09/30/201

Last week review:

C	S

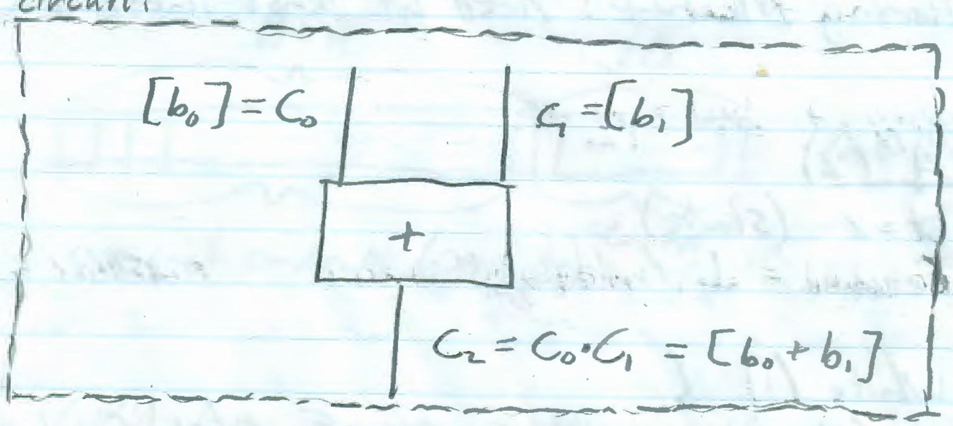
$(pk, sk) \leftarrow Gen(1^n)$

$\xrightarrow{pk}$

$\xrightarrow{Enc_{pk}(x_1), \ldots, Enc_{pk}(x_\ell)}$

$Enc_{pk}(y_1), \ldots, Enc_{pk}(y_\ell)$

circuit:



Fully homomorphic encryption (FHE):

C	S

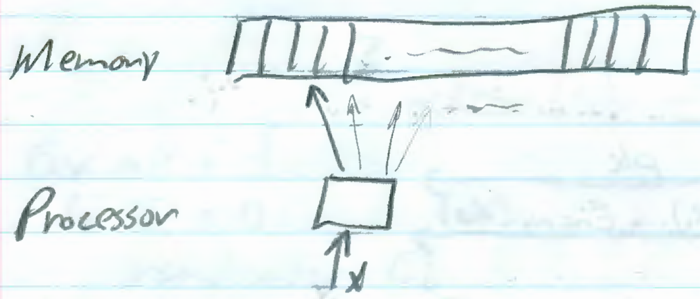
local hom. eval of circuit

$\xleftarrow{Enc_{pk}(out_1), \ldots, Enc_{pk}(out_\ell)}$

+ client can off load computations to server

- hom. enc is <u>expensive</u>

Secure computation in the RAM model:



Turing Machine: need at least linear time for computation

$\underline{A^M(x)}$

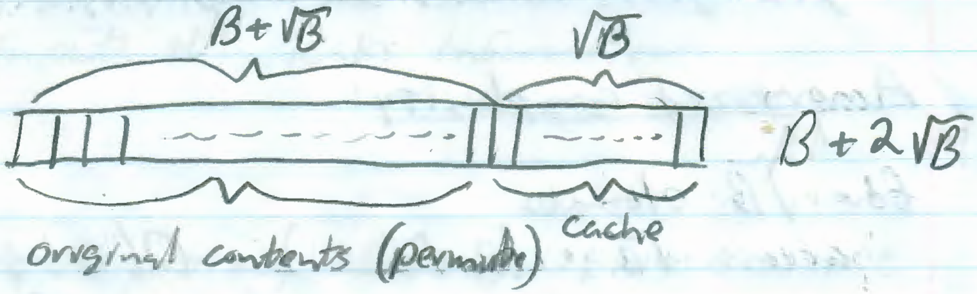
```
st = x   (state)
fetched = ⊥ (nothing)

While (1) {
  (st, addr, val) ← NextInst(st, fetched)

  if st == halt
     output val
  else {
     fetched = M(addr)
                   ? MWC? MVLC?
     if (val != None)
        M(addr)
  }
}
```

Oblivious RAM (ORAM)

Trivial ORAM:
- to read address v, do linear scan over M (and encrypt contents)

Non-trivial ORAM scheme:
- (Goldreich–Ostrovsky '94)

Space:



Initialize:
- Store in CPU key k for pseudorandom permutation over $\{1, \dots, B+\sqrt{B}\}$
- In virtual memory, store $\{(i, M[i])\}_{i=1}^{B}$ in position $F_k(i)$
- In virtual memory, store $(i, null)_{i=B+1}^{B+\sqrt{B}}$

To read address i do:
1) Perform linear scan of cache for element of the form (i, v)
   $\Rightarrow$ If found, set val $= v$
2) If not found, probe position $F_k(i)$ to get value
   If found, probe position $F_k(B + ctr)$, ctr++
3) Linear scan of cache to write the (new) value at $M[i]$

$\sqrt{B}$ times then refresh

Refresh (every $\sqrt{B}$ steps)
- choose fresh key k'
- (obliviously) re-shuffle elements according to k'
- empty cache

$O(B \log B)$ sorting +
$O(n)$ additional operations

- get good amortized complexity

Amortized complexity:

for $\sqrt{B}$ elements:
access $\sqrt{B} \cdot (2\sqrt{B} \pm 1) + O(B \log B)$ memory patterns

$$\frac{O(B \log B)}{\sqrt{B}} = \boxed{O(\sqrt{B} \log B)}$$

cache B^{ε}:

$$\frac{B^{\varepsilon} \cdot O(B^{\varepsilon}) + O(B \log B)}{B^{\varepsilon}} = \boxed{O(B^{1-\varepsilon})}$$