FA2022 Week 15

Introduction to Secure Computation

Very Random Object No.79

ctf.sigpwny.com

sigpwny{but_wh4t_1f_b0b_w4s_eve}

ALICE SENDS A MESSAGE TO BOB SAYING TO MEET HER SOMEWHERE.
UH HUH.
BUT EVE SEES IT, TOO, AND GOES TO THE PLACE.
WITH YOU SO FAR.
BOB IS DELAYED, AND ALICE AND EVE MEET.
YEAH?
I'VE DISCOVERED A WAY TO GET COMPUTER SCIENTISTS TO LISTEN TO ANY BORING STORY.

What is Secure Computation?

- Multi-Party Computation (MPC)
- Adversaries: participating parties
- Threat models: semi-honest security vs malicious security

Motivations of MPC

Using a safe password when creating your google account.

- what are the challenges?

Disclaimer…

This is trivial and is left to the reader as an exercise.

Disclaimer…

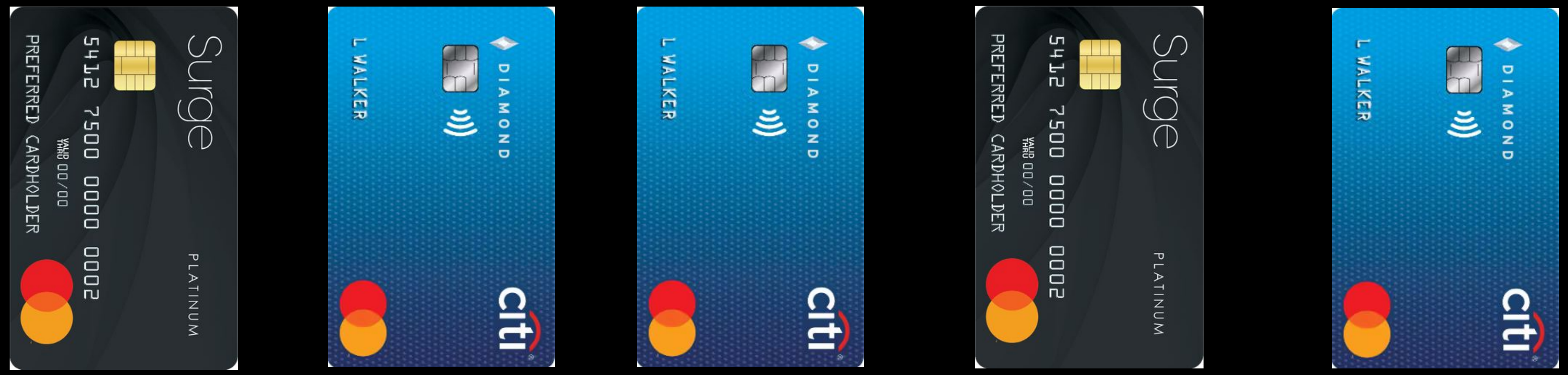
Just kidding. This is done through something called private set intersection and it’s… complicated.

Let’s Start With a Simpler Example…

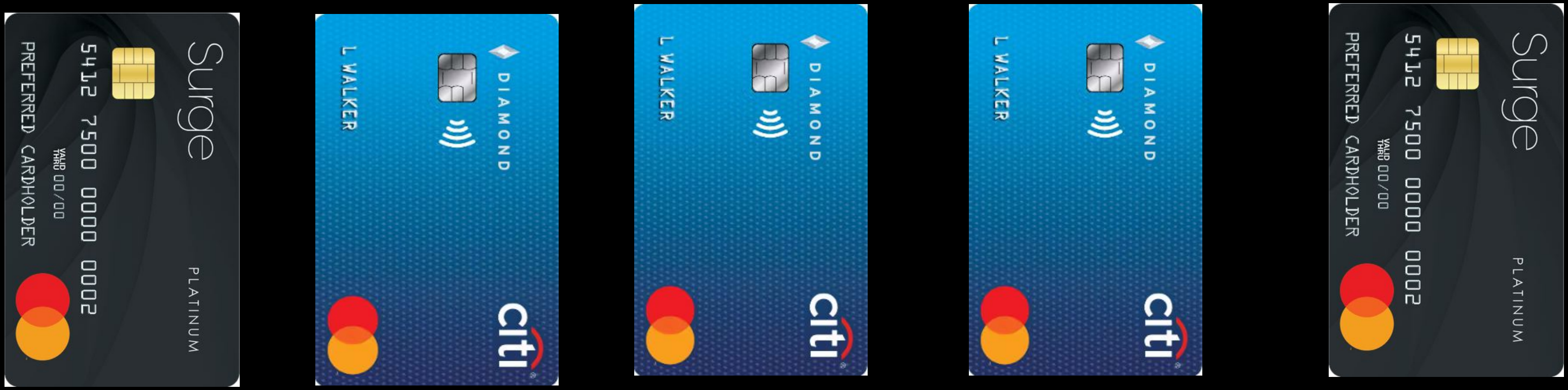
Securely computing AND… how?

First, you Need 5 Credit Cards.

No.


Surge
PLATINUM
5412 7500 0000 0002
VALID THRU 00/00
PREFERRED CARDHOLDER
DIAMOND
L WALKER
citi
DIAMOND
L WALKER
citi
Surge
PLATINUM
5412 7500 0000 0002
VALID THRU 00/00
PREFERRED CARDHOLDER
DIAMOND
L WALKER
citi

Yes!


Surge
PLATINUM
5412 7500 0000 0002
VALID THRU 00/00
PREFERRED CARDHOLDER
DIAMOND
L WALKER
citi
DIAMOND
L WALKER
citi
DIAMOND
L WALKER
citi
Surge
PLATINUM
5412 7500 0000 0002
VALID THRU 00/00
PREFERRED CARDHOLDER

A Few Things to Notice…

- it can be a bit more complicated and harder than first sight
- it works! when both parties are nice…
- wait, what about when one side inputs yes (or 1)?

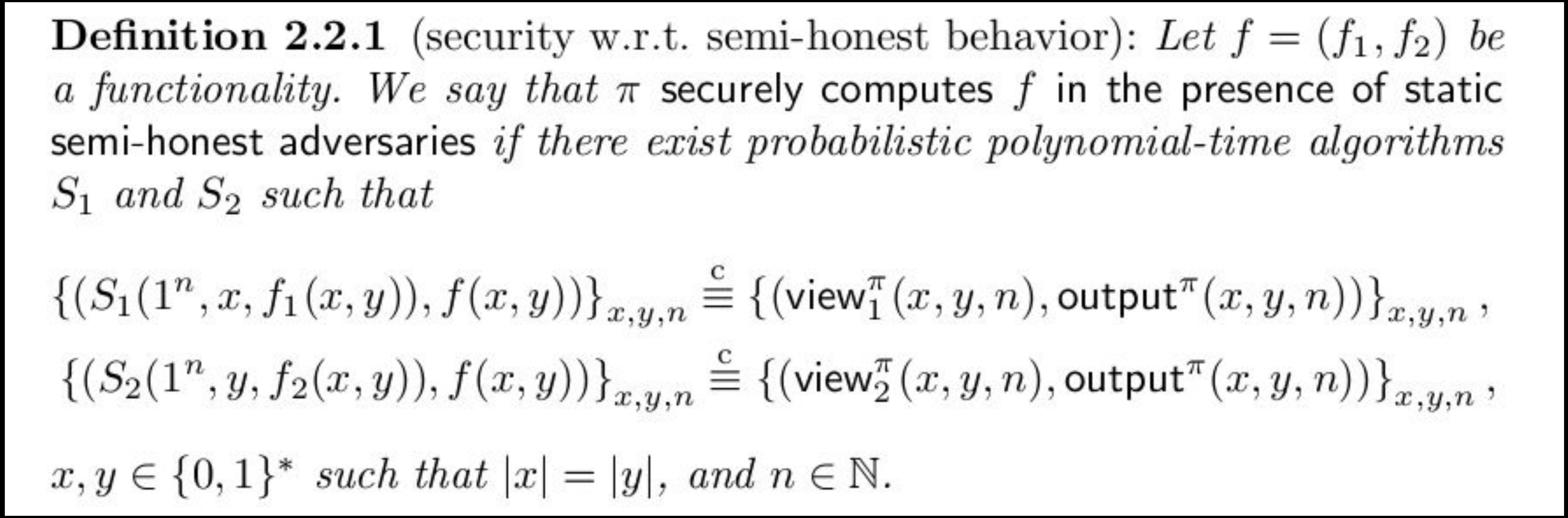
Some Examples of Functionalities?

- securely compute AND
- key exchange
- voting

Semi-Honest Security

- works with an "ideal world" and a "real world"
- has a specified "functionality" parties wish to achieve
- under the assumption that both parties follow the rules

Semi-Honest Security



Definition 2.2.1 (security w.r.t. semi-honest behavior): *Let* $f = (f_1, f_2)$ *be a functionality. We say that* π securely computes f in the presence of static semi-honest adversaries *if there exist probabilistic polynomial-time algorithms* S_1 *and* S_2 *such that*

$$\{(S_1(1^n, x, f_1(x,y)), f(x,y))\}_{x,y,n} \overset{\text{c}}{\equiv} \{(\mathsf{view}_1^\pi(x,y,n), \mathsf{output}^\pi(x,y,n))\}_{x,y,n},$$

$$\{(S_2(1^n, y, f_2(x,y)), f(x,y))\}_{x,y,n} \overset{\text{c}}{\equiv} \{(\mathsf{view}_2^\pi(x,y,n), \mathsf{output}^\pi(x,y,n))\}_{x,y,n},$$

$x, y \in \{0,1\}^*$ *such that* $|x| = |y|$*, and* $n \in \mathbb{N}$*.*

Semi-Honest Security

- A party has a view in the ideal world
- A party has a view in the real world
- If we can construct a simulator (i.e. program) that can use the ideal world to simulate the real world, a protocol is secure under the semi-honest setting

What is a View?

- a party P’s input
- a party P’s output
- things P receive throughout communication

Essentially, what P sees.

Functionality: Securely Computing XOR

Protocol:

- Parties A, B, C, D have inputs a, b, c, d
- A randomly samples a random one time pad r
- A sends $r \oplus a$ to B
- B sends $r \oplus a \oplus b$ to C
- C sends $r \oplus a \oplus b \oplus c$ to A
- A announces $r \oplus r \oplus a \oplus b \oplus c = a \oplus b \oplus c$

So, this is Secure?

For party A

- ideal world view: $\{a, a \oplus b \oplus c\}$
- real world view: $\{a, r, a \oplus b \oplus c\}$

So, this is Secure?

For any party that’s not A:

- ideal world view: {input, $a \oplus b \oplus c$}
- real world view: {input, random thingy, $a \oplus b \oplus c$}

Next Meetings

2023 Spring Semester: lots of fun!

- I won’t be here :(

Special Thanks:
Professor David Heath

He’s also teaching a class in secure computation (CS598 DH) next semester!

Special Thanks:
SIGPwny

I would’ve never made it here if it weren’t for all of you :)

Last Words

- Keywords to google if you are interested:
    - Oblivious Transfer (OT), Zero Knowledge Proof (ZKP), the GMW Protocol, Malicious Security, Covert Security, Public Verifiable Security
- Why do we want MPC?
- What are some current challenges in MPC?

- An example of what protocols that are secure against malicious security could allow…

RICK ASTLEY
NEVER GONNA GIVE YOU UP

SIGPwny