LECTURE 1

WHAT IS CRYPTOGRAPHY?

- ORIGINALLY, PRIVACY
  - ROMAN SCALE ENCRYPTION
  - ENIGMA MACHINE
  - SECURITY BY OBSCURITY

WATERSHED MOMENTS:

- 1970s: PK ENCRYPTION (DIFFIE, HELLMAN)
  - ANYONE CAN ENCRYPT TO YOU USING YOUR PK
  - ONLY YOU WITH SECRET KEY CAN DECRYPT
- 1980s: "PROVABLY SECURE" PRG (MICALI-BLUM)
  - BREAKING PRG AS HARD AS SOLVING DISCRETE LOG

- ESTABLISHED METHOD OF PROVING CRYPTOSYSTEM IS "HARD" TO BREAK VIA MATHEMATICAL REDUCTION TO SOME "STANDARD" ASSUMPTIONS

NP-Completeness

P – POLY-TIME COMPUTABLE PROBLEMS

↖ $|x|=n$, $\exists c$ S.T. YOU CAN SOLVE WHETHER $x \in L$ IN TIME $O(n^c)$

NP – POLY-TIME VERIFIABLE PROBLEMS

↖ $x \in L$, $|x|=n$, $\exists c$ S.T. YOU CAN VERIFY THAT $x \in L$ IN TIME $O(n^c)$ (WITH SOME POLY-SIZE WITNESS w)

NP-COMPLETE – NP PROBLEM L SUCH THAT ANY NP PROBLEM CAN BE SOLVED IN POLY-TIME GIVEN A POLY-TIME ALGORITHM FOR L

EXAMPLE OF "HARD" PROBLEM: FACTORING

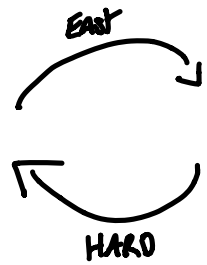
PRIME PRIME
$p * q \rightarrow N$

GIVEN N (ASSUME PRODUCT OF 2 PRIMES) $\longrightarrow$ FIND p, q

- NOT NP-COMPLETE
- BEST ALGORITHM IS $O\left(2^{\sqrt[3]{N}(\log \log N)^2}\right)$
- SEEMS HARD, BUT MIGHT NOT BE IN 10 YEARS (QUANTUM, ETC.)
- NOT A GREAT ASSUMPTION FOR HARDNESS

QUESTION: WHAT IS THE MINIMAL ASSUMPTION I CAN MAKE TO BUILD INTERESTING CRYPTOSYSTEMS?

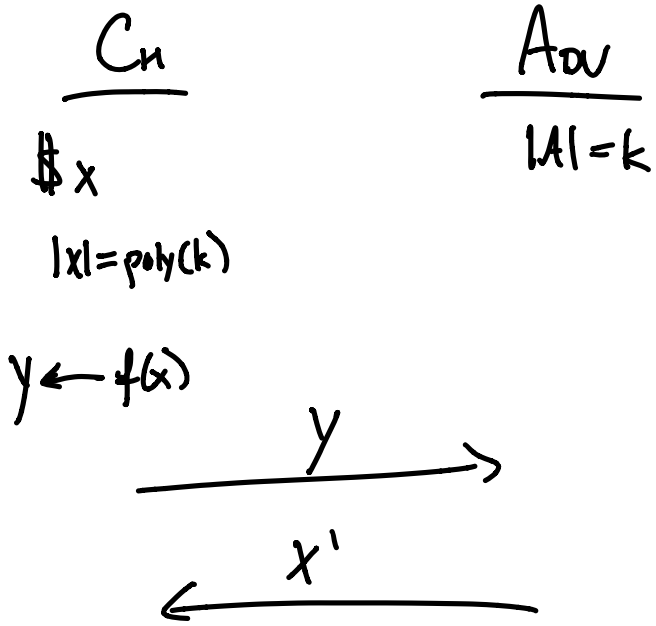
ANSWER: ONE-WAY FUNCTIONS (OWF, 1WF)

1-WAY FUNCTIONS: x 

$f(x) = y$

WHAT DOES "HARD TO INVERT" MEAN?

- FIRST ATTEMPT DEFINITION: HARD = NOT POLY-TIME
  - NOT GOOD ENOUGH. ADVERSARY MIGHT USE RANDOMNESS
- SECOND ATTEMPT: GAME-BASED DEFINITION



Adv "WINS" IF $f(x')=y$

* Adv CAN RANDOMLY GUESS + GET LUCKY, SO OUR DEFINITION CAN'T SAY Adv NEVER GETS IT RIGHT.

SOLUTION: NO POLY-TIME (PROBABILISTIC POLY-TIME (PPT)) ADVERSARY Adv WHO USES RANDOMNESS HAS A "SIGNIFICANT" PROBABILITY OF WINNING.

↑ OUR DEFINITION OF f BEING "HARD" TO INVERT.

WHY IS THIS IMPORTANT?

- RANDOMNESS IS POWERFUL.
- SOLVING A PROBLEM WITH 100% CERTAINTY + NO RANDOMNESS IS USUALLY HARDER THAN 99% CERTAINTY WITH RANDOMNESS
- E.G. DETERMINING PRIMALITY

SO... f IS A OWF IF:

1. f IS POLY-TIME COMPUTABLE
2. f IS HARD TO INVERT: $\forall c$, $\forall A \in PPT$, $\exists N_c$ s.t. $\forall x$ s.t. $|x| = n > N_c$

$$\Pr\left[A(f(x)) = x' \;\middle|\; \begin{matrix} f(x') = f(x) \\ x \xleftarrow{R} \{0,1\}^n \end{matrix}\right] < \frac{1}{n^c}$$

"NEGLIGIBLE" PROBABILITY

WHAT'S WITH THE N_c STUFF?

- NEED TO MAKE INPUT LARGE ENOUGH FOR ANY SIZED ADVERSARY W/ BIG LOOKUP TABLE.

WHY PROBABILITY?

- IN CASE ADVERSARY RANDOMLY GUESSES

② In English: f hard to invert IF

$\Pr[A \text{ inverts } f(x)]$ is "negligible" $\longrightarrow$ $\Pr[A \text{ inverts } f(x)] < \frac{1}{\text{any polynomial in } n, \text{ e.g. } 2^{128}}$

for "large enough" input x,

for any $A \in PPT$.

Alternative to 1WFs: Correlated Randomness

- Random but related strings between parties
- Can build most crypto from CR
- Hard part is generating it.
  - Usually need 1WFs

Coin-Flipping Protocol:

☆ How can 2 people fairly flip a coin over the phone?

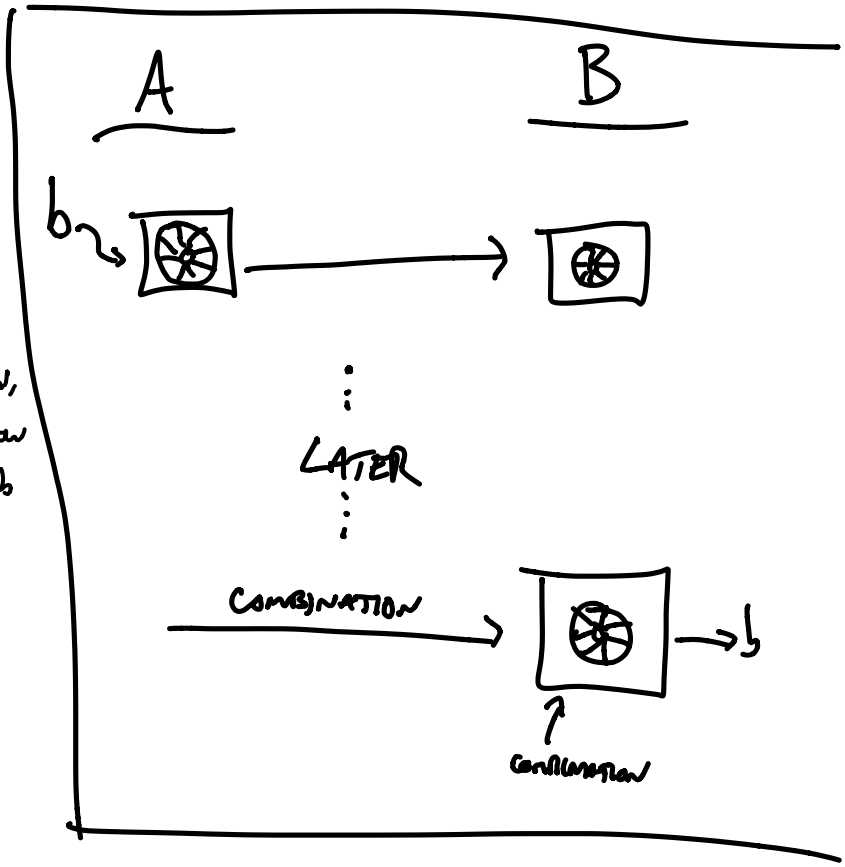
Key Primitive: Commitment Protocol

Definition:

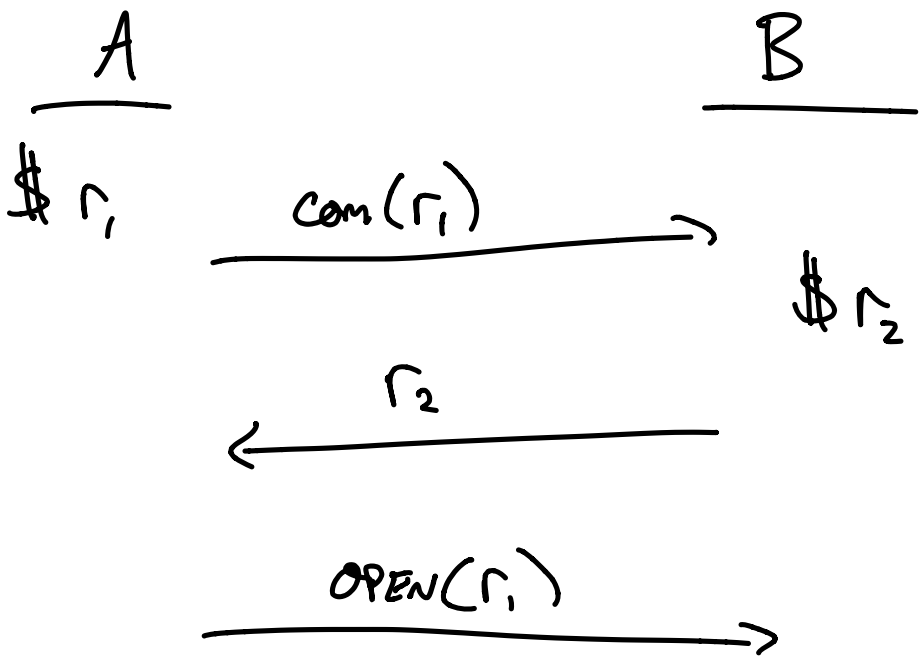
2 properties:

Hiding - w/o combination, B does not know anything about b

Binding - After locking b in safe, A cannot change mind about b



Coin Flipping via Bit Commitments



Common Coin = $r_1 \oplus r_2$

Why is this fair?

- A can't cheat by choosing r_1 based on r_2 because of <u>binding</u> property
- B can't choose r_2 based on r_1 because of <u>hiding</u> property

ASIDE: P vs. NP — IS P = NP? OR, ARE THERE HARD PROBLEMS?

ave P vs. ave NP — ARE THERE PROBLEMS WHERE, ON AVERAGE, INSTANCES ARE HARD?

ave $P \neq$ ave $NP \Rightarrow P \neq NP$

$P \neq NP \not\Rightarrow$ ave $P =$ ave NP

$\exists$ 1WF IS EVEN STRONGER THAN ave $P \neq$ ave NP

↳ $\exists$ HARD "SOLVED" PROBLEMS.

A CAN GENERATE "PUZZLES" W/ SOLUTIONS, WHICH ARE HARD TO SOLVE

$\exists$ 1WF

$\Downarrow$ $\Uparrow$?

ave $P \neq$ ave NP

$\Downarrow$ $\not\Uparrow$

$P \neq NP$

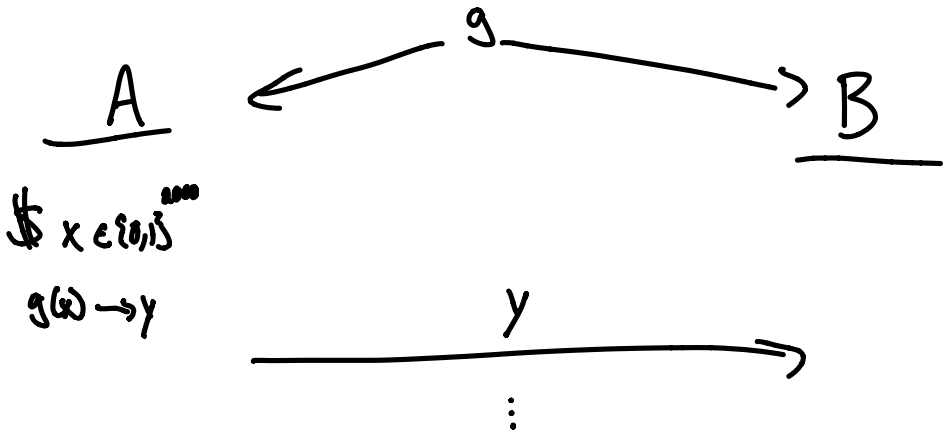
STUDENT QUESTION: WHY STOP AT "HARD" TO INVERT? WHY NOT MAKE IT UNSOLVABLE?

ANSWER: THERE MUST BE A SOLUTION x WHICH A USED TO GENERATE THE PUZZLE.

Building a Commitment Protocol

Assume: g is a 1-way permutation

- g is 1-to-1 & onto
- g is a 1WF



Problem: x is 2000 bits long, we only want to commit to a single bit. Which bit do we use?

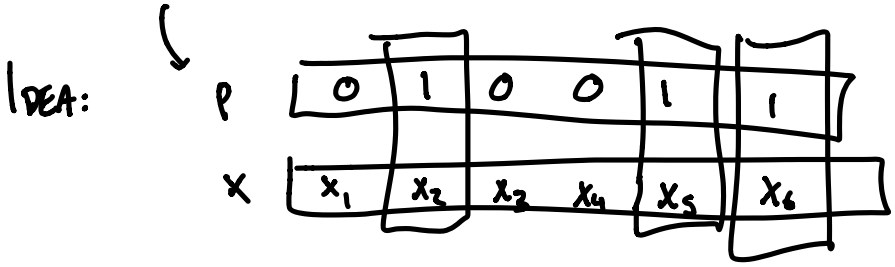
- If we use the first bit, can construct specific 1WP which leaks the first bit.
  - $f(b,x) = b \| g(x)$
- Same if we use xor tricks

Solution: Hardcore Bits

Thm (Goldreich, Levin):

For any 1WF f, $\exists$ hardcore bit

Idea:



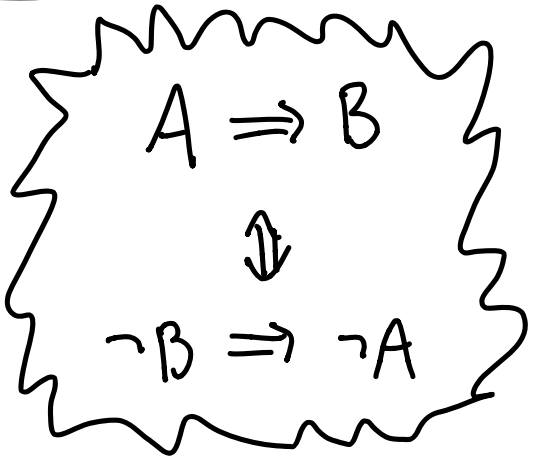
$x_2 \oplus x_5 \oplus x_6$ is a hardcore bit of x

Formal def: Predicting HCB w/ prob $\frac{1}{2} + \frac{1}{n^c}$ can be used to invert 1WF

Next time: Finish constructing bit commitment from 1WP w/ HCB

LECTURE 2 | How do we prove security?

Converse Law:



Important in Crypto!

Thm: Assume assumption A holds. Then, Protocol B is secure

Proof: Assume protocol B is **not** secure.

($\exists$ PPT adversary A_{dv} that breaks protocol B)

Then we can use A_{dv} as a subroutine to break assumption A.

KEY IDEA: WE MAKE NO ASSUMPTIONS ABOUT THE ALG THAT BREAKS B. THUS, RULES OUT EVERY ATTACK (AS LONG AS ASSUMPTION A IS TRUE)

EXAMPLE OF PROOF VIA CONVERSE LAW:

THM: (GOLDREICH, LEVIN)

A "RANDOM" SUBSET OF BITS OF INPUT X XOR'D TOGETHER IS A HARDCORE BIT FOR 1WP $g(x)=y$

Proof (Simplified):

Want to show:

If Adv R predicts $\sum x_i \cdot p_i \bmod 2$ w/ probability $\frac{1}{2} + \varepsilon$ (Given $p, g(x)$)

then Adv can be used to invert $g(x)$ to get x with probability $\frac{1}{n_2^c}$.

Reminder - f is a OWF if,

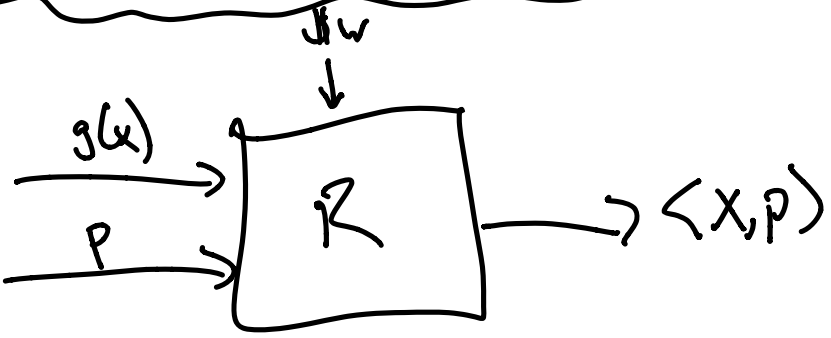
for large enough inputs (size $= n$),

$\Pr[\text{Adv inverts } f] < \frac{1}{n^c}$

for all c.

- b is a hardcore bit of function f if an adversary which predicts b w/ probability $\frac{1}{2} + \varepsilon$ can be used as a subroutine to invert f w/ probability $\geq \frac{1}{n^c}$

STEP 1: SUPPOSE R PREDICTS $\langle x, p \rangle$ W/ PROBABILITY 1.



$p = 1000\ldots0 \rightarrow [R] \rightarrow x_1$

$p = 0100\ldots0 \rightarrow [R] \rightarrow x_2$

$\vdots$

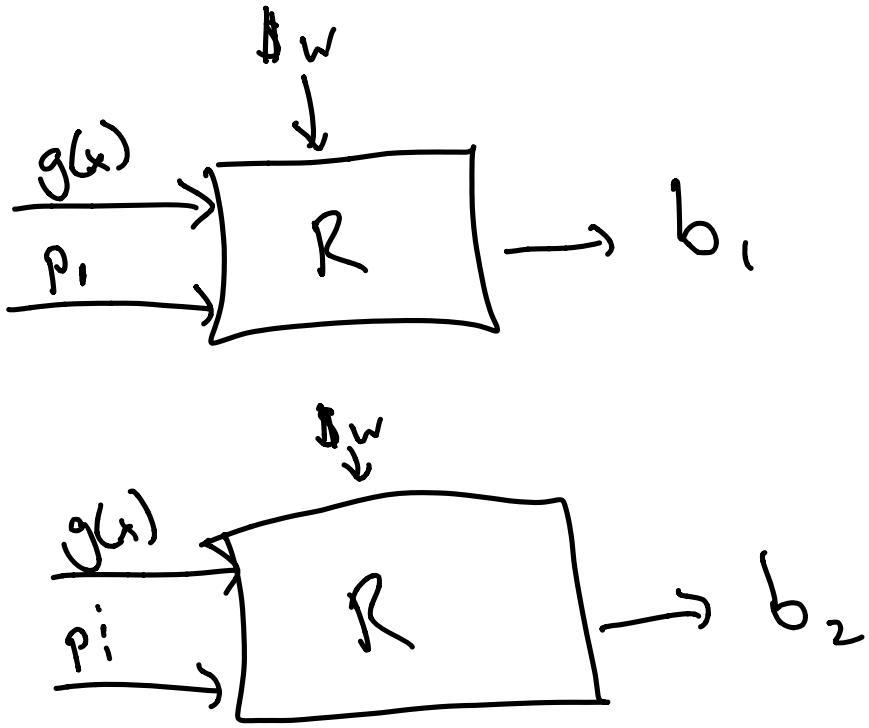
$p = 000\ldots1 \rightarrow [R] \rightarrow x_n$

CAN DETERMINE x USING n CALLS TO R AS SUBROUTINE

STEP 2: R PREDICTS $\langle x, p \rangle$ W/ PROBABILITY $3/4 + \varepsilon$

$$\Pr_R[R \text{ MAKES MISTAKE}] = \frac{1}{4} - \varepsilon$$

$p_k^i := p_k$ W/ i^{TH} BIT FLIPPED



IF BOTH ARE CORRECT, ONLY

i^{TH} BIT DOESN'T GET CANCELLED OUT

IN $b_1 \oplus b_2$. SO $b_1 \oplus b_2 = x_i$

IF BOTH ARE CORRECT, WHICH

OCCURS WITH PROBABILITY AT LEAST

$$1 - \Pr[b_1 \text{ IS WRONG}] - \Pr[b_2 \text{ IS WRONG}]$$

$$= 1 - \left(\tfrac{1}{4} - \varepsilon\right) - \left(\tfrac{1}{4} - \varepsilon\right)$$

$$= \tfrac{1}{2} + 2\varepsilon$$

SO WE CAN PREDICT EACH BIT OF X W/ PROBABILITY $\frac{1}{2}+2\varepsilon$ USING 2 CALLS TO R.

AMPLIFICATION

WE CAN AMPLIFY THIS PROBABILITY AS CLOSE TO 1 AS WE WANT BY REPEATING k TIMES + TAKING THE MAJORITY.

PREDICTING X_i:

TRIAL	1	2	3	4	5	6	7	8	9	...	k
OUTPUT	0	0	1	0	1	1	0	0	0		1

MORE 0'S THAN 1'S, SO X_i PROBABLY 0.

AS k INCREASES, PROBABILITY THAT MAJORITY IS NOT CORRECT ANSWER APPROACHES 0 EXPONENTIALLY FAST (CHERNOFF BOUND)

Aside on Amplification:

Majority only necessary for 2-sided errors (BPP). 1-sided error (RP, co-RP) is simpler.

$L \in RP$ if $\exists A \in PPT$ s.t.

$$\forall x \in L,\ Pr[A(x)=1] > \frac{2}{3}$$
$$\forall x \notin L,\ Pr[A(x)=1] = 0$$

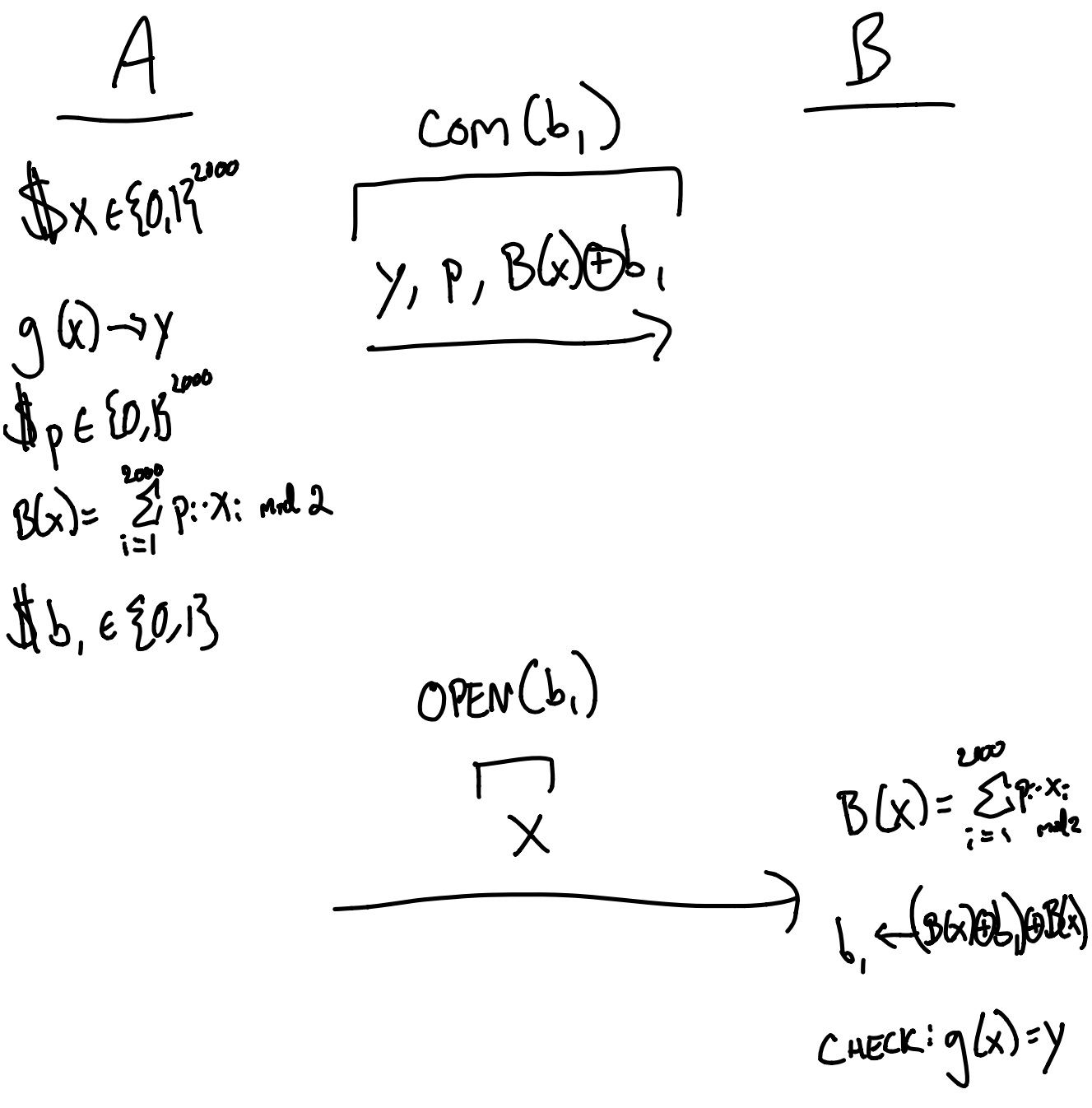
$L \in$ co-RP if $\exists A \in PPT$ s.t.

$$\forall x \in L,\ Pr[A(x)=1] = 1$$
$$\forall x \notin L,\ Pr[A(x)=1] < \frac{1}{3}$$

FOR RP, AMPLIFY BY REPEATING k TIMES. OUTPUT $x \in L$ IF $A(x)=1$ IN ANY SINGLE TRIAL. OUTPUT $x \notin L$ IF $A(x)=0$ FOR ALL TRIALS.

FOR CO-RP, OUTPUT $x \in L$ IF $A(x)=1$ FOR ALL TRIALS. OUTPUT $x \notin L$ IF $A(x)=0$ FOR ANY SINGLE TRIAL.

Building Bit Commitment from HCB



ALICE CAN'T CHANGE MIND ABOUT b, BECAUSE SHE CAN'T CHANGE MIND ABOUT x, BECAUSE f IS A PERMUTATION, AND SHE ALREADY SENT p WHICH DETERMINES $B(x)$.

BOB CAN'T DETERMINE b, FROM THE COMMITMENT BECAUSE IT IS MASKED BY $B(x)$, AND PREDICTING $B(x)$ WITHOUT KNOWING x IS AS HARD AS INVERTING f, WHICH IS A 1WF.

* IF ALICE HANGS UP W/O OPENING, BOB WINS. TO PREVENT "ABORT" ATTACKS.