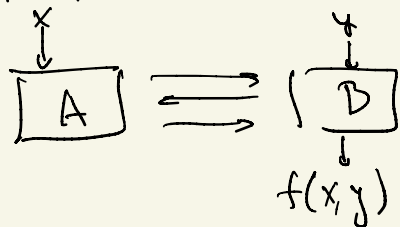


SECURE TWO-PARTY COMPUTATION

HONEST-BUT-CURIOUS



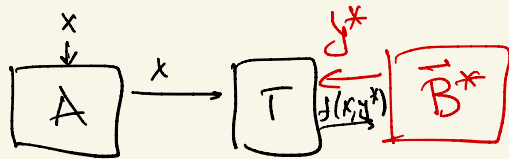
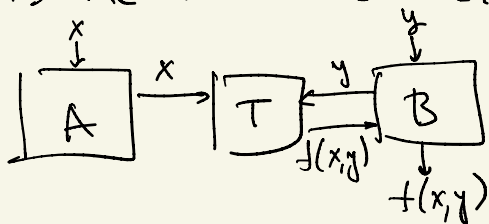
$f = \text{AND}$
 $y^* = 1 \rightarrow B^* \text{ FINDS } x$

MALICIOUS

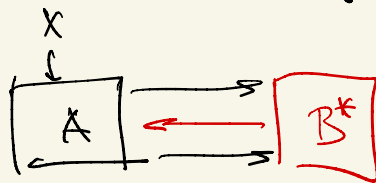
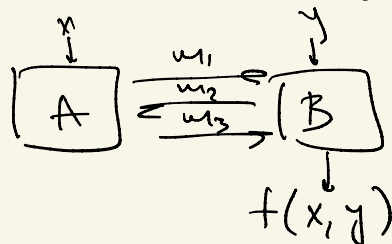
CAN CHANGE THEIR
INPUT TO y^*

$f(x, y) = 1(x > y)$
 $y^* = 1000 \text{ BILLION}$

IDEAL FUNCTIONALITY



REAL PROTOCOL



A 2PARTY PROTOCOL IS SECURE FOR Alice
 IF FOR EVERY B^* THERE EXISTS A $\tilde{B}^*$ (OF
 SIZE $\geq$ oh LARGER) S.T. B^* VIEW WHEN INTERACTING
 WITH A CAN BE SIMULATED FROM $\tilde{B}^*$ VIEW
 WHEN INTERACTING WITH T .

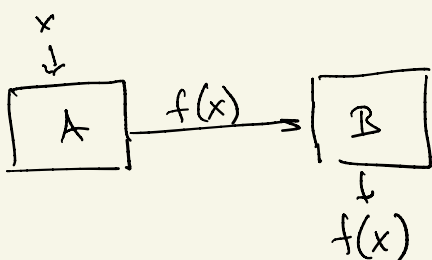
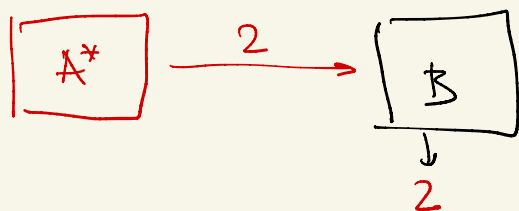


IMAGE TRANSMISSION

TRIVIAALLY SECURE
IN HONEST BUT
CURIOUS MODEL



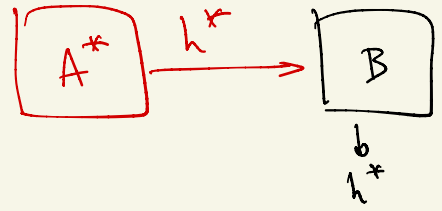
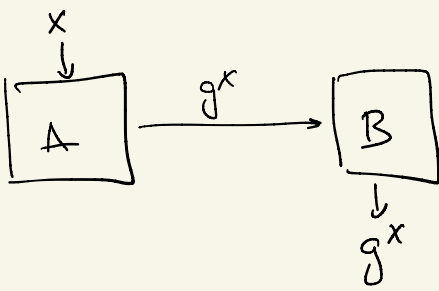
EG. $f: \{0,1\} \rightarrow \{0,1,2\}$
 $f(x) = x$

Bob CAN NEVER OUTPUT
2 IN IDEAL FUNCTIONALITY

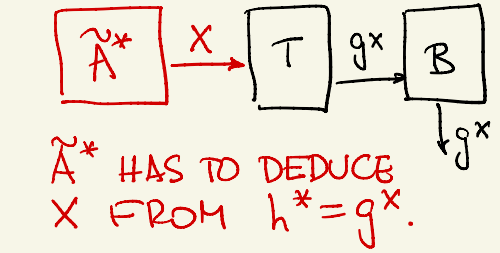
SECURE FOR BOB IF $\forall A^* \exists \tilde{A}^*$ OF SIZE $\leq o_h$
LARGER S.T. JOINT DV (A^* 'S VIEW, B'S OUTPUT)
INDISTINGUISHABLE FROM ($\tilde{A}^*$ 'S VIEW, B'S OUTPUT)
IN IDEAL FUNCTIONALITY

IN IMAGE TRANSMISSION EXAMPLE Bob's OUTPUT
CAN NEVER EQUAL 2 IN IDEAL FUNCTIONALITY SO
TRIVIAL PROTOCOL IS INSECURE.

ZERO-KNOWLEDGE ALLOWS Alice TO PROVE
" $\exists x$ S.T. $f(x) = 2$ ". HELPFUL BUT NOT ENOUGH.



Alice PROVES SHE KNOWS
 x TO Bob. THEN $\tilde{A}^*$
 CAN EXTRACT x FROM A^* .



PROOFS OF KNOWLEDGE

SCHNORR : $SK = x$ $\xrightarrow{\text{I KNOW } x}$ $PK = g^x$ [Alice] [Bob]

PROOF RELATION $R:(x, \pi)$ (EG. (g^x, x))

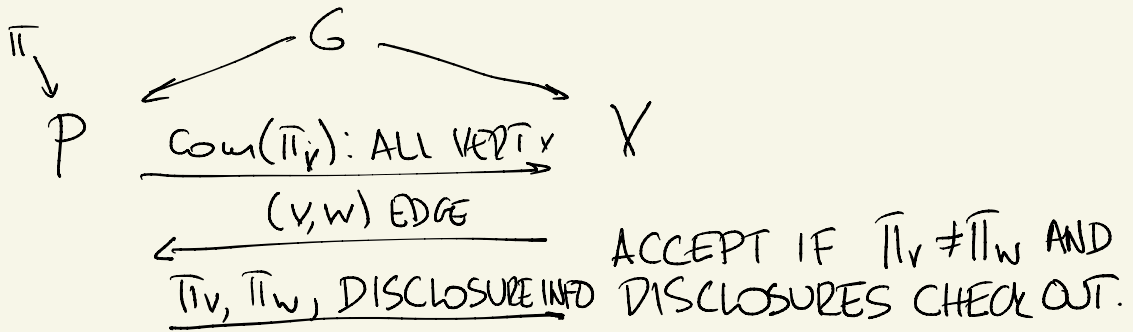
A PROTOCOL IS A PoK FOR R IF $\forall P^*$
 $\exists K$ KNOWLEDGE EXTRACTOR OF SIZE $\leq o(n)$
 LARGER S.T. IF P^* PASSES VERIFICATION ON x
 WITH SUFFICIENTLY LARGE PROBABILITY THEN
 K OUTPUTS π WITH PROBABILITY $\geq 1/2$.

ZKPOK FOR UNIVERSAL PROOF RELATIONS

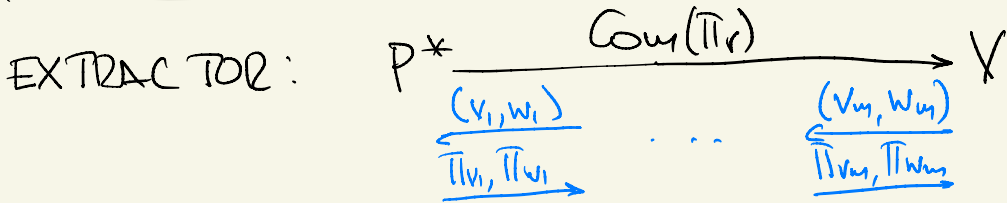
$$R = \{(G, \pi) : \pi \text{ IS A 3-COLORING OF } G\}$$

LAST LECTURE: ZK PROOF OF FACT

GMW PROTOCOL



GMW IS A ZK PROOF OF KNOWLEDGE.

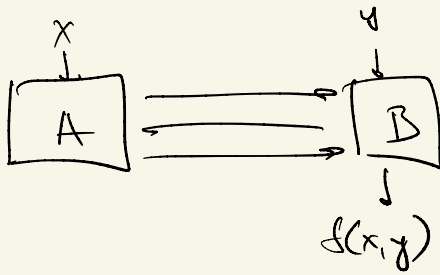


P^* PASSES W/P $1 - \frac{1}{2^m} \rightarrow$ W/P $\frac{1}{2}$

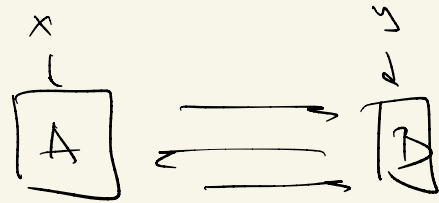
ALL π_v CONSISTENT ($\pi_{v_i} = \pi_{v_j}$ WHEN $v_i = v_j$)

AND $\pi_{v_i} \neq \pi_{w_i} \rightarrow \pi$ IS A 3COL OF G

GMW COMPILER

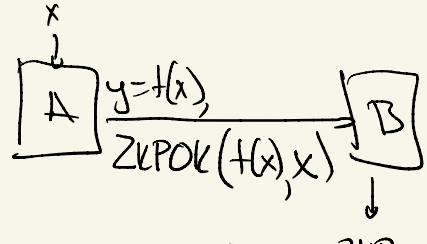
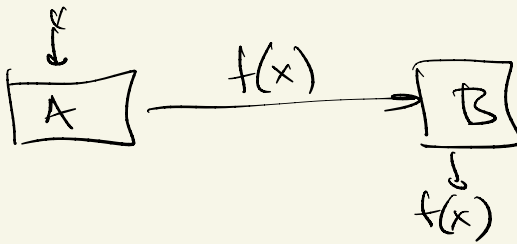


SECURE AGAINST
HONEST BUT CURIOUS

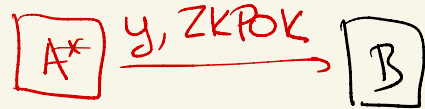
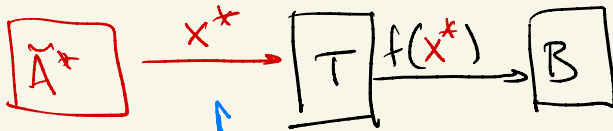


SECURE AGAINST
MALICIOUS

IMAGE TRANSMISSION

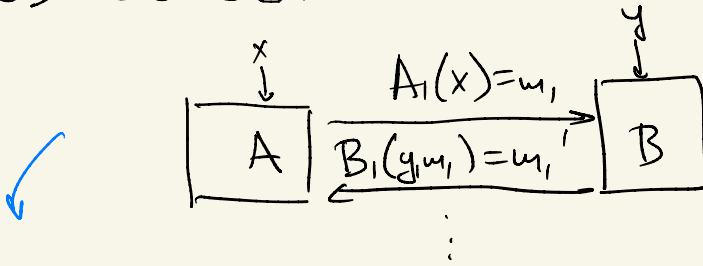


VERIFIES ZKPOK
OUTPUTS $f(x)$
IF IT ACCEPTS

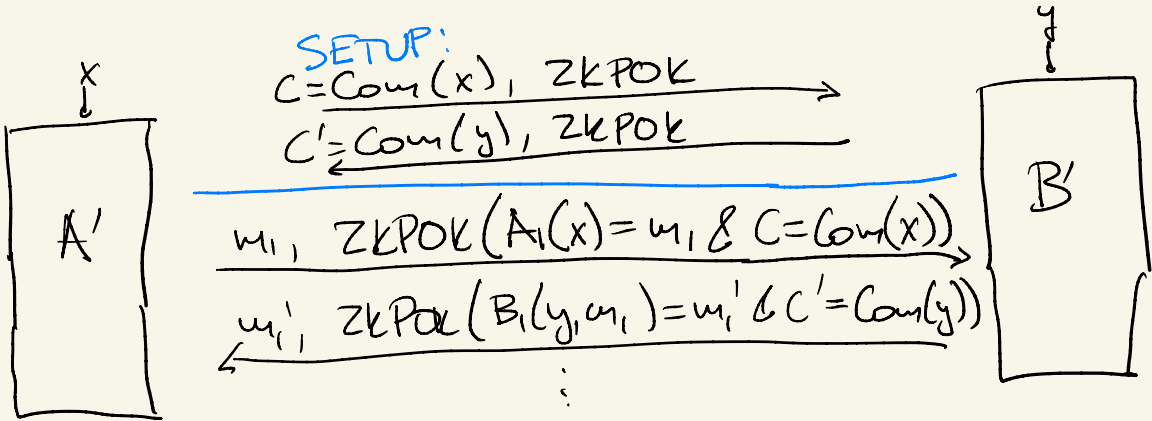


$Ext(ZKPOK) = x^*$
S.T. $f(x^*) = y$

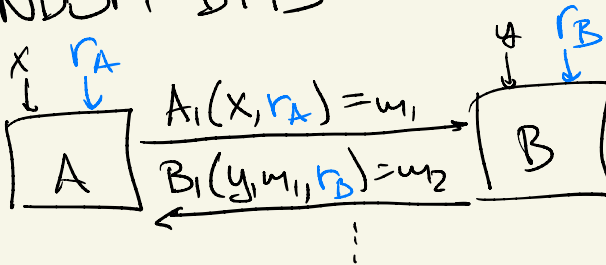
ALMOST GENERAL CASE



GMW COMPILER

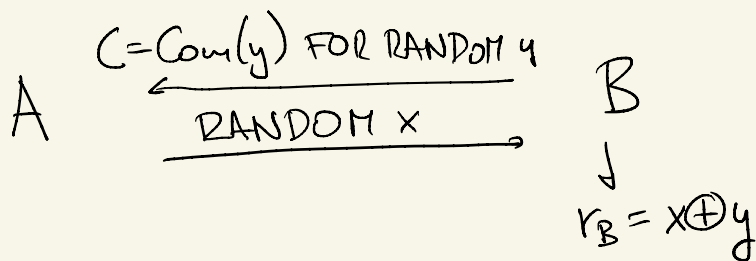


IN FULL GENERALITY A AND B USE RANDOM BITS



NEED TO IMPLEMENT IDEAL RANDOM COIN TOSS

COIN TOSSING PROTOCOL



SECURITY FOR Alice : x RANDOM $\rightarrow r_B$ RANDOM

SECURITY FOR Bob : $(A^*'s \text{ VIEW}, r_B)$

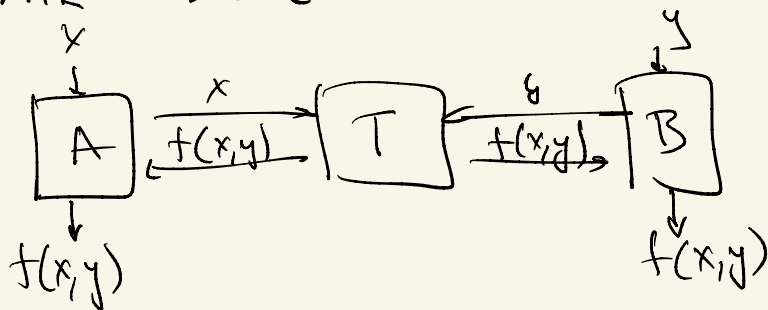
$$= (\text{Com}(y), x^*(\text{Com}(y)) \oplus y)$$

C.I. FROM $(\text{Sim}, \underbrace{x^*(\text{Sim})}_{\text{IDEAL FUNC. INPUT}} \oplus y)$

AUGMENT PROTOCOL WITH RANDOMNESS GENERATION PHASE AND INCLUDE ZKPOK FOR "C IS A COMMITMENT OF y S.T. $r_B = x \oplus y$ ".

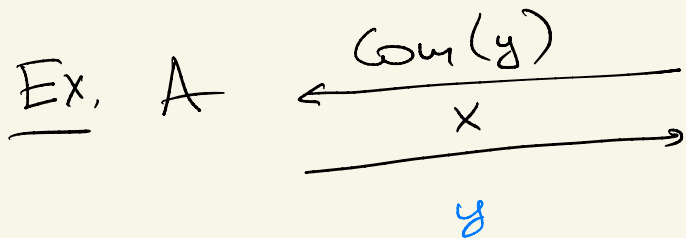
FAIRNESS: WHAT IF BOTH Alice & Bob
NEED TO COMPUTE $f(x,y)$?

FAIR IDEAL FUNCTIONALITY



WHEN $f(x,y) = x \oplus y$ AND x, y RANDOM
THIS IS A COIN TOSS: Alice & Bob
OUTPUT SAME RANDOM BIT.

Thm. (Cleve) FAIR COIN TOSS IS IMPOSSIBLE.
IN ANY k -ROUND PROTOCOL COIN MUST
HAVE BIAS $\geq 1/(8k+1)$.



IF Bob ABORTED $\leftarrow$
WHAT SHOULD
OUTPUT r_A BE?

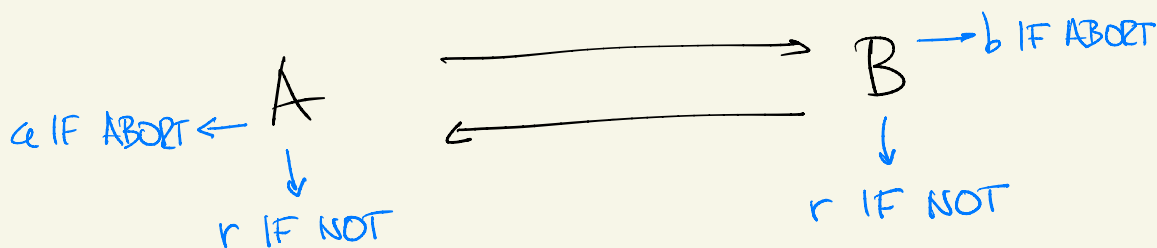
B^*

IF $r_B = x \oplus y = 0$
OUTPUT 0 & SEND y
ELSE ABORT
(SEND GARBAGE)

OPTION 1. IF BOB ABORTS, Alice SAMPLES OUTPUT r_A ON HER OWN.

$$\begin{aligned}
 r_A &= (r_A | \text{NOT ABORT}) P(\text{NOT ABORT}) + (r_A | \text{ABORT}) P(\text{ABORT}) \\
 &= 0 \cdot \frac{1}{2} + \text{RANDOM} \cdot \frac{1}{2} \\
 &= \begin{cases} 0 & \text{w/p } 3/4 \\ 1 & \text{w/p } 1/4. \end{cases}
 \end{aligned}$$

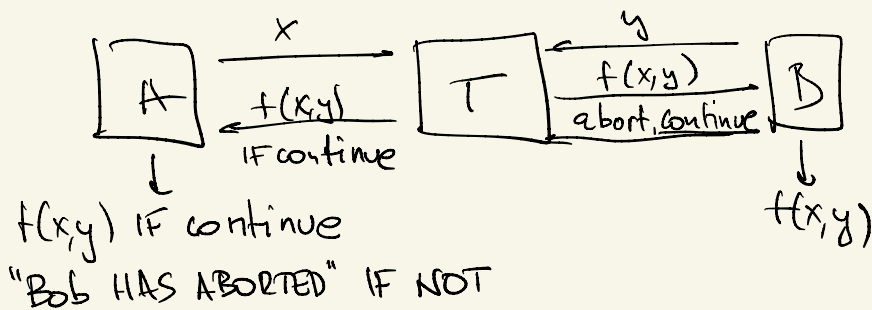
INTUITION FOR CLEVE'S THEOREM



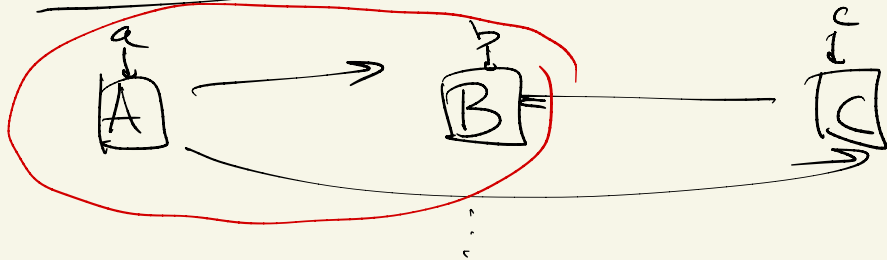
OPTION 1. a UNCORRELATED WITH $r \rightarrow$
Bob CAN BIAS OUTPUT AS ABOVE

OPTION 2. a (STRONGLY) CORRELATED W/ r
 $\rightarrow$ Alice "KNOWS" r BEFORE ANY INTERACTION SO Alice CAN BIAS Bob's OUTPUT UNLESS b ALSO CORRELATED WITH r

IF a, b, r ALL STRONGLY CORRELATED
 THEN Alice & Bob "KNOW" COMMON RANDOM
 BIT WITHOUT ANY INTERACTION!



SECURE MULTIPARTY COMPUTATION



HONEST-BUT-CURIOUS SECURITY

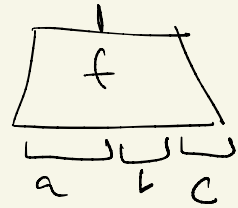
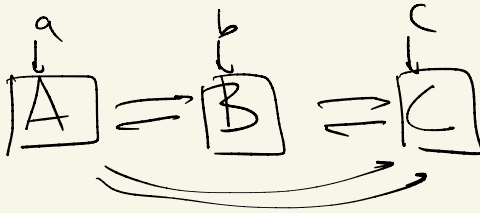
OPTION 1. ✓ NO PARTY FINDS ANY INFO
 BEYOND ITS OUTPUT.

OPTION 2. NO TWO PARTIES FIND ANY INFO
 BEYOND THEIR OUTPUTS

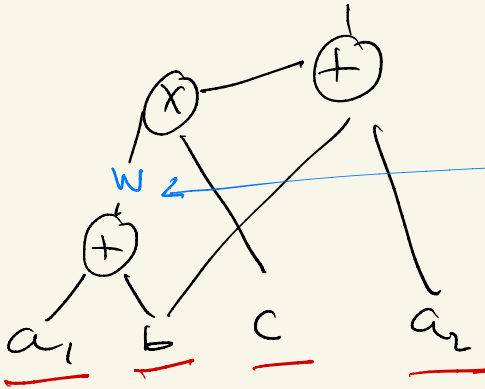
FEATURES: ONLY NEED SECURE POINT-TO-POINT CHANNELS. EVERYTHING ELSE IS PERFECTLY SECURE

INGREDIENT: SECRET SHARING

BGW, CCD SECURE MULTIPARTY PROTOCOL



ARITHMETIC CIRCUIT IF $(+, \times)$
IF $= \{0, 1\}$ $+$ = XOR, $\times$ = AND



w_A, w_B, w_C
NO SINGLE PARTY KNOWS w
BUT ANY 2 CAN RECOVER IT.

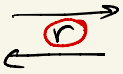
A
 a

B
 b

C

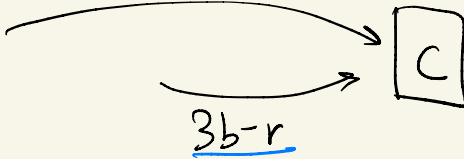
WANTS $2a+3b$

①



$2a+r$

②



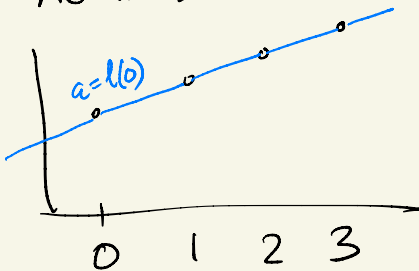
$\oplus = 2a+3b.$

CHARLIE'S VIEW: TWO RANDOM
VALUES THAT SUM TO HIS
OUTPUT

Sim BY $(r, \text{out}-r).$

① SHARE INPUTS

EG. Alice's INPUT a IS SHARED AS
 (q_A, q_B, q_C) USE SHAMIR FOR SECURITY
AGAINST 1 PARTY.

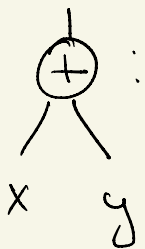


$$q_A = l(1) = a + r \cdot 1 \rightarrow$$

$$q_B = l(2) = a + r \cdot 2 \rightarrow \text{Bob}$$

$$q_C = l(3) = a + r \cdot 3 \rightarrow \text{Charlie}$$

② COMPUTE SHARES OF GATE OUTPUT FROM SHARES OF INPUTS.

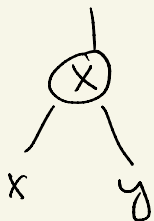


$$x = p(0)$$

A	B	C
$p(1)$	$p(2)$	$p(3)$

$y = q(0)$	$q(1)$	$q(2)$	$q(3)$
------------	--------	--------	--------

$$x+y = p(0)+q(0) \quad \underbrace{p(1)+q(1) \quad p(2)+q(2) \quad p(3)+q(3)}_{\text{SHARES OF } x+y}$$

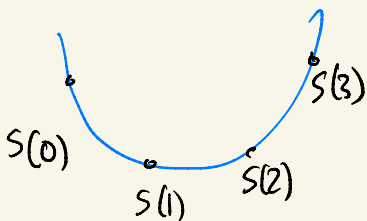


$$xy = s(0) = p(0)q(0) \quad s(1) = p(1)q(1) \quad s(2) = p(2)q(2) \quad s(3) = p(3)q(3)$$

s IS A QUADRATIC FUNCTION
S.T. $s(0) = xy$

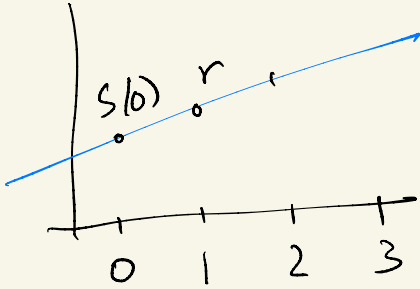
ENGAGE IN A PROTOCOL THAT CONVERTS THEIR SHARES $s(1), s(2), s(3)$ INTO SHARES $\ell(1), \ell(2), \ell(3)$ WHERE $\ell(t)$ IS A RANDOM LINE S.T. $\ell(0) = s(0)$

$$s(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} s(1) + \frac{(x-1)(x-3)}{(2-1)(2-3)} s(2) + \frac{(x-1)(x-2)}{(3-1)(3-2)} s(3)$$



LAGRANGE INTERPOLATION

$$s(0) = 3s(1) - 3s(2) + s(3)$$



Alice GETS r

$$l(t) = (1-t)s(0) + tr$$

Bob GETS $l(2) = -s(0) + 2s(1) = -s(1) + 3s(2) - s(3)$

Ch. GETS $l(3) = -2s(0) + 3s(1) = -3s(1) + 6s(2) - 2s(3)$

ENGAGE IN PROTOCOL FOR LINEAR FUNCTIONS

- ③ ONCE OUTPUT GATE IS REACHED,
Alice SENDS Charlie HER SHARE OF OUTPUT.

HOMOMORPHIC ENCRYPTION

El Gamal ENCRYPTION

$$\text{Enc}(pk, M) = (g^R, pk^R \cdot M)$$

$$\text{Enc}(pk, M') = (g^{R'}, pk^{R'} \cdot M')$$

ENCRYPTIONS OF $M \cdot M' \leftarrow (g^{R+R'}, pk^{R+R'}(M \cdot M'))$

HOMOMORPHISM

VOTING $x_1, \dots, x_n \in \{1, 0, -1\}$

$$f(x_1, \dots, x_n) = x_1 + \dots + x_n$$

ELECTION COMMITTEE: $(sk, pk = g^{sk})$ FOR
El Gamal ENCRYPTION

VOTE x_i : $Enc(pk, x_i) = (g^r, pk^r \cdot g^{x_i})$

HOMOMORPHISM: $\prod \text{VOTES} = (g^{R^*}, pk^{R^*} g^{\sum x_i})$

1978 RAD: IS THERE SECURE Enc

THAT SUPPORT HOMOMORPHIC $\times$ AND $+$?

SECURE OUTSOURCING

