Confidentiality, Integrity and Authentication across the Memory Hierarchy

KARIM AIT LAHSSAINE
UNIV. GRENOBLE ALPES
CEA, LETI
F-38000 GRENOBLE, FRANCE
KARIM.AITLAHSSAINE@CEA.FR

OLIVIER SAVRY
UNIV. GRENOBLE ALPES
CEA, LETI
F-38000 GRENOBLE, FRANCE
OLIVIER.SAVRY@CEA.FR

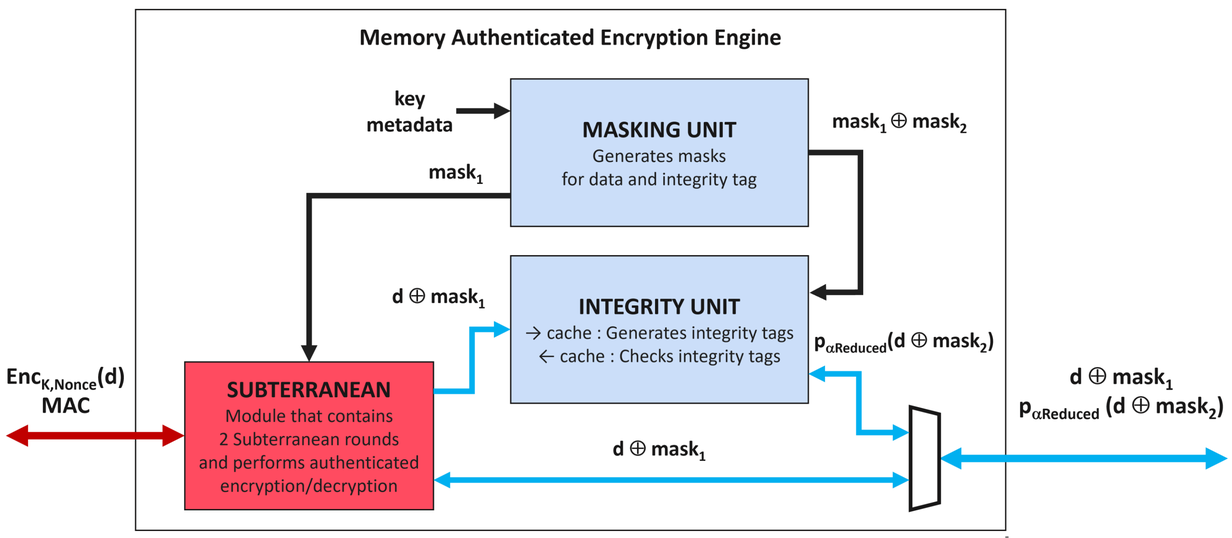
Objectives

Guarantee a chain of trust for data from RAM to CPU registers

Confidentiality : Ensured through encryption in DRAM and masking in caches

Integrity : Guaranteed by associating integrity tags with data and by checking these tags at each level of the hierarchy to detect data corruption

Authentication : Facilitated by authenticated encryption in DRAM and by the presence of integrity tags that are dependent on a unique key

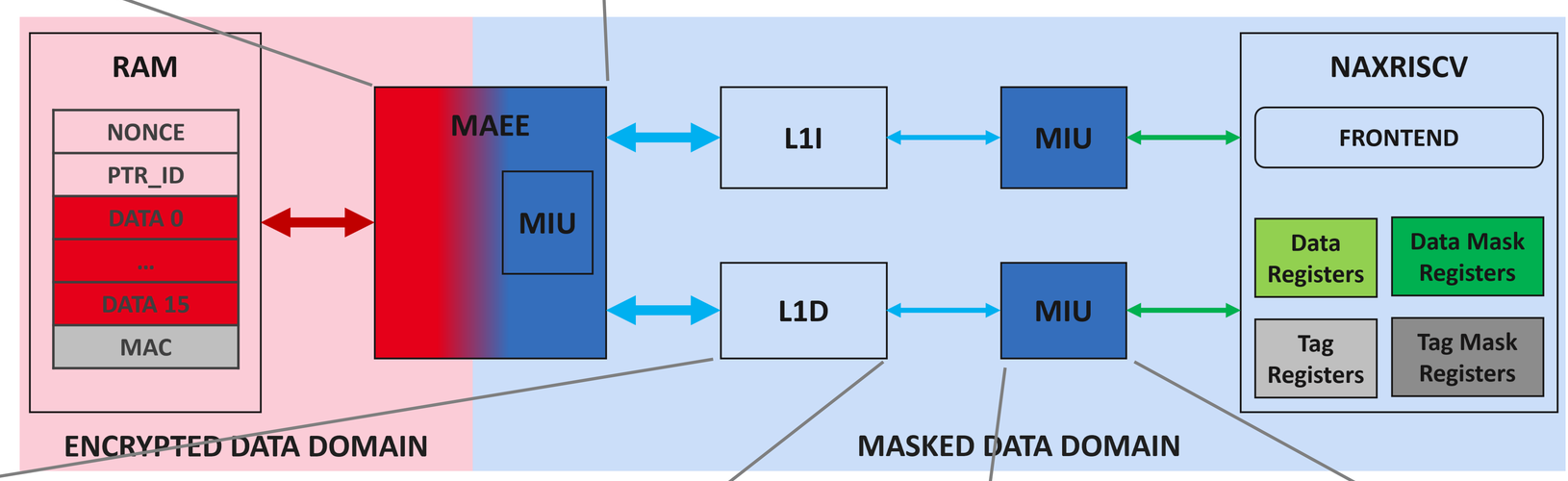


Authenticated Encryption

Read : The cache line coming from the DRAM is decrypted and subsequently masked. For each word, an integrity tag is calculated in parallel and also masked. Finally, at the conclusion of the process, the MAC is checked.

Write : MAEE[1] unmasks and encrypts the cache lines, then associates a MAC (Message Authentication Code) with them. In order to limit the latency overhead, a lightweight authenticated encryption algorithm is employed, namely Subterranean 2.0[2]. The words on the cache line are unmasked and encrypted as they arrive, one by one, in the MAEE.

The transition between encrypted and masked data is made without revealing the data in plaintext, thus avoiding any breach of confidentiality.



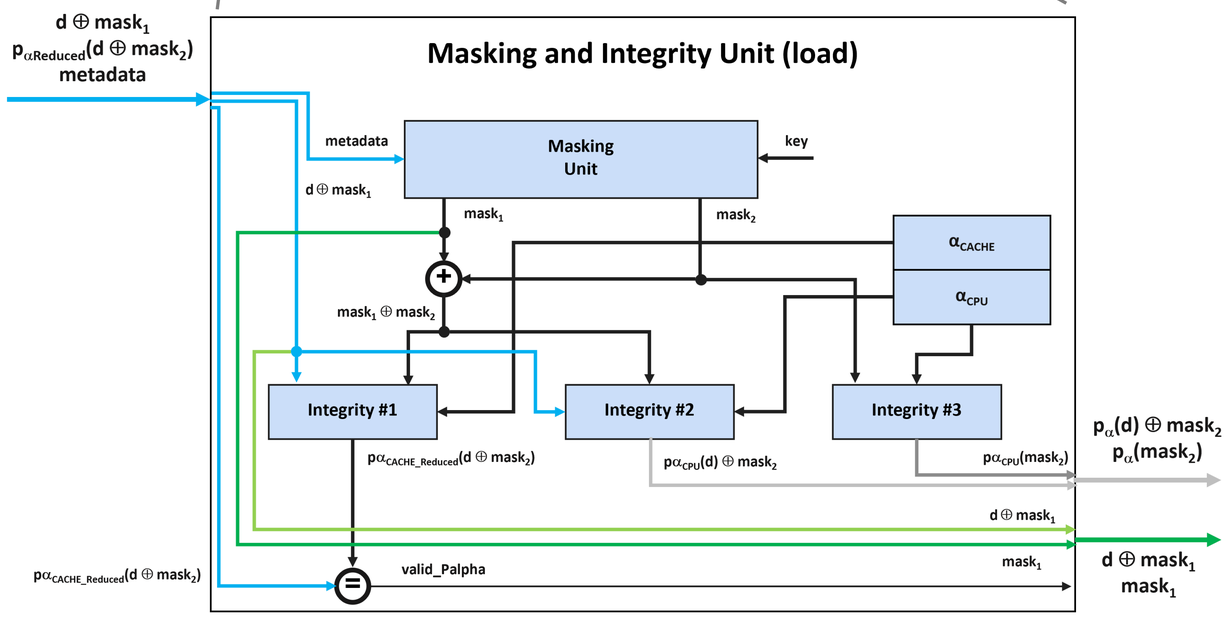
Masked cache line (16 * 64-bit data) with integrity tags and metadata

Cache/CPU Interface

Read : MIU recalculates the mask of the data coming from the cache, and sends the masked data and its mask to their associated CPU registers.
The reduced integrity tag is recalculated and verified with the one from the cache to guarantee the integrity and authenticity of the cached data.

Write : MIU checks the integrity and authenticity of the data to be cached.
At the same time, a new mask is generated and the cached data is masked using transmasking between the new and old masks.

Different α keys (α_{CACHE},α_{CPU}) are used between the CPU and the cache to isolate the two domains and verify integrity and authenticity at the interface.



Modularity

The modularity of the architecture enables users to select the protection of DRAM and/or caches according to their specific use cases, depending on two parameters :

- ***withMIU***
- ***withEncryption***

Results

Synthesised using Yosys for Xilinx associated with NaxRiscv[3] and a L1 cache

	SoC LUTs (overhead)	SoC FFs (overhead)
With MAEE alone	1,4%	0,4 %
With MIU alone	63,5 %	54,1 %
With MAEE + MIU	66,7 %	55 %

References

1 Karim Ait Lahssaine and Olivier Savry. “Memory Authenticated Encryption Engine for a RISC-V processor”. In: RISC-V Summit Europe (June 2023)

2 Joan Daemen et al. “The Subterranean 2.0 Cipher Suite”. In: IACR Transactions on Symmetric Cryptology 2020.S1 (June 2020), pp. 262–294

3 NaxRiscv Project : https://github.com/SpinalHDL/NaxRiscv