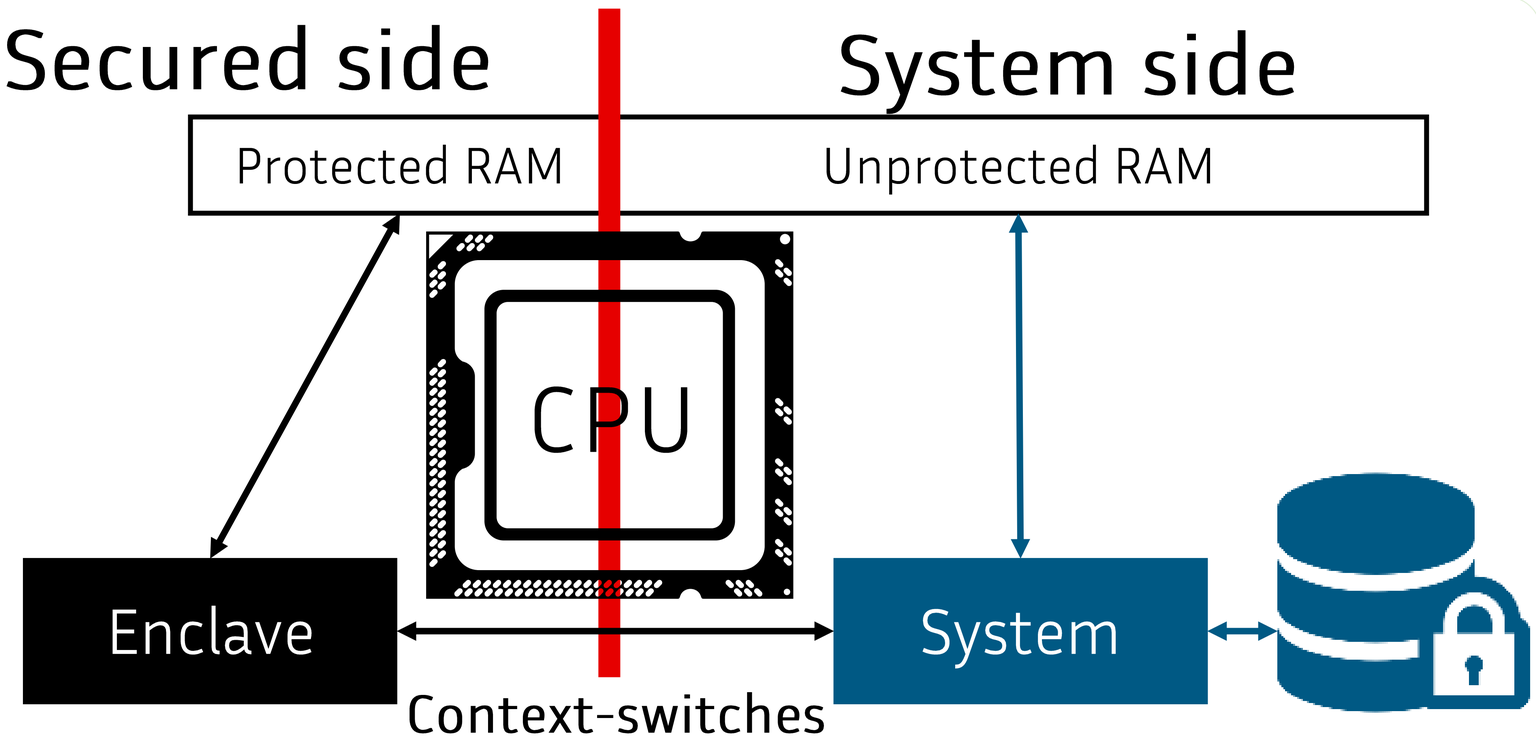
Performance of Large Scale Data-Oriented Operations under the TEE Constraints

Robin Carpentier, Nicolas Anciaux, Iulian Sandu Popa, Guillaume Scerri -- PETRUS Team

Context

- Personal Cloud solutions are flourishing.
- Need to rely on Trusted Execution Environments.
- Intel CPU with Software Guard Extensions (SGX) are already on the market.



Intel SGX security features

- **Isolation** of the enclave program
- **Confidentiality** and **integrity** of the code
- **Attestation** capabilities

→ on all recent Intel CPUs

Constraints implied by SGX

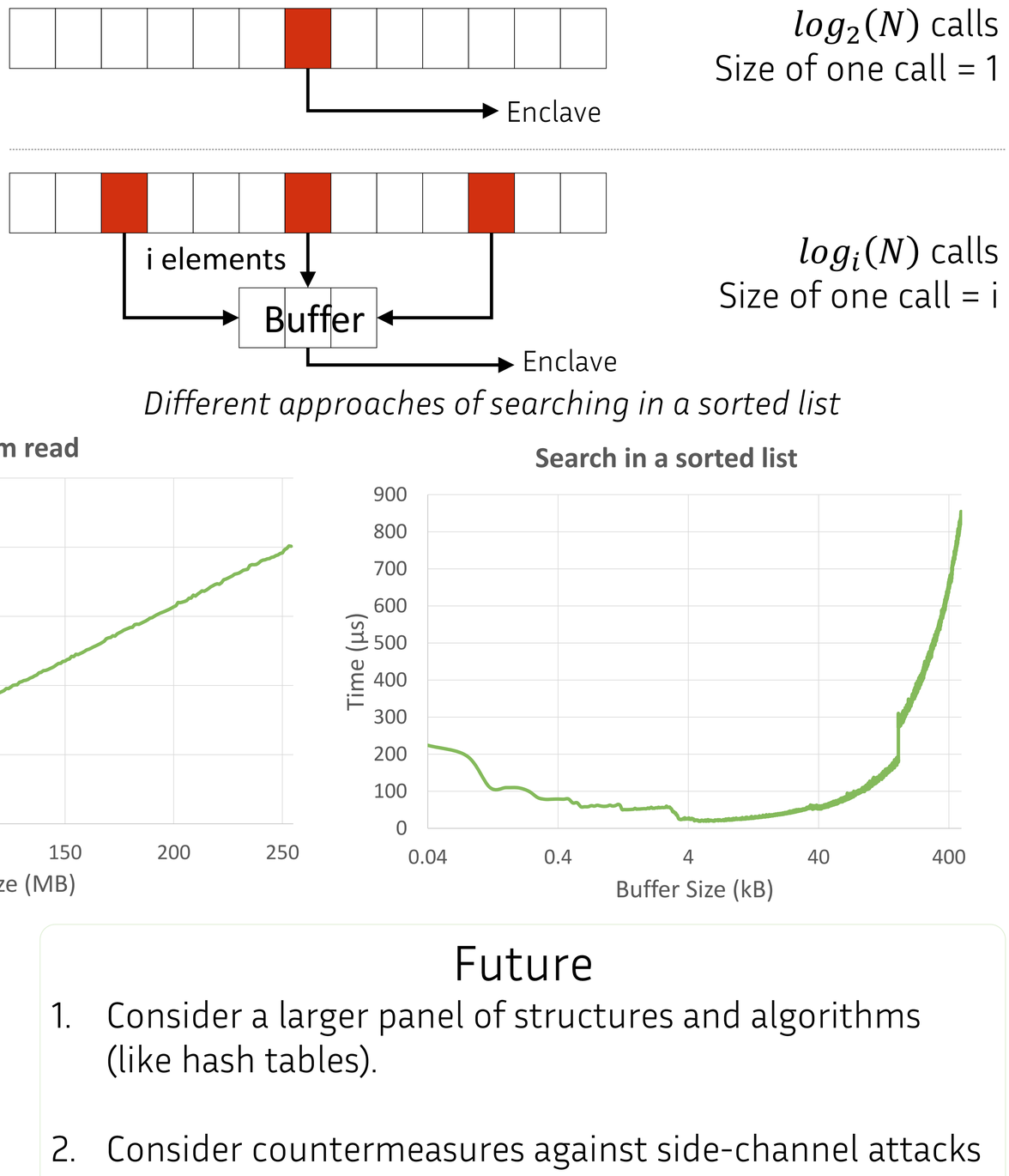
- Enclave memory limit ≈ **90 MB**
- Cost of **context-switching** to enclave mode
- **Cryptographic cost** of accessing data saved outside the enclave
- **Side-channel attacks** are a real threat to SGX security

Goal

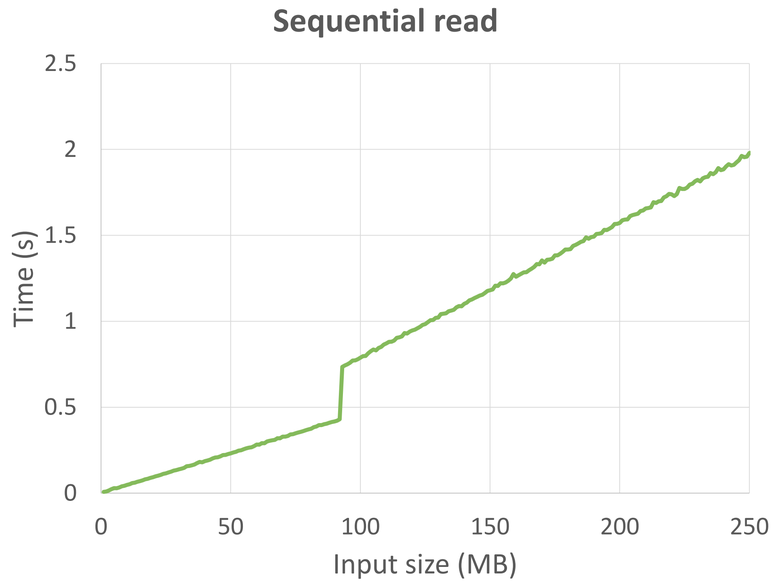
Benefit from Intel SGX security properties while optimizing database structures and algorithms for its specific constraints.

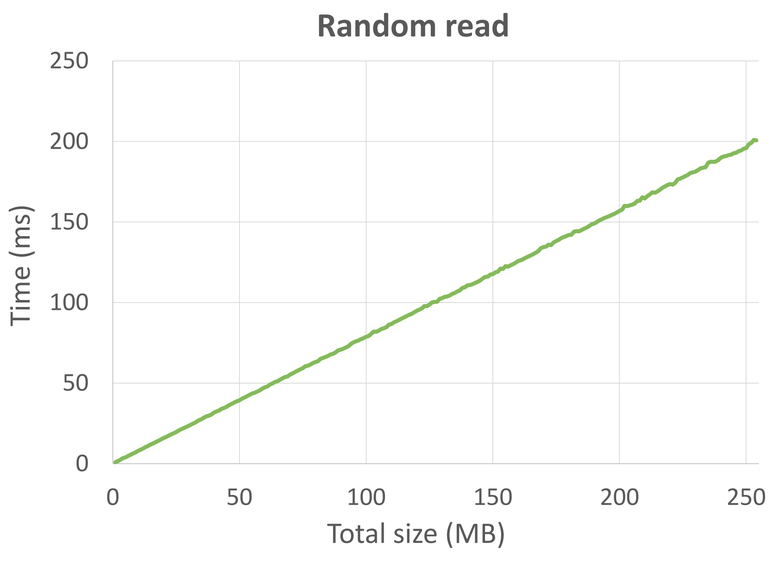
Roadmap

1. Determine the impact of SGX constraints on fundamental database operations.
2. Propose design rules for database structures and algorithms to fully benefit from the **performance** and **security** of Intel SGX computations.



Different approaches of searching in a sorted list





- Sequential reads are impacted by the memory limit.
- Random reads benefit from RAM to RAM linearity.
- Binary search is not the ideal algorithm to perform searches in a sorted list.

Future

1. Consider a larger panel of structures and algorithms (like hash tables).
2. Consider countermeasures against side-channel attacks and their impact on performance.