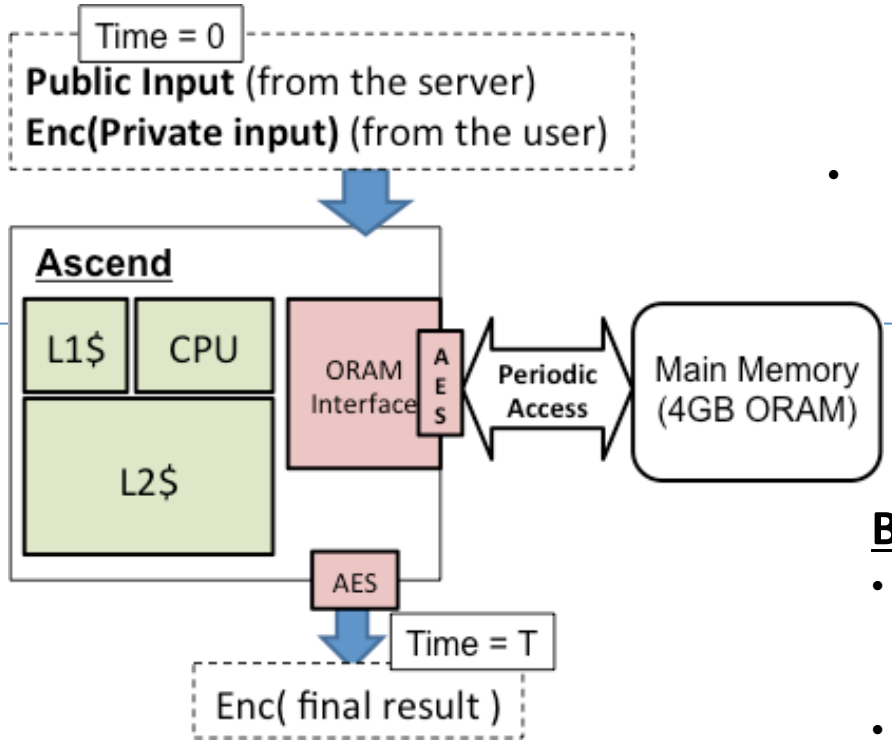
TWC: Small: Ascend: Architecture for Secure Computation on Encrypted Data

Challenge:

- Memory access patterns leak sensitive information from processors.



Solution:

- Use Oblivious Random Access Memory (ORAM)
- New ORAM primitive called Path ORAM that is substantially more efficient than prior ORAMs

CNS 1411208
MIT

Scientific Impact:

- Secure processors that can use untrusted memory without leaking information through access patterns can be built
- Deeper understanding of cryptographic primitives such as ORAM

Broader Impact:

- Secure processors can improve security of computing systems
- PRIMES high school research outreach program