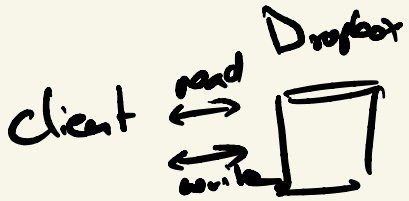
Privacy Enhancing Technologies

ORAM

Florian Tramèr

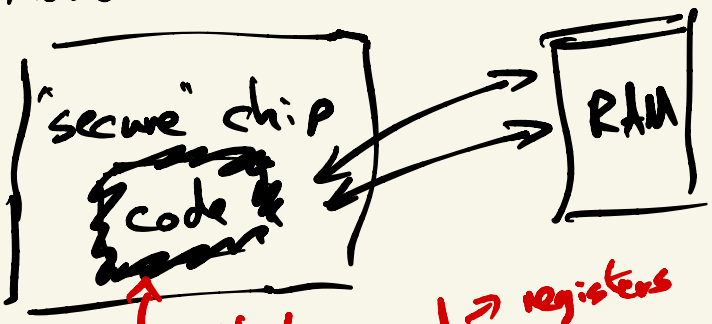
Motivation

1) Private Dropbox



Dropbox learns nothing about file contents and access patterns

2) Hardware enclaves

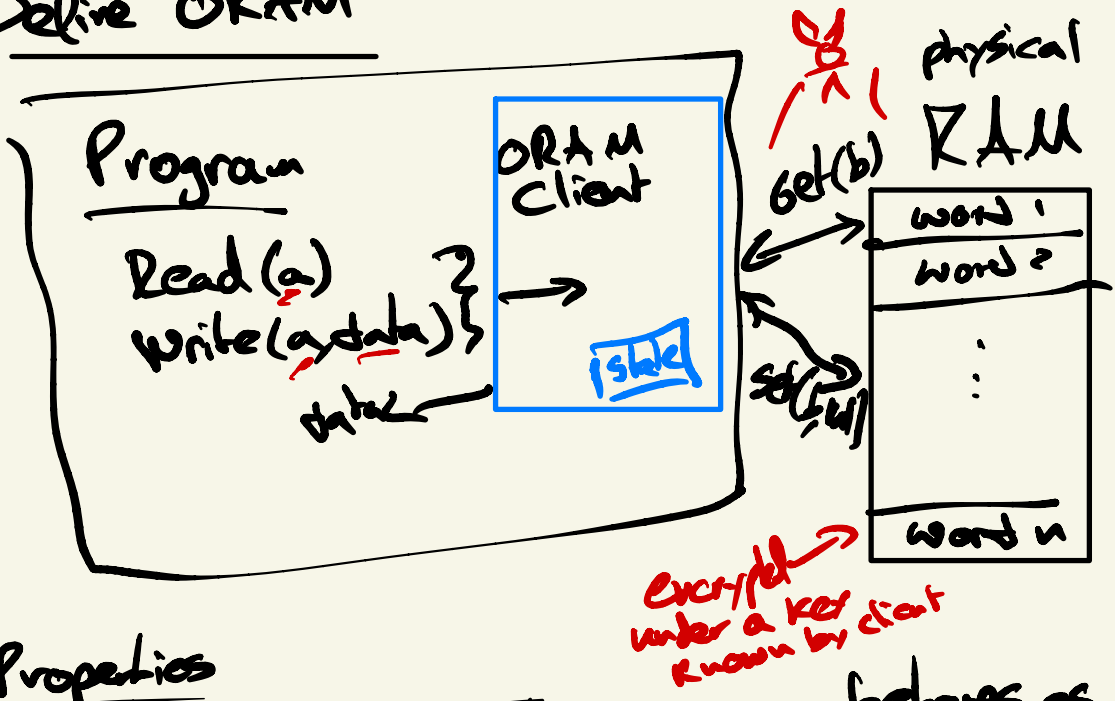


can't be read → registers
or tampered
with by OS (in theory)

```
if (secret) {
    read mem[0x0]
} else {
    read mem[0x1]
}
```

even if mem is encrypted the OS learns the secret by observing memory accesses

Define ORAM



Properties

- Correctness: The program behaves as if it had access to the RAM
- Security: The access patterns to the RAM do not leak anything besides the # of read/write ops

Formally:

- Correctness: For any sequence $O = \{op_1, op_2, \ldots, op_k\}$ of read/writes from the program, the ORAM answers the ops correctly

- Security: Let $O = \{op_1, \ldots, op_k\}$
  $O' = \{op'_1, \ldots, op'_k\}$

$\{Access(op_1), \ldots, Access(op_k)\}$
$\overset{NC}{\approx}$ $\{Access(op'_1), \ldots, Access(op'_k)\}$

Trivial solutions

- Put the RAM in the secret state
  - n words of state
  - O RAM accesses per op.
- Linear scan for each op.
  - $O(1)$ word of storage in state
  - n RAM accesses per op.

Best possible solution (lower bound)

- $\Omega(\log n)$ RAM accesses per op.
  even if state is of size n^ε for any $0 < \varepsilon < 1$

A $\sqrt{n}$ construction

Idea: Suppose the RAM is permuted according to a random permutation Π known to the ORAM client ↪ pseudo random

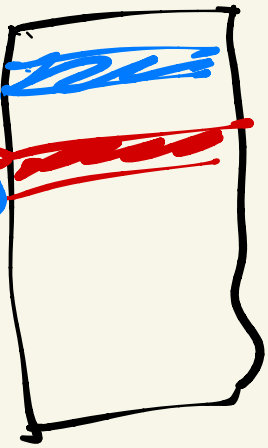
Then, any sequence of $K \leq n$ RAM operations that access distinct locations are indistinguishable

Program
- read(0)
- write(2, val)
- read(7)

ORAM client

id ← Get($\Pi^{-1}(0)$)
Set(id, Enc(val))

id ← Get($\Pi^{-1}(2)$)
Set($\Pi^{-1}(2)$, Enc(val))



View of the RAM:
read+write (of a ciphertext) at K distinct random locations

The strategy

- Encrypt & shuffle the RAM
- Do K operations, for address a
  - if a is in the stash, do a random RAM access (not in the stash)
  - else GET(a) from RAM and store (a, val) in stash
  - if the op is a write, perform it in the stash
- Reshuffle !