Migrating SGX Enclaves with Persistent State

- Trusted execution environments, like Intel’s Software Guard Extensions (SGX), can be used to enhance the security critical parts of an application.
- Secrets are bound to physical hosts, which conflicts with cloud virtualization and migration.
- Challenge: Design a secure migration protocol for SGX-enabled virtual machines (VMs).

Migration Library provides migratable versions of sealing and monotonic counter operations. Migration Enclave handles actual migrations and communicates across machines.

### Implementation
- Small trusted computing base of 940 (library) and 217 lines of code (Migration Enclave).
- Migration Enclave resides in non-migratable Management VM.

### Evaluation
- A complete migration from source to target enclave takes ~0.47 seconds.
- Migration duration is independent of number of counters or sealed data size.

---

Average duration of monotonic counter operations
- Migration library
- Baseline

Average duration of initialization and sealing operations
- Migration library
- Baseline