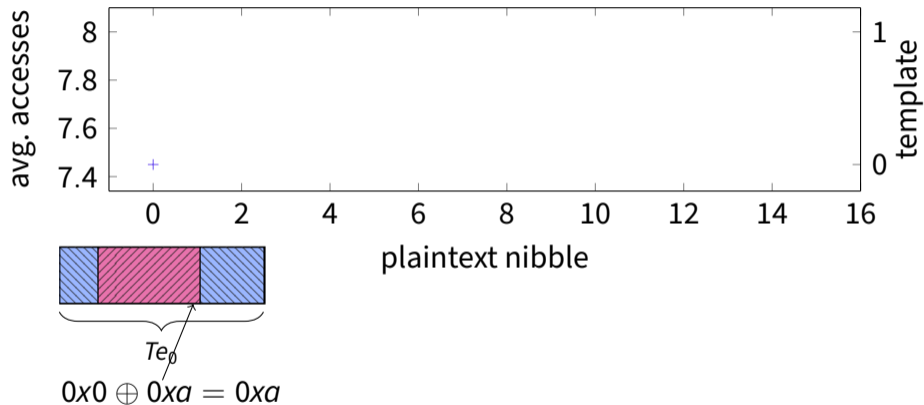


Figure: AES T-table memory alignment in OpenSSL.

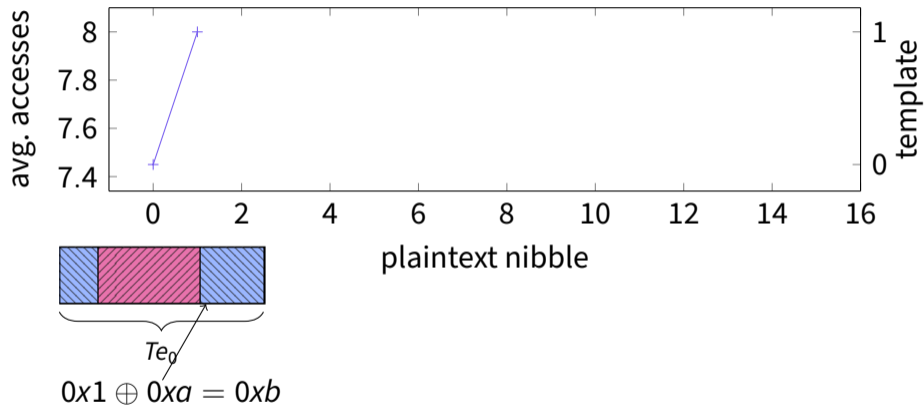


Figure: AES T-table memory alignment in OpenSSL.

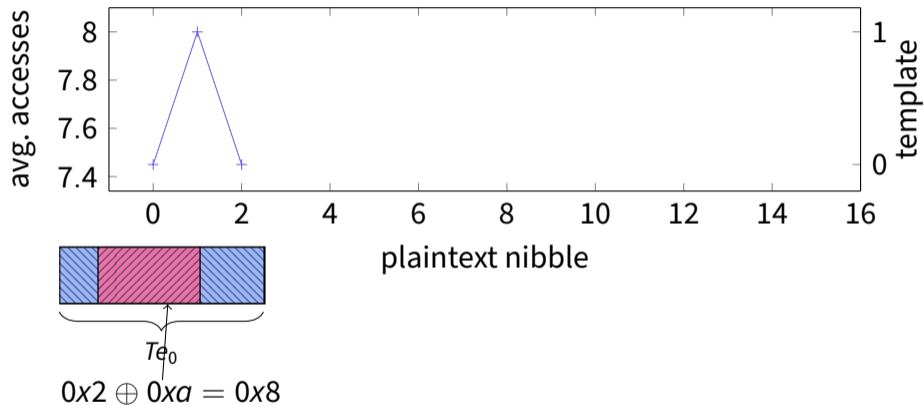


Figure: AES T-table memory alignment in OpenSSL.

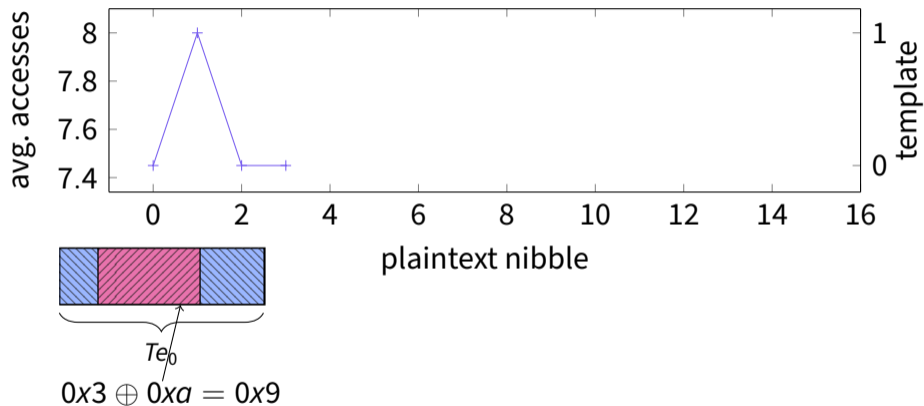


Figure: AES T-table memory alignment in OpenSSL.

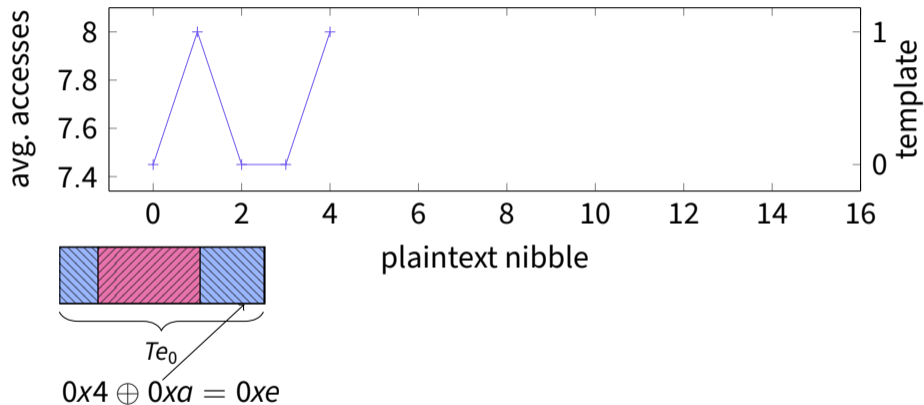


Figure: AES T-table memory alignment in OpenSSL.

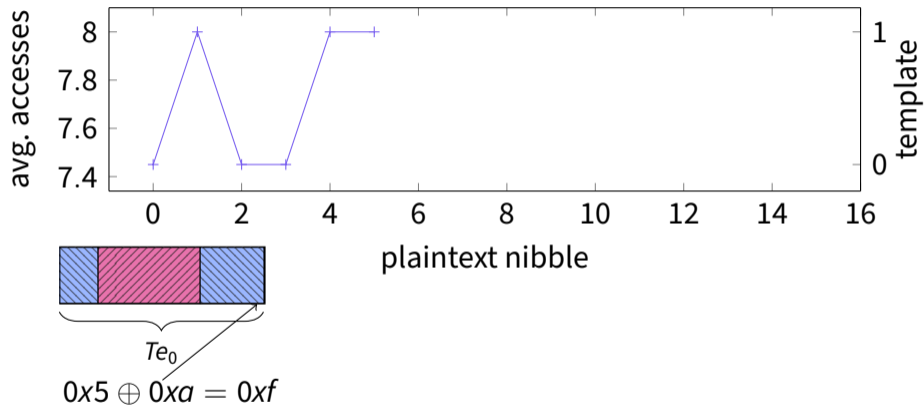


Figure: AES T-table memory alignment in OpenSSL.

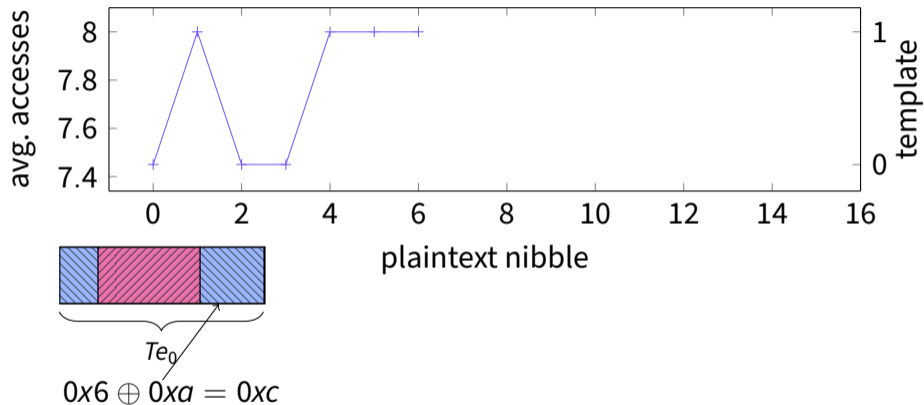


Figure: AES T-table memory alignment in OpenSSL.

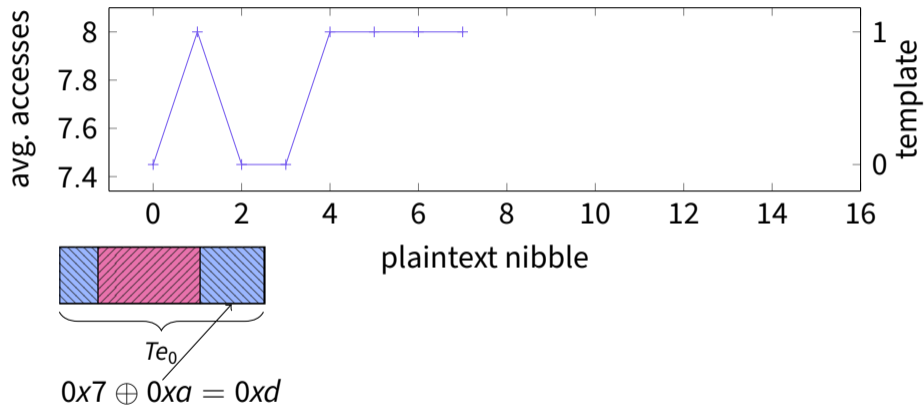


Figure: AES T-table memory alignment in OpenSSL.

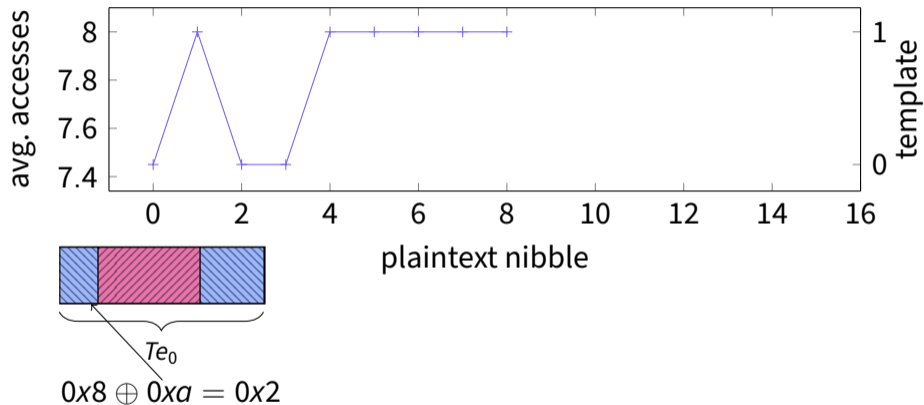


Figure: AES T-table memory alignment in OpenSSL.

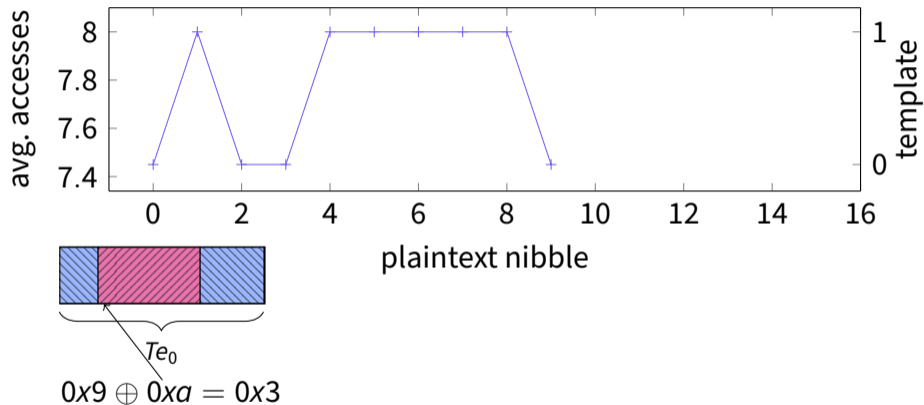


Figure: AES T-table memory alignment in OpenSSL.

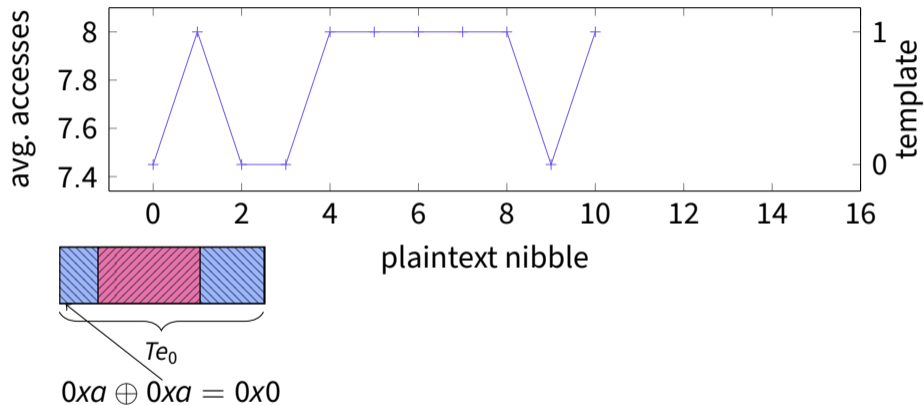


Figure: AES T-table memory alignment in OpenSSL.

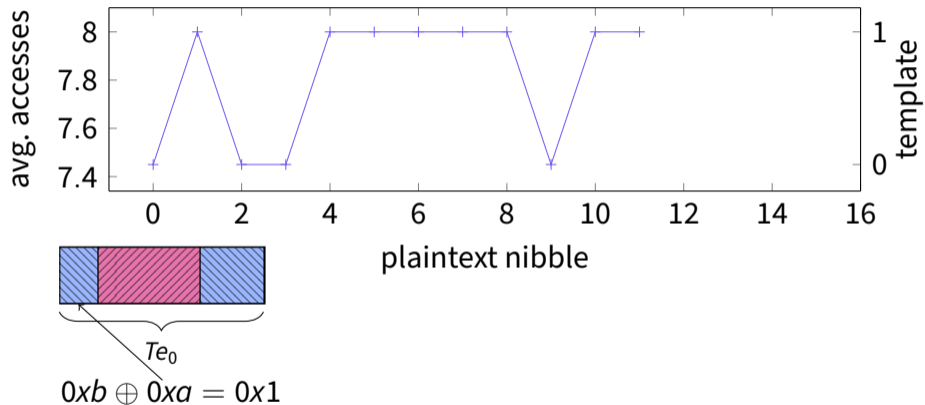
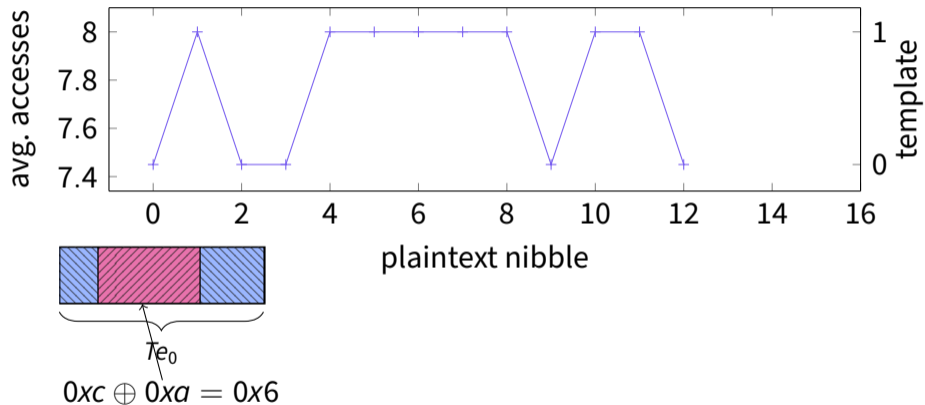


Figure: AES T-table memory alignment in OpenSSL.



**Figure:** AES T-table memory alignment in OpenSSL.

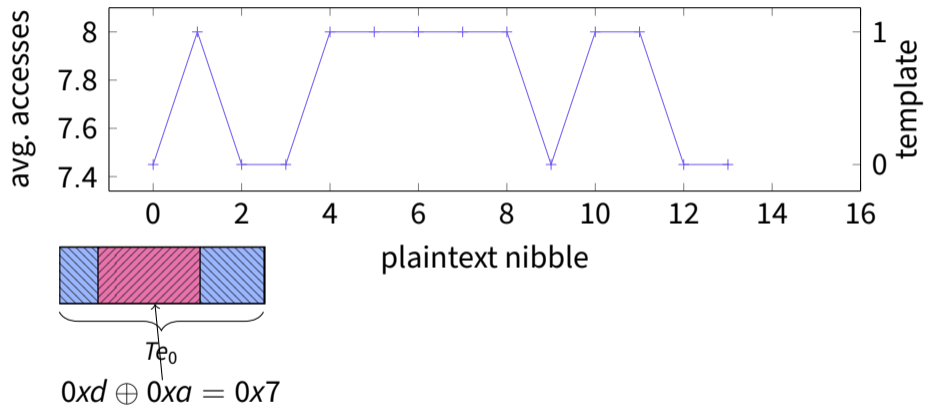


Figure: AES T-table memory alignment in OpenSSL.

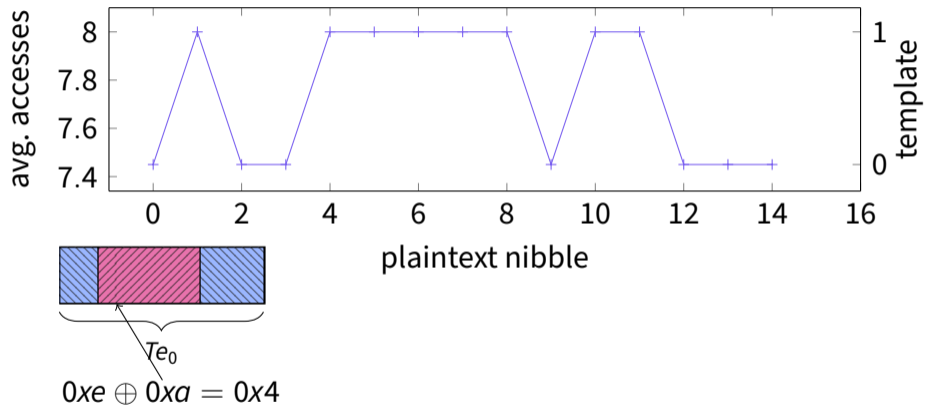


Figure: AES T-table memory alignment in OpenSSL.

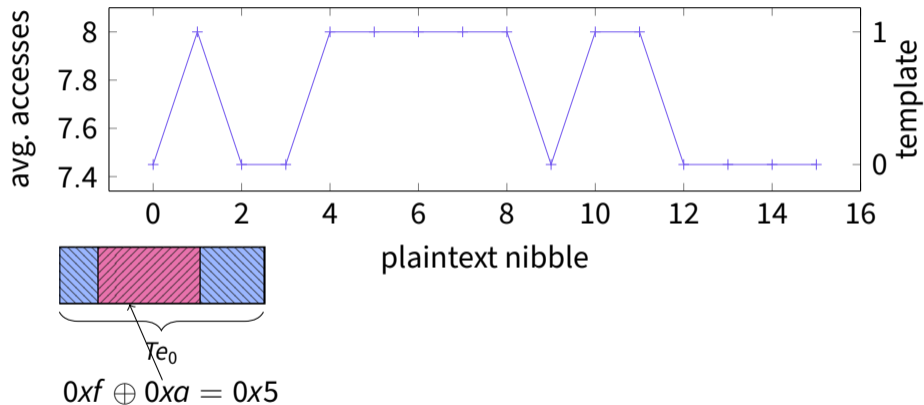


Figure: AES T-table memory alignment in OpenSSL.

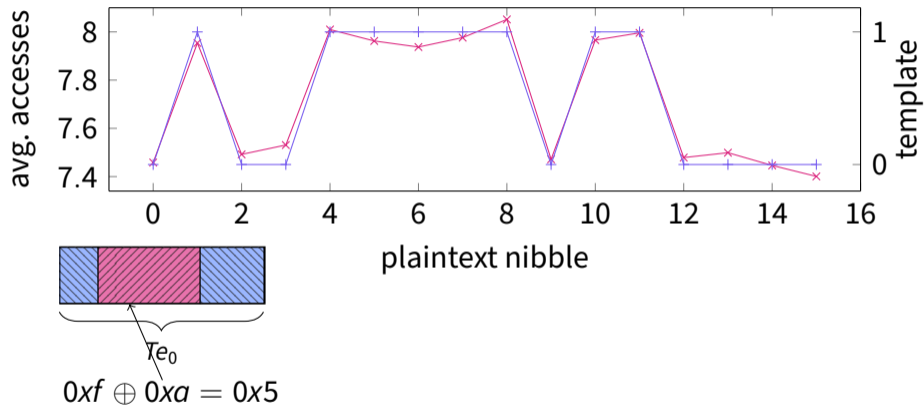
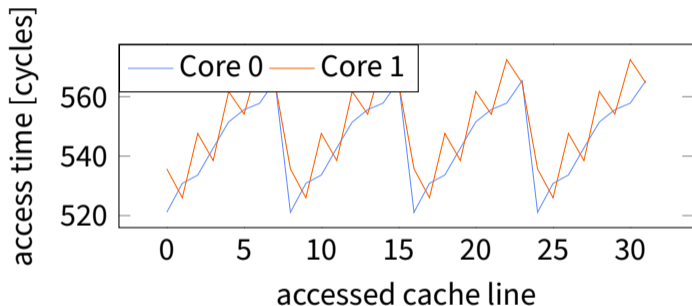


Figure: AES T-table memory alignment in OpenSSL.

**Figure:** Cohere+Reload access trace for a single AES encryption.

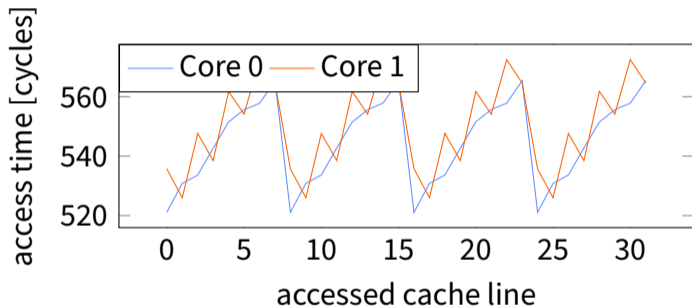
# Diving Deeper - Access Times



■ repeating pattern

**Figure:** Average access time for one plaintext access at position  $n$  in 512 B partition.

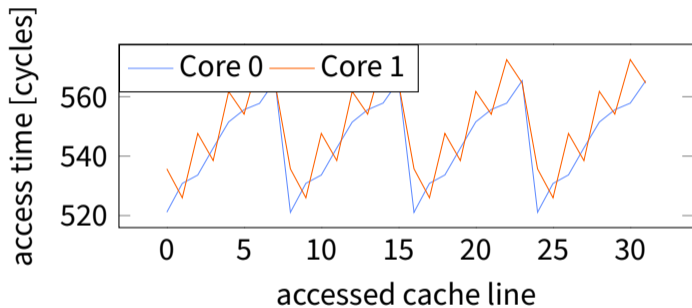
# Diving Deeper - Access Times



- repeating pattern
- unique behavior per core

**Figure:** Average access time for one plaintext access at position  $n$  in 512 B partition.

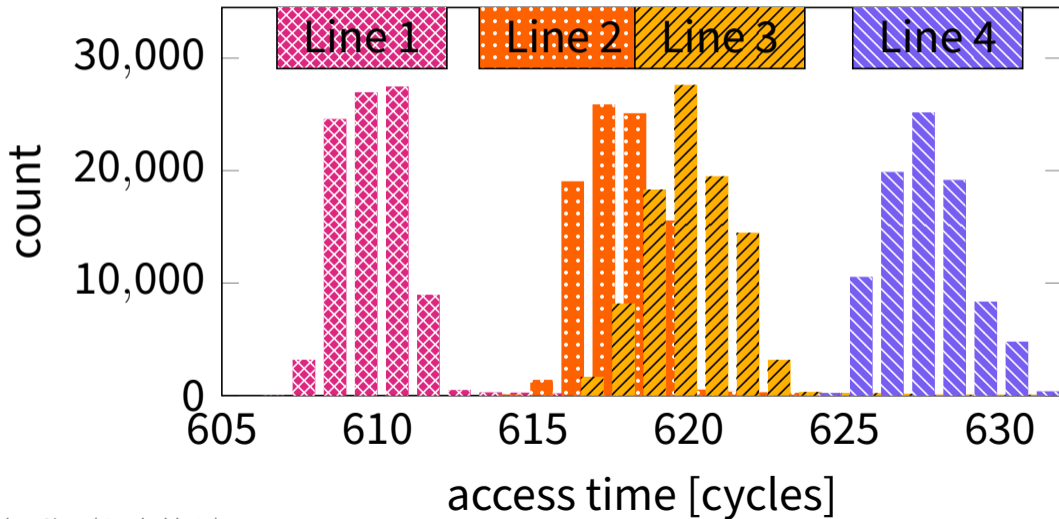
# Diving Deeper - Access Times



- repeating pattern
- unique behavior per core
- consistent between CCX

**Figure:** Average access time for one plaintext access at position  $n$  in 512 B partition.

# Diving Deeper - Access Times





- Disable automatic coherence



- Disable automatic coherence
- Disable ciphertext access for host



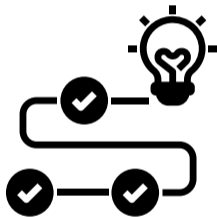
- Disable automatic coherence
- Disable ciphertext access for host
- Constant-time code



- Disable automatic coherence
- Disable ciphertext access for host
- Constant-time code
- Uncacheable memory for secrets

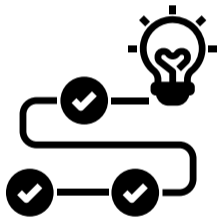
# Conclusion

- Very high temporal resolution



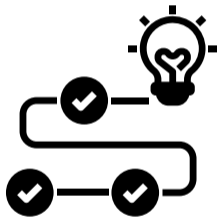
# Conclusion

- Very high temporal resolution
- Patterned groups enhance attacks

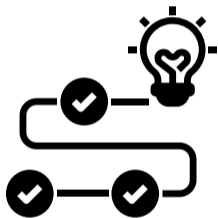


# Conclusion

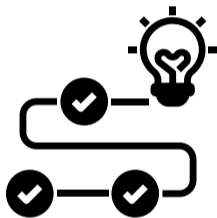
- Very high temporal resolution
- Patterned groups enhance attacks



- Very high temporal resolution
- Patterned groups enhance attacks
- Coherence undermines SEV confidentiality



- Very high temporal resolution
  - Patterned groups enhance attacks
  - Coherence undermines SEV confidentiality
- Is this coherence necessary?



# Acknowledgments

This research was made possible by generous funding from:



Funded by  
the European Union



European Research Council  
Established by the European Commission



Der Wissenschaftsfonds.



Der Wissenschaftsfonds.

Deutsche  
Forschungsgemeinschaft



Supported in part by the European Research Council (ERC project FSSEC 101076409) and the Austrian Science Fund (FWF SFB project SPyCoDe 10.55776/F85 and FWF project NeRAM 10.55776/I6054). Additional funding was provided by a generous gift from Intel. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding parties.

# | Cohere+Reload

## Re-enabling High-Resolution Cache Attacks on AMD SEV-SNP

Lukas Giner (@redrabbbyte), Sudheendra Raghav Neela, and Daniel Gruss

DIMVA 2025