A 2-party 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**

TRIVIALLY 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 $\forall A^* \exists A^* \text{ of size } \leq 0 \text{ larger }$

Larger S.T. joint RV ($A^*$'s View, B's Output)

Indistinguishable from ($A^*$'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

"$\exists x \text{ s.t. } f(x) = 2$". HELPFUL BUT NOT ENOUGH.
Alice proves she knows $x$ to Bob. Then $A^*$ can extract $x$ from $A^*$.

PROOFS OF KNOWLEDGE

SCHNORR:

Proof relation $P:(x,\xi)$ (e.g., $(g^x, x)$)

A protocol is a POK for $P$ if $\forall P^*$

$\exists K$ [knowledge extractor] of size $\leq \omega$

Larger s.t. if $P^*$ passes verification on $x$

with sufficiently large probability then

$K$ outputs $\xi$ with probability say $\frac{1}{2}$.
ZKPOK for Universal Proof Relations

\[ R = \{ (G, \pi) : \pi \text{ is a 3-coloring of } G \} \]

Last lecture: ZK proof of fact

**GMW Protocol**

\[ P \xrightarrow{\text{com}(\pi_i)} P' \]

\( G \)

\[ P \xrightarrow{(v,w) \text{ edge}} Y \]

Accept if \( \pi_v \neq \pi_w \) and \( \pi_v, \pi_w \), disclosure info, disclosures checkout.

GMW is a ZK proof of knowledge.

**Extractor:**

\[ \overline{P^*} \xrightarrow{\text{com}(\pi_i)} \overline{Y} \]

\[ (v_i, w_i) \]

\[ \pi_{v_i}, \pi_{w_i} \]

\[ \overline{\pi_{v_i}, \pi_{w_i}} \]

\[ (v_m, w_m) \]

\[ \overline{\pi_{v_m}, \pi_{w_m}} \]

\( P^* \) passes w/p \( 1 - \frac{1}{2^m} \) \( \rightarrow \) w/p \( \frac{1}{2} \)

All \( \pi_v \) consistent (\( \pi_{v_i} = \pi_{v_j} \) when \( v_i = v_j \)) and \( \pi_{v_i} \neq \pi_{w_i} \) \( \rightarrow \) \( \pi \) is a 3-col of \( G \)
GMW Compiler

\[ x \xrightarrow{\text{A}} y \xrightarrow{\text{B}} x \]

\[ f(x, y) \]

Secure Against Honest But Curious

Image Transmission

\[ x \xrightarrow{\text{A}} f(x) \xrightarrow{\text{B}} y = f(x) \]

\[ \text{ZKPOK}(f(x), x) \]

Secure Against Malicious

\[ f(x^*) = y \]

\[ \text{Ext}(\text{ZKPOK}) = x^* \]

S.T. \[ f(x^*) = y \]
Almost General Case

\[ A_1(x) = y \]

\[ B_i(y, u_i) = y_i' \]

GMW Compiler

\[ \text{SETUP: } C = \text{Com}(x) \text{, ZKPOK} \]
\[ C' = \text{Com}(y) \text{, ZKPOK} \]

\[ y_i, \text{ ZKPOK} (A_i(x) = y_i, \& C = \text{Com}(x)) \]
\[ y_i', \text{ ZKPOK} (B_i(y, u_i) = y_i', \& C' = \text{Com}(y)) \]

In Full Generality A and B Use Random Bits

\[ A_1(x, r_A) = y \]
\[ B_i(y, u_i, r_B) = y_i' \]

Need to Implement Ideal Random Coin Toss
COIN TOSSING PROTOCOL

\[ A \xleftarrow{\text{RANDOM}} \text{RANDOM} x \]

\[ C = \text{Com}(y) \text{ FOR RANDOM } y \]

\[ B \]

\[ r_B = x \oplus y \]

SECURITY FOR Alice : \( x \text{ RANDOM } \rightarrow r_B \text{ RANDOM} \)

SECURITY FOR Bob : \( (A^x \text{ 'S VIEW}, r_B) \)

\[ = (\text{Com}(y), x^x(\text{Com}(y)) \oplus y) \]

C.I. FROM \( (\text{Sim}, x^x(\text{Sim}) \oplus y) \)

IDEAL FUNC. INPUT

AUGMENT PROTOCOL WITH RANDOMNESS GENERATION PHASE AND INCLUDE ZKPOK FOR "C IS A COMMITMENT OF y S.T. \( r_B = x+y \)."
FAIRNESS: WHAT IF BOTH Alice & Bob NEED TO COMPUTE \( f(x, y) \)?

FAIR IDEAL FUNCTIONALITY

\[
\begin{array}{c}
A \\
\xrightarrow{f(x, y)} x \\
\xrightarrow{f(x, y)} y \\
\xrightarrow{f(x, y)} B
\end{array}
\]

When \( f(x, y) = x \oplus y \) and \( x, y \) random

this is a COIN TOSS: Alice & Bob OUTPUT same random bit.

Thus, (clever) fair coin toss is impossible.

In any \( k \)-round protocol coin must have bias \( \geq \frac{1}{(8k+1)} \).

Ex. A \( \xrightarrow{\text{coin}(y)} x \xrightarrow{y} \) B

IF Bob aborted

WHAT SHOULD OUTPUT \( y \) BE?

ELSE ABORT

SEND GARBAGE

IF \( f_B = x \oplus y = 0 \)

OUTPUT 0 & SEND y
**Option 1.** If Bob aborts, Alice samples output $r_a$ on her own.

$$r_a = (r_a | \text{NOT ABORT})P(\text{NOT ABORT}) + (r_a | \text{ABORT})P(\text{ABORT})$$

$$= \frac{1}{2} \cdot \frac{1}{2} + \text{RANDOM} \cdot \frac{1}{2}$$

$$= 0 \text{ w/p } \frac{3}{4},$$

$$1 \text{ w/p } \frac{1}{4}.$$  

**Intuition for Cleve's Theorem**

![Diagram](image)

- **Option 1.** $a$ Uncorrelated with $r$  
  - Bob can bias output as above.

- **Option 2.** $a$ (Strongly) Correlated w/ $r$  
  - 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!

![Diagram](image)

"Bob HAS ABORTED" IF NOT

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

\[
\frac{a}{A} = \frac{b}{B} = \frac{c}{C}
\]

Arithmetic Circuit: IF \((+, X)\)

\[IF = \{0, 1\}, \quad + = XOR, \quad X = AND\]

W_A, W_B, W_C

No single party knows W

But any 2 can recover it.
1. **SHARE INPUTS**
   
   Eg. Alice’s input $a$ is shared as $(a_A, a_B, a_C)$. Use Shamir for secrecy against $1$ party.

   \[ a = l(0) \]

   \[ a_A = l(1) = a + r \cdot 1 \rightarrow Bob \]

   \[ a_B = l(2) = a + r \cdot 2 \rightarrow Charlie \]

2. **C** WANTS $2a + 3b$.

   \[ 2a + r \]

   \[ 3b - r \]

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

   \[ \text{Sim by } (r, \text{out} - r) \]
② **COMPUTE SHARES OF GATE OUTPUT FROM SHARES OF INPUTS.**

\[
\begin{align*}
x &= p(0) & p(1) & p(2) & p(3) \\
y &= q(0) & q(1) & q(2) & q(3)
\end{align*}
\]

\[
x + y = p(0) + q(0) & p(1) + q(1) & p(2) + q(2) & p(3) + q(3)
\]

**SHARES OF** \(x + y\)

\[
x y = s(0) = p(0) q(0) & s(1) = p(1) q(1) & s(2) = p(2) q(2) & s(3) = p(3) q(3)
\]

**S IS A QUADRATIC FUNCTION**

\[S(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} s(1) + \frac{(x-1)(x-3)}{(2-1)(2-3)} s(2) + \frac{(x-1)(x-2)}{(3-1)(3-2)} s(3)\]

**LAGRANGE INTERPOLATION**

ENGAGE IN A PROTOCOL THAT CONVERTS THEIR SHARES \(s(1)\), \(s(2)\), \(s(3)\) INTO SHARE \(l(1), l(2), l(3)\) WHERE \(l(t)\) IS A RANDOM LINE

\[l(0) = s(0)\]
\[ s(0) = 3s(1) - 3s(2) + s(3) \]

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**

\[ \text{(3) Once output gate is reached, Alice sends Charlie her share of output.} \]

**Homomorphic Encryption**

**ElGamal Encryption**
\[
\begin{align*}
\text{Enc} (PK, M) &= (g^R, PK^R \cdot M) \\
\text{Enc} (PK, M') &= (g'^R, PK'^R \cdot M')
\end{align*}
\]

Encryption of \( M \cdot M' \leftarrow (g^{2+R}, PK^{2+R}(M \cdot M')) \)
VOTING \( x_1, \ldots, x_n \in \{1, 0, -1\} \)

\(+ (x_1, \ldots, x_n) = x_1 + \cdots + x_n\)

ELECTION COMMITTEE: \((sk, pk = g^{sk})\) FOR El-GAMAL ENCRYPTION

\[ \text{VOTE } x_i : \quad \text{Enc}(pk, x_i) = (g^{x_i}, pk^{x_i} \cdot g) \]

HOMOMORPHISM: \( \prod \text{votes} = (g^{\sum x_i}, pk^{\sum x_i} \cdot g) \)

1978 RAD: IS THERE SECURE Enc THAT SUPPORT HOMOMORPHIC + AND \(
\underline{\text{SECURE OUTSOURCING}}\)

\[ Alice \xrightarrow{\text{Enc}(pk, x_i), \ldots, \text{Enc}(pk, x_n)} C \text{ THAT ENCRYPTS} \]

\[ f(x_1, \ldots, x_n) \xrightarrow{\text{out} = f(x_1, \ldots, x_n)} \text{Dec}(sk, C) = \text{out} \]