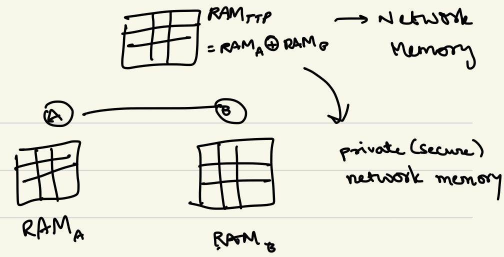


Review:

- Oblivious Transfer (OT) using PKC
- From OT to ANY two-party fn. (private evaluation)

OT:

A ——— B

i $\quad$ $A[\quad]$

$\leftarrow A[i]$ $\quad$ no knowledge of i

Not $A[j]$s, $j \neq i$

$f(x, y) = r_A + r_B$

r_A A ——— B r_B

x $\quad$ y

x, y are (locally) private

$r_A \xleftarrow{R} \{0,1\}^n$

$[\ \ldots\ ]$ all possible r_B

for $i \in [0, 2^n - 1]$
$f(x, i) - r_A$

Using y, B chooses r_B

Exponential length array, not practical.

What if length is long?

$f(x,y) = r_A + r_B$

A ——— B

x $\quad$ y

Generalization:

In GF2, Ex:

$RAM_A = r_1\ r_2$ $\quad$ $RAM_B = x \oplus r_1, y \oplus r_2,$

$RAM_{TTP} = x\ y$

Reduced ISA secure computation:

- Only XOR & AND operations supported

Let $z = x \oplus y$ which we want in RAM_{TTP}

$z = a \oplus b = x \oplus y$

$= r_1 \oplus (x \oplus r_1) \oplus r_2 \oplus (y \oplus r_2)$

In RAM_A: $\boxed{r_1 \mid r_2}$ $\boxed{a}$ $\quad$ $a = r_1 \oplus r_2$

RAM_B: $\boxed{x \oplus r_1 \mid y \oplus r_2}$ $\boxed{b}$ $\quad$ $b = (x \oplus r_1) \oplus (y \oplus r_2)$

In RAM_{TTP}: $a \oplus b = r_1 \oplus r_2 \oplus x \oplus r_1 \oplus y \oplus r_2$
$= x \oplus y = z$

XOR with AND is universal

$$z = a \oplus b = x \wedge y$$
$$= (r_1 \oplus (x \oplus r_1)) \wedge (r_2 \oplus (y \oplus r_2))$$
$$= (r_1 \wedge r_2) \oplus ((x \oplus r_1) \wedge (y \oplus r_2))$$
$$\oplus\ r_1 \wedge (y \oplus r_2) \oplus (x \oplus r_1) \wedge r_2$$

Secure AND:

$$a \oplus b = x \wedge y = [r_1 \oplus (x \oplus r_1)] \wedge [r_2 \oplus (y \oplus r_2)]$$
$$b = a \oplus [r_1 \oplus 1] \wedge [r_2 \oplus 1]$$

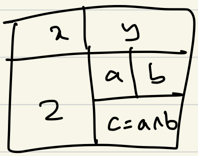
① A chooses $a \leftarrow_R \{0,1\}$

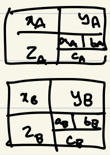
② A creates array $A[0,1,2,3]$ as

 00 01 10 11

$a \oplus (r_1 \wedge r_2)$, $a \oplus (r_1 \wedge \bar{r}_2)$, $a \oplus (\bar{r}_1 \wedge r_2)$, $a \oplus (\bar{r}_1 \wedge \bar{r}_2)$

③ B obliviously transfers the value $A[2(x \oplus r_1) + y \oplus r_2] = b$





$z = x \wedge y$, Publish $x \oplus a$ & $y \oplus b$

$$x \wedge y = (x \oplus a) \wedge (y \oplus b) \oplus (x \oplus a) \wedge b \oplus (y \oplus b) \wedge a \oplus a \wedge b$$

$$z_A \leftarrow (x \oplus a) \wedge (y \oplus b) \oplus (x \oplus a) \wedge b_A \oplus (y \oplus b) \wedge a_A \oplus c_A$$

$$z_B \leftarrow (x \oplus a) \wedge b_B \oplus (y \oplus b) \wedge a_B \oplus c_B$$

$$z = z_A \oplus z_B$$

Summary:

Goal: Build a secure (virtual) server on top of 2 real (insecure) servers

Procedure: XOR = local XORs

AND: OT (1 out of 4)

Secure Memory = $Mem_A \oplus Mem_B$

No perfect soln. exists for secure AND if $n \le 2t$ (n: no. of servers, t: no. of adversary servers) ⇒ semi honest (passive) adversary

∃ perfect solutions in active adv. model if $n > 3t$

- Perfect ($n > 3t$)
- Computational (PKI) — ZKP
- Unconditional
- Computational (without PKI)

Blockchains (computational, open system)

Other impossibilities (quantum, noisy channel, space constraints...)