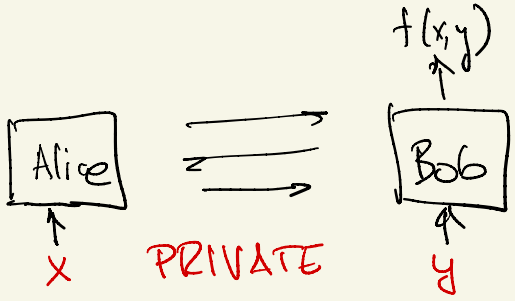
SECURE 2-PARTY COMPUTATION



Alice GAINS NO INFO ABOUT y

Bob GAINS NO INFO ABOUT x BEYOND $f(x,y)$.

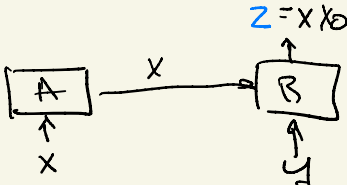
YAO'S MILLIONAIRE PROBLEM

$$f(x,y) = \begin{cases} 1 & \text{IF } x \geq y \\ 0 & \text{IF NOT} \end{cases} \qquad f(\text{lm}, \text{lb}) = 0$$

FUNCTIONALITY PROTOCOL IN WHICH GIVEN INPUTS x FOR Alice AND y FOR Bob, Bob'S OUTPUT EQUALS $f(x,y)$.

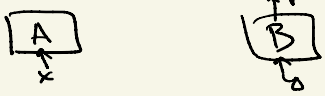
SECURITY. (s,ε) - SIMULATABILITY: AGAINST HONEST-BUT-CURIOUS PARTIES. $\exists$ SIMULATORS S_A, S_B S.T. $\forall x,y$, $S_A(x)$ IND. FROM A'S VIEW AND $S_B(x, f(x,y))$ IND. FROM Bob'S VIEW.

Ex. $f(x,y) = x \text{ XOR } y$.



$\text{Sim}_B(y,z) = y \text{ XOR } z$

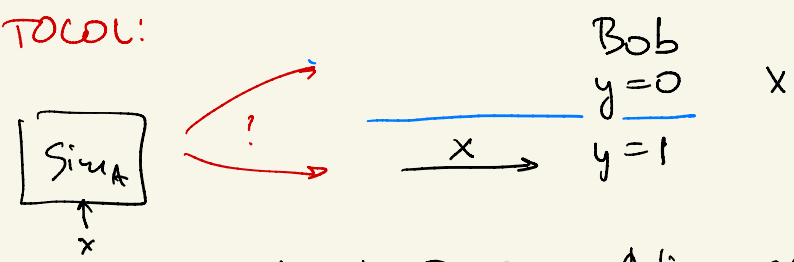
$f(x,y) = y$



NO INTERACTION

$f(x,y) = x$ AND $y = \begin{cases} x & \text{WHEN } y=1 \\ 0 & \text{WHEN } y=0 \end{cases}$

PROTOCOL:



BOB CAN SIMULATE, BUT Alice CAN'T.

IDEA. Alice $\xrightarrow{Enc(Pk,x)}$ Bob $\begin{cases} y=0: \text{DOESN'T KNOW Sk} \\ y=1: \text{KNOWS Sk} \end{cases}$

Bob $\begin{cases} y=1: \text{SAMPLES } (Sk, Pk) \text{ FOR El Gamal ENC.} \\ y=0: \text{SAMPLE } Pk \text{ WITHOUT KNOWING Sk} \end{cases}$

$Pk = g^{Sk}$ (PICK RANDOM Q.R.)

Pk → Alice

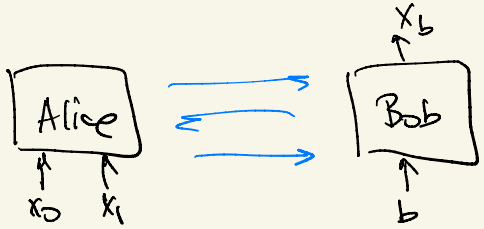
$C = Enc(x, Pk)$ ←

Bob: IF $y=1$ OUTPUT $Dec(C)$.
IF $y=0$ OUTPUT 0.

$Sim_B(y, \underbrace{f(x,y)}_{2})$ $\begin{cases} y=0 \\ y=1 \end{cases}$ $(Pk, Enc(x, Pk))$

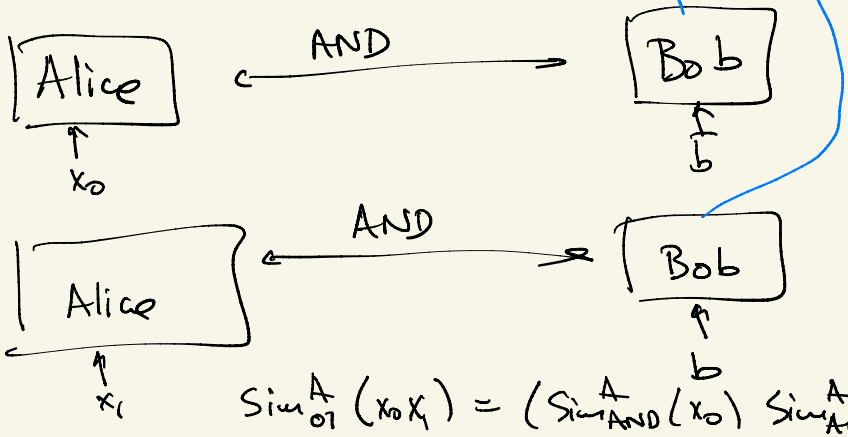
USE Sim FOR El Gamal
CHOOSE RANDOM Pk
OUTPUT $(Pk, Enc(g, Pk))$.

OBLIVIOUS TRANSFER



$$OT(x_0 x_1, b) = (x_0 \text{ AND } \bar{b}) \text{ OR } (x_1 \text{ AND } b)$$

OT PROTOCOL

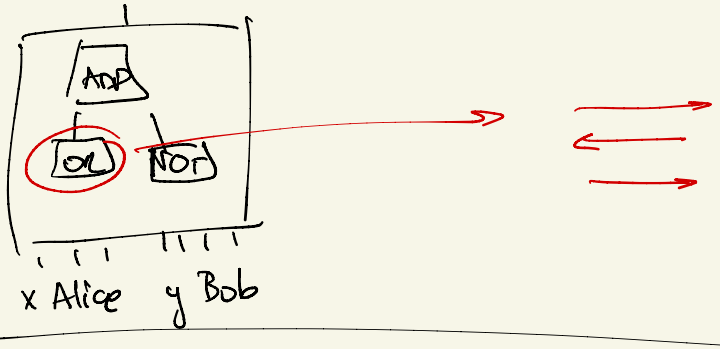


$$Sim^A_{OT}(x_0 x_1) = (Sim^A_{AND}(x_0)\ Sim^A_{AND}(x_1)$$

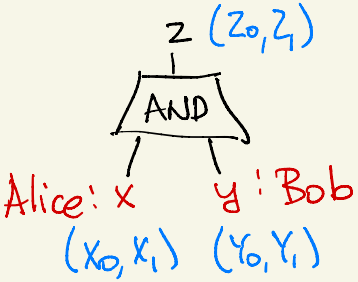
SECURITY

$$Sim^B_{OT}(b, x_b) = \begin{cases} (Sim^B_{AND}(1, x_b), Sim^B_{AND}(0,0)) & \text{IF } b=0 \\ (Sim^B_{AND}(0,0), Sim^B_{AND}(1, x_b)) & \text{IF } b=1 \end{cases}$$

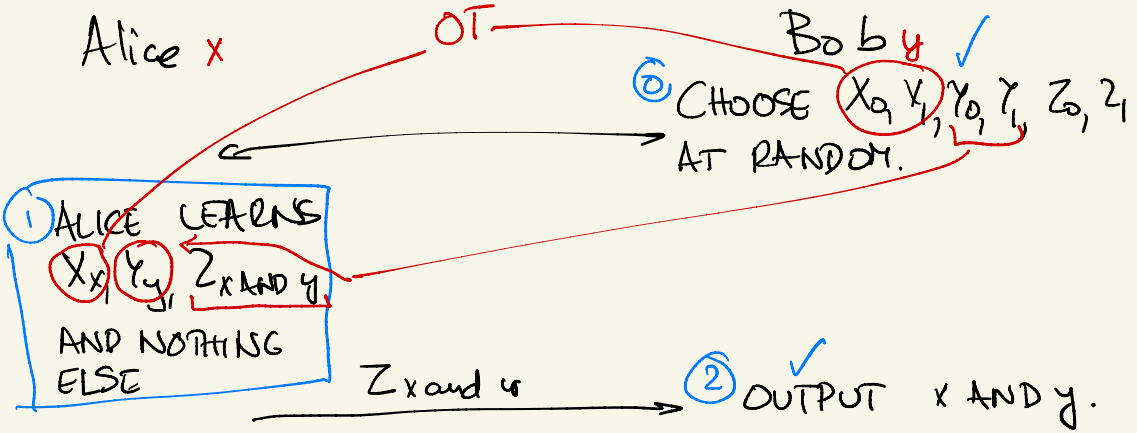
GENERAL f IS SOME CIRCUIT

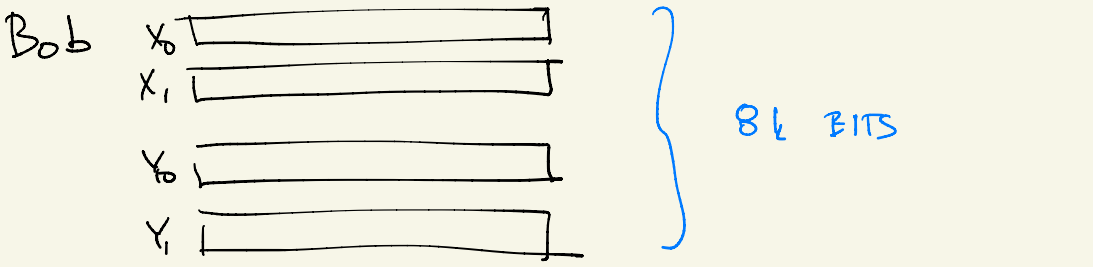


A DIFFERENT PROTOCOL FOR AND



GOAL: Alice TO COMPUTE $z_{x \text{ AND } y}$ WITHOUT LEARNING ANYTHING EXCEPT x_x, y_y (AND $z_{x,y}$)





$Z_0, Z_1 \in \{0,1\}^\ell$ ℓ BITS

IDEA ENCRYPT

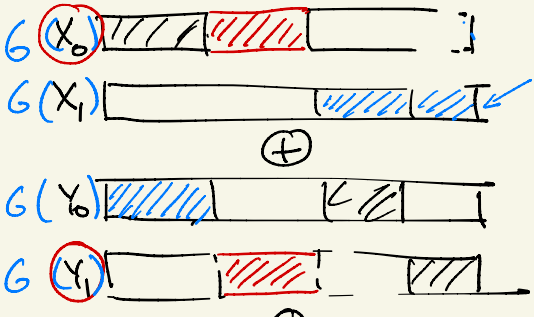
- Z_0 UNDER KEY X_0 Y_0
- Z_0 " X_0 Y_1
- Z_0 " X_1 Y_0
- Z_1 " X_1 Y_1

RANDOMLY PERMUTED

- Alice CAN ONLY DECRYPT Z_x AND y

  EG. $x=0, y=1$

- Alice SHOULD NOT KNOW WHAT SHE DECRYPTED.



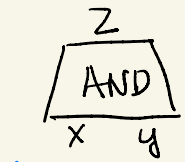
USE OTP TO ENCRYPT $0^k Z_{\ell \text{ AND } b}$

$8k$ BITS

EG. $x=0$, $y=1$

CAN SIMULATE (IF IN RANDOM ORDER) FROM $X_x, Y_y, Z_{x \text{ AND } y}$

$\therefore$ (1 OF 4 SUCCEEDS) $= 1 - 3 \cdot 2^{-k}$



(Z_0, Z_1) k BITS LONG

(X_0, X_1) (Y_0, Y_1) $8k$ BITS LONG

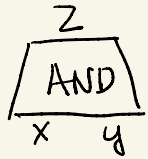
IF WE TRY TO COMPOSE GARBLED DATA WILL GROW EXPONENTIALLY

GARBLED AND TRANSFER

$X_0, X_1, Y_0, Y_1 \in \{0,1\}^k$

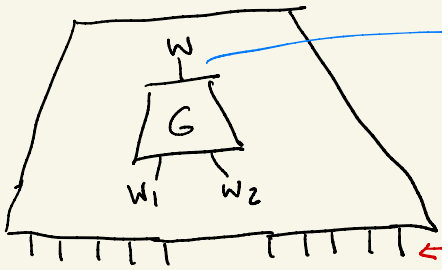
USE $G(X_0), G(X_1) | G(Y_0), G(Y_1)$, FOR PRG $G: \{0,1\}^k \to \{0,1\}^{8k}$

(Z_0, Z_1) k BITS LONG



(X_0, X_1) (Y_0, Y_1) k BITS LONG

GARBLED CIRCUIT PROTOCOL



W_0^w, W_1^w FOR EACH WIRE

INPUT WIRES

Alice Bob

0. Bob SAMPLES W_0^w, W_1^w FOR EACH WIRE w.
1. Bob's INPUT WIRES: SEND $W^b_{val(b)}$ TO Alice.
   Alice's INPUT WIRES: RUN OT WITH Alice CHOOSING $W^a_{val(a)}$ FROM (W_0^a, W_1^a).
2. RUN GARBLED GATE PROTOCOL IN ORDER OF GATES SO Alice LEARNS $W^w_{val(w)}$ IN SEQUENCE.
3. Alice SENDS OUTPUT $Z = W^{out}_{val(out)}$ TO Bob. Bob OUTPUTS $z \in \{0,1\}$ S.T. $Z = W^{out}_z$.

FUNCTIONALITY: UNLESS ANY GARBLED GATE PROTOCOL FAILS, z MUST EQUAL $f(x,y)$. SO IT WORKS WITH PROB. $1 - O(\text{size}(C) \cdot 2^{-k})$.

SECURITY: Alice's VIEW = RANDOM VALUES $W^w_{val(w)}$ + VIEWS IN OT/GARBLED GATE PROTOCOLS. CAN COMPOSE SIMULATORS FOR THEM.

Bob's OT/GARBLED GATE PROTOCOL VIEWS CAN BE SIMULATED FROM HIS RANDOMNESS W^w_0, W^w_1. Alice's LAST MESSAGE $W^{out}_{val(out)}$ CAN BE SIMULATED AS W^{out}_z.

Bob CAN EXECUTE GARBLED GATE PROTOCOLS IN PARALLEL → 3 MESSAGE PROTOCOL

INDEPENDENT OF size(C)!

NEXT 2 LECTURES: MALICIOUS Alice/Bob THAT MAY DEVIATE FROM PROTOCOL INSTRUCTIONS.

STRATEGY: COMMIT TO FOLLOW INSTRUCTIONS AND PROVE THAT YOU DID

WITHOUT REVEALING YOUR INPUTS! ZERO-KNOWLEDGE

SECURITY ASSUMES Alice & Bob FOLLOW INSTRUCTIONS.

ENSURE SECURITY AGAINST ADVERSARIES THAT MIGHT DEVIATE FROM INSTRUCTIONS.

STRATEGY COMPILE PROTOCOL SECURE AGAINST HONEST-BUT-CURIOUS TO SECURITY AGAINST MALICIOUS.

ZERO-KNOWLEDGE PROOFS